

TRABAJO FIN DE GRADO

Pasaporte Digital de Producto para el Sector Jamonero basado en Blockchain e IoT

TRABAJO FIN DE GRADO PARA
LA OBTENCIÓN DEL TÍTULO DE
GRADUADO EN INGENIERÍA EN
TECNOLOGÍAS INDUSTRIALES

NOVIEMBRE 2025

Pablo Bernat Gallardo

DIRECTORES DEL TRABAJO FIN DE GRADO:

Joaquín Ordieres Meré

Jaime Señor Sánchez

AGRADECIMIENTOS

Quisiera dedicar este trabajo, con especial cariño y admiración, a mi abuelo Paco, doctor ingeniero industrial, ejemplo de rigor, pasión y entrega. Aunque ya no esté presente, siento que desde el Cielo me ha guiado e inspirado a lo largo de este camino. Gracias a su huella, elegí esta carrera, esta Escuela y esta manera de entender el mundo y la ingeniería, buscando siempre la excelencia y el sentido último de lo que hacemos.

Agradezco de corazón a Beatriz, mi compañera y apoyo incondicional, que ha vivido conmigo cada momento de esfuerzo, desánimo y alegría. Su paciencia, comprensión y cariño han sido una fuente constante de fuerza, especialmente en los días más exigentes de esta etapa.

A mi familia, por su respaldo inquebrantable, por su amor y por enseñarme a valorar la constancia y el sacrificio, celebrando siempre cada pequeño logro y animándome a seguir adelante. Soportando los momentos más críticos y desafortunados, así como compartiendo los más felices y de logros excepcionales.

Mi reconocimiento sincero a mis tutores, Joaquín y Jaime, por su generosidad, paciencia y sabiduría. Gracias a ellos he podido adentrarme en el fascinante mundo de la innovación tecnológica europea y en la importancia de la trazabilidad, la transparencia y la excelencia, con el jamón ibérico como producto y símbolo de nuestra identidad y cultura.

RESUMEN

Este trabajo diseña y valida, a nivel de prototipo, un Pasaporte Digital de Producto (DPP) aplicable al jamón ibérico que integra estándares GS1/EPCIS, sensórica IoT y registro inmutable en IOTA Tangle para reforzar la trazabilidad, autenticidad y transparencia del sector. El enfoque se alinea con el marco europeo del DPP conforme a la regulación de diseño ecológico (ESPR), si bien su aplicación a alimentos no es aún obligatoria; por ello se plantea una arquitectura voluntaria y sectorialmente adaptada que pueda evolucionar sin bloqueo de proveedor y con compatibilidad futura.

El objetivo general es demostrar la viabilidad técnica y el valor operativo de un DPP para piezas de jamón ibérico a lo largo de toda la cadena de valor, desde la cría en dehesa hasta el consumo, incluyendo circularidad posconsumo. Se persigue: (i) identificar los datos mínimos y ampliados del DPP (origen, alimentación, certificaciones, lotes, condiciones de proceso, auditorías), (ii) definir perfiles de acceso diferenciados (consumidor, operador, auditor/autoridad) con salvaguardas RGPD, (iii) justificar la elección de IOTA frente a alternativas DLT (Hyperledger Fabric, Ethereum, OriginTrail) y (iv) cuantificar costes y riesgos de adopción para pymes.

La metodología combina análisis normativo-técnico, modelado GS1 (GTIN+lote, Digital Link y eventos EPCIS), simulación de datos de proceso y un piloto funcional sobre red de pruebas de IOTA con ingestión IoT. Se especifica un metamodelo de datos compatible con el Anexo de datos del DPP y con vocabularios GS1; se diseñan flujos EPCIS (*Commissioning*, *Aggregation*, *Transformation* y *Object Events*) y un visor web con QR para la capa pública. El prototipo publica anclajes hash de paquetes EPCIS en Tangle (inmutabilidad y sellado temporal) y mantiene los datos detallados *off-chain*, optimizando coste, privacidad y rendimiento.

El caso demostrador integra mediciones representativas de la cadena del ibérico y emplea datos simulados plausibles para validar el flujo extremo a extremo. En concreto, se contemplan pesos y mermas, tiempos de salazón y curado, temperatura-humedad en cámaras y la relación con certificaciones y precintos, junto con registros documentales (albaranes, controles veterinarios, lotes, auditorías). Para la alimentación en cebo se prevé la referencia a piensos y cereales, con capacidad de enlazar PDP *anidados* de insumos cuando existan. La sensórica se aborda de forma pragmática: datos simulados con perfiles de variación verosímiles y envío por lotes para tolerar conectividad intermitente y reducir consumo energético.

Los resultados esperados se concentran en eficiencia operativa, detección temprana de manipulaciones y confianza del consumidor con costes contenidos. En particular: (i) reducción del TIE (tiempo de investigación de expedientes) ante no conformidades, (ii) detección temprana de manipulaciones *off-chain* por desalineación entre EPCIS y anclajes, (iii) mejora de la confianza

del consumidor y de la diferenciación internacional del producto, y (iv) costes operativos ajustados gracias a la ausencia de comisiones en IOTA y a una arquitectura híbrida *on/off-chain*. La comparación de DLTs muestra que IOTA ofrece ventajas en entornos IoT y en escalabilidad sin tasas, mientras que plataformas permissionadas como Fabric encajan mejor en consorcios B2B cerrados; se motiva así la elección de IOTA para un caso B2B2C con verificación pública.

El análisis económico estima inversiones moderadas aprovechando infraestructura existente y desglosa CapEx/OpEx a tres años con sensibilidad a volúmenes y automatización. Se reutiliza la identificación GS1 y los QR, así como la sensórica de cámaras; el coste total se estructura en *software*, operación de nodos ligeros, *hosting*, soporte y formación. Se discuten incentivos y modelos de adopción para pymes, junto con fases graduales de despliegue que minimicen riesgo y eviten *vendor lock-in*.

El trabajo reconoce limitaciones y define líneas futuras concretas, presentando el PDP como *blueprint* adaptable y listo para evolucionar. Se prioriza el acceso a datos reales de productores, la integración con sistemas DOP/IGP y con DID/credenciales verificables, la evaluación de impacto ambiental con métricas comparables y la posible extensión del PDP al conjunto de jamones curados. La propuesta se plantea como base técnicamente fundamentada para avanzar conforme se concrete el marco regulatorio del PDP en alimentos.

Palabras clave

Pasaporte Digital de Producto; Trazabilidad; GS1 Digital Link; EPCIS 2.0; JSON-LD; IOTA Tangle; Notarization; IPFS; QR; Verificación Pública; Node.js; Express; TypeScript; PostgreSQL/Timescale; Integridad de Datos; Auditabilidad; PyME; Sostenibilidad; Jamón Ibérico.

Códigos UNESCO

120317 INFORMÁTICA
120323 LENGUAJES DE PROGRAMACIÓN
120324 SISTEMAS DE INFORMACIÓN
330412 DISPOSITIVOS DE CONTROL
330413 DISPOSITIVOS DE TRANSMISIÓN DE DATOS
330417 SISTEMAS EN TIEMPO REAL
330418 DISPOSITIVOS DE ALMACENAMIENTO
331101 TECNOLOGÍA DE LA AUTOMATIZACIÓN
330901 TECNOLOGÍA DE ALIMENTOS
310601 PRODUCCIÓN ANIMAL

ÍNDICE GENERAL

1. INTRODUCCIÓN	1
1.1. Antecedentes y Justificación del DPP para Jamón Ibérico	1
1.1.1. Trazabilidad Alimentaria: Sistemas Tradicionales, Certificación y Problemas de Fraude	1
1.1.2. Competitividad	2
1.1.3. Casos de Uso y Comparativas Relevantes de Pasaportes Digitales	4
1.2. Diferencias entre Jamón Ibérico y Jamón Serrano y Confusiones de Mercado .	8
1.2.1. Diferencias Técnico-Legales	8
1.2.2. Confusión Terminológica en Etiquetado, Percepción y Mercado	9
1.3. Cadena de Suministro y Cadena de Valor del Jamón Ibérico y su Contexto Comercial	12
1.3.1. Etapas, Sensórica y Trazabilidad	12
1.3.2. Sostenibilidad en la Industria del Jamón Ibérico	16
1.4. Definición del Problema, Objetivos del Trabajo y Alcance	16
1.5. Metodología	17
1.6. Limitaciones, Hipótesis de Partida y Estructura de la Memoria	18
2. MARCO NORMATIVO	21
2.1. Normativa Española y Europea Aplicable	21

2.1.1.	Reglamento (UE) 2024/1781 (ESPR) y Pasaporte Digital de Producto (DPP)	21
2.1.2.	REACH y «sustancias preocupantes» en el DPP	22
2.1.3.	Trazabilidad Alimentaria y la Norma de Calidad del Ibérico (Reg. 178/2002, RD 4/2014, DOP)	23
2.1.4.	Pacto Verde Europeo y Estrategias Conexas	24
2.1.5.	RGPD y Protección de Datos desde el Diseño	24
2.1.6.	Sistemas Sectoriales Existentes (ASICI-ÍTACA) y Complementaridad con el DPP	25
3.	ESTADO DEL ARTE	28
3.1.	Internet de las Cosas (IoT)	29
3.2.	Pasaporte Digital de Producto: Arquitectura y Especificaciones	31
3.3.	Directrices Técnicas del ESPR para el DPP	33
3.4.	Tecnologías de Registro Distribuido (DLT)	35
3.4.1.	La Función <i>Hash</i> y la <i>Blockchain</i>	35
3.4.2.	Mecanismos de Consenso	37
3.4.3.	Limitaciones de Escalabilidad, Costes y Alternativas	38
3.5.	La Tangle de IOTA	39
3.5.1.	Pesos Individuales y Acumulados	40
3.5.2.	Gestión de <i>tips</i> y <i>Edges</i>	40
3.5.3.	Confirmación de Transacciones	41
3.5.4.	Transacciones <i>Milestone</i> y Coordinador	41
3.5.5.	Tipos de Redes IOTA	42
3.5.6.	Prevención de <i>Spam</i>	43
3.5.7.	Soluciones de «Capa 1» y «Capa 2»	43

3.5.8. Evolución hacia IOTA 2.0 (<i>Coordicide</i>)	44
3.6. IOTA para el DPP: ¿ <i>Notarization</i> o Verificación Manual?	45
3.6.1. IOTA <i>Notarization</i>	45
3.6.2. Verificación Manual con <i>Tagged Data</i>	46
3.6.3. Comparación y Decisión	47
3.7. Estándares de Identificación y Datos: GS1, EPCIS 2.0 y Digital Link	49
3.7.1. Sistema de Identificación GS1	49
3.7.2. EPCIS 2.0: Modelo de Eventos de Trazabilidad	50
3.7.3. GS1 Digital Link: Puentes hacia el Mundo Digital	51
3.8. Normativa Sectorial Ibérica: Integración con Sistemas ASICI-ÍTACA	53
3.9. Casos de Uso Implementados: Pasaportes Digitales en Baterías y Productos Agroalimentarios	56
3.10. Plataformas DLT Aplicadas a Trazabilidad	57
3.10.1. IOTA Tangle	57
3.10.2. Ethereum	58
3.10.3. Hyperledger Fabric	59
3.10.4. OriginTrail	59
3.11. Consideraciones de Seguridad en DPP e IoT	61
3.12. Requisitos y Criterios de Diseño	63
3.12.1. Requisitos Funcionales	63
3.12.2. Requisitos No Funcionales	65
3.12.3. Criterios de Diseño Arquitectónico	66
4. DISEÑO DEL DPP	69
4.1. Modelo de Datos del DPP	69

4.1.1.	Identificación Única de Productos y Entidades (GS1)	70
4.1.2.	Entidades y Relaciones del Modelo de Trazabilidad Ibérica (RD 4/2014)	71
4.1.3.	Eventos de trazabilidad EPCIS 2.0 y campos mínimos	73
4.1.4.	Capas de Información y Organización por Niveles de Acceso	78
4.2.	Arquitectura del Sistema Propuesto	81
4.2.1.	Visión general de la arquitectura y componentes principales	81
4.2.2.	Viabilidad de la Solución IoT: Sensores, Comunicaciones y Almacenamiento	89
4.2.3.	Gobierno, Identidad y Control de Acceso Descentralizado	92
4.2.4.	Justificación de decisiones técnicas	97
5.	IMPLEMENTACIÓN	102
5.1.	Entorno y Desarrollo	102
5.2.	Simulación de datos (GTIN, lotes, sensores, eventos EPCIS)	103
5.3.	Codificación e implementación del <i>backend</i> y API para IOTA Notarization	104
5.4.	Desarrollo del visor web del DPP y generación del QR	107
5.5.	Validaciones funcionales e integridad del sistema	109
6.	Evaluación y Análisis	114
6.1.	Seguridad de la Información	114
6.2.	Evaluación Económica para Pymes Jamoneras	115
6.3.	Sostenibilidad y Análisis Cualitativo Ambiental	117
6.3.1.	Contribución al Ecosistema de la Dehesa	117
6.3.2.	Análisis de Ciclo de Vida: Huella de Carbono e Hídrica	118
6.4.	Riesgos y Barreras Tecnológicas	120
6.5.	Amenazas Potenciales: Manipulación de QR y Otros Ataques	122

6.6. Comparativa con Soluciones Alternativas	123
7. Conclusiones	129
7.1. Logro de Objetivos y Hallazgos Clave	129
7.2. Grado de Cumplimiento de Objetivos Específicos	130
7.3. Principales Aportaciones Técnicas y Sociales	131
8. Planificación y Costes Estimados por Fases y Componentes	134
8.1. Fases de Desarrollo y Hitos Principales	134
8.1.1. WBS (Estructura de Descomposicion del Trabajo)	135
8.2. Perfil del Estudiante y Dedicación Temporal	137
8.2.1. Cronograma (Gantt)	138
8.3. Costes Estimados por Fases y Componentes	140
9. LÍNEAS FUTURAS DE INVESTIGACIÓN	144
9.1. Mejoras Viables al MVP Desarrollado	144
9.2. Extensión a Otros Productos y Sectores	146
9.3. Propuestas de Investigación Técnica Avanzada	148
BIBLIOGRAFÍA	151

ÍNDICE DE FIGURAS

1.1. Precintos oficiales del jamón ibérico según la Norma de Calidad	10
8.1. Cronograma del proyecto (Gantt) con fases, solapes y hitos.	139
8.2. Cronograma del proyecto (Gantt) con fases, solapes y hitos. (Continuación) . .	140

ÍNDICE DE TABLAS

3.1. Application Identifiers (AI) de GS1 relevantes para el DPP de jamón ibérico.	53
5.1. Benchmark del resolutor DPP (n=100, dataset <code>bench-latest-100.csv</code>). Tiempos en milisegundos (ms) [137].	111

ÍNDICE DE CÓDIGOS

4.1. Ejemplo simplificado de evento EPCIS 2.0.	77
5.1. Evento EPCIS 2.0 (simulado) para una pieza identificada por SGTIN	103
5.2. Anclaje de un evento en IOTA Notarization utilizando IPFS para almacenamiento off-chain	105
5.3. Ruta Express para resolver una URL Digital Link y generar la vista del DPP . .	107
5.4. Generación de código QR para la URL Digital Link de un producto	108

Capítulo 1

INTRODUCCIÓN

1.1. Antecedentes y Justificación del DPP para Jamón Ibérico

1.1.1. Trazabilidad Alimentaria: Sistemas Tradicionales, Certificación y Problemas de Fraude

En el sector ibérico ya existen mecanismos de identificación y registro que cumplen con la trazabilidad legal mínima: lotes, albaranes, precintos vinculados a la Norma de Calidad y, en su caso, controles adicionales de las Denominaciones de Origen Protegido (DOP) e Indicaciones Geográficas Protegidas (IGP) [1]-[6]. Sistemas sectoriales como ÍTACA agregan parte de esta información y facilitan su consulta por operadores y autoridades [7]. Sin embargo, la evidencia apunta a limitaciones recurrentes: fragmentación de fuentes (*silos* de datos en los sistemas de Planificación de Recursos Empresariales [ERP] y hojas de cálculo), correlación manual entre documentos, verificación *ex post* ante incidencias, asimetría informativa para el consumidor y escasa granularidad legible por máquina para auditorías digitales [8], [9].

ÍTACA (Identificación, Trazabilidad y Calidad del Ibérico) es la plataforma sectorial centralizada gestionada por la ASICI (Asociación Interprofesional del Cerdo Ibérico), implantada al amparo del RD 4/2014 y de las extensiones de norma que financian y ordenan su operativa en toda la cadena del ibérico [7], [10]. Su objetivo fue dotar al sector de un registro digital único, obligatorio y casi en tiempo real, que garantizase la verificación de raza, alimentación, pesos y categorías comerciales, asociando precintos oficiales únicos a cada pieza apta [11].

ÍTACA integra a ganaderos, mataderos e industrias a través de un sistema web multiusuario. En origen, el ganadero registra nacimientos y parentales, crea lotes de engorde y comunica envíos a sacrificio. En matadero, dispositivos integrados (e.g., capturas de pesajes) vuelcan pesos de canal e informes de sacrificio y habilitan la colocación de precintos de Norma de Calidad, cada uno con código único que queda asociado a la trazabilidad [7]. En la industria, se registran entradas, movimientos, fin de curación y posibles transformaciones (deshuesado, loncheado), manteniendo el vínculo con el precinto. Para el consumidor, ASICI ofrece la *app* Ibérico, que, al escanear el código del precinto muestra los atributos básicos (categoría, alimentación, porcentaje

racial, añada, Comunidad Autónoma) [12]. La cobertura de DOP/IGP puede articularse con precintos propios del Consejo Regulador, lo que limita la consulta directa de esos precintos en la *app* genérica [1].

Los datos residen en una base central administrada por ASICI; el acceso completo es para operadores y autoridades, y el público dispone de una vista resumida a través de la *app* Ibérico. ÍTACA cumple con creces la trazabilidad legal del ibérico, pero opera con identificadores y formatos propietarios del sector y no fue concebido como un *pasaporte* interoperable *multi-sector* (GS1/EPCIS) ni como registro público abierto [13]-[15]. En este trabajo, el Pasaporte Digital de Producto (DPP, por sus siglas en inglés) se plantea como capa complementaria: reutiliza el identificador físico existente (precinto) y aporta un modelo estandarizado, resoluble por QR (GS1 Digital Link), con eventos EPCIS y anclajes verificables, ampliando transparencia, interoperabilidad y cobertura de sostenibilidad [13], [16], [17].

El DPP que se propone en este trabajo no sustituye estos registros, sino que los ordena y los hace verificables: define un identificador global resoluble (GS1 Digital Link), normaliza eventos de trazabilidad (EPCIS 2.0), ancla resúmenes criptográficos en una *DLT* (Tecnología de Registro Distribuido, por sus siglas en inglés) sin comisiones (IOTA Tangle) y publica vistas diferenciadas por rol, incorporando, además, métricas de sostenibilidad y circularidad [9], [18]. Así, se reduce el tiempo de investigación de expedientes, se acota el riesgo de error humano en la inserción documental y se incrementa la confianza del mercado en la autenticidad del jamón ibérico [9], [18]-[20].

1.1.2. Competitividad

El jamón ibérico es un emblema gastronómico español y su creciente fama global trae oportunidades, pero también retos competitivos. Uno de los riesgos recientes es la aparición de jamones *ibéricos* producidos en otros países, especialmente China:

Desde hace más de una década se conoce el interés chino por replicar el jamón español: ya en 2010-2011, empresas chinas comenzaron a criar cerdos de razas similares al ibérico e implementar técnicas de salado y curado aprendidas de productores españoles [21]. De hecho, productores españoles sospechan que delegaciones chinas que visitaron sus fábricas hace años (oficialmente para habilitar importaciones) recopilaron *know-how* que luego aplicaron en plantas de jamón en China. El resultado ha sido los primeros *jamones ibéricos made in China* [21], [22].

Si bien su calidad organoléptica aún dista de la de un auténtico jamón ibérico español, a la vista pueden parecerse mucho, al menos a ojos de un consumidor poco experto. Esto supone un riesgo de plagio comercial: jamones chinos de menor calidad y precio inundando mercados asiáticos, haciendo sombra al producto español auténtico [22]. Ya en 2018 se manifestaba que jamones chinos estaban logrando un sabor aproximado al jamón serrano estándar, con tiempos de curación menores, y los productores españoles mostraban preocupación por ser desplazados en Asia por ese producto más barato [22]. Además, existe la posibilidad de uso fraudulento de términos protegidos: por ejemplo, llamar *jamón ibérico* en China a un jamón de raza local, aprovechando la falta de regulación en el país. Aunque la denominación *Jamón Ibérico* está protegida en la UE (y en China, en principio, solo puede usarse para los productos importados

legítimos a través de acuerdos bilaterales), en la práctica la protección legal internacional es limitada [23].

Este contexto hace urgente proteger la autenticidad: mecanismos como la trazabilidad avanzada, DLT y DPP pueden garantizar la identidad de origen de cada pieza, de modo que en cualquier parte del mundo se pueda verificar si un jamón con etiqueta *Ibérico de España* realmente proviene de una granja y secadero españoles certificados [24], [25]

Otra arista competitiva es la expansión de la demanda internacional: China es también un gran comprador de jamón español (tras la apertura de las exportaciones, se ha vuelto un mercado importante con un crecimiento de más de un 100 % en cinco años) [23], [26]. Esto ha motivado a ASICI y la UE a invertir en promoción exterior: por ejemplo, la campaña *Jamones Ibéricos de España, Embajadores de Europa* con giras en varias ciudades chinas [23], [27]. El objetivo es afianzar la imagen de prestigio del ibérico y educar al consumidor chino para que reconozca el auténtico. El Pasaporte Digital podría ser una herramienta en estas campañas: incitar a un comprador extranjero que escanee el QR del jamón y compruebe datos de trazabilidad, certificaciones, incluso un saludo del maestro jamonero en la dehesa (algo difícil de falsificar por imitadores). Asimismo, un DPP basado en blockchain aportaría inamovilidad de datos: un competidor no podría simular fácilmente la información de años de crianza y curación que están registradas en una cadena de bloques pública [18], [28].

Más allá de China, hay otros competidores: por ejemplo, en Italia algunos productores han empezado a criar cerdos de raza ibérica importados, intentando producir *jamón ibérico italiano*. Y países como USA han desarrollado sus propios jamones curados tipo *serrano* (aunque no ibéricos aún) [23].

España debe por tanto proteger la Marca Ibérico como sinónimo de calidad y origen único, similar a cómo la Champaña francesa se protege. Las denominaciones de origen (e.g., Jabugo) ayudan, pero no cubren a todo el espectro ibérico (que también se produce fuera de las DOP) [1]. Por eso, la marca colectiva *Ibérico de España* y herramientas tecnológicas de trazabilidad son clave. En 2024 hubo casos de intervención en frontera de productos cárnicos etiquetados engañosamente: se denunció la incautación en Mallorca de un lote importado de China con etiquetado irregular que simulaba jamón español [19]. Esto demuestra que el riesgo es real y actual.

Todo lo anterior demuestra que la competencia internacional (legal o ilícita) exige redoblar esfuerzos en trazabilidad, autenticación y diferenciación. Un Pasaporte Digital de Producto fortalecería la posición competitiva del jamón ibérico español al proporcionar transparencia total y verificación instantánea de autenticidad, dificultando las falsificaciones y aportando un argumento de valor añadido en mercados globales. Además, permitiría destacar las cualidades únicas (dehesa, bellota, tradición) frente a imitaciones más industriales, protegiendo así la reputación ganada por la Marca España en este producto gourmet [27].

1.1.3. Casos de Uso y Comparativas Relevantes de Pasaportes Digitales

Aunque el concepto de Pasaporte Digital de Producto es relativamente nuevo, ya existen diversas iniciativas y casos de uso en distintos sectores que sirven de referencia para el caso del jamón ibérico. A continuación, se identifican algunos ejemplos reales de implementación de pasaportes digitales (en sectores preferentemente distintos al cárnico), las lecciones aprendidas y cómo podrían adaptarse al contexto ibérico [29], [30]:

- **Pasaporte Digital en el sector textil (moda sostenible):** La industria de la moda ha sido pionera en probar los DPP para proveer transparencia sobre origen de materiales y condiciones de producción. Un ejemplo es la marca británica Nobody's Child, que ha implementado pasaportes digitales en sus prendas mediante un código QR en la etiqueta de cuidado. Al escanearlo, el cliente puede explorar la cadena de suministro de la prenda: desde la procedencia de la tela, fábrica de confección, hasta datos de impacto ambiental (agua, CO₂) de esa prenda. Este proyecto, en colaboración con la plataforma Fabacus, busca no solo cumplir con futuras regulaciones sino «conectar cómo se hizo el producto con el cliente». La lección aquí es la importancia de la conectividad: el QR lleva a una experiencia interactiva y fácil de entender para el consumidor, convirtiendo la trazabilidad en una historia de marca. De igual forma se podría aplicar al jamón ibérico, un QR en la vitola del jamón podría llevar a una página o *pass app* con un recorrido «De la dehesa a tu mesa», mostrando la granja, la bodega de curación, y métricas de sostenibilidad. Este caso demuestra que los consumidores sí escanearán un código si ofrece información interesante, y refuerza la confianza en la marca (Nobody's Child se posiciona así como transparente y responsable). Además, a nivel técnico, está construido sobre GS1 Digital Link y JSON-LD, similar a lo que necesitaría un DPP alimentario, lo cual validaría la elección de esos estándares [13], [29], [31].
- **Impact Receipts y transparencia de huella (ASKET, moda):** La marca sueca ASKET introdujo en 2023 Impact Receipt, un recibo de compra detallando la huella ambiental de cada prenda (CO₂, agua, energía). Esto acompaña al producto vendiéndose, mostrando al cliente el «precio oculto» en recursos naturales. Si bien no es un pasaporte en sí mismo, va en la línea de lo que los DPP deben hacer: comunicar indicadores de sostenibilidad. En la implementación de ASKET, integran datos de todo el ciclo productivo. Lo que queda demostrado con este ejemplo es que presentar datos de impacto de forma comprensible añade valor educativo y posiblemente cambia el comportamiento del consumidor hacia más responsabilidad. Para el jamón ibérico, un DPP podría incluir algo semejante a una «etiqueta de impacto» alimentario: e.g., «Este jamón implicó 30 kg CO₂e de emisiones, 1500 L de agua, y apoya un ecosistema de dehesa que almacena CO₂». Traducir la sostenibilidad a números concretos hace más tangible el concepto al comprador. La experiencia de ASKET sugiere que la transparencia radical puede ser bien recibida y generar diálogo (sus fundadores dicen que es para «combatir el sobreconsumo haciendo visible el coste real») [29], [32].
- **Digital ID para circularidad en moda (PANGAIA ReWear):** La empresa PANGAIA, conocida por innovación sostenible, implementó pasaportes digitales en sus prendas con tecnología EON (Digital ID) y lanzó PANGAIA ReWear, una plataforma de reventa de segunda mano habilitada por esos pasaportes. Cada prenda tiene un QR único; al escanearlo, se accede al historial del producto. Además, si un cliente quiere revender la prenda, la

plataforma toma automáticamente la información del pasaporte (materiales, imágenes, etc.) para listar el producto, facilitando la reventa. Esto es muy innovador porque cierra el ciclo: el DPP no solo informa al primer comprador, sino que viaja con el producto a su siguiente dueño, extendiendo su vida útil. Un pasaporte digital puede habilitar modelos de negocio circulares (reventa, alquiler, reciclaje) al eliminar fricciones de información. Si bien un alimento no se revende para consumo, esta idea se podría trasladar a, por ejemplo, reutilización de envases o certificados de calidad reutilizables. Un caso de uso más cercano es el que hace PANGAIA del pasaporte para proveer consejos de cuidado y reciclaje de la prenda, análogo a cómo un DPP de jamón puede dar consejos de conservación (cómo guardar el jamón, recetas para aprovechar restos, etc.) y opciones de disposición final (reciclar envoltorio). PANGAIA demuestra que los pasaportes pueden crear una comunidad alrededor del producto (vendedores y compradores de segunda mano confiando en la info del DPP). En alimentos, esto podría transformarse en confianza en intercambios B2B (un distribuidor extranjero confía en la información del DPP sin necesidad de certificaciones físicas adicionales) [29].

- Pasaporte de baterías (sector automoción, Global Battery Alliance): Uno de los casos más directamente relacionados con la idea de DPP en la UE es el *Battery Passport*. La Global Battery Alliance (GBA), que incluye empresas como Ford, Tesla, etc., ha pasado pruebas piloto de un pasaporte digital para baterías de vehículos eléctricos. Usan *blockchain*, IA y *auto-ID* para documentar toda la vida de una batería: desde la extracción de minerales (cobalto, litio) hasta la fabricación, uso en coche, y reciclaje final. Ford, por ejemplo, colabora con Everledger en un piloto de este tipo, buscando asegurar origen responsable de materiales y trazabilidad hasta reciclaje [29]. Esta iniciativa está muy alineada con las regulaciones: la UE aprobó en 2023 el Reglamento de baterías, que exige un pasaporte digital para baterías de EV a partir de 2026 [33]. Las enseñanzas que nos da este caso son:
 1. Gran complejidad de la cadena: integrar datos de múltiples proveedores, cada uno con su sistema, requirió definir un estándar común de datos (en GBA desarrollaron un *Data Blueprint*). El equivalente en el jamón sería integrar datos de ganaderos, mataderos, secaderos; es una cadena más corta que la de una batería, pero similar desafío de interoperabilidad [17].
 2. Importancia de la verificación de sostenibilidad: El *battery passport* se enfoca en confirmar que ciertos criterios se cumplieron (materiales libres de trabajo infantil, contenido de reciclado, etc.). Para el jamón, un DPP podría incluir verificación de que el cerdo pastó X meses o que se respetó bienestar animal – quizás auditado por terceros y subido al DPP como certificado [34].
 3. Uso de *blockchain* para confianza multi-actor: En la batería, competidores colaboran pero no confían ciegamente, por eso *blockchain* es útil para crear un registro compartido. En la cadena ibérica, ya hay más confianza central, pero si se integran otros (distribuidores internacionales, autoridades de distintos países), tener un ledger neutro puede ser valioso. El jamón ibérico podría inspirarse en GBA en cuanto a gobernanza: la interprofesional ASICI podría hacer de «alianza» para desarrollar el pasaporte de jamón, similar al rol de GBA en baterías, reuniendo a todos los actores implicados (productores, certificadoras, tecnología). Esto facilitaría la adopción sectorial [29].
- Grandes minoristas y trazabilidad digital (Decathlon, alimentos varios): fuera del DPP formal, es relevante mencionar cómo los gigantes del *retail* abordan la trazabilidad, porque

impulsan a los proveedores. Decathlon, por ejemplo, implementó RFID en 50.000 puntos (fábricas, almacenes, tiendas) para rastrear todos sus productos deportivos. Si bien su motivación es más logística, esa infraestructura permite que un cliente escanee una etiqueta RFID/QR y obtenga información del producto [35]. En alimentación, Walmart (EE. UU.) exigió a sus proveedores de hojas verdes unirse a su plataforma IBM Food Trust (*blockchain*) para trazabilidad después de brotes de *E.coli*. El resultado fue que algunos proveedores como Zespri (kiwis) usan *blockchain* para trazabilidad integral, reduciendo tiempos de respuesta en retiradas de días a segundos. Cuando un líder de mercado impone un estándar de trazabilidad digital, los productores deben adaptarse o arriesgan perder ese canal. Para el jamón ibérico, imaginemos que en unos años, cadenas como Carrefour o El Corte Inglés dijeran «solo compraremos productos ibéricos con pasaporte digital conforme a la normativa UE». Estar preparados con un sistema interoperable (idealmente basado en estándares GS1/EU) sería crucial para mantener mercados. Además, casos como IBM Food Trust mostraron que la trazabilidad *blockchain* mejoró la eficiencia: Walmart logró rastrear un mango del supermercado a la finca en 2.2 segundos usando *blockchain*, cuando antes les tomaba 7 días con métodos tradicionales [36]. Aunque el jamón no es producto de retiradas urgentes (no es perecedero inmediato), esta eficiencia en la retirada de productos es valiosa para seguridad alimentaria.

- Ejemplos en alimentación *premium*: Dentro del sector alimentario, hay algunos ejemplos más cercanos (empresas de vinos y espirituosos han experimentado con DPP o similares). En el sector vitivinícola, la startup Wine Blockchain en Italia permitió a consumidores escanear una botella y ver desde el viñedo hasta la bodega. Incluso la UE ya exige que a partir de diciembre 2023 las etiquetas de vino tengan información digital accesible (ingredientes, calorías) mediante QR [37]. Ese es un precursor de DPP en bebidas. La digitalización de la información de producto puede ser impulsada mediante regulación (como en vino) y normalmente comienza por datos que antes no se daban (nutricionales, en este caso). En el jamón ibérico, podría ocurrir algo parecido, quizás la normativa futura exija dar al consumidor información sobre huella ambiental o bienestar; un DPP facilita esa provisión sin sobrecargar la etiqueta física. Otro ejemplo es el de productores de aceite de oliva *premium* empleando un código QR *blockchain* para certificar origen de las aceitunas y fecha de molturación, creando confianza en mercados asiáticos donde hay falsificaciones. Esto es similar a la necesidad de jamón en China: se han detectado falsificaciones de jamones 5J Joselito para ser exportados a China. Y algunas marcas han puesto sistemas de autenticación digitales (códigos alfanuméricos únicos bajo rascado). Un DPP más completo reemplazaría esos sistemas aislados con uno estándar.

De los usos enumerados, se pueden extraer lecciones globales y mejores prácticas aplicables al jamón ibérico:

1. Centrarse en la historia y la conexión emocional. No saturar al usuario final con datos técnicos, sino presentar la información del pasaporte de forma narrativa y visual (como la moda lo hace mostrando el recorrido de la prenda, o un vídeo del chef embajador hablando del jamón en la campaña en Hong Kong) [23]. En el DPP del jamón, podría haber pequeños vídeos o fotos de la dehesa al atardecer, del maestro jamonero realizando el calado, etc., para darle vida a los datos.
2. Interactividad y utilidad. Hacer que el pasaporte no sea solo un PDF estático, sino una

plataforma interactiva. Por ejemplo, permitir al consumidor hacer preguntas al chatbot sobre el producto, o registrarse para recibir un certificado de autenticidad a su nombre, etc; esto aumenta el *engagement*. Pangaia mostró que la utilidad (facilitar la reventa) fomenta el uso del pasaporte [29]. En el jamón, donde no existe casi posibilidad de reventa (se contempla la posibilidad de sorteos y trofeos en campeonatos), podría haber un esquema de fidelización: escaneas el DPP y acumulas puntos si reciclas el envase o si completas una encuesta de cata, etc.

3. Estandarización y colaboración. Todos los casos de éxito han surgido de colaboraciones: GBA para baterías con un estándar de datos común, proyectos con GS1 en moda, etc. Para jamón ibérico, la colaboración entre productores, la interprofesional, organismos certificadores y *tech partners* es crucial. Esto asegurará que el DPP propuesto cumpla con las normativas de la UE (ESPR, etc.) y sea reconocido. Por ejemplo, en el sector textil la Comisión Europea encargó un estudio en 2022 sobre DPP en textiles para guiar la implementación [38]; sería conveniente que el sector cárnico se anticipe creando sus propios criterios antes de que se los impongan.
4. Privacidad de datos empresariales. Un aprendizaje de proyectos en otros sectores es equilibrar transparencia con resguardo de secretos comerciales. No todo dato interno debe hacerse público en el DPP. Por ejemplo, Ford no va a publicar la receta exacta de su batería, pero sí los indicadores exigidos (contenido reciclado, huella CO₂) [29]. Similarmente, un productor de jamón podría no querer revelar la ubicación exacta de todas sus fincas (por seguridad o competencia) – en su lugar, podría indicar región y características sin dar coordenadas precisas; igualmente, puede no querer decir sus proveedores de pienso. El DPP debe estructurarse de modo que cumpla con la normativa (que pedirá ciertos datos obligatorios) pero proteja información sensible. Se pueden usar *verifiable credentials* o certificaciones de terceros en el pasaporte en lugar de datos crudos: por ejemplo, en vez de publicar la lista de campos donde pastaron, incluir un sello digital de autoridad (Junta Andalucía) que certifica «este jamón proviene de una dehesa inscrita y supervisada». Esto da confianza sin exponer todo detalle.
5. Afrontar la brecha digital del consumidor. No todos los consumidores de jamón (sobre todo generaciones mayores) van a escanear códigos QR o entender un pasaporte digital complejo. Hay que diseñar con simplicidad. El pasaporte debería ofrecer valor incluso a quien no es experto: por ejemplo, un simple «semáforo» de sostenibilidad, o una breve historia en texto más multimedia, y luego un botón «ver datos técnicos» para quien sí quiere profundizar. La experiencia de lecherías y otros es que demasiada información puede abrumar, así que la interfaz debe ser clara (el marco GS1 Digital Link sugiere esto, con capa para máquinas y otra presentable a humanos) [13], [14].
6. Resultados medibles. De los pilotos existentes, conviene observar resultados: ¿aumentaron ventas? ¿mejoró la confianza? Algunos son muy nuevos para saberlo. No obstante, hay indicios: H&M con su ID digital dijo que buscaba ofrecer servicios postventa (reciclaje, etc.) para fidelizar clientes [29]. Si el jamón ibérico implementa un DPP, se podría medir el efecto en protección de marca en mercados lejanos (menos reclamaciones de falsificación, etc.), o en eficiencia (tiempo de auditorías reducido porque todo está en sistema). Documentar estos beneficios ayudará a la expansión del proyecto dentro del sector.

En conclusión, los casos de uso reales muestran que el Pasaporte Digital de Producto no es ciencia ficción, sino una tendencia en marcha en diversas industrias. En sectores como

moda, automoción, electrónica y alimentación de lujo ya se está comprobando su valor para transparencia, cumplimiento regulatorio y habilitación de modelos circulares. El sector del jamón ibérico, con su fuerte componente de calidad diferenciada y necesidad de proteger autenticidad, puede aprovechar esas lecciones: implementando un DPP que combine información rigurosa (validada por *blockchain*) con una narrativa atractiva, asegurando interoperabilidad con estándares europeos, y anticipando los requerimientos futuros de sostenibilidad y trazabilidad que vienen en el marco normativo [39]. De esta forma, el jamón ibérico podría posicionarse internacionalmente no solo como un producto tradicional exquisito, sino también como un producto trazable 100 % transparente y sostenible, alineado con las exigencias del consumidor y la sociedad del siglo XXI. Cada jamón llevaría no solo su aroma y sabor, sino también su «historia digital» imborrable, fortaleciendo la confianza y el valor de la marca ibérica en cualquier lugar del mundo.

1.2. Diferencias entre Jamón Ibérico y Jamón Serrano y Confusiones de Mercado

1.2.1. Diferencias Técnico-Legales

Aunque ambos son jamones curados tradicionales de España, el jamón ibérico y el jamón serrano se diferencian por la raza del cerdo, su alimentación, normativas de calidad y denominaciones asociadas.

El jamón ibérico proviene exclusivamente de cerdos de raza ibérica (negros) o cruzados con, al menos, un 50 % de sangre ibérica, criados bajo las condiciones definidas por la Norma de Calidad del Ibérico (Real Decreto 4/2014) [10]. Esta norma española establece categorías según la pureza racial (100 % ibérico, 75 % o 50 %) y el tipo de alimentación del cerdo (bellota, cebo de campo, cebo) [10], [11]. Cada combinación se identifica con un precinto de color en la pata del jamón (negro, rojo, verde o blanco) que garantiza y certifica ante el consumidor la categoría del producto [11], [40]. Además, la trazabilidad del ibérico está muy vigilada: los cerdos deben nacer, criarse y sacrificarse en explotaciones registradas; se controla su alimentación (e.g. tiempo mínimo en montanera) y el tiempo de curación mínimo (por ejemplo, un jamón ibérico de bellota suele curar más de 36 meses) [10].

Por su parte, el jamón serrano típicamente proviene de cerdos de raza blanca (Landrace, Large White, Duroc) y sigue un proceso de curado más corto (mínimo de 7 a 12 meses según peso). Existe una especialidad tradicional reconocida por la UE llamada ETG (Especialidad Tradicional Garantizada) Jamón Serrano que estipula ciertos estándares de elaboración para usar la denominación *Serrano* [41]. Sin embargo, *jamón serrano* en general no es una DOP, sino un término genérico para jamón curado de cerdo blanco, por lo que su regulación de base es la normativa general de alimentos y carnes.

Las diferencias técnicas incluyen que el jamón serrano suele tener menor infiltración grasa y un sabor más suave, dado que la raza y la alimentación (piensos) difieren de los ibéricos de bellota en que acumulan ácido oleico en su grasa por la dieta de bellotas.

Legalmente, la Norma de Calidad del Ibérico no aplica a jamones serranos; estos pueden acoger otras figuras de calidad: por ejemplo, Jamón de Teruel es una DOP de jamón serrano de Aragón con pliego propio (cerdos raza Duroc con cruce de Landrace, criados y curados en Teruel) [1]. Entonces, mientras un jamón serrano estándar no tiene un sistema de precintos obligatorio, el jamón ibérico sí lo tiene – es obligatorio colocar el precinto de norma a cada pieza ibérica en el matadero, con un código único trazable en la base de datos ÍTACA [7], [10].

En términos técnico-legales: existen diferencias de raza y cría (ibérico y blanco), regulación específica nacional para ibérico y especialidad tradicional para serrano, sistemas de trazabilidad y certificación distintos, y protección del término *ibérico* dentro de España. Esto se traduce en el mercado a productos de segmento distinto: el jamón ibérico es un producto de calidad de mayor precio, con producción limitada y parcialmente ligada a territorios concretos por sus DOP e IGP (Extremadura, Andalucía, Salamanca etc.), mientras que el jamón serrano se produce a gran escala en toda España; y otros países llegan a producir jamón de cerdo blanco similar, como *prosciutto* en Italia o jamones *tipo serrano* en USA o incluso China.

1.2.2. Confusión Terminológica en Etiquetado, Percepción y Mercado

A pesar de las normas, persisten confusiones y usos indebidos de términos en la comercialización de jamones, lo que afecta la percepción del consumidor. Un caso clásico es el término *pata negra*, popularmente asociado al mejor jamón ibérico. Desde 2014, legalmente Pata Negra está reservado únicamente para jamón de bellota 100 % ibérico (precinto negro) en España. Sin embargo, en el lenguaje coloquial e incluso en publicidad internacional, a veces se llama *pata negra* a cualquier jamón español de calidad, lo cual puede inducir a error. Otra confusión surge entre la etiqueta y el precinto: muchos consumidores no saben que el color del precinto (cinta de plástico en la caña del jamón) tiene un significado oficial; a veces se fijan solo en la marca comercial o en expresiones como «reserva» o «gran selección» que pueden figurar en la etiqueta del fabricante sin un estándar claro. Por ello, las autoridades y ASICI han hecho campañas informativas enfatizando: «Fíjate en el color del precinto, no te dejes llevar solo por la etiqueta»[40]. Cada precinto lleva además un código de barras único ligado al registro ÍTACA, que puede escanearse con la *app* Ibérico de ASICI para verificar la trazabilidad de esa pieza. En la siguiente imagen, se ilustran los cuatro precintos de norma con sus colores y categorías correspondientes (negro, rojo, verde, blanco), que son la única forma fiable de identificar la calidad o categoría de un jamón ibérico en el punto de venta [11]:

- Negro: jamón de bellota 100 % ibérico. Estos jamones tienen una pureza racial 100 % ibérico, (ambos progenitores, y los de éstos, son cerdos 100 % ibéricos), y son alimentados únicamente con bellotas y demás recursos de la dehesa durante el periodo de montanera (periodo de engorde del cerdo).
- Rojo: jamón de bellota ibérico. Estos jamones también han sido alimentados únicamente con bellotas y demás recursos de la dehesa, durante el periodo de montanera, pero sin embargo designa a animales con al menos el 50 % de su porcentaje genético correspondiente a la raza ibérica, pudiendo ser del 75 %, «provenientes de hembras de raza 100 % ibérica y machos procedentes del cruce de madre de raza 100 % ibérica y padre de raza 100 % duroc», o del 50 %, que son «provenientes de hembras de raza 100 % ibérica y machos de

raza 100 % duroc».

- Verde: de cebo de campo ibérico. Aquellos jamones que han sido alimentados tanto de bellotas y recursos naturales de la dehesa como de piensos y con al menos el 50 % de su porcentaje genético de raza ibérica, bajo las mismas condiciones del precinto rojo.
- Blanco: de cebo ibérico. Estos jamones también están sujetos al término y restricciones de la terminología ibérico (con un mínimo de 50 % de raza ibérica correspondiente a las descripciones anteriores), pero en su defecto son alimentados únicamente con pienso, sin recursos de la dehesa.

Cada uno de los cerdos descritos anteriormente en la explicación de los precintos, así como sus progenitores, deben estar registrados en el los libros genealógicos correspondientes.



Figura 1.1: Precintos oficiales del jamón ibérico según la Norma de Calidad (negro: bellota 100 % ibérico; rojo: bellota ibérico 75 % o 50 %; verde: cebo de campo ibérico; blanco: cebo ibérico) [42]

Así, el conocimiento básico del consumidor para diferenciar el jamón ibérico debe ser por una parte la pureza racial del cerdo (100 %, 75 %, 50 % ibérico) y por otra la alimentación del cerdo (bellota, para los cerdos alimentados únicamente con bellotas y recursos naturales de la

dehesa durante la montanera; cebo de campo, para aquellos que han sido alimentados con bellota y recursos naturales de la dehesa y, además, piensos; y cebo, para aquellos cerdos que han sido alimentados únicamente con piensos).

La percepción de los consumidores a veces mezcla ibérico y serrano por simple desconocimiento. En mercados extranjeros, el término «jamón ibérico» ha ganado fama y en ocasiones comerciantes inescrupulosos podrían denominar «ibérico» a jamones que no lo son. Para atajar esto, España protege la marca «Jamón España» y las denominaciones de origen ibéricas (DOP Guijuelo, DOP Jabugo, etc.) en tratados internacionales, pero aun así es un desafío educar al mercado.

Otra fuente de confusión es que los jamones de Denominaciones de Origen Protegidas (DOP) ibéricas (como Jabugo, Guijuelo) llevan sus propios precintos y vitolas de consejo regulador: aunque respetan el mismo código de colores de la Norma, el consumidor podría no entender que un precinto blanco de DOP Dehesa de Extremadura también indica cebo ibérico. ASICI recomienda que el comprador «Siempre busque el logotipo de ASICI en el precinto de norma de calidad» cuando adquiera un ibérico estándar (las DOP llevan su sello particular) [10], [11].

Queda claro, pues, que existe cierta terminología compleja (porcentajes raciales y nombres de alimentación) que puede resultar confusa sin información accesible. Aquí es donde un Pasaporte Digital podría aportar claridad: escaneando un código, el consumidor podría ver en su idioma una explicación sencilla del producto: e.g. «Jamón Ibérico de Cebo – Cerdo 50 % raza ibérica alimentado con pienso en granja. Curación: 24 meses en Badajoz. Granja certificada en bienestar animal.», eliminando ambigüedades. Esto mejoraría la transparencia y la confianza, combatiendo la confusión intencionada o accidental en el etiquetado.

También hay un aspecto de percepción de calidad: el jamón serrano de alta gama (por ejemplo, de Teruel) puede ser excelente, pero muchos consumidores asumen que «ibérico» es siempre superior. En realidad, son productos diferentes, y cada uno con gradaciones internas. Educar al público en esas diferencias es parte de la labor del sector. Un hallazgo de la Secretaría de Consumo en España fue que una proporción significativa de consumidores no distingue la raza (100 % vs 50 % ibérico) con solo ver la etiqueta, de ahí la importancia del sistema de precintos de colores introducido en 2014 [40].

Por último, en mercados internacionales pueden darse traducciones o *naming* confusos: en China al jamón curado español se le llama a veces «jamón Parma español» o similares, lo que mezcla denominaciones. La creación de una identidad digital unívoca por producto (pasaporte) ayudaría a uniformar la información presentada en todos los mercados, evitando que en cada país se use una terminología distinta que pueda crear confusión.

1.3. Cadena de Suministro y Cadena de Valor del Jamón Ibérico y su Contexto Comercial

1.3.1. Etapas, Sensórica y Trazabilidad

El proceso productivo del jamón ibérico abarca una secuencia de etapas bien definidas, cada una de las cuales añade valor y requiere controles de calidad y trazabilidad específicos. A continuación, se describen las principales fases de la cadena de valor del jamón ibérico, identificando sus particularidades y necesidades de sensorización/trazabilidad:

1. **Genética y Cría Inicial:** todo comienza con la selección genética de los reproductores. En el ibérico, asegurar la pureza racial (100 %, 75 % o 50 % ibérico según el producto final que se quiere obtener) es crucial. Las granjas reproductoras mantienen libros genealógicos y hoy día usan chips o crotales RFID en las madres con el propósito de mantener la identificación. Una cerda ibérica pare generalmente en primavera; momento en el que los lechones son identificados individualmente. Aquí la trazabilidad se inicia registrando el origen de cada animal (pedigrí, explotación de nacimiento). Añadir sensórica en esta etapa no tiene mucho sentido, aunque los datos genéticos y de nacimiento que se registran en ÍTACA podrían integrarse al DPP (por ejemplo, % de raza ibérica del cerdo).
2. **Cría y engorde en la dehesa o cebadero:** tras el destete, los cerdos pasan a fase de crecimiento. Si son de bellota, se crían en libertad en la dehesa hasta, aproximadamente, los 18 meses, con una fase final de montanera (de octubre a febrero) donde se alimentan de bellotas y pastos. Si son de cebo, pueden criarse en granjas intensivas o semi-extensivas (cebo de campo). En ambos casos, se requieren controles sanitarios (medicación administrada, etc.). La sensórica aquí podría incluir geolocalización GPS de algunos animales en dehesa para asegurar que realmente pastan cierta superficie, o sensores de actividad (existen collares que miden pasos para ganado, podrían aplicarse a cerdos). También puede haber sensores ambientales: estaciones meteorológicas en la dehesa registrando la climatología durante la montanera (que influye en la bellota). Todo esto aportaría al pasaporte digital información sobre el bienestar animal y alimentación: p. ej., número de hectáreas por cerdo (derivado del movimiento), alimentación recibida (certificada por el ganadero). En cebo intensivo, sensores de granja (temperatura de la nave, calidad del aire) también pueden registrarse. Desde el punto de vista de la trazabilidad, cada lote de pienso que se da a los animales se documenta, y en cría extensiva se acredita el período de montanera (mínimo 60 días comiendo bellota, con incremento de peso mayor a X kg según la Norma). Estos eventos (entrada del cerdo a montanera, fin de montanera, etc.) se registran en el sistema y podrían registrarse en *blockchain* para mayor confianza. En la etapa de cría, se hacen a menudo pesajes periódicos: básculas ganaderas podrían volcar automáticamente el peso a un registro digital cada vez que se pesa un cerdo, combatiendo el posible fraude (el peso de entrada/salida de montanera es clave para ver si engordó a base de bellota y en los casos de las DOP y las IGP, si cumple con los límites estipulados por la Norma).
3. **Transporte al matadero:** cuando los cerdos alcanzan el peso adecuado (normalmente más de 160 kg en bellota), se envían al sacrificio. Aquí, la trazabilidad exige documentación del transporte: fecha, hora, matrícula del camión, certificado de limpieza del vehículo, etc. Al

llegar, se verifica la identidad de los animales (lectura de crotales) y se asigna un número de lote de matanza. En un DPP, se podría incluir toda esta información como parte de la historia de la pieza, lo cual es relevante para la calidad de la carne.

4. En el matadero autorizado, se sacrifica al animal siguiendo protocolos sanitarios estrictos. Cada cerdo genera dos piernas (futuros jamones) y dos paletas, además de otros productos. En este punto, se asocia la identificación individual del cerdo con las piezas resultantes. Tradicionalmente, se tatuaba o marcaba el número de lote en la piel de las piernas. Con tecnología moderna, podría hacerse mediante código QR o RFID en las piezas inmediatamente después del faenado para una identificación inequívoca. Tras el faenado, un veterinario oficial realiza la inspección sanitaria; si el cerdo no pasa la inspección, no entra en la cadena alimentaria. Este resultado se registra. Para los aprobados, cada canal se pesa y clasifica. En ibéricos, además se toma nota del grado de engrasamiento, que es importante (una característica del bellota es el «toqueado» de grasa infiltrada). Además del resto de datos (número de identificación individual, número de pieza resultante, resultado de la inspección sanitaria), este dato de calidad podría incluirse en el pasaporte digital: por ejemplo, «Grado de grasa dorsal: alto, apto bellota», pudiendo identificar lotes de calidad excepcional que podrían venderse como ediciones especiales, ediciones únicas, etc. Lo más relevante es mantener la trazabilidad: esto se logra con etiquetas en cada jamón fresco con un código único (muchos usan códigos de barras pegados). En esta etapa también hay controles de pH de la carne y temperatura post-mortem; estos datos podrían almacenarse en el DPP. Desde el punto de vista de las DLT, cada jamón tendría ya su «identidad digital» lista para seguirle la pista independiente del resto. Se puede emitir un evento de trazabilidad tipo EPCIS *Transformation Event* que dice: Animal X (ID) -¿Jamón Y (ID), Paleta Z, etc., con links a los IDs de piezas. Este es un punto crítico donde el pasaporte digital toma entidad propia para cada jamón.
5. Salado y postsalado: las piernas frescas pasan a la fase de salazón, donde se cubren en sal marina por 1 día por kilo de peso, aproximadamente. Luego se lavan y equilibran en cámara fría (postsalado) durante semanas. En esta etapa, las variables ambientales son muy importantes: temperatura típicamente de entre 0°C y 5°C y humedad entre el 80 % y el 90 % en salado, luego un poco menos frío en postsalado. Sensores de temperatura y humedad son imprescindibles; muchos secaderos ya monitorizan digitalmente estas cámaras. Para garantizar la calidad, se debe asegurar que cada lote estuvo el tiempo correcto en sal. El pasaporte digital podría contener por lote: «Salazón del 10/2/2025 al 25/2/2025 a 3°C – 85 % HR, sal marina de origen Alicante». Incluso se podría integrar información sobre la sal usada (hay normas que requieren que sea sal marina sin aditivos, etc.), integrando el pasaporte digital de la sal marina. Un sensor IoT en la sala de salazón podría registrar cada hora esas condiciones y anclarlas a la cadena; en caso de desviación (por ejemplo, si la temperatura subió por encima de los 5°C), ese registro queda y sirve para auditoría. Tras el salado, en la fase de reposo en cámara, la pierna va perdiendo agua lentamente. Podría medirse el peso de las piezas antes y después del salado; esas mediciones se apuntan en control de calidad y podrían subirse al DPP para reflejar la evolución («pérdida de X % de peso tras salado, normal»).
6. Secado y maduración (curado): esta es la etapa más larga y característica; los jamones se cuelgan en secaderos naturales o cámaras, primero a temperaturas suaves primaverales (15-20°C) y luego pasan a bodegas frescas (verano-invierno siguiente) donde maduran a 18-25°C con humedades decrecientes. El proceso completo dura mínimo 14 meses en jamones

serranos, pero en ibéricos de bellota se alarga hasta los 24, 36 o más meses. Durante este tiempo, las condiciones ambientales son críticas: tradicionalmente se usaban ventanas para regular, hoy en el ámbito industrial se usan controles climáticos automáticos. Sensores de temperatura, humedad y circulación de aire se despliegan por todo el secadero. Un sistema IoT recogería miles de datos de clima a lo largo de los años de curación. No se registrarían todos en el pasaporte por practicidad, pero sí se pueden generar indicadores clave: por ejemplo, número de días que el jamón estuvo dentro de ciertos rangos de temperatura, o perfiles estacionales. Un enfoque interesante sería colocar sensores electrónicos dentro de piezas piloto (hay investigaciones con sensores de humedad internos en jamones para estudiar el secado); esos podrían aportar datos de difusión de sal, etc., aunque eso sería más para I+D que para cada pasaporte de consumo. En cuanto a controles de calidad en esta fase: maestros jamoneros realizan «calado» (pinchar con un hueso de caña para oler) para comprobar el aroma. Ese resultado sensorial (apto o no apto) podría digitalizarse como un evento: «QualityInspectionEvent – aroma OK en mes 18». Además, se realizan movimientos internos: se suele cambiar las piezas de sitio, moverlas de planta, etc. Cada movimiento (por lotes) dentro del secadero puede registrarse para mantener orden. Un DPP podría reflejar «Curado: X meses en secadero natural de Jabugo (Huelva), altitud 650m)», poniendo en valor características geográficas que interesan al marketing también. Sensores externos como estaciones meteorológicas simples podrían registrar cómo fueron las condiciones climáticas reales en esos años para aquellos secaderos naturales que dependen del clima exterior. Esos datos podrían asociarse al pasaporte para verdaderamente contar la historia del jamón: por ejemplo, «año de secado con verano caluroso, que potenció la sudación de la grasa». Desde la perspectiva de trazabilidad formal, durante la curación no se mezclan lotes, es más bien un almacenamiento controlado. Sin embargo, existe una merma considerable (al final se pierde un 35 % del peso inicial). Sería interesante registrar el peso final de cada jamón al descolgar, porque indica concentración de sabor; un pasaporte digital podría listar: peso inicial en comparación con peso final, porcentaje de merma. Ese dato hoy se usa internamente para la clasificación, pero no llega al consumidor – en un DPP podría ser un sello de calidad (ej. «curación lenta, perdió 34 % de su peso»).

7. Clasificación final, etiquetado y precintado: tras la maduración, cada jamón ibérico es evaluado para su categoría de venta. En el jamón ibérico, aquí es donde se coloca el precinto de color de la Norma (negro, rojo, etc.) si no se puso antes. Según la norma RD 4/2014, el precinto obligatorio debe colocarse antes de la salida del jamón de la industria y va asociado a la trazabilidad del animal [10]. En la práctica, la mayoría de industrias coloca el precinto al inicio de la curación o incluso en fresco. Pero supongamos que se hace al final para confirmar que cumplió todos los requisitos. El precinto lleva un código (código de barras o *datamatrix*) que identifica la pieza en la base de datos ÍTACA. Aquí la *app* Ibérico permite a cualquiera escanear ese código y ver información básica: raza, alimentación, fecha de sacrificio, empresa elaboradora [12]. Este es ya una especie de pasaporte digital centralizado actual. Al etiquetar, también se añade la etiqueta comercial con marca, lote, peso, y a veces un código QR de la empresa que apunta a su web o certificado *blockchain* privado (algunas marcas han implementado sus propios códigos de autenticidad). Es crucial en esta etapa que toda la información recopilada se sincronice: la base de datos interna de la empresa, ÍTACA, y eventualmente la *blockchain*/DPP deben concordar. Un posible procedimiento es generar automáticamente el registro en la DLT en cuanto se asigna un precinto a una pieza, cerrando así la trazabilidad con un evento final *Object Event*: «Jamón #XYZ precintado como Bellota 100 % Ibérico». Sensórica aquí no aplica mucho.

8. Distribución y venta: los jamones terminados se envían al mercado (ya sea a distribuidores, tiendas gourmet, exportación, etc.). En esta fase logística, la trazabilidad legal continúa en forma de documentos de envío (albaranes con lotes). Un pasaporte digital puede registrar la primera salida comercial: por ejemplo, «Jamón #XYZ enviado el 10/10/2025 a Almacén Madrid para distribución». Si se quisiera afinar más, se podrían equipar contenedores de jamones con sensores de temperatura si van en rutas largas, para asegurar que no superen cierto umbral (aunque el jamón curado no requiere frío estrictamente, temperaturas muy altas podrían dañar la calidad). De cara al consumidor, es interesante saber la fecha de expedición y quizá el tiempo que ha pasado desde que salió de bodega hasta que lo compra, por frescura del corte (los jamones enteros pueden conservarse mucho tiempo, pero envasados loncheados tienen fecha de consumo preferente). Otro aspecto relevante a tener en cuenta son las exportaciones, donde se requiere a veces certificados sanitarios adicionales (p.ej., China exige que la pieza pase 30 días a -20°C si no está cocida, para eliminar riesgo de triquina). Si esto ocurre, debería reflejarse: «congelación preventiva realizada del 01/06/2025 al 30/06/2025». Un sensor de temperatura podría validar que se cumplió esa congelación. Esto dotaría al pasaporte de datos de seguridad alimentaria en mercados lejanos. Cuando el jamón llega a un punto de venta, se podría registrar un evento de recepción en el sistema del agente minorista, integrando la trazabilidad B2B con la DLT. Realísticamente, en una primera implementación, la trazabilidad DLT podría detenerse al salir de la fábrica, y luego retomar con el escaneo por el consumidor final [36].
9. Postventa y consumo: una vez en manos del consumidor (ya sea un particular que compra un jamón entero, un restaurante, etc.), la vida técnica del producto termina con su consumo. Sin embargo, el concepto de pasaporte digital debe extenderse a esta fase para fines de retroalimentación y circularidad. Por ejemplo, el pasaporte (vía un código QR en la etiqueta) puede permitir al consumidor registrar que consumió el producto y dar su *feedback* (calificación de sabor, etc.), lo cual la empresa podría captar para control de calidad. También, como mencionamos, puede guiar en la disposición final (reciclaje de envases). Incluso podría incentivar la reutilización: en productos textiles hay pasaportes que fomentan reventa de segunda mano; en jamón no aplica la reventa, pero podría aplicar programas de recogida de restos (por ejemplo, una marca podría ofrecer recoger el hueso a cambio de algún descuento, para aprovecharlo industrialmente). Son ideas quizás no maduras comercialmente, pero el DPP abre la puerta a innovaciones en la relación postventa. Desde un punto de vista distinto, si pensamos en la trazabilidad en caso de incidencias: si hubiera que hacer una retirada (por ejemplo, se descubre que cierta partida de sal estaba contaminada), tener cada pieza identificada digitalmente hasta el consumidor facilitaría notificarles. Un sistema DPP podría enviar alerta (si el consumidor registró su producto escaneándolo) de «no consuma el producto X». Esto se alinea con los objetivos de seguridad alimentaria mejorada [36], [43]. Por último, en postconsumo, se podría emitir un «fin de vida» en el pasaporte cuando el producto es consumido o descartado, aunque es más relevante en productos duraderos que en alimentos. En general, tener un pasaporte digital extiende la cadena de valor hasta el consumidor final informado, convirtiendo la tradicional trazabilidad B2B (del corral a la tienda) en una trazabilidad también B2C (hasta la mesa del consumidor) [44].

A lo largo de todas estas etapas, existe documentación oficial que define requerimientos y buenas prácticas: la Norma de Calidad del Ibérico (RD 4/2014) ya citada, las guías de trazabilidad de ASICI, manuales del MAPA sobre inspección de jamones, etc. Por ejemplo, ASICI con su

sistema ÍTACA ha logrado identificar con precinto más de 7,15 millones de jamones ibéricos en 2022, lo que muestra la escala de datos manejados (cada uno con su historial). Asimismo, las 4 DOP ibéricas añaden control extra a unos 256.000 jamones anuales [27], [45]. Toda esta documentación (registros de campo, guías de prácticas, normas de calidad) sería la base sobre la que el pasaporte digital extraería datos. El DPP no viene a reinventar la trazabilidad, sino a unificarla y enriquecerla: consolidar en un solo recurso digital datos actualmente dispersos en etiquetas, precintos, albaranes y certificados, y presentarlos de forma coherente y verificable. De este modo, cada capítulo de la vida del jamón (desde la encina de la dehesa hasta el plato) queda reflejado y respaldado por evidencias en la cadena de bloques, alineándose con el enfoque de *del campo a la mesa* promovido por la UE [46].

1.3.2. Sostenibilidad en la Industria del Jamón Ibérico

El sector del jamón ibérico se ha alineado firmemente con los objetivos de sostenibilidad de la UE. De hecho, el propio sector se ha adherido al Pacto Verde Europeo (*Green Deal*) y a sus compromisos de lograr un impacto climático neutro en 2050, avanzando hacia un sistema alimentario más sostenible. Este compromiso se refleja en múltiples iniciativas ambientales, como el aprovechamiento de la dehesa (ecosistema mediterráneo donde se cría el cerdo ibérico) como sumidero de CO₂, la reducción de emisiones de gases de efecto invernadero y la compensación de huella ecológica mediante reforestación. Asimismo, la industria está implementando medidas de economía circular, con uso eficiente de recursos, planes de gestión de residuos (e.g., envases más ecológicos y disminución de plásticos de un solo uso) y reducción del consumo de agua (optimización hídrica con hasta un 30 % menos de uso en los últimos años [47], [48]).

En línea con las estrategias europeas («De la Granja a la Mesa», biodiversidad, clima, etc.), el modelo extensivo del ibérico en la dehesa presenta ventajas sostenibles: promueve el bienestar animal (cría al aire libre con alimentación natural) y contribuye al desarrollo rural. El sector ibérico actúa como motor socioeconómico en zonas rurales, fijando población y generando empleo local, en concordancia con los Objetivos de Desarrollo Sostenible de la ONU [46], [47].

Todas estas iniciativas sitúan al ibérico en sintonía con las políticas del *European Green Deal*, que busca una Europa climáticamente neutra, circular y justa. La propia Comisión Europea, en el Pacto Verde Europeo de 2019, recalcó la necesidad de transformar la economía hacia la neutralidad climática al 2050 y destacó que los productos sostenibles (incluidos los agroalimentarios) desempeñan un papel esencial en esa transición [32], [49]. En suma, la industria del jamón ibérico está incorporando la sostenibilidad medioambiental, social y económica en su cadena de valor, preparándose para las exigencias presentes y futuras de la UE en materia de impacto ambiental, trazabilidad y economía circular [32], [49], [50].

1.4. Definición del Problema, Objetivos del Trabajo y Alcance

La cadena de valor del jamón ibérico opera con múltiples fuentes de datos heterogéneas y con obligaciones de trazabilidad que, si bien se cumplen, dificultan la verificación ágil de autenticidad y condiciones de proceso a nivel de pieza. Esta dispersión limita la transparencia

hacia consumidores y distribuidores internacionales y complica auditorías rápidas ante incidencias o sospechas de fraude [8], [19].

El objetivo general del proyecto persigue diseñar y prototipar un *blueprint* de Pasaporte Digital de Producto, DPP por sus siglas en inglés, para el jamón ibérico, alineado con el marco ESPR y estándares GS1, que integre datos *on/off-chain* y ofrezca vistas diferenciadas por rol, empleando IOTA Tangle como capa de inmutabilidad [13], [16], [18], [50], [51].

Los objetivos específicos son:

- Modelar un esquema mínimo del DPP para el jamón ibérico (identificación GS1, eventos EPCIS, metadatos de calidad y certificación) y su control de accesos por rol [13], [16].
- Implementar un prototipo funcional del DPP: ingesta de eventos simulados, anclaje en IOTA Tangle y visor web a través de un código QR basado en roles para vista pública, operativa, auditor; incluyendo la interoperabilidad de otros DPP [51].
- Evaluar beneficios operativos: reducción del TIE, integridad frente a manipulaciones *off-chain* y esfuerzo de adopción para pymes (CapEx/OpEx) [9], [36].
- Delimitar implicaciones regulatorias (ESPR, RGPD, RD 4/2014, DOP/IGP) y compatibilidades con sistemas sectoriales (ÍTACA) [7], [10], [43], [50].

El prototipo cubre todas las categorías comerciales del jamón ibérico según la RD 4/2014; abarca desde la cría y engorde hasta los puntos de clasificación, precintado y expedición, e incorpora circularidad postventa a nivel conceptual. Se emplean datos simulados realistas y se prioriza sensórica de cámaras de curado y eventos documentales clave; quedan fuera despliegues masivos de geolocalización animal y visiones por computador *in situ* (se consideran como líneas futuras). El enfoque es sectorial y extensible a DOP/IGP como capas adicionales.

1.5. Metodología

El trabajo se condujo en cuatro fases iterativas:

Fase I — Marco y requisitos. Revisión normativa (ESPR, RD 4/2014, RGPD), estándares GS1 (EPCIS 2.0, Digital Link) y sistemas sectoriales (ÍTACA). Derivación de requisitos funcionales y no funcionales del DPP y de sus vistas por rol [7], [10], [13], [16], [50].

Fase II — Modelo de datos. Definición del identificador resoluble (GTIN + Lote/Serie), del diccionario de campos mínimos y de los tipos de evento EPCIS para cada etapa (salazón, post-salado, curado, clasificación/precintado, expedición). Diseño de perfiles de acceso y políticas de *data minimization* [13], [15], [16], [52].

Fase III — Prototipo. Desarrollo de *scripts* en Python, anclaje en IOTA Tangle mediante *client* SDK, almacenamiento *off-chain* de detalles y visor QR (vista pública y operativa).

Generación de *datasets* simulados con variabilidad realista (temperatura y humedad relativa en cámaras; pesos y mermas) [51], [53].

Fase IV — Evaluación. Pruebas de integridad (detección de desalineaciones entre eventos y anclajes), estimación del TIE (Tiempo de Investigación de Expedientes), análisis de sensibilidad de costes de adopción y discusión de riesgos y limitaciones [36].

1.6. Limitaciones, Hipótesis de Partida y Estructura de la Memoria

En cuanto a las limitaciones de la memoria, el trabajo se acotó por disponibilidad de datos y alcance técnico. No se dispuso de acceso a bases de datos industriales ni a integraciones en producción con sistemas sectoriales (ÍTACA), por lo que se emplearon *datasets* simulados con rangos y variabilidad coherentes con documentación pública y normativa aplicable [10]. La instrumentación IoT se redujo a supuestos verosímiles de sensórica ambiental en cámaras (temperatura y humedad) y a registros documentales clave (fechas, pesos, precinto), sin desplegar geolocalización masiva de animales ni visión artificial en línea. Los datos de alto volumen y «granularidad fina» se almacenaron *off-chain* y se anclaron mediante resúmenes criptográficos en IOTA Tangle, priorizando integridad y eficiencia [51], [53]. Se definieron campos y pautas compatibles con el Pacto Verde y con el DPP europeo para su progresiva incorporación [49], [50]. La comparación exhaustiva entre distintas DLT no formó parte del alcance, se realizó una comparación de funcionalidades básicas basada en la integración para entornos B2B2C. La verificación de cumplimiento de la RGD se limitó al diseño de capas de acceso y minimización de datos personales.

Como hipótesis de partida, se asumió que el DPP del jamón ibérico debía alinearse con el marco europeo del DPP (ESPR) y con estándares GS1 (EPCIS 2.0 y Digital Link) para garantizar interoperabilidad y escalabilidad [13], [16], [50]. Se consideró que las obligaciones de trazabilidad alimentaria vigentes persistían en sus sistemas de origen (ÍTACA, ERP), y que el DPP actuaría como capa integradora y verificable, sin sustituir los registros establecidos por la norma [7]. Se planteó que la gobernanza de identificadores y resoluciones podría recaer en una entidad interprofesional (ASICI), posibilitando un modelo de servicios comunes y minimizando cambios para pymes. Se adoptó que la sensórica prioritaria para el prototipo correspondía a cámaras de salazón, post-salado y secado/maduración; que el consumidor consultaría el DPP mediante QR (GS1 Digital Link) con vista pública; y que operadores, auditores y autoridades accederían a vistas ampliadas controladas por permisos y credenciales verificables. Se contempló que el reporte REACH sería relevante principalmente para materiales en contacto con alimentos y para ingredientes auxiliares (sal y piensos), más que para el producto cárnico en sí. Se asumió que la circularidad posconsumo tendría tratamiento conceptual y campos ampliables, sin exigir la involucración del consumidor final.

La memoria se estructuró para conducir desde el contexto sectorial y normativo hasta el diseño, la implementación y la evaluación de la propuesta:

- **Capítulo 1. Introducción:** antecedentes, diferencias entre jamón ibérico y serrano, cadena de suministro y de valor, definición del problema, objetivos, metodología, limitaciones e

hipótesis.

- **Capítulo 2. Marco normativo:** ESPR y DPP, trazabilidad alimentaria obligatoria y voluntaria, RGPD, REACH, Norma de Calidad del Ibérico (RD 4/2014), DOP/IGP como capas adicionales, y encaje con sistemas sectoriales (ASICI-ÍTACA).
- **Capítulo 3. Estado del arte:** fundamentos de DLT/IoT y foco en IOTA Tangle como infraestructura de inmutabilidad y direccionamiento de datos.
- **Capítulo 4. Diseño del DPP:** requisitos funcionales y no funcionales, modelo de datos (EPCIS 2.0 y GS1 Digital Link), roles y controles de acceso, y mapeo por etapas del proceso.
- **Capítulo 5. Implementación:** entorno, simulación de datos, anclaje en IOTA, API de ingestión y visor público (MVP); vistas por rol – trabajo futuro.
- **Capítulo 6. Evaluación y análisis:** pruebas de integridad y coherencia, estimación del tiempo de investigación de expedientes, escalabilidad/interoperabilidad, y análisis económico (CapEx/OpEx) con sensibilidad para pymes.
- **Capítulo 7. Conclusiones:** principales hallazgos, aportación y limitaciones.
- **Capítulo 8. Planificación y presupuesto:** Estructura de Desglose de Trabajo, cronograma y costes de adopción.
- **Capítulo 9. Ética:** consideraciones éticas en datos y transparencia.
- **Capítulo 10. ODS:** contribución del DPP a objetivos de sostenibilidad.
- **Capítulo 11. Líneas futuras:** ampliaciones técnicas (integración real con ÍTACA, ACV sectorial, credenciales verificables para roles) y extensión a otros curados.

Este esquema aseguró coherencia con el marco regulatorio europeo y español, facilitó el mapeo entre etapas del proceso y el modelo de datos del DPP, y permitió evaluar la viabilidad técnica y económica de la solución propuesta en un contexto realista del sector ibérico.

Capítulo 2

MARCO NORMATIVO

2.1. Normativa Española y Europea Aplicable

2.1.1. Reglamento (UE) 2024/1781 (ESPR) y Pasaporte Digital de Producto (DPP)

En junio de 2024 la UE adoptó el Reglamento (UE) 2024/1781 sobre ecodiseño de productos sostenibles, conocido por sus siglas en inglés ESPR (*Ecodesign for Sustainable Products Regulation*) [50]. Este reglamento (de aplicación directa en todos los Estados Miembro) establece un nuevo marco legal para impulsar productos más sostenibles en el mercado europeo. A diferencia de la antigua directiva de ecodiseño (centrada solo en productos energéticos), el ESPR abarca prácticamente todos los bienes físicos (electrónica, textiles, muebles, materiales de construcción, baterías, etc.), y tiene como objetivos principales reducir los impactos medioambientales y sociales de los productos, promover la economía circular (mejor reparabilidad, reutilización y reciclaje), minimizar residuos y emisiones, y mejorar la transparencia para consumidores e industrias mediante pasaportes digitales de producto [49], [50].

El elemento clave del ESPR es el Pasaporte Digital de Producto (DPP): según el artículo 9 del reglamento, el DPP será obligatorio para los productos que determine la Comisión y servirá como herramienta para recopilar y compartir información detallada del producto a lo largo de toda su cadena de valor [50, art. 9]. En otras palabras, cada producto deberá ir acompañado de un «perfil digital» accesible mediante un identificador (por ejemplo, un código QR escaneable) que contendrá datos como: composición de materiales (incluyendo contenido reciclado o sustancias peligrosas), huella ambiental (carbono, agua), información sobre reparabilidad y disponibilidad de repuestos, vida útil estimada y opciones de reciclaje al final de su vida, uso de energía o recursos, e incluso certificados o documentos de cumplimiento normativo. El objetivo es que todos los agentes (fabricantes, distribuidores, consumidores, recicladores, autoridades) tengan acceso a información verificada y actualizada del producto, cada uno según su nivel de autorización. Por ejemplo, un consumidor podría escanear el DPP de un jamón ibérico y consultar datos de sostenibilidad (procedencia de la dehesa, huella de carbono, certificaciones de bienestar animal, etc.), mientras que un inspector podría verificar información de trazabilidad o cumplimiento de

estándares [17], [50].

Cabe destacar que la implantación del DPP será progresiva: el ESPR entró en vigor en julio de 2024, pero los requisitos del pasaporte digital se introducirán gradualmente entre 2025 y 2027, mediante actos delegados que concretarán las obligaciones para cada grupo de productos. Los primeros sectores prioritarios (textil, electrónica, baterías, etc.) servirán de piloto, y se espera que con el tiempo se amplíe a más productos en función de su impacto ambiental y volumen de mercado. Aunque actualmente los alimentos no aparecen entre los sectores iniciales, la visión a largo plazo de la UE es cubrir «¡la gama más amplia posible de productos», por lo que no se descarta que en el futuro también productos agroalimentarios de calidad como el jamón ibérico deban incorporar un DPP para informar sobre su sostenibilidad y trazabilidad [30], [50].

Desde el punto de vista del diseño del DPP, el ESPR insiste en un enfoque descentralizado y en la protección de los datos. En sus considerandos, el reglamento señala expresamente que el pasaporte digital de producto debe basarse en «un sistema de datos descentralizado, establecido y gestionado por los operadores económicos», en aras de la flexibilidad, innovación y alineación con las prácticas de mercado. Esto implica que no habrá una única base de datos central controlada por la administración para todos los DPP; más bien cada fabricante u operador mantendrá los datos de sus productos de forma interoperable, mientras que la Comisión creará un registro central únicamente de los identificadores únicos de pasaporte para facilitar la supervisión por las autoridades. En paralelo, el ESPR establece la creación de un portal web público de la UE donde consumidores y partes interesadas puedan consultar y comparar datos de los pasaportes digitales, garantizando así la transparencia.

Todo ello deberá cumplirse respetando la normativa de protección de datos personales: cualquier tratamiento de datos personales en el contexto del DPP debe observar el RGPD (Reglamento (UE) 2016/679), incorporando los principios de protección de datos desde el diseño y por defecto en la arquitectura del sistema [54]. De hecho, el reglamento aclara que no debe almacenarse información personal de clientes en el pasaporte digital del producto. En definitiva, el nuevo marco legal europeo (ESPR) conecta sostenibilidad, trazabilidad digital y economía circular, y proporciona el fundamento normativo para desarrollar un Pasaporte Digital de Producto aplicado incluso a productos tradicionales como el jamón ibérico [50].

2.1.2. REACH y «sustancias preocupantes» en el DPP

El Reglamento REACH establece un marco para el registro, evaluación, autorización y restricción de sustancias químicas en la UE, incluyendo la lista de «sustancias extremadamente preocupantes» (SVHC) [55]. El ESPR prevé que, cuando aplique, el DPP declare la presencia de sustancias preocupantes para facilitar su gestión a lo largo del ciclo de vida [50]. En productos alimentarios como el jamón ibérico, la relevancia de REACH es indirecta y se vincula principalmente a materiales en contacto con alimentos (envases, tintas, adhesivos) más que al jamón en sí. El DPP propuesto contempla campos para declarar la conformidad de estos materiales, alineado con el principio de «seguridad por diseño».

2.1.3. Trazabilidad Alimentaria y la Norma de Calidad del Ibérico (Reg. 178/2002, RD 4/2014, DOP)

En el ámbito alimentario, la trazabilidad es un requisito legal consolidado en la UE desde hace años (Reglamento (CE) 178/2002, art. 18). Cada operador debe poder identificar y registrar el origen y destino de los alimentos («una etapa atrás y una adelante» en la cadena) para permitir retiradas rápidas en caso de alertas sanitarias. En el caso del jamón ibérico, además de esta trazabilidad general de seguridad alimentaria, existe un marco normativo específico de calidad que refuerza el seguimiento del producto desde la crianza del animal hasta la etiqueta final [10].

Este marco normativo es la Norma de Calidad del Ibérico, aprobada por Real Decreto 4/2014, que establece las características de calidad que deben cumplir la carne, jamones, paletas y lomos ibéricos [10]. Esta norma introdujo mejoras importantes en etiquetado y trazabilidad, fijando requisitos más estrictos para el uso del término «ibérico» con el fin de proteger al consumidor y los atributos diferenciadores del producto. En concreto, el Real Decreto 4/2014 clasifica los productos por tipo de alimentación y pureza de raza («100 % ibérico de bellota», «cebo de campo», etc.) con precintos de distinto color en cada pieza, y obliga a un etiquetado detallado indicando la categoría.

Asimismo, impone controles oficiales e independientes (autoridades autonómicas, entidades certificadoras acreditadas por ENAC[Entidad Nacional de Acreditación], y Consejos Reguladores en productos DOP) para verificar el cumplimiento de la norma. Gracias a esta regulación, hoy cada jamón o paleta ibérica lleva un código único en su precinto que permite rastrear su origen y proceso de producción. Por ejemplo, el código enlaza con datos como la explotación ganadera de nacimiento, la alimentación recibida (bellota y pastos o pienso), fecha de sacrificio, registro del secadero y bodega donde se curó, y fecha de finalización de curación, entre otros [10], [11].

Esta trazabilidad completa «de la granja a la mesa» queda registrada en un sistema informático centralizado del sector (Sistema ITACA), proporcionando garantías de autenticidad al consumidor [7]. Adicionalmente, existen cuatro Denominaciones de Origen Protegidas (DOP) de jamón ibérico (DOP Jabugo, DOP Dehesa de Extremadura, DOP Los Pedroches y DOP Guijuelo), cada una con su propio pliego de condiciones geográficas y de calidad adicionales a la Norma de Calidad [1]-[3]. Las DOP, reguladas por el Reglamento (UE) 1151/2012, vinculan el producto a su territorio y método tradicional de elaboración, aportando un nivel extra de trazabilidad y prestigio. Solo los jamones criados, elaborados y curados en la zona geográfica delimitada pueden llevar el sello DOP, y cada Consejo Regulador de DOP gestiona y verifica la trazabilidad e identidad de las piezas amparadas.

Con todo ello, un Pasaporte Digital para el jamón ibérico deberá conciliar ambos planos: cumplir con las normas obligatorias actuales (trazabilidad 178/2002, etiquetado 1169/2011, calidad del ibérico RD 4/2014) al tiempo que incorpora información ampliada de forma voluntaria (huella ambiental, historia de alimentación del animal, etc.), anticipándose a futuras exigencias regulatorias en materia de sostenibilidad [10], [50], [56].

2.1.4. Pacto Verde Europeo y Estrategias Conexas

En línea con las estrategias europeas («de la Granja a la Mesa», biodiversidad, clima, etc.), el modelo extensivo del ibérico en la dehesa presenta ventajas sostenibles: promueve el bienestar animal (cría al aire libre con alimentación natural) y contribuye al desarrollo rural. El sector ibérico actúa como motor socioeconómico en zonas rurales, fijando población y generando empleo local, en concordancia con los Objetivos de Desarrollo Sostenible de la ONU. Todas estas iniciativas sitúan al ibérico en sintonía con las políticas del *European Green Deal*, que busca una Europa climáticamente neutra, circular y justa. La propia Comisión Europea, en el Pacto Verde Europeo de 2019, recalcó la necesidad de transformar la economía hacia la neutralidad climática al 2050 y destacó que los productos sostenibles (incluidos los agroalimentarios) desempeñan un papel esencial en esa transición [46].

El Pacto Verde impulsa transparencia, eficiencia de recursos y digitalización del ciclo de vida de productos. La estrategia «de la Granja a la Mesa» promueve sistemas alimentarios más sostenibles y trazables; la PAC (Política Agraria Común) 2023–2027 incentiva prácticas ambientales y bienestar animal [46], [57]. El DPP propuesto se alinea con estos vectores al ofrecer datos verificables sobre procesos (curado, mermas, condiciones ambientales) y certificaciones (bienestar animal), facilitando comunicación responsable hacia mercados internacionales [34], [46].

2.1.5. RGPD y Protección de Datos desde el Diseño

Por otro lado, al diseñar un sistema digital como el DPP, es imprescindible considerar la legislación de protección de datos personales. El Pasaporte Digital de un alimento como el jamón ibérico podría incluir datos referentes a productores (nombre o ubicación de una finca, que a veces puede ser una persona física) u otros datos sensibles a nivel comercial.

El Reglamento General de Protección de Datos (RGPD, UE 2016/679) exige que cualquier tratamiento de datos personales respete principios como minimización (solo recoger los datos necesarios), limitación de la finalidad y seguridad y confidencialidad (art. 5.1 RGPD) [54, art. 5.1]. Además, el RGPD consagra en su artículo 25 la «protección de datos desde el diseño y por defecto», lo que significa que desde la concepción misma del DPP deben integrarse medidas técnicas y organizativas que garanticen la privacidad (control de accesos, seudonimización, plazos de retención limitados, etc.) [54, art. 25]. El Reglamento EPR refuerza explícitamente este punto, indicando que el diseño técnico y funcionamiento de los pasaportes digitales de producto deben trasladar los datos de forma segura y respetando las normas de privacidad, prestando especial atención a «los principios de protección de datos desde el diseño y por defecto» [50].

De hecho, se prohíbe almacenar datos personales de los clientes en el pasaporte digital del producto, ya que la finalidad del DPP es la información del producto, no del comprador. Por tanto, en la implementación del DPP para el jamón ibérico se deberá asegurar que cualquier dato personal (por ejemplo, información de contacto de un ganadero si es persona física, usuarios que consulten el pasaporte, o veterinarios oficiales) esté adecuadamente protegido bajo el RGPD: posiblemente recurriendo a anonimización o seudonimización de datos de operadores, obteniendo consentimientos cuando proceda, y garantizando derechos de acceso y rectificación [50, art.

13][54, art. 40].

En resumen, el marco normativo que rodea al DPP abarca no solo las regulaciones sectoriales de trazabilidad y calidad alimentaria (que proveerán muchos datos al pasaporte), sino también la normativa horizontal de privacidad, que impondrá requisitos de diseño *privacy-by-design* en nuestra solución tecnológica [50].

2.1.6. Sistemas Sectoriales Existentes (ASICI-ÍTACA) y Complementariedad con el DPP

La Norma de Calidad del Ibérico, establecida por el Real Decreto 4/2014, introdujo el uso obligatorio de precintos inviolables de distinto color (negro, rojo, verde o blanco) para identificar cada jamón y paleta según su categoría comercial [10], [11]. Estos precintos llevan un código único correlacionado con la canal de origen y son asignados bajo la supervisión de la Asociación Interprofesional del Cerdo Ibérico (ASICI), a la cual el Real Decreto encomienda funciones de control sobre su correcta colocación y registro [10]. Para garantizar el cumplimiento de estas obligaciones de trazabilidad y calidad, en 2015 se puso en marcha el sistema informático ÍTACA mediante una extensión de norma aprobada por el Ministerio de Agricultura (Orden AAA/1549/2014) [10].

ÍTACA constituye la plataforma sectorial integral de identificación, trazabilidad y calidad del Ibérico, que recopila de forma unificada la información de todos los operadores (ganaderos, mataderos, industrias) involucrados en la cadena productiva. A través de este sistema, por ejemplo, los ganaderos gestionan la identificación individual de los animales mediante crotales; los mataderos registran el pesaje de las canales e identifican con precintos oficiales los jamones y paletas aptos de cada lote (según exige el artículo 9 del RD 4/2014) [10, artc. 9]; y las industrias anotan el movimiento, transformación y reposición de precintos de las piezas durante su curación y distribución. De este modo se logra una trazabilidad completa «de la granja a la mesa», quedando todos los datos respaldados en la base de datos común de ÍTACA. Desde su implantación, el sistema se ha consolidado como fuente de información en tiempo real para el sector; entre 2015 y 2020 acumuló más de 19 millones de páginas consultadas y 234.000 usuarios registrados, reflejando su adopción generalizada y la transparencia que brinda al consumidor [7], [27].

La propuesta de Pasaporte Digital de Producto (DPP) se plantea como complementaria a ÍTACA, aprovechando la infraestructura existente sin duplicarla. En concreto, reutiliza los identificadores únicos ya asignados en ÍTACA a animales y productos, y agrega eventos de trazabilidad adicionales siguiendo el estándar EPCIS para enriquecer la historia del producto. Además, proporciona un mecanismo de verificación pública *tamper-evident* mediante anclajes criptográficos periódicos de esos datos en la red distribuida IOTA, añadiendo así una capa de transparencia y confianza accesible a cualquier interesado. Un modelo plausible de despliegue sería una gobernanza liderada por la entidad interprofesional (ASICI), que ofrezca servicios comunes de generación y resolución de identificadores digitales, habilitando a los operadores industriales a integrar el DPP en sus sistemas con cambios mínimos. Esto aseguraría que el DPP refuerza la trazabilidad y confianza en el sector ibérico de forma alineada con la normativa vigente, actuando como un complemento que potencia la utilidad de ÍTACA en lugar de reemplazarlo [7],

[15], [51].

Capítulo 3

ESTADO DEL ARTE

La trazabilidad de productos ha experimentado una profunda transformación digital en la última década. Tradicionalmente dependiente de sistemas centralizados y documentación física, este ámbito encuentra ahora en la convergencia entre el Internet de las Cosas (IoT, *Internet of Things*) y las tecnologías de registro distribuido (DLT, *Distributed Ledger Technology*) un horizonte de posibilidades antes inimaginable [58], [59]. Esta convergencia no surge por casualidad, sino de una necesidad creciente de transparencia, verificabilidad y confianza en las cadenas de suministro globales. El IoT aporta la capacidad de capturar datos del mundo físico de manera automatizada y continua, mientras que las DLT proporcionan la infraestructura necesaria para garantizar la integridad, inmutabilidad y transparencia de esos datos a lo largo de toda la cadena de valor.

En el contexto específico de los pasaportes digitales de producto (DPP), esta sinergia resulta especialmente apropiada. Por un lado, sensores IoT pueden monitorizar condiciones ambientales críticas durante procesos como el curado del jamón ibérico (temperatura, humedad, tiempo), mientras que por otro lado, la DLT asegura que estos registros no puedan ser alterados retroactivamente, proporcionando una garantía criptográfica de autenticidad que trasciende la confianza en intermediarios centralizados [59], [60]. En otras palabras, cada dato capturado sobre el producto queda anclado de forma inmutable, de modo que cualquier actor (ya sea un inspector, un distribuidor o un consumidor final) puede confiar en que la información reflejada corresponde fielmente a la realidad histórica del producto.

En este capítulo se aborda una comprensión integral del contexto reglamentario, técnico y sectorial necesario para fundamentar los requisitos y criterios de diseño del Pasaporte Digital del Jamón Ibérico. Se establecen así los cimientos conceptuales sobre los cuales construir una solución que sea técnicamente sólida, normativamente alineada y sectorialmente viable. Para ello, se examinan las tecnologías IoT aplicables a la captura de datos en entornos agroalimentarios, las arquitecturas propuestas para los pasaportes digitales de producto, las directrices del marco regulatorio europeo (ESPR) que condicionan su implementación, el papel de las DLT (con especial énfasis en IOTA Tangle) como infraestructura subyacente de confianza, los estándares de identificación y datos (GS1, EPCIS, Digital Link) que garantizan interoperabilidad, la integración con sistemas sectoriales existentes (ASICI-ÍTACA en el caso ibérico), casos de uso implementados en otros sectores que sirven de referencia, una comparación motivada de posibles plataformas DLT, y finalmente las consideraciones de seguridad y los requisitos derivados para el diseño de

la solución.

3.1. Internet de las Cosas (IoT)

El Internet de las Cosas (IoT) representa un paradigma tecnológico en el que objetos físicos cotidianos se conectan a internet, adquiriendo la capacidad de recopilar, intercambiar y actuar sobre datos sin intervención humana directa [61]. Esta definición, aunque simple en apariencia, encierra una complejidad técnica considerable que abarca desde sensores miniaturizados capaces de medir múltiples parámetros, hasta protocolos de comunicación especializados para entornos con recursos limitados. La esencia del IoT es permitir que el mundo físico sea leído y procesado por sistemas digitales en tiempo real. La arquitectura clásica del IoT suele estructurarse en tres capas fundamentales [61]:

1. Capa de percepción: incluye sensores, actuadores y dispositivos de recolección de datos que interactúan directamente con el entorno físico, capturando variables como temperatura, humedad, movimiento, posición, etc.
2. Capa de red: comprende los protocolos de comunicación, *gateways* e infraestructuras de transmisión que conectan los dispositivos con sistemas remotos. Esta capa asegura que los datos capturados por los sensores viajen desde el entorno local hasta los servidores o la nube donde serán procesados.
3. Capa de aplicación: engloba las plataformas de procesamiento, almacenamiento, análisis y presentación de datos que transforman la información bruta en conocimiento útil para la toma de decisiones. Incluye bases de datos, algoritmos de analítica (incluso IA) y las interfaces (por ejemplo, aplicaciones web o móviles) mediante las cuales los usuarios interactúan con el sistema.

En el contexto agroalimentario, los dispositivos IoT típicos incluyen sensores de temperatura y humedad para monitorización ambiental en secaderos, sensores de pH y conductividad para control de calidad en procesos de curado o salazón, sistemas GPS para seguimiento logístico de envíos o incluso del movimiento de animales en extensivo, y sensores de proximidad o cámaras para control de acceso a instalaciones. Estos dispositivos deben operar frecuentemente en condiciones adversas (alta humedad, temperaturas extremas, exposición al polvo o interferencias electromagnéticas) y con restricciones severas de energía (a menudo funcionan con baterías durante largos periodos) y conectividad (ubicaciones remotas con cobertura limitada) [61].

Las tecnologías de comunicación IoT presentan características distintivas en comparación con redes convencionales, adaptándose a los requisitos de largo alcance, bajo consumo y tolerancia a pérdidas de datos:

- LoRaWAN (*Long Range Wide Area Network*). Destaca por su capacidad de transmitir datos a distancias de varios kilómetros con un consumo energético extremadamente bajo, a costa de un ancho de banda reducido. Esto la hace ideal para aplicaciones rurales, como

el seguimiento de animales en las dehesas o la monitorización de sensores en fincas de gran extensión, donde no hay cobertura WiFi o celular cercana [61] [62]. Gracias a su modulación *chirp-spread spectrum*, LoRaWAN puede penetrar vegetación y edificios, permitiendo que un gateway cubra amplias zonas con pocos repetidores.

- NB-IoT (*Narrowband Internet of Things*). Utiliza la infraestructura de redes celulares existentes (es una tecnología LPWAN dentro del estándar 4G/5G) para proporcionar cobertura casi ubicua con excelente penetración en interiores. Está optimizada para enviar pequeñas cantidades de datos con muy baja frecuencia y bajo coste, por lo que es adecuada para dispositivos IoT en ubicaciones fijas (por ejemplo, un sensor en un almacén o dentro de un camión refrigerado) que deban transmitir lecturas periódicamente, incluso desde sótanos o zonas de baja señal [61].
- Zigbee y Bluetooth Low Energy (BLE). Ofrecen comunicaciones de corto alcance, típicamente decenas de metros, con protocolos especialmente optimizados para dispositivos alimentados por baterías. Son habituales en redes de sensores dentro de una instalación o en comunicación de campo cercano (por ejemplo, etiquetas BLE para seguimiento de activos dentro de una fábrica o sensores Zigbee en un almacén que reportan a un *gateway* central). Aunque su alcance es limitado, su bajo consumo y la capacidad de formar redes malladas (en el caso de Zigbee) permiten cubrir espacios locales de forma eficiente [61].

Una tendencia importante en IoT es el procesamiento en el borde (*edge computing*). En lugar de transmitir todos los datos brutos a la nube, dispositivos o *gateways* de *edge* realizan análisis local, filtrado y agregación de datos. Esto reduce significativamente el ancho de banda requerido, disminuye la latencia y alivia la carga de los servidores centrales. Por ejemplo, para un DPP de jamón ibérico, un *gateway* local en el secadero podría procesar miles de mediciones de temperatura y humedad diarias, detectando desviaciones fuera de rangos óptimos. Sólo enviaría a la nube (y potencialmente anclaría en la DLT) eventos críticos como una alerta de temperatura excesiva prolongada, o resúmenes estadísticos diarios, en lugar de cada medición individual. De esta manera se garantiza una respuesta rápida a condiciones anómalas (pues el *gateway* puede disparar alarmas localmente, como encender ventilación) y se optimiza el uso de la red [61].

Los protocolos de datos IoT están específicamente diseñados para manejar las restricciones de estos entornos. Por ejemplo, MQTT (*Message Queuing Telemetry Transport*) sigue un modelo publicador-suscriptor que minimiza el *overhead* de comunicación y permite intercambios asíncronos tolerantes a desconexiones intermitentes [61]. Un sensor en un secadero puede publicar sus lecturas en un tema (*topic*) MQTT, y múltiples suscriptores (como la base de datos local, una aplicación de monitoreo o el módulo de pasaporte digital) recibirán la información cuando estén conectados, sin que el sensor deba conocerlos directamente. Por su parte, CoAP (*Constrained Application Protocol*) proporciona funcionalidad similar a HTTP (métodos GET, POST) pero con un formato compacto basado en UDP, optimizado para dispositivos con recursos limitados. Es útil para escenarios donde se requiera petición-respuesta directa a dispositivos (solicitar el estado de un sensor bajo demanda) dentro de redes locales de sensores. Por otro lado, estándares de datos de más alto nivel como EPCIS (*Electronic Product Code Information Services*) de GS1 definen estructuras de datos estándar para eventos de trazabilidad, facilitando la interoperabilidad entre diferentes sistemas IoT y de gestión de la cadena de suministro. A modo de ejemplo, un evento EPCIS podría representar que «el lote X de jamones entró en la cámara de curado Y el día Z», encapsulando qué ocurrió, cuándo, dónde y por qué. Utilizar EPCIS 2.0 desde la captura de

datos significa que la información generada por los sensores y sistemas locales puede integrarse fácilmente en plataformas globales de trazabilidad y en el pasaporte digital, hablando todos los actores el mismo lenguaje de datos [63].

En suma, la infraestructura IoT proporciona los *ojos* y *oídos* digitales que capturan la historia de cada producto en tiempo real. Estas capacidades sientan la base para un pasaporte digital rico en información, pero para que dichos datos se conviertan en confianza y valor añadido, es necesario estructurarlos adecuadamente y asegurarlos contra manipulación, objetivos que se logran combinando el IoT con arquitecturas de pasaporte digital y tecnologías DLT, como se explora a continuación.

3.2. Pasaporte Digital de Producto: Arquitectura y Especificaciones

El Pasaporte Digital de Producto (DPP) trasciende la simple noción de un «carné» de identidad digital estático. Se trata de un sistema de información complejo y distribuido que actúa como repositorio dinámico de datos críticos sobre un producto específico a lo largo de todo su ciclo de vida [58], [59]. En lugar de limitarse a almacenar información fija (como podría ser una etiqueta electrónica con unos pocos datos), el DPP evoluciona con el producto, incorporando todos los eventos relevantes desde su creación hasta su disposición final. Así, un DPP es tanto una base de datos histórica como una herramienta activa de trazabilidad y gestión.

Desde una perspectiva técnica, un DPP efectivo debe abordar múltiples capas de complejidad, cada una encargada de un aspecto clave del sistema:

- **Capa de datos:** define la estructura, formato y semántica de la información contenida en el pasaporte. Esto incluye qué tipo de datos se almacenan (composición del producto, huella ambiental, fechas y lugares de procesamiento, resultados de inspecciones de calidad, etc.), cómo se organizan (modelos relacionales, documentos JSON-LD, ontologías) y qué significado tienen (ontología común para denominar atributos como «fecha de producción» o «lote de materia prima»). Es crucial que esta capa esté bien diseñada para asegurar interoperabilidad [58].
- **Capa de identificación:** establece los sistemas de identificadores únicos y persistentes para los productos y sus componentes. Un DPP necesita asociarse inequívocamente a un objeto físico; para ello se utilizan identificadores como códigos QR, RFID, o URL únicas. Estos deben ser globalmente únicos (un mismo código no puede referir a dos productos distintos) y persistentes en el tiempo (aunque cambie el propietario o la localización del producto, el identificador sigue siendo el mismo). En el caso del jamón ibérico, esto implica enlazar el pasaporte digital con identificadores como el precinto físico del jamón o códigos GS1 (GTIN + número de serie) que identifiquen cada pieza [63].
- **Capa de acceso:** contempla los mecanismos de autenticación (verificación de identidad de quien accede) y autorización por roles (determinación de qué información puede ver o editar cada tipo de usuario). Dado que el DPP contendrá información sensible de distintos

niveles, es necesario un control de acceso granular (un consumidor final puede estar autorizado a ver ciertos datos públicos, un distribuidor puede ver información logística adicional, un productor los detalles técnicos, y una autoridad datos completos) [59].

- **Capa de verificación:** se refiere a las garantías criptográficas de integridad y autenticidad de los datos. Incluye los métodos para asegurar que la información no ha sido manipulada (e.g., firmas digitales de los datos por parte de quien los generó, o *hashes* anclados en una *blockchain* que evidencien cualquier alteración). También abarca cómo se validan las interrelaciones de datos (por ejemplo, que un certificado de calidad referido en el DPP sea auténtico y esté vigente) sin confiar ciegamente en una entidad central [58].

La arquitectura conceptual de un DPP moderno se fundamenta en la separación entre los datos del producto propiamente dichos y los «metadatos» de control que gobiernan su acceso y validación. Los primeros incluyen información sobre composición, sostenibilidad, trazabilidad y cumplimiento normativo, es decir, todos los datos de hecho sobre el producto. Los segundos comprenden estructuras como esquemas de permisos (quién puede ver qué), historial de modificaciones (registro inmutable de quién añadió o cambió datos y cuándo) y certificados o huellas digitales que permiten verificar la autenticidad de las informaciones (como la firma digital de un veterinario certificando el origen del cerdo). Esta separación modular aporta flexibilidad: se pueden actualizar o corregir ciertos datos del producto sin alterar la capa de control, y viceversa, actualizar permisos o revocar certificados sin tocar los datos base [60].

En el contexto agroalimentario, y concretamente para productos de producción lenta y artesanal como el jamón ibérico, el DPP debe capturar la complejidad inherente de un proceso que se extiende durante años y abarca múltiples ubicaciones geográficas. Un jamón ibérico pasa por numerosas etapas: la cría del cerdo, el sacrificio en matadero, el despiece, el salado, el etiquetado y certificación, la distribución, etc. Cada etapa genera datos únicos que deben ser correlacionados y preservados. Un buen DPP de jamón ibérico integrará todos esos datos dispersos en un único hilo narrativo digital. Así, un consumidor que escanee el código QR de un jamón ibérico en una tienda debería poder acceder a información verificable [64].

El diseño general de las soluciones DPP según los estándares y recomendaciones europeas sigue ciertos patrones arquitectónicos específicos.

En primer lugar, los datos se estructuran siguiendo ontologías reconocidas (Schema.org o GS1 *Web Vocabulary*), lo que permite interoperabilidad semántica entre sistemas heterogéneos. Esto significa que si distintos sectores o países implementan pasaportes digitales, todos describan conceptos comunes (peso, fecha de producción, fabricante, huella de carbono, etc.) de forma consistente, facilitando intercambios y comparaciones [58].

En segundo lugar, los identificadores de productos en el DPP suelen seguir estándares como GS1 Digital Link, que permiten la resolución web de códigos (un mismo código QR puede ser interpretado por cualquier aplicación para obtener la URL del pasaporte digital en internet, evitando códigos propietarios) [65].

Finalmente, la verificabilidad de la información en un DPP se logra mediante anclaje criptográfico en una DLT: en lugar de almacenar todos los datos sensibles en una *blockchain* (lo cual podría ser inviable por volumen y privacidad), se calculan *hashes* de los datos críticos y se

almacenan de manera inmutable en el ledger distribuido [66].

Con todo ello, cualquier tercero puede posteriormente tomar los datos del pasaporte, recalcular su *hash* y comparar con el registrado en la DLT, detectando cualquier discrepancia (lo que indicaría manipulación). Esta técnica asegura integridad sin comprometer la confidencialidad de los datos originales, ya que el *hash* no revela el contenido específico [66].

En resumen, el Pasaporte Digital de Producto es una pieza clave para dotar de transparencia y confianza a cadenas de valor complejas e integra capas de tecnología y gobierno de datos para acompañar al producto durante toda su vida útil. Una vez sentadas estas bases técnicas, es fundamental considerar el marco normativo en el que se basa la creación de los DPP bajo ciertas directrices técnicas.

3.3. Directrices Técnicas del ESPR para el DPP

El Reglamento (UE) 2024/1781 de Ecodiseño para Productos Sostenibles, que ya introdujimos en el Capítulo 2, establece no solo la obligatoriedad de implantar Pasaportes Digitales de Producto para ciertos bienes, sino también directrices técnicas específicas que condicionan su arquitectura e implementación [58], [59]. Este marco legal representa un cambio de paradigma en cómo se gestiona la información de producto en la Unión Europea, integrando objetivos de sostenibilidad, economía circular y transformación digital.

El ESPR define criterios técnicos concretos para los DPP que van más allá de simples declaraciones de intenciones genéricas. Por ejemplo, el artículo 9 del reglamento establece que los pasaportes digitales deben garantizar la interoperabilidad técnica mediante el uso de formatos de datos abiertos y estándares reconocidos internacionalmente [67, art. 9]. Esta exigencia tiene implicaciones directas en la elección de tecnologías y formatos por parte de los desarrolladores de DPP: sistemas propietarios o formatos cerrados quedan prácticamente descartados, favoreciéndose soluciones basadas en estándares abiertos como JSON-LD (para representación de datos enriquecidos y vinculados), XML Schema (en contextos donde aplique) o los formatos definidos por GS1 para datos de producto y trazabilidad. De este modo se busca que un DPP implementado en un Estado miembro pueda ser leído y verificado en cualquier otro sin trabas, y que las empresas no se vean obligadas a costosas conversiones o integraciones personalizadas por falta de armonización [58].

Además, la arquitectura descentralizada mandatada por el ESPR presenta desafíos técnicos significativos. El reglamento especifica que no debe existir una base de datos central única controlada por la administración para almacenar todos los DPP, sino que cada operador económico (fabricantes, importadores, distribuidores) mantendrá los datos de sus productos de forma interoperable y verificable [67], [58]. En otras palabras, el sistema europeo será federado: los datos permanecen donde se generan (en las bases de datos de las empresas), pero accesibles mediante estándares comunes cuando alguien consulta un pasaporte. Para lograr esto, se requiere el desarrollo de protocolos de comunicación estándar entre sistemas heterogéneos (como unas API web uniformes que respondan a las solicitudes de datos de DPP), mecanismos de descubrimiento de datos distribuidos (saber dónde consultar el DPP de un producto en particular a partir de su identificador) y esquemas de validación cruzada que permitan a las autoridades verificar la

coherencia y veracidad de la información sin necesidad de acceso directo a las bases de datos privadas de cada operador. En la práctica, la Comisión prevé mantener solo un registro central de los identificadores únicos de pasaporte (una especie de índice o catálogo de pasaportes emitidos), para facilitar la supervisión, manteniéndose los datos descentralizados [67].

El marco también establece categorías específicas de información que deben incluirse en el DPP, organizadas según criterios de accesibilidad y confidencialidad [67]:

- **Categoría A:** información pública para consumidores. Incluye datos básicos de identificación del producto (modelo, fabricante, referencias básicas), indicadores de sostenibilidad (huella de carbono, porcentaje de material reciclado), certificaciones ecológicas u otras acreditaciones de calidad, instrucciones de uso y mantenimiento, y orientaciones sobre reciclaje o disposición final. Esta información debe ser accesible sin restricciones mediante interfaces públicas y fáciles de usar, típicamente disponible con solo escanear el código QR del producto desde un smartphone, de modo que cualquier consumidor pueda consultarla al instante.
- **Categoría B:** información restringida para profesionales. Comprende datos técnicos más detallados que resultan de interés para actores de la cadena de suministro o personal técnico cualificado. Por ejemplo: especificaciones de materiales (composición exacta, aleaciones, etc.), historial de mantenimiento o reparación (en caso de productos duraderos), y documentación de cumplimiento normativo técnico (como resultados de tests de seguridad, compatibilidad electromagnética, etc.). El acceso a esta categoría requiere autenticación y autorización específica, pues puede incluir información que un consumidor común no necesita o no sabría interpretar, pero que es valiosa para un reparador, un reciclador, un auditor o un comprador industrial.
- **Categoría C:** información confidencial para autoridades. Abarca datos de trazabilidad completa (la lista completa de proveedores involucrados, información sanitaria o de control), información sobre componentes sujetos a regulación estricta (sustancias químicas preocupantes), y documentación regulatoria sensible. Solo es accesible para autoridades competentes (organismos de inspección, aduanas, agencias medioambientales) mediante protocolos de alta seguridad. En esta categoría podría entrar, en el caso de un jamón ibérico, los DPP de cada lote de pienso administrado, o los resultados individualizados de inspecciones veterinarias, que una autoridad podría solicitar auditar.
- **Categoría D:** información comercial sensible. Incluye secretos comerciales, fórmulas específicas, datos de costos de producción, listados detallados de clientes o cualquier dato que, de hacerse público, podría comprometer la ventaja competitiva de la empresa. El reglamento indica que esta información «no debe ser accesible ni siquiera para otras empresas o autoridades de manera abierta»; sin embargo, si es relevante para fines del pasaporte (demostrar que cierta proporción de material proviene de una fuente certificada sin revelar el proveedor exacto), debe preservarse mediante técnicas criptográficas avanzadas que permitan verificación sin revelación. Esto sugiere el uso de «pruebas de conocimiento cero» (*zero-knowledge proofs*) u otras formas de evidencia matemática donde se pueda verificar una afirmación (e.g., «el 50 % del alimento del cerdo fue bellota certificada») sin exponer los datos subyacentes (qué fincas proveían esas bellotas, cantidades exactas, etc.).

Los mecanismos de verificación y cumplimiento contemplados por el ESPR requieren la implementación de sistemas de auditoría distribuidos e innovadores. Las autoridades deben poder verificar la veracidad de la información declarada en los DPP sin necesidad de tener acceso directo a los sistemas internos de las empresas. Esto favorece arquitecturas basadas en pruebas criptográficas, como las mencionadas «pruebas de conocimiento cero» o «estructuras de Merkle» (*Merkle proofs*), que permiten demostrar propiedades específicas de los datos sin revelar los datos mismos. Por ejemplo, se podría demostrar a un inspector que «todos los componentes plásticos de este producto están libres de sustancias prohibidas» aportando un *hash* o prueba calculada sobre la lista de materiales, en lugar de entregarle la lista completa con las formulaciones, preservando así los secretos comerciales pero cumpliendo con la inspección [58].

3.4. Tecnologías de Registro Distribuido (DLT)

Las Tecnologías de Registro Distribuido (DLT) se han erigido como la columna vertebral tecnológica para sistemas de trazabilidad avanzados, proporcionando garantías de inmutabilidad, descentralización y transparencia que los sistemas tradicionales centralizados difícilmente pueden igualar [64]. En esencia, una DLT es una base de datos compartida entre múltiples participantes que se sincronizan para acordar un historial común de transacciones o eventos, sin confiar en una entidad única que la controle. Esto resulta especialmente útil en cadenas de suministro con múltiples actores, donde ningún participante debería poder alterar unívocamente los registros de trazabilidad en su favor.

Para comprender su aplicabilidad a los DPP, es fundamental examinar los mecanismos técnicos que las sustentan. Entre ellos destacan las funciones *hash*, la estructura de la *blockchain* con su propiedad de inmutabilidad, y los mecanismos de consenso que permiten a los nodos distribuidos acordar el estado del *ledger* (registro). Asimismo, es necesario reconocer las limitaciones actuales (como problemas de escalabilidad o coste) y las alternativas emergentes que intentan superarlas.

3.4.1. La Función *Hash* y la *Blockchain*

Una función *hash* constituye el elemento criptográfico básico de las DLT [68]. Es una función matemática que convierte datos de entrada de cualquier tamaño en una cadena (secuencia) de caracteres de longitud fija, normalmente representada en formato hexadecimal, llamada *hash* o *digest*. Por ejemplo, SHA-256, utilizada tanto en Bitcoin como en IOTA, produce *hashes* de 256 bits (64 caracteres hexadecimales) independientemente del tamaño de la entrada. Las funciones *hash* criptográficas presentan varias propiedades críticas:

1. Son deterministas: la misma entrada produce siempre el mismo resultado *hash*.
2. Presentan efecto «avalancha»: un cambio mínimo en la entrada (como modificar una letra en un documento) produce un cambio drástico y aparentemente aleatorio en el *hash* resultante.

3. Resistencia a preimagen (unidireccionalidad): dado un valor *hash* h , es computacionalmente inviable encontrar un mensaje m tal que $H(m) = h$, siendo $H(m)$ la función *hash* de m [69], [70].
4. Resistencia a segunda preimagen: dado un mensaje concreto m_1 (y su *hash* público), es computacionalmente inviable encontrar otro mensaje $m_2 \neq m_1$ con $H(m_2) = H(m_1)$ [71], [72].
5. Resistencia a colisiones: es computacionalmente inviable encontrar cualquier par de mensajes distintos (m_1, m_2) con la misma huella $H(m_1) = H(m_2)$. Por el *límite del cumpleaños*, para salidas de L bits la complejidad esperada de búsqueda de colisiones escala como $2^{L/2}$, mientras que la preimagen y la segunda preimagen escalan como 2^L [71], [73].

Gracias a estas propiedades, un *hash* funciona como una «huella digital» de los datos: es único con altísima probabilidad, y cualquier alteración de los datos lo cambia por completo, permitiendo detectar la alteración.

Conviene recordar, además, que las funciones *hash* evolucionan con el tiempo: algunas quedan obsoletas por debilidades prácticas o por la aparición de colisiones publicadas, y otras (más modernas) pasan a recomendarse en su lugar. En el ecosistema de IOTA, las bibliotecas actuales y los *toolkits* de *smart contracts* exponen varias primitivas de 256 bits hoy consolidadas (*SHA2-256*, *SHA3-256*, *Keccak-256* y *Blake2b-256*), que cubren la mayor parte de necesidades de firma, direccionado y notarización [74], [75].

La insistencia en primitivas estandarizadas no es casual: el uso de funciones *hash* no revisadas por la comunidad ha demostrado ser arriesgado; el caso de Curl-P en los orígenes de IOTA, donde se demostraron colisiones prácticas, es ilustrativo y motivó la migración a primitivas estándar [76], [77].

La inmutabilidad en *blockchain* se logra mediante el encadenamiento lineal de bloques por *hashes*. Cada nuevo bloque referencia el *hash* del anterior en su cabecera, creando una única secuencia temporal. Si se alteran datos en un bloque histórico, cambia su *hash* y, por «cascada», dejan de coincidir los *hashes* de todos los bloques posteriores, que resultan inválidos salvo que se rehaga la cadena desde ese punto y, además, se supere el consenso de la red [68], [78], [79]. Esta propiedad es la que permite afirmar que, en *blockchain*, la inmutabilidad práctica crece con la profundidad del registro en la cadena.

Ahora bien, no todas las DLT implementan una cadena lineal de bloques. En arquitecturas basadas en Grafos Acíclicos Dirigidos (DAG), como IOTA Tangle, no existen «bloques» ni una única cadena temporal; cada nueva transacción aprueba (mediante *Proof-of-Work* ligero) dos transacciones anteriores y se añade como un vértice más del grafo. En este contexto, la irreversibilidad no depende de un «bloque global de cierre», sino de la confirmación acumulativa: cuantas más transacciones posteriores aprueban directa o indirectamente una operación, mayor es su peso acumulado y más improbable resulta revertirla [68], [80]-[82], [83]. Los nodos, que operan de forma local y asíncrona, seleccionan *tips* mediante recorridos tipo *random walk* ponderados; los caminos alternativos con menor peso quedan estadísticamente desfavorecidos y tienden a no propagarse. En la práctica, esto hace la alteración de transacciones antiguas

estadísticamente inviable, sin que exista, como en *blockchain*, una imposibilidad matemática garantizada por una cadena lineal de *hashes*.

3.4.2. Mecanismos de Consenso

Los mecanismos de consenso resuelven el problema fundamental de las DLT: cómo lograr que múltiples nodos distribuidos (que pueden no confiar unos en otros e incluso ser maliciosos) lleguen a un acuerdo sobre el estado válido del sistema sin depender de una autoridad central. Existen numerosos algoritmos de consenso, pero los dos principales y más utilizados en la industria son:

1. *Proof of Work* (PoW). El PoW requiere que los nodos (llamados comúnmente «mineros») resuelvan problemas criptográficos computacionalmente intensivos para poder añadir nuevos bloques al ledger. En concreto, en redes como Bitcoin, estos mineros compiten para encontrar un valor (*nonce*) que, al combinarse con los datos del bloque, produzca un *hash* que cumpla ciertos criterios (típicamente, que el *hash* resultante empiece por un número específico de ceros en notación hexadecimal). Encontrar tal *nonce* es un proceso de prueba y error intensivo en CPU/GPU, de ahí el término «prueba de trabajo» (*Proof of Work*). El primer minero que resuelve el problema presenta su bloque a la red, y los demás nodos lo validan rápidamente (verificando que el *hash* cumple la dificultad establecida y que las transacciones son válidas). Este proceso de minería consume energía deliberadamente como mecanismo de seguridad: para atacar la red y reescribir la historia, un actor malicioso necesitaría controlar más del 50 % de la potencia computacional global (tasa de *hash*), lo que se vuelve astronómicamente caro en términos energéticos y de hardware [68], [78]. El algoritmo PoW, por tanto, hace que los ataques sean teóricamente posibles pero prácticamente inviables, a costa de un alto consumo energético en el funcionamiento normal de la red.
2. *Proof of Stake* (PoS). El PoS reemplaza el trabajo computacional con participación económica como base de la seguridad. En un sistema PoS, los validadores deben «apostar» (*stake*) una cierta cantidad de los *tokens* nativos de la red como garantía para poder participar en la creación de nuevos bloques. La probabilidad de que un validador sea seleccionado para validar o forjar el siguiente bloque suele ser proporcional a la cantidad de *tokens* que tiene apostados: a mayor *stake*, mayor probabilidad (aunque se introducen aleatorizaciones para evitar que sean siempre los mismos). Si un validador actúa maliciosamente (como firmando bloques inválidos o intentando un doble gasto), se arriesga a perder parte o la totalidad de sus *tokens* apostados mediante un mecanismo llamado *slashing*. Esto crea incentivos económicos para comportarse honestamente, sin requerir el enorme gasto energético del PoW [80], [83]. Redes modernas como Ethereum (tras su actualización *The Merge*) han adoptado PoS para mejorar escalabilidad y sostenibilidad, aunque PoS trae sus propios desafíos, como garantizar una suficiente descentralización (evitar que unos pocos validadores con grandes stakes dominen) y asegurar la complejidad de implementar el *slashing* sin perjudicar a nodos honestos por errores menores.

3.4.3. Limitaciones de Escalabilidad, Costes y Alternativas

A pesar de sus virtudes, las *blockchains* públicas enfrentan limitaciones inherentes de escalabilidad. Bitcoin, la primera red *blockchain*, procesa en promedio alrededor de 7 transacciones por segundo (TPS) debido a su tamaño de bloque y tiempos de bloque deliberadamente limitados; Ethereum, antes de soluciones de escalado de capa 2, manejaba entre 15 y 30 TPS. Estas cifras palidecen frente a sistemas tradicionales centralizados (como redes de tarjetas de crédito procesando miles de TPS). Las limitaciones surgen del conocido «trilema de la *blockchain*»: es difícil, con la tecnología actual, optimizar simultáneamente descentralización, seguridad y escalabilidad [84], [83]. Aumentar la capacidad de transacciones suele implicar sacrificar descentralización (mediante nodos más potentes que no cualquiera puede mantener) o relajar la seguridad (bloques más grandes pero más difíciles de propagar rápidamente por la red, lo que aumenta riesgos de bifurcación).

Otro desafío práctico son los costes o tasas por transacción (*gas fees*) en *blockchains* como Ethereum. Estas tarifas surgen de la competencia por espacio de bloque limitado: cuando la demanda de procesar transacciones supera la capacidad de la red, los usuarios pujan incrementando voluntariamente la comisión que están dispuestos a pagar para que su transacción sea incluida antes que las demás. Durante picos de congestión (por ejemplo, el auge de los NFT en 2021 o de DeFi), estas tarifas pueden dispararse a valores de decenas de dólares por transacción sencilla, volviéndose prohibitivas para aplicaciones IoT que requerirían potencialmente registrar miles de microtransacciones diarias [60]. En un escenario de DPP para jamones, no sería viable pagar, por ejemplo, 1 € en comisiones por anclar el dato de temperatura diaria de un secadero; los costes deben ser prácticamente cero o del orden de fracciones de céntimos para que el sistema sea sostenible económicamente, especialmente para PYMEs.

Las *blockchains* *permissionadas* (aquellas donde solo entidades autorizadas pueden validar y escribir datos, a diferencia de las públicas donde cualquiera puede participar) han surgido en parte para abordar estas limitaciones de escalabilidad y coste. Por ejemplo, Hyperledger Fabric y plataformas similares permiten procesar cientos o miles de TPS gracias a que el consenso se simplifica (los nodos validadores suelen ser pocos y conocidos, eliminando la necesidad de PoW) y a que se pueden hacer operaciones en paralelo o fragmentar datos en canales privados. Además, en redes *permissionadas* normalmente no hay tasas por transacción o son fijas, ya que no hay un mercado abierto de *gas*. Sin embargo, estas mejoras vienen al precio de disminuir la transparencia pública (ya que la red está cerrada a participantes externos) y exigir una gobernanza consorcial compleja [85], [86]. En otras palabras, pasamos de confiar en código abierto a confiar en un consorcio de empresas, lo que puede ser adecuado para ciertos casos (como un grupo de compañías que montan una DLT para trazabilidad entre ellas, entornos B2B) pero no cumple la visión de un sistema universalmente verificable por cualquier parte interesada, B2C.

Por otro lado, han aparecido arquitecturas DLT alternativas más allá de la cadena de bloques lineal. Los Grafos Acíclicos Dirigidos (*Directed Acyclic Graphs*, DAG) como la *Tangle* de IOTA representan una aproximación fundamentalmente diferente. En un DAG no existen bloques que agrupen transacciones secuencialmente; en su lugar, cada transacción nueva puede referenciar y validar múltiples transacciones anteriores, formando una red entrelazada de confirmaciones. Esto permite un procesamiento en paralelo de transacciones y elimina ciertos cuellos de botella inherentes a las arquitecturas lineales [80], [81]. En teoría, a más actividad en la red, más capacidad de procesamiento total, resolviendo en parte el cuello de botella de TPS. Además,

algunas implementaciones DAG, como IOTA, no requieren tarifas por transacción (*zero-fee*), pues el acto de validar es intrínseco al acto de enviar transacciones (cada nodo que envía contribuye a validar otras). Estas características resultan atractivas para escenarios IoT con alto volumen de mensajes pero bajo valor individual, donde las soluciones *blockchain* tradicionales no encajan bien [84].

Para implementar un DPP escalable, económico y eficiente para el jamón ibérico, es necesario seleccionar cuidadosamente la plataforma DLT que mejor se alinee con los requisitos identificados. Es por ello que profundizaremos en la Tangle de IOTA, una DLT de tipo DAG que se ha diseñado pensando especialmente en entornos IoT y que, como se verá, ofrece soluciones innovadoras a varios de los problemas mencionados.

3.5. La Tangle de IOTA

IOTA representa una evolución paradigmática en las tecnologías de registro distribuido, diseñada específicamente para superar las limitaciones inherentes de las *blockchains* tradicionales en entornos IoT (saturación de red, aumento de tasas de transacción a medida que crece el uso, etc.) [68], [82]. Su arquitectura, denominada *Tangle* (enredo), se basa en un Grafo Acíclico Dirigido (DAG) en lugar de en una cadena de bloques lineal. Esto conlleva la eliminación de algunos conceptos fundamentales de las *blockchains* clásicas, como los bloques secuenciales en los que agrupar transacciones, los mineros dedicados que compiten por validar, y las comisiones por transacción pagadas a esos mineros. En IOTA, la red pretende que cada actor que realiza transacciones también colabore en la validación de las transacciones de otros, distribuyendo el trabajo de mantenimiento de la red entre todos los participantes.

El funcionamiento esencial de la Tangle se sustenta en un principio sencillo en su concepción, aunque disruptivo en su efecto: cada nueva transacción debe aprobar (validar) dos transacciones anteriores antes de poder ser añadida al grafo [80]. Este proceso de aprobación implica verificar la corrección de las transacciones referenciadas (comprobar las firmas digitales de sus emisores, asegurarse de que no haya doble gasto, etc.) y realizar un pequeño cálculo de PoW, muy inferior al de Bitcoin, apenas del orden de magnitudes que un dispositivo modesto puede hacer en segundos, para prevenir el spam. De esta forma, al enviar una transacción, el dispositivo o nodo emisor contribuye con algo de poder computacional para ayudar a confirmar las transacciones previas de otros, en vez de delegar esa tarea en mineros externos.

Cuando un usuario desea emitir una nueva transacción en IOTA, el protocolo ejecuta un algoritmo de selección de *tips* (puntas). Los *tips* son transacciones que aún no han sido referenciadas por otras transacciones, representando las «hojas» actuales del grafo (análogo a transacciones pendientes) [80], [83]. El algoritmo de selección utiliza un «paseo aleatorio» (*random walk*) ponderado que favorece *tips* con mayor peso acumulado, de manera que se reduce la probabilidad de que haya transacciones que queden olvidadas o aisladas sin ser nunca confirmadas.

3.5.1. Pesos Individuales y Acumulados

Cada transacción en el Tangle posee un peso individual determinado principalmente por la cantidad de trabajo PoW que se realizó durante su emisión, es decir, si un dispositivo realiza un PoW ligeramente más intenso, puede asignar un peso mayor a su transacción (aunque en la práctica, el protocolo estandariza estos pesos para que todas las transacciones normales tengan similar peso individual, reservando la posibilidad de pesos mayores para casos especiales o nodos con más capacidad durante congestión) [80].

El peso acumulado de una transacción es la suma de su peso individual más los pesos acumulados de todas las transacciones que la aprueban directa o indirectamente. En otras palabras, si muchas transacciones futuras (incluso a varias «capas» de distancia en el grafo) han descendido de una transacción inicial, esa transacción inicial adquiere un gran peso acumulado, señal de que ha sido ampliamente respaldada por la actividad de la red [80].

Este sistema de pesos crea un mecanismo de selección natural dentro del Tangle: las transacciones con mayor peso acumulado tienen mayor probabilidad de ser referenciadas por transacciones nuevas (porque el algoritmo de selección de *tips* tiende a inclinarse hacia ellas), lo que a su vez sigue aumentando su nivel de confirmación. Por el contrario, transacciones con peso acumulado bajo corren el riesgo de quedarse «colgadas» en ramas laterales del grafo, especialmente durante períodos de baja actividad de la red en que no llegan suficientes nuevas transacciones que las referencien [81].

El diseño está pensado para que, en condiciones normales de uso, cada transacción termine siendo confirmada al ser integrada en la estructura cada vez más pesada del grafo. El peso acumulado sirve como un indicador de la confiabilidad o profundidad de confirmación de una transacción: una transacción con un peso acumulado muy alto es extremadamente difícil de revertir porque requeriría rehacer toda la cascada de aprobaciones que tiene encima.

3.5.2. Gestión de *tips* y *Edges*

Los *edges* (aristas) en el Tangle representan las referencias directas entre transacciones, creando la estructura del grafo dirigido [83]. Cada nueva transacción crea dos *edges* salientes (ya que aprueba a dos anteriores), pero teóricamente puede recibir un número ilimitado de *edges* entrantes (otras transacciones futuras que la referencien). En un Tangle ideal con alta tasa de transacciones, los *tips* se van convirtiendo rápidamente en nodos intermedios a medida que nuevas transacciones los aprueban, y el grafo crece densamente entrelazado.

El problema de los *tips* «colgantes» surge cuando, debido a la aleatoriedad del algoritmo de selección, se favorecen consistentemente ciertas ramas del grafo, dejando otros *tips* sin referencias durante un tiempo prolongado. Si no se les referencia nunca, esas transacciones permanecerían perpetuamente pendientes. Para mitigar esto, IOTA implementa mecanismos de promoción y *reattach*. La promoción implica que nodos (generalmente los mismos emisores, si detectan que su transacción no ha sido confirmada tras cierto tiempo) emitan transacciones especiales denominadas de «valor cero» cuyo único propósito es referenciar *tips* con bajo peso acumulado, ayudando a su eventual confirmación. Asimismo, el *reattach* permite, en caso de necesidad, volver

a emitir una transacción (con un nuevo PoW) para vincularla a una zona más activa del grafo, incrementando sus posibilidades de ser aprobada. De esta manera, el protocolo proporciona herramientas para que incluso en momentos de baja actividad, las transacciones pendientes puedan ser consolidadas.

3.5.3. Confirmación de Transacciones

La confirmación de transacciones en el Tangle es un proceso gradual y probabilístico, diferente del modelo discreto de las *blockchains*. En una *blockchain* tradicional, una transacción se considera confirmada cuando es incluida en un bloque minado y luego ese bloque es seguido por una cierta cantidad de bloques adicionales («confirmaciones profundas»). En IOTA, al no haber bloques, las transacciones se confirman a medida que van siendo aprobadas por transacciones posteriores [80].

Una transacción en IOTA se considera confirmada cuando es referenciada (directa o indirectamente) por otras transacciones en tal número o de tal manera que alcanza un nivel de confianza suficiente. En la red IOTA 1.0 (la implementada hasta 2021), esta confirmación era marcada de forma definitiva por las transacciones *milestone* emitidas por un coordinador. En redes IOTA totalmente descentralizadas (objetivo de IOTA 2.0), se definirá que una transacción está confirmada cuando alcanza un umbral específico de peso acumulado o aprobación por parte de la red, según el mecanismo de consenso probabilístico que se implemente [80].

En la práctica, esto significa que la confianza en una transacción aumenta gradualmente con el tiempo y la actividad de red subsiguiente. Al principio, justo tras ser emitida, es un *tip* sin confirmar. Tras un corto intervalo, unas cuantas transacciones la habrán aprobado y ya tendrá cierto peso acumulado; en ese momento se la puede considerar «probablemente» confirmada con un grado X % de certidumbre. Pasado más tiempo, si la red sigue activa, decenas o cientos de transacciones (incluyendo transacciones especiales de consenso) la habrán referenciado, alcanzando prácticamente el 100 % de certidumbre y considerándose irreversiblemente confirmada. Para un usuario final, la experiencia es similar a una *blockchain*: tras unos segundos o minutos, su transacción aparece como confirmada en el explorador, pero bajo el capó el proceso fue progresivo [81].

3.5.4. Transacciones *Milestone* y Coordinador

Las transacciones *milestone* constituyeron un mecanismo temporal para asegurar la red IOTA durante su fase de crecimiento inicial [82]. El Coordinador, un nodo especial operado por la Fundación IOTA, emitía periódicamente estas transacciones de *milestone* (hitos) que servían como puntos de control (*checkpoints*) para consolidar el estado de la red. Un *milestone* aprobaba (directa o indirectamente) todas las transacciones pendientes hasta ese momento que consideraba válidas; cualquier transacción no aprobada por el último *milestone* se consideraba no confirmada [82].

El problema que resolvían los *milestones* era garantizar que la red no pudiera ser atacada

cuando tenía pocos participantes. En una red pequeña, un atacante podría, teóricamente, crear una rama paralela del Tangle con mayor peso acumulado (por ejemplo, generando muchas transacciones falsas con alta potencia de cálculo) y confundir a los nodos honestos reorganizando el historial de transacciones (*double spending*). Los *milestones* proporcionaban *checkpoints* inmutables emitidos por una entidad confiable (la fundación de IOTA) que prevenían estos ataques de doble gasto [68], [81]. Es decir, actuaban como anclas que marcaban «hasta aquí todo es correcto», de modo que los nodos ignoraban cualquier rama que no estuviese alineada con los últimos *milestones*.

Si bien el Coordinador y los *milestones* introducían un elemento centralizado (y por tanto fueron concebidos como una solución temporal), resultaron prácticos para llevar a IOTA a un nivel de madurez suficiente. Actualmente (2025), IOTA está en transición para eliminar el Coordinador con el proyecto denominado *Coordicide*, implementando nuevas formas de asegurar la red sin un nodo privilegiado central [80].

3.5.5. Tipos de Redes IOTA

IOTA mantiene múltiples redes para diferentes propósitos [84]:

- **Mainnet:** es la red principal de IOTA, utilizada para transacciones con valor económico real y aplicaciones de producción. Es donde operan las aplicaciones comerciales y donde los *tokens* IOTA (MIOTA) tienen valor monetario. Cualquier implementación seria, una vez probada, terminará desplegándose aquí para interacción con usuarios finales.
- **Testnet:** red de pruebas pública que replica la funcionalidad de Mainnet pero utiliza *tokens* sin valor (*tokens* de prueba). Es ideal para desarrollo y prueba de entornos de aplicaciones, ya que permite experimentar sin arriesgar fondos reales. Los desarrolladores pueden enviar transacciones observando el comportamiento en un entorno similar al real.
- **Shimmer:** esta es una red de *staging* o preproducción lanzada por IOTA (Shimmer net) que actúa como banco de pruebas para nuevas características antes de su despliegue en Mainnet. Por ejemplo, innovaciones en el protocolo base, nuevos módulos de consenso o funcionalidades de capa 2 se habilitan en Shimmer para que la comunidad las use y las ponga a prueba en condiciones económicas. Tras suficiente madurez, esas características migran a mainnet. Para el desarrollo de un DPP, Shimmer podría usarse para validar el sistema bajo las versiones más recientes del protocolo IOTA.
- **Devnet:** es la red de desarrollo, históricamente usada para probar características experimentales muy tempranas, a menudo ni siquiera públicas para todos los nodos. Actualmente, gran parte de las pruebas se realizan en Testnet y Shimmer, por lo que el concepto de Devnet se ha difuminado, pero esencialmente es un entorno manejado por desarrolladores de la fundación para simulaciones y experimentos internos.

3.5.6. Prevención de *Spam*

La prevención de *spam* en IOTA se logra mediante múltiples mecanismos complementarios [81]. El mencionado *Proof of Work* requerido para cada transacción impone un coste computacional mínimo a quien envía, haciendo prohibitivo el spam masivo para cualquier actor que no disponga de recursos muy elevados (y aun teniéndolos, sus ataques serían rápidamente contrarrestados por la red aumentando la dificultad adaptativamente). Adicionalmente, los nodos de la red pueden implementar políticas de *rate limiting*, limitando la tasa de transacciones aceptadas desde una misma dirección IP o nodo vecino, para prevenir que un solo origen inunde la red. También se contempla un mecanismo de *Adaptive PoW*, por el cual la dificultad del PoW requerido puede ajustarse dinámicamente en función de la carga actual de la red: si la red detecta un aluvión anómalo de transacciones (posible ataque), puede exigir un PoW ligeramente mayor para frenar a los *spammers* sin afectar significativamente a usuarios legítimos con dispositivos IoT. En conjunto, estas medidas mantienen la Tangle saludable y libre de saturación malintencionada, asegurando que incluso dispositivos de bajo coste puedan seguir participando sin verse desplazados por ataques de denegación de servicio (DoS, *Denial of Service*) [80].

3.5.7. Soluciones de «Capa 1» y «Capa 2»

En la jerga de las DLT, la «Capa 1» (*Layer 1*) se refiere al protocolo base del Tangle, incluyendo el mecanismo de consenso, la estructura de datos fundamental y las reglas de validación que todos los nodos siguen [84], [87]. En IOTA, la Capa 1 proporciona ya de por sí transacciones sin comisiones y una confirmación futura de las mismas. Sin embargo, igual que en las *blockchains*, existe interés en ampliar funcionalidades sin sobrecargar ni modificar la capa base.

Ahí entran las soluciones de «Capa 2» (*Layer 2*), que engloban desarrollos construidos sobre la Tangle base, extendiendo su funcionalidad sin alterar el protocolo original. Estas soluciones permiten manejar casos de uso especializados o escalar ciertas operaciones, mientras se aprovecha la seguridad y consenso de la capa 1 para su funcionamiento final [84].

Ejemplos de *Layer 2* en el ecosistema IOTA incluyen:

- IOTA Smart Contracts: una implementación que permite correr cadenas de bloques o entornos de ejecución paralelos anclados en IOTA, donde se pueden ejecutar «contratos inteligentes» (*smart contracts*). Estas cadenas de Capa 2 usan la Capa 1 de IOTA para anclar puntos de estado y asegurar su ejecución, pero las operaciones intermedias ocurren fuera del Tangle principal, lo que habilita lógica compleja sin ralentizar la capa base.
- IOTA Streams: anteriormente conocido como MAM (*Masked Authenticated Messaging*), es un protocolo de mensajería cifrada sobre IOTA que permite crear canales seguros para transmitir datos de forma ordenada. Es muy útil para IoT, donde un sensor puede emitir un stream de datos continuo que solo ciertas partes con la clave pueden leer, mientras los mensajes quedan inmutables en el Tangle.
- IOTA Identity: un marco para gestión de identidades descentralizadas (DID, *Decentralized Identifiers*) y credenciales verificables, construido sobre IOTA. Permite emitir, anclar y

verificar identificadores únicos y atributos asociados (por ejemplo, la identidad de una empresa productora) de manera que puedan ser usados en el DPP para firmar datos o probar atribuciones, reforzando la confianza sin depender de autoridades centrales de certificación.

Estas soluciones aprovechan la finalización y el consenso de la Capa 1 para registrar sus resultados (por ejemplo, una credencial firmada se puede anclar en el Tangle para que cualquiera valide su huella), mientras proporcionan capacidades especializadas que la base no tiene. Para el Pasaporte Digital del jamón ibérico, esto implica que, si bien la Capa 1 (transacciones IOTA básicas) puede usarse para anclar datos brutos de trazabilidad, las Capas 2 pueden aportar funcionalidades adicionales como canales cifrados de datos de sensores (Streams) o prueba de identidades de los actores que aportan datos (Identity) [84].

3.5.8. Evolución hacia IOTA 2.0 (*Coordicide*)

El proyecto Coordicide representa la transición de IOTA hacia una red completamente descentralizada, eliminando la dependencia del Coordinador y los *milestones* mencionados previamente [82], [83]. Para lograrlo, IOTA 2.0 introduce varios componentes clave que sustituyen y mejoran las funciones que antes realizaba el Coordinador, manteniendo al mismo tiempo las ventajas de escalabilidad y ausencia de comisiones:

- *Autopeering*: un protocolo para descubrimiento automático de nodos vecinos sin configuración manual. En una red P2P(*Peer-to-Peer*) global, cada nodo debe conectarse con algunos otros para intercambiar mensajes. El *autopeering* permite que nuevos nodos encuentren y se conecten a pares de forma autónoma, distribuyendo la topología de la red de forma más homogénea y resistente a particiones o ataques dirigidos.
- *Identidades de Nodo*: cada nodo en IOTA 2.0 tendrá una identidad criptográfica única, derivada de claves, que sirve para evitar ataques Sybil (donde un actor crea multitud de nodos falsos para ganar influencia). Estas identidades permiten cuantificar la participación de cada nodo en la red y asignar reputación.
- *Mana*: es un sistema de reputación o peso asignado a los nodos basado en la cantidad de *tokens* IOTA que poseen o que otros les han delegado. Mana no es exactamente como *stake* bloqueado, sino más bien un poder cuasi-voto que determina la influencia de cada nodo en decisiones de consenso y acceso a recursos de red. La idea es que un nodo con mucho mana (porque posee muchos *tokens*, demostrando inversión en el sistema) tendrá proporcionalmente más poder para, por ejemplo, emitir transacciones en épocas de congestión o para ser tenido en cuenta en votaciones de consenso.
- *Fast Probabilistic Consensus (FPC)*: un mecanismo de consenso descentralizado y ligero que utiliza votos aleatorizados y rondas de consulta entre nodos para resolver conflictos (por ejemplo, transacciones dobles) sin requerir un líder central. Cada nodo, ante un conflicto, pregunta a un subconjunto aleatorio de otros nodos cuál debería ser la preferencia correcta. Los nodos ponderan las respuestas según mana y repiten el proceso varias rondas con distintos vecinos. Finalmente, gracias a teoría de probabilidades, toda la red converge con alta probabilidad en la misma decisión mayoritaria.

Esta arquitectura permite que IOTA 2.0 mantenga las ventajas de escalabilidad y ausencia de tarifas de IOTA 1.0, mientras logra una completa descentralización. Para el usuario final y para aplicaciones como el DPP, la transición a Coordicide significa que se podrá confiar plenamente en la red IOTA sin ningún punto central, incrementando aún más la robustez y confianza del sistema. A medida que IOTA evolucione, un DPP implementado sobre esta tecnología heredará esas mejoras en seguridad y rendimiento sin cambios drásticos en su funcionamiento [80].

3.6. IOTA para el DPP: ¿*Notarization* o Verificación Manual?

Para la implementación del DPP con IOTA, existen dos aproximaciones principales para el anclaje y verificación de datos en la Tangle. La primera es utilizando IOTA *Notarization*, que es el método oficial promovido por la Fundación IOTA. La segunda es una estrategia más manual a través de *Tagged Data* (transacciones de datos etiquetados).

3.6.1. IOTA Notarization

El *framework* Oficial IOTA Notarization es un *framework* oficial diseñado específicamente para crear registros verificables en la Tangle, sirviendo como una capa de confianza universal para cualquier tipo de dato digital [80], [88]. La idea central es proporcionar un conjunto de herramientas y estándares para anclar datos (o la huella de datos) en IOTA de forma consistente y fácilmente verificable por terceros, sin que estos tengan que conocer de antemano los detalles del sistema que generó esos datos. El flujo típico de Notarization sigue seis pasos clave [80], [88]:

1. Preparación de datos. Los datos originales que se desean anclar (e.g., un evento de trazabilidad como «lote X pasó a secadero Y el día Z con temperatura T») se estructuran en un formato estándar y canónico. En el caso de trazabilidad, podría utilizarse un JSON-LD siguiendo el estándar EPCIS 2.0, de forma que el contenido tenga semántica conocida y un orden determinista.
2. *Hashing* criptográfico. Se calcula un *hash* (SHA-256) del contenido estructurado y canonizado. En IOTA Notarization se usa *JSON Canonicalization Scheme* (JCS) para generar una representación única del JSON antes de sacar el *hash*, asegurando que cualquier otro que repita el proceso con los mismos datos obtendrá exactamente el mismo *hash*.
3. Creación del objeto de *notarización*. Se genera un objeto de metadatos de *notarización* que incluye el *hash* calculado y otra información relevante, como *timestamps*, identificadores del contexto y, opcionalmente, firmas digitales de los actores que avalan ese dato.
4. Anclaje en IOTA. Este objeto, o la información esencial de él, se almacena en la Tangle mediante una transacción. Dependiendo del nivel de visibilidad elegido, puede ser que se guarde en texto claro o cifrado, pero en todo caso se convierte en una entrada inmutable en IOTA con un identificador único (*transaction ID*).
5. Generación de prueba. A partir de la información anclada, se obtiene una prueba verificable (el ID de la transacción anclada en la DLT y el *hash* original), que puede ser incluida o

referenciada en el Pasaporte Digital. Esta prueba suele ser una pequeña estructura JSON con campos como el *hash*, la dirección de la transacción en la Tangle y posiblemente el estado de confirmación.

6. Verificación. Cualquier parte interesada, en cualquier momento futuro, puede tomar la prueba, recalcular el *hash* a partir de los datos originales y consultar la Tangle para verificar que ese *hash* está efectivamente registrado en la transacción indicada. Si coincide, la información se da por válida e intacta; si no, significaría que los datos fueron alterados o la prueba es inválida. Este proceso garantiza que, por ejemplo, un dato de temperatura/humedad crítico registrado durante el curado queda sellado en la Tangle. Aunque el DPP muestre al usuario la lectura en texto (y posiblemente cifre esos datos por confidencialidad), el usuario puede obtener el *hash* y la transacción anclada para corroborar que coincide, sin tener que confiar ciegamente en el operador del sistema.

IOTA Notarization ofrece, además, tres niveles de visibilidad para los datos anclados [80]:

1. *Clear text* (texto claro): los datos se almacenan en la Tangle de forma legible y directamente visible para cualquiera. Esto es útil para registros públicos que no contienen información sensible, como por ejemplo una declaración de sostenibilidad general de un producto.
2. *Encrypted data* (datos cifrados): los datos se cifran en el cliente antes del envío a la Tangle. En la DLT se almacena el contenido cifrado (junto con, típicamente, alguna etiqueta que indique qué tipo de datos son). Solo usuarios con las claves de descifrado adecuadas pueden leerlos, manteniendo la confidencialidad pero permitiendo la verificabilidad de la existencia e integridad del dato (uno puede verificar que un cierto *hash* cifrado está, aunque no sepa descifrarlo). Este nivel es ideal para información sensible que deba compartirse selectivamente.
3. *Hash only* (solo huella): solo se almacena la huella criptográfica (*hash*) de los datos, no el contenido ni siquiera cifrado. El contenido completo permanece en sistemas privados *off-chain* (la base de datos del fabricante). Esta es la opción más conservadora de la privacidad, puesto que la DLT solo contiene un identificador abstracto que no revela nada del dato original, pero sirve para verificarlo posteriormente. Es el modo preferido para secretos comerciales o datos voluminosos, manteniendo el *ledger* ligero.

En todos los casos, la DLT actúa como testigo imparcial de que un determinado hecho o dato existió en un momento dado con un determinado valor. La selección entre texto, cifrado o *hash* dependerá del equilibrio entre transparencia y confidencialidad que se necesite para cada tipo de información del DPP, en línea con las categorías A, B, C, D mencionadas en el apartado 3 de este Capítulo.

3.6.2. Verificación Manual con *Tagged Data*

El método de verificación manual implementado en el trabajo *Implementación de Dispositivo IoT de Monitorización de temperatura y Posición para Aplicaciones en Alimentación y Salud* (un

estudio previo de IoT y trazabilidad) utiliza las transacciones de *Tagged Data* para almacenar directamente información en la Tangle [61]. Este enfoque prescinde de *frameworks* externos: el desarrollador del sistema diseña por su cuenta cómo formatear y anclar los datos en IOTA. Requiere típicamente los siguientes pasos:

1. Codificación manual: Los datos que se quieren guardar deben convertirse a un formato que quepa en una transacción IOTA. Normalmente se codifican en hexadecimal o Base64 para ser incluidos en el campo de datos de la transacción. Esto implica tomar la cadena JSON y transformarla a su representación *hex* correspondiente.
2. Publicación directa: se envían transacciones *Tagged Data* al nodo IOTA (a través de la API REST de un nodo Hornet) que contienen los datos codificados. Se suele asignar una etiqueta (*tag*) legible para filtrar las transacciones del proyecto, por ejemplo «DPPJAMON» o un identificador único del producto.
3. Verificación manual: para comprobar la integridad en el futuro, se necesita desarrollar una lógica propia que recalculé el *hash* de los datos originales y lo compare con el almacenado. A diferencia de IOTA Notarization, donde el *framework* provee funciones de verificación, aquí la responsabilidad recae en el implementador.
4. Gestión de metadatos: dado que al almacenar datos directamente es fácil perderlos entre miles de transacciones, se debe implementar un sistema de indexación y búsqueda. Por ejemplo, mantener en una base de datos local los ID de transacción correspondientes a cada evento de trazabilidad, o usar las etiquetas para localizar transacciones de cierto producto.

Este enfoque manual otorga control total sobre cómo y qué se guarda, pero tiene ciertas desventajas: mayor esfuerzo de desarrollo, riesgo de cometer errores sutiles en la implementación de seguridad, y falta de estandarización. No obstante, fue la ruta que adoptaron algunos pioneros antes de que existieran *frameworks* más maduros, y brinda conocimiento valioso sobre el funcionamiento de bajo nivel.

3.6.3. Comparación y Decisión

Comparando ambos métodos, IOTA Notarization presenta ventajas significativas para un proyecto de Pasaporte Digital profesional:

- Alineación técnica: el *framework* oficial está diseñado para ser compatible con la evolución hacia IOTA 2.0 y la hoja de ruta futura, evitando dependencias de componentes que puedan quedar obsoletos. Utiliza las librerías y recomendaciones actualizadas de la Fundación IOTA, mientras que una solución manual podría quedarse ligada a llamados específicos de una versión de nodo.
- Menor fricción de verificación: la verificación viene «empaquetada» en el *framework*, con herramientas o especificaciones claras de cómo comprobar pruebas. Un tercero, sin conocer nada del proyecto, pero sabiendo que se usó IOTA Notarization, podría verificar la información siguiendo documentación pública. En cambio, en la aproximación manual, habría que proveer documentación propia para enseñar a verificar.

- Estándar industrial emergente: a medida que más iniciativas adopten DPP, es de esperar que converjan en patrones similares. IOTA Notarization mantiene el patrón típico de DPP: datos sensibles *off-chain* y pruebas públicas *on-chain*. Esto facilita que el sistema de jamón ibérico no sea un *unicornio* aislado, sino que pueda integrarse en un ecosistema más amplio de verificaciones.
- Documentación y soporte: al ser oficial, hay documentación completa y actualizada de la Fundación IOTA, así como una comunidad de desarrolladores probando y mejorando la herramienta. Ante dudas o problemas, es más fácil encontrar soluciones o ayuda, en contraste con una solución artesanal donde el equipo desarrollador está solo ante cualquier inconveniente.
- Flexibilidad de privacidad: El soporte nativo para distintos niveles de visibilidad (texto, cifrado, *hash*) permite ajustar caso a caso cómo anclar cada tipo de información, cumpliendo requisitos regulatorios.

La verificación manual, por su parte, podría ser apropiada únicamente en casos muy específicos donde se requiera un control total sobre el proceso y quizá no se confíe en marcos externos, o para aprendizaje o experimentación. Sin embargo, para una implementación de Pasaporte Digital de Producto que se pretende llevar a producción y mantener a largo plazo, IOTA Notarization representa la mejor práctica actual. Es una solución robusta, mantenible y alineada con los estándares, lo que aumentará la probabilidad de éxito y la facilidad de evolución del sistema.

En cuanto a la integración con Sensores IoT y EPCIS es importante señalar que ambos métodos de anclaje (Notarization y manual) son completamente compatibles con la arquitectura general planteada y con los demás componentes:

- Sensores LoRaWAN: la forma en que se anclan los datos no afecta la recolección inicial. Los datos recopilados por sensores en campo (vía The Things Network, almacenados en InfluxDB, etc.) se procesarán normalmente. La diferencia está en cómo luego se toma un resumen o evento de esos datos y se envía a IOTA (sea via Notarization API o via API REST manual).
- Estándares GS1: los eventos de trazabilidad se estructurarán según EPCIS 2.0, utilizando vocabularios GS1 CBV (Core Business Vocabulary) para describir la información. Esto permanece igual; simplemente en un caso se tomaría ese evento EPCIS y se pasaría al módulo de notarización para calcular *hash* y anclar, y en el otro caso se podría insertar directamente en Tangle (aunque es más probable anclar solo su *hash* si es muy grande) [63].
- Identificadores únicos: se mantiene el uso de identificadores GS1 (GTIN/SGTIN para productos, GLN para ubicaciones, etc.) o de precintos ÍTACA como claves. Estos identificadores pueden incorporarse en los metadatos anclados (por ejemplo, en la etiqueta de transacción o en el JSON que se *hashea*) para vincular claramente cada transacción DLT con un producto específico.
- Códigos QR (Digital Link): independientemente del método de anclaje, el código QR impreso en el producto (formato GS1 Digital Link) continuará funcionando como punto de entrada al DPP. Es decir, un consumidor escanea, accede a la URL del pasaporte digital en

una aplicación web, y allí ve la información. Esa aplicación web «bajo el capó» consultará bases de datos y también la Tangle para verificar pruebas. Pero todo esto es transparente al usuario final; su experiencia no varía según se use notarización o no, salvo quizás en la presentación de un icono o estado «información verificada» [65].

En suma, la elección del método de anclaje de datos en IOTA es una decisión técnica interna que no afecta a la arquitectura general ni a la experiencia de usuario final, siempre y cuando se garantice la integridad y disponibilidad de las pruebas. Dado el análisis, la recomendación clara es adoptar IOTA Notarization por sus ventajas de estandarización y facilidad, asegurando así que el Pasaporte Digital de Producto del Jamón Ibérico esté respaldado por la solidez de la Tangle de la manera más profesional y confiable posible.

3.7. Estándares de Identificación y Datos: GS1, EPCIS 2.0 y Digital Link

La interoperabilidad global de los sistemas de trazabilidad depende fundamentalmente de la adopción de estándares reconocidos internacionalmente. En este contexto, GS1 emerge como el organismo de estandarización más relevante para la identificación y trazabilidad de productos, proporcionando un lenguaje común que trasciende fronteras geográficas y sectoriales [63], [89], [90]. Para un Pasaporte Digital de Producto basarse en estos estándares asegura que los datos de nuestro sistema puedan entenderse e integrarse con los de otros sistemas a lo largo de la cadena de suministro.

3.7.1. Sistema de Identificación GS1

El Sistema GS1 constituye la columna vertebral de la identificación de productos a nivel mundial, utilizado por más de un millón de empresas en más de 150 países [63]. Su importancia para los DPP radica en proporcionar identificadores únicos, globales y persistentes que permiten referenciar productos, ubicaciones y activos de manera inequívoca a lo largo de complejas cadenas de suministro, sin ambigüedades.

El elemento más conocido del sistema GS1 es el *Global Trade Item Number* (GTIN), que representa el identificador fundamental para productos comerciales [63], [89]. El GTIN es la serie numérica que aparece codificada en los códigos de barras de los productos de consumo; suele tener 13 dígitos (GTIN-13) o 14 dígitos para casos especiales, e identifica de forma única la combinación «fabricante + referencia de producto». En el contexto del jamón ibérico, un GTIN podría identificar un tipo específico de jamón como categoría comercial («Jamón Ibérico de Bellota 100 % Ibérico DOP Jabugo, pieza entera 7-8 kg»). Todas las piezas que cumplan esas características compartirían el mismo GTIN. Sin embargo, dado que en un DPP nos interesa llegar al detalle de pieza individual, se complementa el GTIN con otros identificadores como el número de serie para tener unicidad a nivel de ítem. GS1 provee el concepto de SGTIN (Serialized GTIN) que combina el GTIN del producto con un serial único por unidad. Así, cada jamón ibérico individual podría tener su propio código combinando GTIN + serie, lo que equivaldría

digitalmente a lo que el precinto físico hace en el mundo real (darle una identidad singular a cada pieza) [63].

Los *Global Location Numbers* (GLN) son otro pilar del sistema GS1, orientado a identificar ubicaciones físicas y también entidades legales dentro de la cadena de suministro [63]. Cada granja, matadero, secadero, almacén, punto de venta, etc., puede tener un GLN asignado. En la trazabilidad del jamón ibérico, por ejemplo, el GLN de la explotación ganadera de origen permitiría vincular al animal con su procedencia exacta. Del mismo modo, un GLN identifica al matadero donde se realizó el sacrificio y certifica que está autorizado, la industria de curado donde se llevó a cabo la maduración, y los puntos de distribución o venta. Incorporar GLNs en el DPP (en los eventos de trazabilidad) evita ambigüedades como tener que confiar en nombres escritos; en su lugar, un GLN es un código numérico único para cada operador o instalación [63].

3.7.2. EPCIS 2.0: Modelo de Eventos de Trazabilidad

Electronic Product Code Information Services (EPCIS) es un estándar de GS1 diseñado para la captura y el intercambio de eventos de trazabilidad a lo largo de la cadena de suministro. La versión 2.0, publicada en 2023, representa la evolución más avanzada de este estándar [63]. Ha sido adoptado como norma ISO/IEC 19987:2023, reflejando su madurez y reconocimiento internacional [63].

EPCIS 2.0 define un modelo conceptual basado en cuatro dimensiones fundamentales, coloquialmente las «4W»: ¿qué? (*What*), ¿cuándo? (*When*), ¿dónde? (*Where*) y ¿por qué? (*Why*). Cada evento de EPCIS responde a estas preguntas: qué objetos o productos estuvieron involucrados, en qué momento ocurrió el evento, en qué ubicación física o logística sucedió, y por qué. Además, añade un quinto componente importante: ¿Quién? (quién es el actor responsable o la empresa que reporta el evento), lo cual puede deducirse a través de identificadores de empresas, GLNs, etc. [63].

Las mejoras semánticas de EPCIS 2.0 incluyen, de forma destacada, el soporte nativo para JSON-LD, lo que facilita la integración con tecnologías web modernas y sistemas de datos enlazados (Linked Data). En la práctica, esto significa que un evento EPCIS ya no es solo un XML estructurado o un CSV, sino que puede representarse como un documento JSON con contextos que permiten expandir sus términos a URI. Por ejemplo, un evento podría tener «*eventType*»:«*TransformationEvent*», y gracias al contexto JSON-LD se entiende universalmente qué significa eso. Para un DPP que debe ser accesible vía API REST y entendible por aplicaciones de distintos desarrolladores: un fabricante, un minorista y una autoridad pueden intercambiar eventos en formato JSON sabiendo que están semánticamente alineados [63].

Otra mejora es la incorporación de nuevas capacidades como la descripción de lotes y productos unitarios simultáneamente, la identificación de eventos relacionados con *sensor data* (tan importante para IoT), y la posibilidad de vincular directamente a documentos externos [63].

Los mecanismos de verificación integrados en EPCIS 2.0 también se han fortalecido, contemplando la firma digital de eventos o grupos de eventos y la inclusión de enlaces a sistemas de verificación externa (como podría ser una DLT). Esto facilita la integración con IOTA u otras

DLT para añadir garantías adicionales de integridad. Por ejemplo, se puede definir que cada evento EPCIS lleve un campo *hash* calculado sobre su contenido, que a su vez está registrado en una *blockchain*; cualquier receptor del evento podría usar ese campo para comprobar contra la *blockchain* que el evento no ha sido alterado [63].

En el caso del jamón ibérico, modelar la trazabilidad con EPCIS 2.0 permite representar con granularidad y claridad cada paso: un *event* de tipo *ObjectEvent* para el nacimiento de un cerdo (con su ID individual), un *AggregationEvent* para asociar ese cerdo a un lote de engorde, más tarde un *TransformationEvent* cuando del cerdo sacrificado se obtienen diferentes piezas (jamones, paletas, etc.), y sucesivos *ObjectEvents* para cada movimiento de esas piezas (entrada a curación, inspección, etiquetado, expedición, etc.). Cada evento capturando What (por ejemplo, qué GTIN/precinto), When (*timestamp*), Where (GLN de la instalación) y Why (por ejemplo «bizStep»: «packing» o «commissioning», etc., y «disposition»: «active» o «expired», etc.). Esta riqueza descriptiva alimentará el DPP para que pueda reconstruir la historia completa del producto [63].

3.7.3. GS1 Digital Link: Puentes hacia el Mundo Digital

GS1 Digital Link representa la evolución de los códigos de barras tradicionales hacia identificadores web nativos [65]. La premisa es que, en la era de internet, todo identificador de producto debería poder expresarse como una URL que, al ser escaneada o accedida, lleve a información relevante en la web. De esta forma, se elimina la necesidad de aplicaciones especializadas o bases de datos locales para interpretar un código: cualquier smartphone con cámara puede acceder al DPP mediante la URL codificada en un QR.

En lugar de los códigos de barras 1D (EAN/UPC) que codificaban solo el GTIN en formato numérico, Digital Link permite incluir en un solo código QR múltiples datos: el GTIN, el número de serie, fechas, lotes, etc., todo embebido en una sintaxis de URL estándar. Por ejemplo, un código QR con Digital Link para un jamón ibérico podría contener una URL como:

`https://dpp.ejemplo.es/01/08412345123456/10/LOTE123/21/PZ001`

Donde cada segmento numérico después del dominio corresponde a un *Application Identifier* (AI) de GS1 específico:

- 01/08412345123456 indica el GTIN (AI 01) del producto (en este caso, 08412345123456 sería el GTIN de la referencia de jamón).
- 10/LOTE123 indica el número de lote (AI 10) al que pertenece, por ejemplo "LOTE123".
- 21/PZ001 indica el número de serie (AI 21) de la pieza, por ejemplo "PZ001".

Esta URL, al ser escaneada, puede ser resuelta por el servidor *dpp.ejemplo.es* para redirigir a la página o API del Pasaporte Digital correspondiente a esa pieza exacta. Lo poderoso es que,

usando el estándar GS1 Digital Link, esta URL es comprensible para cualquier otra aplicación que soporte Digital Link, no solo la del productor [65].

Además, GS1 Digital Link permite que en la URL se puedan pedir directamente diferentes representaciones (usando el concepto de «Linked Data»): por ejemplo, añadiendo `.json` se podría obtener los datos en JSON, o `.html` para una página amigable, o fragmentos específicos. Esto alinea muy bien con la filosofía de datos abiertos e interoperables del ESPR [65].

Como podemos apreciar, los estándares GS1, EPCIS 2.0 y Digital Link conforman un ecosistema integral: identifican inequívocamente los productos y lugares, estructuran los datos de eventos de trazabilidad de forma rica y estandarizada, y vinculan el mundo físico con el digital a través de identificadores web. Incorporarlos al Pasaporte Digital del jamón ibérico es esencial para lograr un sistema interoperable, escalable y preparado para integrarse en la visión europea de trazabilidad digital unificada.

Adicionalmente, para facilitar la identificación precisa y estandarizada de cada pieza de jamón ibérico dentro del DPP, se incorporan los *Application Identifiers* (AIs) más relevantes del estándar GS1 Digital Link. Estos identificadores permiten codificar en la URL múltiples atributos esenciales para la trazabilidad, integrando tanto claves primarias como cualificadores de clave y atributos opcionales.

El URI Digital Link codificado en el QR del precinto de una pieza podría tener la forma:

`https://dpp.jamon.io/01/08412345123456/10/LOTE123/21/PZ001?17=251231&414=8412345000019`

donde:

- `/01/08412345123456` corresponde al GTIN (AI 01).
- `/10/LOTE123` es el lote (AI 10).
- `/21/PZ001` es el número de serie o precinto ÍTACA (AI 21).
- `?17=251231` es la fecha de caducidad (31/12/2025).
- `414=8412345000019` es el GLN de la ubicación física (secadero).

Para mayor claridad, la Tabla 3.1 recoge los principales *Application Identifiers* (AI) de GS1 empleados en el sistema DPP de jamón ibérico para garantizar interoperabilidad y cumplimiento de normativas [91], [92]:

AI	Significado	Dónde va	Formato / notas
01	GTIN (Global Trade Item Number)	path (clave primaria)	14 dígitos (rellena a 14 si GTIN-13)
21	Serial Number (número de serie)	path (key qualifier)	≤20 caracteres alfanuméricos; mapea precinto ÍTACA
10	Lote (Batch/Lot Number)	path (key qualifier)	≤20 caracteres alfanuméricos
414	GLN ubicación física (Physical Location GLN)	query (si se desea indicar origen)	13 dígitos
11	Fecha de producción (Production Date)	query (opcional)	YYMMDD
13	Fecha de envasado (Packaging Date)	query (opcional)	YYMMDD
15	Fecha «best before»	query (opcional)	YYMMDD
17	Fecha de caducidad (Expiration Date)	query (opcional)	YYMMDD
422	País de origen (Country of Origin)	query (opcional)	Código ISO 3166-1 numérico (3 dígitos)
310n	Peso neto en kg (Net Weight, kg)	query (opcional)	6 dígitos; <i>n</i> indica posición decimal
8200	URL extendida de empaquetado (Extended Packaging URL)	query (opcional)	Hasta 70 caracteres

Tabla 3.1: Application Identifiers (AI) de GS1 relevantes para el DPP de jamón ibérico.

Esta sintaxis modular y compatible con GS1 Digital Link permite la construcción de un sistema de trazabilidad interoperable y alineado con estándares globales y normativas europeas, asegurando que el DPP pueda ser integrado y validado en un ecosistema digital amplio, a la vez que mantiene la estabilidad y unicidad de los códigos QR físicos [91], [93].

3.8. Normativa Sectorial Ibérica: Integración con Sistemas ASICI-ÍTACA

El sistema ÍTACA (Identificación, Trazabilidad y Calidad del Ibérico) representa uno de los sistemas sectoriales de trazabilidad más completos y maduros a nivel europeo en el ámbito agroalimentario [94]. Fue desarrollado específicamente para gestionar la trazabilidad del jamón ibérico y sus productos derivados, en cumplimiento de la Norma de Calidad del Ibérico (establecida por el Real Decreto 4/2014 y regulaciones relacionadas) [10]. Dada su relevancia, cualquier DPP para jamón ibérico debe contemplar una integración o convivencia con ÍTACA, aprovechando sus fortalezas y rellenando sus huecos sin duplicar innecesariamente funciones.

ÍTACA funciona como una plataforma centralizada gestionada por ASICI (Asociación

Interprofesional del Cerdo Ibérico) bajo mandato del mencionado Real Decreto 4/2014 [94]. Básicamente, todas las explotaciones, mataderos, industrias y operadores del sector ibérico están obligados a registrar en ÍTACA los eventos clave del ciclo productivo: nacimiento y alta de animales, movimientos entre explotaciones, sacrificios, producciones de canales y piezas, inspecciones, etc. De esta manera, ÍTACA actúa como repositorio unificado donde, por ejemplo, se puede consultar cuántos cerdos nacieron en tal dehesa en cierto año, a qué matadero fueron, cuántos jamones salieron de ellos y con qué precintos, etc. [95].

El modelo de datos de ÍTACA organiza la información en entidades jerárquicas que reflejan ese proceso productivo. A grandes rasgos:

- Animales individuales (identificados por su código de crotal o identificación individual) registrados junto con su raza y genética (100 %, 75 %, 50 % ibérico) y su explotación de origen.
- Lotes de engorde, que agrupan animales generalmente en función de su alimentación y manejo (montanera, cebo de campo, cebo).
- Canales de sacrificio: cuando los animales se sacrifican, cada canal (el cuerpo del animal dividido en dos mitades o cada pierna posterior o anterior, depende de la interpretación) se identifica y vincula a los lotes anteriores.
- Piezas de despiece: de cada canal salen piezas nobles (jamones, paletas, lomos) que se registran.
- Productos finales con precinto: cada jamón o paleta que va a ser comercializado recibe un precinto inviolable con un código único, y ese código es registrado en ÍTACA junto con la información del animal de origen, la alimentación recibida (lo cual determina el color del precinto), la fecha de entrada en curado, etc.

Los precintos oficiales constituyen el elemento central del sistema de identificación ibérica [96]. Cada precinto es una brida plástica de color (blanco, verde, rojo o negro, según la categoría de alimentación y pureza racial) que se coloca en la pezuña del jamón o paleta en el momento en que inicia su curación. En él aparece un código único alfanumérico (y a veces un código de barras interno para escaneo) que vincula físicamente la pieza con su registro digital en ÍTACA. La estructura del código de precinto suele incluir información codificada sobre el matadero de origen (letras que identifican la instalación), el año de sacrificio, y un número secuencial único para esa planta en ese año. Esto garantiza que no haya dos jamones con el mismo código, y que a partir del código se puedan inferir ciertos datos (como año y lugar), útiles por ejemplo para la inspección en campo [94].

La existencia de ÍTACA supone que gran parte de la información básica de trazabilidad del jamón ibérico ya se está recopilando por obligación legal. Entonces, ¿qué aporta un Pasaporte Digital DPP por encima de ÍTACA? La estrategia de complementariedad propuesta se basa en utilizar ÍTACA como fuente de datos autoritativa para la información regulatoria básica (pureza racial, tipo de alimentación, origen del animal, fecha de sacrificio, categoría del producto), mientras que el DPP proporciona una capa adicional de transparencia, verificabilidad y enriquecimiento de datos [94].

En la práctica, esto significa que los identificadores ÍTACA (códigos de precinto, números de lote, GLN de operadores registrados) se reutilizarán como claves primarias en el DPP para asegurar consistencia entre ambos sistemas. Por ejemplo, cuando el DPP despliegue la información de un jamón, internamente utilizará su código de precinto para consultar (a través de API o base de datos sincronizada) los datos asociados en ÍTACA, como la descripción oficial del producto (e.g., «Jamón de Cebo de Campo 50 % ibérico»), su fecha de entrada en curado y el municipio de la explotación de origen. Esos datos se presentan al usuario con la garantía de que provienen del sistema oficial supervisado por las autoridades [95].

Adicionalmente, el DPP puede ampliar la información más allá de lo que ÍTACA recoge. Por ejemplo, ÍTACA no registra condiciones de curado día a día, ni huella ambiental del proceso, ni resultados detallados de análisis de calidad. El DPP podría incorporar datos de sensores IoT del secadero (temperaturas, humedades a lo largo de los meses), datos de sostenibilidad (huella de carbono estimada de esa pieza, información sobre bienestar animal durante la cría obtenida de certificadoras), historias narrativas (descripciones de la dehesa, del maestro jamonero que supervisó la curación, etc.), e incluso contenido multimedia (fotos del animal en montanera o vídeos del proceso artesanal, accesibles al escanear el pasaporte). Estas son capas de valor añadido que ÍTACA, como sistema estrictamente trazabilidad-regulación, no provee [94].

Otra área donde el DPP complementa es en la verificación distribuida: ÍTACA es centralizado, por lo que los usuarios finales no tienen manera de verificar de forma independiente la información (han de confiar en ASICI y en los datos que cada operador introdujo). Al anclar ciertos datos o «huellas» en IOTA, el DPP introduce una forma de auditoría abierta. Incluso se podría pensar que, en el futuro, algunas partes de los registros de ÍTACA (una vez que un jamón está certificado y precintado) podrían anclarse en una DLT pública para fortalecer la confianza en exportaciones, etc. El DPP puede servir de puente para eso [94].

Finalmente, la integración con ÍTACA deberá hacerse de modo que no se generen duplicidades ni incoherencias. Idealmente, a través de servicios web o intercambios de datos, de forma segura, el DPP puede consultar o recibir actualizaciones de ÍTACA (por ejemplo, cuando se registran nuevos precintos o cuando se detecta que una pieza ha sido marcada como expedida o inspeccionada). También, si se introduce información en el DPP que pueda ser útil para ÍTACA, se podría enviar de vuelta [95].

En resumen, ÍTACA aporta la base de datos fiable de la trazabilidad legal del ibérico; el DPP la toma como pilar y construye encima un relato más amplio y tecnológicamente transparente para el consumidor y demás actores. Esta complementariedad asegura que el DPP no nace de cero, sino que se apoya en un sistema robusto preexistente, aprovechando sus datos mediante integración, y dedicando los recursos a cubrir los espacios que quedan para alcanzar los objetivos de transparencia total y confianza que se persiguen.

3.9. Casos de Uso Implementados: Pasaportes Digitales en Baterías y Productos Agroalimentarios

Para visualizar cómo un DPP puede materializarse en distintos sectores, resulta útil revisar casos de uso ya implementados, tanto obligatorios (marcados por regulación) como voluntarios. Aquí examinaremos brevemente dos ámbitos: el de las baterías (pionero en la introducción reglamentaria de DPP en la UE) y el agroalimentario, donde existen iniciativas de trazabilidad avanzada que ofrecen lecciones aplicables.

El DPP de baterías, que será mandatorio en la UE a partir de febrero de 2027 conforme al nuevo Reglamento de baterías, representa el primer caso de implementación obligatoria de DPP a escala industrial en la Unión [97]-[99]. Dado que las baterías son un producto tecnológicamente complejo y crítico para la transición energética (vehículos eléctricos, almacenamiento renovable), la UE ha impulsado su pasaporte para asegurar sostenibilidad, trazabilidad de materias primas (algunas conflictivas, como el cobalto) y promover economía circular (reciclaje eficiente de componentes) [97].

La arquitectura del *battery passport* se basa en una estructura de datos jerárquica que abarca desde materias primas hasta la etapa de reciclaje final [97]. Cada batería (o lote de baterías, dependiendo del fabricante) recibe un identificador único accesible vía código QR, similar al Digital Link, que enlaza a su pasaporte digital. Dentro de este se incluye información sobre: composición química, rendimiento y capacidad, huella de carbono de su fabricación, desde la extracción de materiales, y opciones de reciclaje o reutilización [97].

Un elemento clave en el DPP de baterías es la necesidad de proteger datos sensibles a la par que demostrar cumplimiento. Los fabricantes de baterías no querrán revelar públicamente la composición exacta de sus cátodos (secreto industrial), pero la regulación les exige proveer métricas de sostenibilidad y prueba de origen responsable de minerales. Para ello, muchas implementaciones están usando soluciones basadas en *blockchain* para anclar pruebas de integridad de datos sin exponerlos directamente [97]. Por ejemplo, plataformas como Circularise o Minespider permiten que distintos actores (minas, refinerías, fabricantes) inscriban en una *blockchain* «huellas» de los datos de sus materiales y certificados. Luego, a nivel de pasaporte, se pueden incluir referencias a esas huellas para que un auditor pueda verificar, sin revelar los detalles comerciales. Así, la *blockchain* asegura que cuando un pasaporte de batería afirma «contiene 20 % de cobalto reciclado», esa afirmación está respaldada por registros inmutables aportados por el reciclador en su momento [98].

Desde la perspectiva organizativa, el desarrollo del pasaporte de baterías ha implicado la creación de consorcios público-privados para definir los datos comunes, la infraestructura técnica (se debate entre un enfoque federado o alguna base de datos común para ciertos metadatos) y la gobernanza de acceso a la información. Estas decisiones marcan una pauta que seguramente influirá a otros sectores [97].

Por otro lado, en el sector agroalimentario, aunque de momento no hay DPP obligatorios, varias iniciativas han explorado el uso de DLT y sistemas digitales avanzados para trazabilidad, buscando mejorar la transparencia al consumidor y la eficiencia en retiradas de producto, entre

otros objetivos.

Un ejemplo destacado en España es la trazabilidad de huevos con *blockchain* implementada por la empresa avícola Rujamar [78]. En su proyecto, Rujamar registró en una *blockchain* privada cada evento desde la puesta del huevo hasta la llegada al supermercado. Esto incluía identificación de la granja y gallina, el tipo de alimentación de las gallinas, las condiciones de almacenamiento y la fecha exacta de envasado. Al colocar un código QR en el envase, el consumidor podía escanearlo y ver datos como el día y hora en que se recogió el huevo, cuánto tiempo tardó en procesarse, e incluso información de bienestar animal. Las motivaciones fueron tanto garantizar frescura (huevos lo más directos posible) como diferenciarse con un producto de calidad trazable. La *blockchain* se utilizó principalmente para asegurar que una vez registrados, los datos no fueran alterables, aumentando la confianza frente a posibles auditorías [100], [101].

En conjunto, estos casos de uso nos demuestran que los Pasaportes Digitales y las tecnologías DLT ya están siendo probados en campo, confirmando tanto su potencial como las áreas a pulir. Nos sirven de inspiración y nos advierten de retos a considerar, de modo que el DPP del Jamón Ibérico pueda diseñarse aprendiendo de lo ya hecho en lugar de partir de cero.

3.10. Plataformas DLT Aplicadas a Trazabilidad

La selección de la plataforma DLT apropiada para un DPP de jamón ibérico requiere una evaluación sistemática de múltiples criterios técnicos, económicos y operacionales. No todas las DLT son iguales ni ofrecen las mismas ventajas en todos los contextos; por ello, es necesario comparar las opciones más relevantes en el ámbito de la trazabilidad y justificar la que mejor se alinea con los requerimientos del proyecto.

A continuación se presenta un análisis comparativo detallado de cuatro plataformas o tecnologías distribuidas que podrían considerarse candidatas: IOTA Tangle, Ethereum (representando *blockchains públicas* con *smart contracts*), Hyperledger Fabric (representando *blockchains permissionadas consorciales*) y OriginTrail (plataforma DLT especializada en trazabilidad). Se abordan sus principales ventajas, desventajas y adecuación al caso.

3.10.1. IOTA Tangle

Ventajas técnicas: IOTA ofrece transacciones sin *fees* (comisiones), lo cual es crítico para un entorno IoT donde puede haber miles de transacciones de bajo valor diariamente. Su arquitectura de grafo acíclico (DAG) proporciona escalabilidad inherente, de modo que el rendimiento de la red puede incluso mejorar cuantas más transacciones se producen, haciéndola adecuada para manejar flujos de datos IoT masivos. Además, IOTA fue diseñada desde cero con IoT en mente: tiene requisitos de hardware bajos, un consumo energético ínfimo comparado con *blockchains* PoW clásicas, y soporta nativamente micropagos y microtransacciones de datos [68] [82]. Esto permite, por ejemplo, anclar lecturas de sensores en tiempo real sin preocuparse del coste por cada envío.

Ventajas operacionales: IOTA pone a disposición del desarrollador API sencillas y bibliotecas en múltiples lenguajes, lo que facilita su integración directa con dispositivos IoT y sistemas backend. Su arquitectura asíncrona tolera conectividad intermitente [84], un rasgo importante considerando que en entornos rurales. La Fundación IOTA proporciona documentación extensa, ejemplos de código y soporte a desarrolladores, lo que reduce la curva de aprendizaje. Por último, al no necesitar mineros ni nodos validadores especializados, cualquier actor del proyecto puede levantar un nodo *full* (por ejemplo ASICI podría tener un nodo IOTA público para el DPP, o cada gran productor el suyo) sin apenas coste, aumentando la descentralización efectiva de la solución.

Adecuación para DPP ibérico: es una excelente opción para manejar datos IoT de alta frecuencia (como las constantes mediciones en secaderos) con una buena relación coste-eficacia. También resulta idónea para pequeños productores, ya que no impone barreras económicas (no hay que comprar criptomoneda para pagar *gas*, ni instalar infraestructura costosa). De cara a un despliegue sectorial completo, IOTA puede escalar sin problema a cientos de miles de productos con múltiples eventos cada uno, sin congestionar ni incurrir en costes insostenibles [86].

3.10.2. Ethereum

Ventajas técnicas: Ethereum es la segunda *blockchain* pública más consolidada (después de Bitcoin) y se ha convertido en una plataforma generalista con capacidad de ejecutar *smart contracts* completos [85]]. Esto significa que es extremadamente flexible: se puede programar lógica compleja (por ejemplo, automatizar liberación de certificaciones, pagos, etc., dependiendo de condiciones de trazabilidad) directamente en la cadena. Cuenta con el ecosistema más maduro, con miles de desarrolladores, herramientas de desarrollo bien establecidas, auditorías de seguridad disponibles, etc. Además, su grado de descentralización es de los más altos, con miles de nodos globalmente, lo que asegura resistencia a censura y longevidad.

Desventajas: Actualmente, Ethereum (*mainnet*) opera bajo un modelo *Proof of Stake* sin minería, lo que redujo su consumo energético pero no solventó totalmente el tema de escalabilidad de *Layer 1*. El rendimiento sigue siendo relativamente limitado (unas pocas decenas de TPS), aunque la visión Ethereum 2.0 incluye fragmentación (*sharding*) y se apoya en soluciones de *Layer 2* (*rollups*) para escalar. Las *gas fees* pueden ser variables y potencialmente altas en momentos de alta demanda, lo que es un riesgo para nuestro caso. Además, desarrollar en Ethereum (contratos en Solidity, por ejemplo) añade complejidad y posibles vectores de ataque si no se hace con sumo cuidado (errores en contratos han llevado a pérdidas millonarias en otros contextos) [85].

Adecuación para un DPP ibérico: Ethereum sería adecuada si quisiéramos implementar lógica financiera o de negocio muy compleja integrada con la trazabilidad (e.g., pagos automatizados a ganaderos en función de datos del DPP, tokenización de jamones para mercados secundarios, etc.). También aporta máxima transparencia pública (cualquiera puede ver los datos en la cadena). Sin embargo, para el simple anclaje de eventos IoT y documentación, resulta «demasiado»: estaríamos infrautilizando su poder computacional pero pagando sus costes. Por tanto, es menos apropiada para datos de alta frecuencia por coste, aunque podría considerarse para aspectos puntuales de alto valor (como emitir un NFT de cada jamón como «gemelo digital» para coleccionismo; pero esto es más marketing que trazabilidad per se) [86].

3.10.3. Hyperledger Fabric

Ventajas técnicas: Hyperledger Fabric es una plataforma DLT permissionada desarrollada con enfoque empresarial. Al ser permissionada, ofrece transacciones con tiempos de confirmación rápidos y alto rendimiento, del orden de cientos o potencialmente miles de TPS, ya que el consenso suele ser más eficiente (no PoW, nodos conocidos) [86]. Permite configuraciones modulares: se puede elegir el algoritmo de consenso (Kafka, Raft, etc.), definir canales privados donde solo cierto subgrupo de nodos ve ciertas transacciones (lo que resulta útil para compartir datos confidenciales solo con quien corresponde), y tiene mecanismos de identidad integrados (cada participante tiene un certificado digital emitido por una autoridad del consorcio). También soporta *smart contracts* (llamados *chaincodes*) en varios lenguajes convencionales (Go, Java, Node.js), lo que facilita desarrollo [85].

Desventajas: Requiere establecer una gobernanza consorcial compleja: las empresas del sector tendrían que acordar quién aloja los nodos, cómo se toma decisión de añadir o quitar participantes, cómo se actualiza el sistema, etc. Esto puede ser incluso más difícil que aspectos técnicos, dado que implica confianza mutua y alineación de intereses entre competidores. Además, aunque no haya *gas fees*, sí tiene costes operativos: se necesitan servidores para los nodos, certificados, etc., y generalmente una entidad (o varias) dedicadas a la administración de la red. Otro punto es que pierde la transparencia pública: solo los miembros del consorcio ven todos los datos; esto es deseable en algunos casos (competencia) pero choca con la idea de un DPP abierto al consumidor a menos que se habiliten puertas de acceso públicas a cierta información [86].

Adecuación para un DPP ibérico: Fabric podría encajar si el sector (ASICI, grandes empresas, certificadoras) decidiera montar su propia red de trazabilidad privada para intercambiar datos de forma segura. Podría soportar bien la carga y personalizarse a las reglas de negocio del jamón. Sin embargo, dado que ya existe un sistema centralizado (ÍTACA) que de facto es un «permissionado central», quizás Fabric no aporte mucho más a nivel consorcial, y sacrificaría la capacidad de verificación abierta que daría IOTA u otra red pública. Además, su adopción por pequeños productores sería más difícil, pues no van a montar nodos ni a involucrarse en la gobernanza: esperarían un servicio ya hecho. En balance, Fabric es potente, pero la complejidad de orquestarlo en este sector podría superar a sus beneficios [86].

3.10.4. OriginTrail

Ventajas técnicas: OriginTrail es una plataforma creada específicamente para la trazabilidad en cadenas de suministro. Utiliza un enfoque híbrido: tiene su propia red descentralizada llamada ODN (*OriginTrail Decentralized Network*) que actúa como capa de datos, pero ancla huellas en *blockchains* públicas (Ethereum, xDai, Polkadot, etc.) para asegurar inmutabilidad [102]. Soporta de forma nativa estándares GS1 como EPCIS, lo que significa que está pensado para ingerir eventos de trazabilidad y enlazarlos con un *Knowledge Graph* descentralizado donde diferentes partes pueden consultar datos según permisos. También ofrece funcionalidades de privacidad con *selective disclosure* (revelación selectiva), es decir, puede probar que cierta información cumple X sin revelarla completa, un concepto muy alineado con lo requerido por ESRP [102].

Desventajas: Aunque la idea es muy adecuada a supply chain, el ecosistema OriginTrail es

mucho menor que las otras opciones, lo que implica menos comunidad de desarrolladores y potencialmente más dependencia del equipo que lo desarrolló. Su uso implica entender tanto su red ODN como las interacciones con *blockchains* subyacentes. Además, para participar en ODN se requieren nodos específicos (llamados *nodes of OriginTrail*) y uso de su *token* TRAC para algunas operaciones, lo que añade otra capa de complejidad y coste. A nivel de *token economics*, proyectos así necesitan suficientes nodos independientes para ser robustos; no está tan probado como Ethereum o IOTA en cuanto a resistencia a gran escala [102].

Adecuación para un DPP ibérico: OriginTrail tiene muchos componentes ya hechos que suenan atractivos: por ejemplo, con un modelo EPCIS podría casi *plug-and-play* una parte del sistema. Y ofrece un equilibrio entre *blockchain* pública y privada con su *knowledge graph* descentralizado. Sin embargo, adoptarlo implicaría ser relativamente pioneros en España con esta tecnología, y asumir riesgos de depender de algo que, si la empresa detrás cambia estrategia o desaparece, pudiera complicar soporte futuro. Además, para muchas funcionalidades se apalanca en Ethereum u otras para anclar, por lo que seguiríamos teniendo posibles «costos de gas» (aunque mitigados con *sidechains*). En resumen, es una opción interesante pero con cierta incertidumbre [102].

Comparando las DLTs presentadas, IOTA destaca por coste cero por transacción y enfoque IoT; Ethereum por su ecosistema maduro pero con coste por transacción y escalabilidad limitada (a menos que se use *Layer 2*); Hyperledger Fabric por control privado y rapidez pero menos transparente; OriginTrail por especialización en cadena de suministro con estándares integrados. Para un proyecto de jamón ibérico, si se prioriza involucrar a muchos pequeños productores y sensores IoT, IOTA u OriginTrail parecen opciones más alineadas (*feeless* e integrables con GS1 respectivamente). Si se prioriza robustez y confianza de marca, quizá una red consorcial (Fabric) entre grandes jamoneros y ASICI podría funcionar, pero perdería apertura. Una estrategia posible es combinar OriginTrail DKG para manejar los datos estandarizados de trazabilidad, y anclar *hashes* tanto en IOTA (pública, barata) como en una red permissionada (para duplicar confianza). De hecho, la complementariedad es tendencia: IOTA se ve como complemento de *blockchains* para IoT, no necesariamente reemplazo [81].

Cabe señalar que esta selección no excluye la posibilidad de interoperabilidad con otras DLT en ciertas funciones. Por ejemplo, si en algún momento se quisiera emitir activos digitales o NFTs de edición limitada asociados a algunos jamones (con fines de marketing o exportación), eso podría hacerse en una red como Ethereum sin por ello cambiar la base del DPP en IOTA. IOTA puede funcionar como *ledger* primario para los datos IoT y de trazabilidad, mientras se mantienen puentes hacia otras DLT para integraciones B2B específicas (quizás algún importador use Hyperledger, etc.). No obstante, para el núcleo de nuestro sistema, IOTA Tangle ofrece la mejor relación entre confianza distribuida y practicidad [86].

En conclusión, tras comparar las opciones, IOTA Tangle se justifica como la columna vertebral tecnológica para el Pasaporte Digital del Jamón Ibérico, ya que maximiza las fortalezas (integridad, disponibilidad, coste cero, escalabilidad) minimizando las debilidades (complejidad, coste variable, barreras de uso) en el contexto específico del proyecto.

3.11. Consideraciones de Seguridad en DPP e IoT

La seguridad de un sistema que combina DPP e IoT presenta desafíos únicos que trascienden las consideraciones tradicionales de ciberseguridad empresarial. Aquí no solo se protegen bases de datos y servidores, sino también dispositivos distribuidos en campo, comunicaciones inalámbricas de largo alcance, y un *ledger* público. La convergencia entre dispositivos IoT con recursos limitados, infraestructuras DLT distribuidas y requisitos regulatorios estrictos crea un panorama de amenazas complejo que debe abordarse mediante aproximaciones de seguridad en múltiples capas [103], [104].

En microcontroladores Cortex-M con Armv8-M, *TrustZone-M* permite particionar el sistema en dominios «Seguro» y «No seguro», con regiones *Non-Secure Callable* para invocaciones controladas. Este aislamiento a nivel de memoria (SAU/IDAU) facilita anclar el *root of trust*, custodiar claves y ejecutar verificaciones críticas sin exponerlas a la aplicación general, reduciendo de forma sustantiva la superficie de ataque del nodo IoT que alimenta el DPP [105], [106].

En primer lugar, los dispositivos IoT (sensores, *gateways*, etc.) suelen ser el eslabón más débil debido a sus limitaciones de *hardware* y energía. A menudo carecen de la capacidad de ejecutar cifrado fuerte de forma sostenida, pueden no tener entornos seguros para almacenar claves (como TPM), y su *firmware* puede quedar desactualizado si no se diseñan bien los mecanismos de actualización. Un atacante que comprometa un sensor de campo (insertando lecturas falsas de temperatura) podría, en teoría, inyectar datos erróneos en el DPP y dañar la credibilidad del sistema o hacer pasar productos de menor calidad como si hubieran cumplido condiciones ideales. Por ello, la seguridad a nivel de dispositivo debe incluir medidas como:

- Uso de módulos de *hardware* seguro (*Hardware Security Modules*, HSM) o al menos microcontroladores con zonas seguras para almacenar credenciales (claves privadas, *tokens* de red). De este modo, aunque alguien tenga acceso físico al dispositivo, le sea muy difícil extraer la información sensible para suplantarlos [107].
- Procesos de arranque seguro (*secure boot*), donde el dispositivo solo ejecute *firmware* firmado por la autoridad de confianza, previniendo *firmware* malicioso [107].
- Empaquetado a prueba de manipulaciones (*tamper-evident*): encapsular sensores de manera que abrirlos deje evidencia o incluso los desactive, lo cual desincentiva adulterarlos [108].
- Políticas de renovación de claves y credenciales en caso de sospecha de compromiso, para que un dispositivo comprometido no suponga riesgo permanente [108].

Además de las medidas anteriores, los nodos IoT están expuestos a ataques de canal lateral (análisis diferencial de potencia, medición de emisiones electromagnéticas) y a técnicas de inyección de fallos (*glitches* de reloj o caídas de tensión) que buscan extraer claves o forzar saltos en comprobaciones criptográficas. Estos ataques no requieren necesariamente abrir el dispositivo: es posible inferir material secreto observando consumo o emisiones durante operaciones de cifrado.

Como mitigación práctica en el contexto del DPP, conviene: (i) proteger rutinas criptográficas con implementaciones *constant-time* y enmascaramiento (*masking*); (ii) añadir desacoples y

detectores de *glitch/brown-out*; (iii) incorporar apantallamiento EM básico en el encapsulado del sensor o *gateway*; y (iv) combinar *tamper-evident* con sensores de intrusión (*tamper detection*) para invalidar credenciales si se detecta manipulación. Estas recomendaciones son coherentes con el enfoque de gestión de riesgos IoT planteado por NIST y guías industriales recientes [109]-[112].

En segundo lugar, las comunicaciones IoT, especialmente LoRaWAN, presentan vulnerabilidades específicas. LoRaWAN en su especificación ofrece encriptación de la carga de datos con claves compartidas (*AppSKey*) y una verificación de integridad a nivel de mensaje (MIC), pero es susceptible a ataques de *eavesdropping* (escucha pasiva) porque las transmisiones de radio pueden ser captadas por cualquiera en rango. Si bien lo captado va cifrado, un atacante podría hacer análisis de tráfico para inferir patrones (metadatos como cuándo y con qué frecuencia se envían datos). También existen los *replay attacks*, donde un intruso graba un mensaje legítimo y lo retransmite más tarde; LoRaWAN mitiga esto con contadores de *frame*, pero es crucial asegurar que los dispositivos no se resetean de forma que el contador vuelva a 0, porque entonces un *replay* podría «colar». Adicionalmente, los ataques de *jamming* (inhibición) son posibles: basta con emitir ruido en la frecuencia para impedir que los sensores comuniquen, lo que podría provocar pérdida de datos importantes (aunque no alteración, sí indisponibilidad). Para enfrentar estos retos, se debe asegurar la gestión adecuada de claves LoRaWAN (OTAA para que cada dispositivo tenga su sesión única y no se reutilicen claves entre dispositivos), monitorizar los contadores de *frame* y eventos de reintento para detectar posibles *replays* o clonaciones de dispositivos, en entornos críticos, podría duplicarse la transmisión por más de un canal o disponer de *backup* de conectividad (por ejemplo, un *gateway* que si detecta fallo en LoRa, conmuta a 4G si está disponible) [103].

Emplear un esquema de *criptografía híbrida* a nivel de aplicación: el dispositivo negocia un secreto compartido mediante *clave pública* (p. ej., ECDH/ECDHE sobre curvas eficientes) y cifra los datos con algoritmos simétricos autenticados (AES-GCM o ChaCha20-Poly1305). Este patrón evita cifrar cada paquete directamente con *clave pública* —ineficiente en IoT— y añade confidencialidad extremo a extremo incluso si un atacante conociera las claves de red LoRaWAN [109], [110].

Pasando a la capa del Pasaporte Digital en sí, la seguridad implica:

- Control de acceso robusto: para la autenticación y autorización por roles en el DPP, se propone un esquema de identidad descentralizada basado en *Decentralized Identifiers* (DID) y *Verifiable Credentials* (VC). Cada actor (personas, organizaciones y dispositivos IoT) dispone de un DID y presenta credenciales verificables que acreditan sus atributos (e.g., «veterinario colegiado», «inspector autorizado»). El visor del DPP validaría criptográficamente dichas credenciales y concedería acceso únicamente a las vistas de datos correspondientes al rol. Esta aproximación permite *privacy by design*, registro de auditoría verificable y evita dependencias de un punto único de confianza [103].
- Seguridad en la interfaz web/API: el portal o aplicación del DPP debe seguir las mejores prácticas (HTTPS obligatorio, protección contra inyecciones SQL/NoSQL, contra XSS y CSRF, etc.). Dado que estará posiblemente abierto a internet para consumidores, estará expuesto a *bots*, intentos de denegación de servicio (DoS), etc. Deberá dimensionarse la infraestructura para resistir tráfico malicioso y tener WAF (*firewall* de aplicaciones web) si

es necesario [104].

- Protección de datos personales: aunque un DPP de un jamón no contiene datos personales directamente (no es el pasaporte de una persona), podría incluir información de personas asociadas (un responsable de calidad, un veterinario certificador con nombre, etc.). En este marco, las VC permiten *verificación sin revelación*: el DPP puede demostrar al público que «la inspección ha sido firmada por un veterinario autorizado» sin exponer su identidad completa. El verificador comprueba la validez y vigencia de la credencial, mientras que el visor sólo muestra el atributo (rol) y un identificador no trazable. Este patrón reduce al mínimo el tratamiento de datos personales, refuerza la confidencialidad y facilita el cumplimiento de RGPD (minimización, limitación de la finalidad y necesidad de consentimiento) [107]. El visor público quedará como parte del MVP; mientras que las vistas por rol quedarán para trabajo futuro.

Finalmente, la integridad de los datos es la piedra angular: aquí entra la DLT. Como ya se diseña, cada dato crítico será firmado o *hasheado*. Concretamente, cada medición o evento importante debería llevar una firma digital generada por la entidad (o dispositivo) que lo produce. Por ejemplo, un sensor *edge gateway* puede firmar sus paquetes diarios de datos con su clave privada antes de almacenarlos; la industria que sube un certificado de calidad puede firmarlo; ASICI podría firmar los datos provenientes de ÍTACA. Estas firmas aseguran que aunque alguien intercepte y modifique datos en tránsito, la alteración será evidente al verificar la firma. Luego, al anclar *hashes* en la DLT, obtenemos una segunda capa de integridad: incluso si un atacante lograra alterar datos en la base de datos central del DPP (imaginemos que *hackea* el servidor y cambia la raza de un cerdo de 50 % a 100 %), no podría recomponer el *hash* original que está en IOTA, así que la discrepancia delataría el fraude [103].

Se debería planificar y tener en cuenta también la respuesta a incidentes: si, por ejemplo, se detecta que un dispositivo IoT fue comprometido y estuvo mandando datos falsos, el sistema debería marcar esos datos en el DPP como posiblemente corruptos (y quizás invalidar ciertas certificaciones vinculadas) hasta que se clarifique. Y en la DLT, se podría añadir anotaciones (transacciones posteriores) para advertir que X dato quedó invalidado por razones de seguridad, manteniendo la trazabilidad del incidente [104].

3.12. Requisitos y Criterios de Diseño

Tras este análisis exhaustivo del estado del arte, podemos extraer los requisitos funcionales y no funcionales clave, así como los criterios de diseño arquitectónico que deben guiar el desarrollo del DPP para el jamón ibérico. Estos requisitos y criterios buscan asegurar que la solución resultante cumpla con las expectativas técnicas, regulatorias y operativas identificadas.

3.12.1. Requisitos Funcionales

A partir de la integración de las áreas estudiadas, se formulan los siguientes requisitos funcionales (RF):

- RF1 – Integración con ÍTACA: el sistema DPP debe sincronizarse automáticamente con la base de datos ÍTACA, utilizando los códigos de precinto existentes como identificadores primarios de las piezas. Esto implica que, cuando un jamón se registre y certifique en ÍTACA, su DPP correspondiente se genere o actualice con esos datos, evitando duplicación de entradas de datos y manteniendo la consistencia con la información oficial regulatoria [94].
- RF2 – Ingesta de Datos IoT: capacidad de ingerir flujos de datos de alta frecuencia provenientes de sensores IoT desplegados en secaderos y otras instalaciones relevantes. Esto abarca mediciones de temperatura, humedad, circulación de aire, etc., con sus marcas de tiempo precisas y el identificador del lote o pieza al que corresponden. Debe soportarse *online* (datos en tiempo real) y también guardar históricos. Además, el sistema debe autenticar la fuente de estos datos para asegurar que provienen de dispositivos válidos [61].
- RF3 – Control de Acceso Multi-Rol: implementación de un control de acceso granular que permita diferentes niveles de visibilidad y acción según el rol del usuario, en correspondencia con las categorías de información definidas por ESPR. Por ejemplo, un consumidor (rol público) solo podrá ver la información categoría A de un producto; un operador profesional (rol empresa) tras autenticarse podrá acceder a categoría B de sus propios productos; un auditor o autoridad (rol regulador) podrá, con credenciales adecuadas, acceder a categoría C; y la categoría D no será visible salvo mediante pruebas criptográficas indirectas. El sistema debe gestionar registros de usuarios, autenticación segura (idealmente multifactor para roles críticos) y autorización por niveles [67].
- RF4 – Conformidad con Estándares GS1: el sistema debe ser totalmente conforme con los estándares GS1 pertinentes. Esto significa: usar identificadores GS1 (GTIN/SGTIN, GLN, etc.) para identificar entidades en los datos; estructurar los eventos de trazabilidad y datos transaccionales según el estándar EPCIS 2.0 (formato JSON-LD, vocabularios de GS1); e implementar la interfaz de identificación de productos mediante GS1 Digital Link (códigos QR que encapsulen AI y puedan resolver a la URL del DPP de la pieza). Esta conformidad garantizará interoperabilidad con sistemas de otros sectores y con futuras iniciativas de la UE [63], [65].
- RF5 – *Audit Trail* Inmutable: el sistema debe proporcionar una pista de auditoría (*audit trail*) inmutable de todas las modificaciones de datos y de los accesos a información sensible. Cada vez que se añada o modifique información en un pasaporte, debe quedar registrado quién lo hizo, cuándo, y qué cambio se realizó. Asimismo, se debe registrar cualquier intento de acceso a información de categorías restringidas. Idealmente, parte de esta *audit trail* (por ejemplo, el *hash* de un registro de actualización) también podría anclarse en la DLT para que ni siquiera administradores puedan alterarla sin dejar rastro [103].
- RF6 – Integración de Notarización IOTA: como corolario de la elección tecnológica, el DPP debe utilizar el *framework* IOTA Notarization para anclar huellas criptográficas de los datos críticos. Esto significa que para cada evento de trazabilidad relevante (nacimiento, sacrificio, precintado, lecturas agregadas de curación, expedición, etc.) se generará una huella (*hash*) que se almacenará en la Tangle de IOTA, obteniendo una prueba de integridad. Cualquier usuario debe poder verificar, a través de la interfaz DPP, que ciertos datos están asegurados en IOTA. La integración debe ser tal que no entorpezca el funcionamiento, pero que esté siempre actualizada con los últimos datos [80].

3.12.2. Requisitos No Funcionales

Más allá de las funcionalidades, el sistema debe cumplir ciertos requisitos de calidad (RNF) para ser viable en un entorno real:

- RNF1 – Escalabilidad: el sistema debe soportar un crecimiento significativo en volumen de productos y datos sin degradación notable del rendimiento. Inicialmente podría manejar, digamos, decenas de miles de piezas, pero debe diseñarse para escalar hasta cientos de miles o millones de productos concurrentemente, considerando futuros escenarios donde quizás no solo jamones ibéricos sino otros productos cárnicos de calidad adopten DPP similares. La arquitectura debe ser escalable horizontalmente (añadiendo más nodos de procesamiento, más instancias de base de datos, etc. según demanda) [86].
- RNF2 – Disponibilidad: puesto que uno de los objetivos es que consumidores y actores puedan consultar la información en cualquier momento, se aspira a una disponibilidad del 99,9 % en las interfaces de acceso de consumidores (página web pública, resolución de QR, etc.). Esto implica tener redundancia (no un único punto de fallo) y planes de recuperación ante desastres. En caso de que la red DLT subyacente experimente problemas o congestión, el sistema DPP debe degradar su funcionalidad de forma elegante (por ejemplo, mostrando los datos almacenados localmente y marcando que la verificación en DLT está temporalmente no disponible, en lugar de simplemente fallar) [104].
- RNF3 – Tiempo de Respuesta: las consultas típicas de consumidores (por ejemplo, escanear un QR en el móvil y cargar el pasaporte digital de un jamón) deben resolverse en menos de 4 segundos bajo condiciones normales de carga. Esto requiere optimizaciones de *caché*, CDN para elementos estáticos, y quizás precálculo de ciertas vistas. Para información muy detallada o pesada, se puede emplear carga progresiva (mostrar primero lo esencial y luego permitir que el usuario explore más datos con cargas adicionales bajo demanda) [61].
- RNF4 – Eficiencia de Coste: los costes operativos del sistema deben mantenerse en un rango asumible por la industria. Como referencia, podríamos establecer que el coste por producto (por ejemplo, por cada jamón a lo largo de toda su vida en el sistema) no exceda los 0,60 € anuales en promedio (máximo estipulado en la extensión de la Norma de Calidad del Ibérico) [10]. Esto englobaría costos de infraestructura *cloud*, mantenimiento de nodos DLT, etc. Un diseño basado en tecnologías *open source* (como IOTA, Hyperledger, etc.) y desplegado en infraestructura escalable ayudará a esto. También se buscarán posibles apoyos públicos ya que se alinea con objetivos regulatorios.
- RNF5 – Seguridad: debe implementarse un conjunto de controles de seguridad que cumplan tanto con el marco europeo de ciberseguridad (e.g., directiva NIS2 si aplicase, o recomendaciones ENISA para IoT) como con las expectativas de protección de datos y resiliencia. Esto implica *pentesting* periódico de la aplicación, monitoreo de intrusos, cifrado de datos en reposo para datos sensibles, políticas estrictas de gestión de secretos (API keys, claves privadas de firma, etc.), y cumplimiento de estándares como ISO 27001 a medio plazo si el sistema escala. Además, para lo referente a privacidad, se deben anonimizar o no recolectar datos personales innecesarios (principio de minimización RGPD) [107].

3.12.3. Criterios de Diseño Arquitectónico

Con base en los requisitos anteriores, se formulan criterios de alto nivel que orientarán las decisiones de diseño arquitectónico (CD):

- CD1 – Arquitectura Híbrida (Centralizada + Distribuida): se optará por una arquitectura híbrida que combine lo mejor de los sistemas centralizados existentes con una capa de verificación distribuida. En la práctica, ÍTACA (centralizado) seguirá manejando ciertos datos regulatorios y el DPP tendrá bases de datos relacionales/noSQL propias para los datos enriquecidos, pero la verificación de integridad se realizará en IOTA (distribuida). Este patrón permite aprovechar inversiones y datos existentes (evitando reinventar toda la rueda) a la vez que añade las garantías de transparencia e inmutabilidad que aporta la DLT [94].
- CD2 – Diseño *API-First*: todos los componentes del sistema expondrán API bien documentadas y estables para facilitar la integración con terceros y la extensibilidad futura. Por ejemplo, una API *REST* para consultar el DPP de un producto, una API para que los productores suban datos de sostenibilidad, otra para que ASICI sincronice datos, etc. Esto no solo permite conectar fácilmente aplicaciones (móvil, web) al *backend*, sino que sienta las bases para que en el futuro otros servicios (e.g., el portal público de la UE de pasaportes digitales) puedan consumir la información de nuestro sistema sin grandes adaptaciones [63].
- CD3 – *Progressive Enhancement*: se seguirá el principio de mejora progresiva en las interfaces de usuario, es decir, la funcionalidad básica (mostrar la información esencial del pasaporte) debe estar disponible incluso en entornos limitados (si un usuario tiene un móvil antiguo o mala conexión, al menos ver datos clave de origen y calidad). Funcionalidades avanzadas (gráficos interactivos de temperaturas, mapas, vídeos) se añadirán sobre esa base de forma que usuarios con mejores dispositivos o conexiones tengan una experiencia enriquecida, pero sin perjudicar la accesibilidad general. También implica que la falta temporal de conexión a DLT no impida ver datos ya registrados (solo la verificación estará ausente en ese momento) [61].
- CD4 – Soberanía de los Datos (*Data Sovereignty*): cada operador (ganadero, industria, etc.) debe mantener control sobre sus propios datos en la medida de lo posible, de acuerdo al principio de soberanía de datos. En la implementación práctica, esto significa que aunque el DPP consolide datos de muchos actores, cada pieza de información crítica irá firmada por la entidad que la generó. Así, la propiedad intelectual y la responsabilidad de esa información se mantienen en quien corresponde. Además, si un operador decide dejar de participar, se debería poder revocar o congelar su aporte de datos (aunque las huellas en la DLT quedarán como registro histórico). Este criterio también facilita el cumplimiento del ESPR de que los operadores gestionan sus datos de forma descentralizada [67].
- CD5 – Neutralidad Tecnológica y Evitar *Vendor Lock-in*: la arquitectura debe evitar dependencia excesiva de proveedores o soluciones propietarias que pudieran comprometer la flexibilidad futura. Siempre que sea viable, se usarán componentes *open source* y estándares abiertos. Por ejemplo, en la nube se podría optar por contenedores y *Kubernetes* para poder migrar entre proveedores, en lugar de servicios altamente propietarios. En DLT,

usar IOTA, *open source*, en vez de una *blockchain* privada de alguna empresa garantizará que, a medida que la tecnología avance, se pueda evolucionar o reemplazar componentes sin rehacer todo el sistema (por ejemplo, si en 5 años surge un nuevo estándar de DPP europeo obligatorio o hay un cambio inesperado de definición del DPP, podríamos adaptarnos integrando sus protocolos, en lugar de quedar atrapados en un diseño inflexible) [86].

- CD6 – Cumplimiento de Estándares: este criterio refuerza formalmente que en cada decisión se dará preferencia a la opción que garantice alineamiento con estándares reconocidos, ya sea en formatos de datos (JSON-LD, GS1 EPCIS), en comunicación (HTTPS, MQTT), en seguridad (OAuth2, JWT para *tokens* de sesión, etc.), o en etiquetado (GS1 Digital Link). Esto no solo facilita la interoperabilidad, sino también la certificación y aceptación del sistema por terceros. Un DPP que «habla» el idioma de la industria será mucho más fácilmente adoptado que uno totalmente ad-hoc [63].

En conjunto, estos requisitos y criterios de diseño constituyen la base técnica para el desarrollo del Pasaporte Digital de Producto del jamón ibérico. Guiarán las próximas fases de diseño detallado, asegurando que la solución resultante sea técnicamente sólida, cumpla con la normativa vigente y sea operacionalmente viable en el contexto real del sector ibérico, teniendo en cuenta a todos sus actores, desde las grandes empresas hasta los artesanos locales. Con este marco claro, se puede avanzar hacia la definición de la arquitectura específica de la solución y su posterior implementación.

Capítulo 4

DISEÑO DEL DPP

En este capítulo se presenta el diseño completo y detallado del sistema de Pasaporte Digital de Producto para el jamón ibérico, dando continuidad a los capítulos previos. Partiendo de los requisitos funcionales y no funcionales identificados en la sección 3.12, se define la arquitectura y modelo de datos propuestos, junto con las decisiones técnicas adoptadas.

El diseño abarca la estructura del DPP (campos mínimos, eventos y capas de información alineadas con estándares GS1/EPCIS), la arquitectura del sistema (integración de sensores IoT, pasarelas, base de datos *off-chain*, integración con la Tangle de IOTA, API de ingesta de datos y *front-ends* específicos por rol de usuario), así como consideraciones de gobierno del sistema e identidad descentralizada (roles, registro de confianza, DID, credenciales verificables y control de acceso).

Todo ello se plantea con tecnologías modernas, robustas y replicables tanto por pequeñas y medianas empresas jamoneras como por grandes productores, asegurando que el diseño aquí definido pueda implementarse como un prototipo funcional en el capítulo 5. A continuación se describen en detalle cada uno de estos aspectos del diseño, incluyendo ejemplos ilustrativos. Se fundamenta la elección técnica teniendo en cuenta la viabilidad práctica (por ejemplo, frecuencia y alcance de sensores, comunicaciones IoT, almacenamiento de datos) y el cumplimiento de los requisitos y criterios de diseño planteados en capítulos anteriores.

4.1. Modelo de Datos del DPP

El modelo de datos del Pasaporte Digital de Producto para el jamón ibérico se ha diseñado siguiendo un enfoque mínimo pero completo, alineado con estándares internacionales para garantizar la interoperabilidad. En esencia, el DPP consolida información de trazabilidad, calidad y sostenibilidad de cada pieza de jamón ibérico a lo largo de todo su ciclo de vida, estructurada en eventos y atributos estáticos, y organizada en distintos niveles o capas de accesibilidad.

A continuación se describen los componentes principales de este modelo de datos: los identificadores únicos de producto, los eventos de trazabilidad EPCIS (incluyendo campos

mínimos por evento) y las capas de información del pasaporte.

4.1.1. Identificación Única de Productos y Entidades (GS1)

Para identificar inequívocamente cada pieza de jamón en el sistema, se adopta el esquema de identificación global de GS1. En concreto, se propone utilizar códigos GTIN (*Global Trade Item Number*) combinados con números de lote y/o serie, tal como recomienda GS1 para dotar de identificadores únicos a nivel de item [17].

Un GTIN identifica la referencia comercial o tipo de producto (por ejemplo, «Jamón 100 % Ibérico de Bellota DOP de 7kg, productor X»), mientras que un número de serie distingue una unidad individual dentro de esa referencia. De este modo, la pareja GTIN + *Serial* (o GTIN + Lote + un identificador de pieza dentro del lote) proporciona un ID global único para cada jamón, válido en cualquier parte del mundo y persistente a lo largo del tiempo. En la práctica, dado que en el sector ibérico ya se emplean precintos físicos con códigos únicos por pieza, dichos códigos pueden mapearse a un GTIN de producto más un número de serie. Por ejemplo, si el precinto «PZ001-LOTE123» identifica una pieza, podríamos asignarle GTIN = 08412345123456 (correspondiente al producto genérico) y *Serial* = PZ001, con Lote = LOTE123 como dato asociado.

En el DPP, cada pieza de jamón tendrá entonces un identificador estructurado que incluye:

- GTIN: código numérico de 14 dígitos que identifica el tipo de producto. Ejemplo: 08412345123456.
- Número de lote (cuando aplique): identificador del lote de producción al que pertenece la pieza. Ejemplo: LOTE123.
- Número de serie O pieza: código único de la pieza dentro del lote o dentro de la producción del productor. Ejemplo: PZ001.

Estos identificadores se integrarán en la URL del pasaporte digital utilizando la sintaxis estándar de GS1 Digital Link; que permite encapsular en una URL web tanto el GTIN como otros identificadores (lote, serie, fechas, etc.) de forma que al escanear un código QR con esa URL, cualquier aplicación pueda resolverla y obtener la información del pasaporte. Por ejemplo, una URL de Digital Link impresa en el precinto podría ser:

<https://dpp.jamon.io/01/08412345123456/10/LOTE123/21/PZ001>

Donde:

- /01/08412345123456 corresponde al GTIN (AI 01 de GS1).
- /10/LOTE123 corresponde al lote (AI 10 de GS1).

- /21/PZ001 corresponde al número de serie de la pieza (AI 21 de GS1) .

Esta URL es resoluble por el servidor del DPP para mostrar la información de esa pieza concreta, y además es entendible por cualquier otro sistema que soporte GS1 Digital Link, garantizando interoperabilidad. Cabe destacar que Digital Link permite pedir distintas representaciones añadiendo sufijos a la URL (e.g., .json para obtener los datos en JSON directamente, .html para una página web, etc.), lo cual se alinea con la filosofía de datos abiertos e interconectados del ESPR.

Además del GTIN para productos, el sistema utilizará otros identificadores GS1 donde sea pertinente, por ejemplo:

- GLN (Global Location Number): para identificar ubicaciones físicas o instalaciones relevantes en la cadena (granjas, mataderos, secaderos, almacenes, etc.) [17]. Cada ubicación clave tendrá su GLN, de modo que los eventos de trazabilidad puedan referenciar origen y destino estandarizados.
- GS1 Party ID (basado en GLN u otro identificador): para identificar actores/organizaciones (productores, transformadores, distribuidores). Alternativamente, podrían usarse DIDs para actores (ver sección 4.2.3), pero se mantendrá una correspondencia con códigos tradicionales para interoperabilidad con sistemas legados.
- GRAI/GIAI: para identificar activos retornables o específicos si los hubiera (como jaulas de transporte), aunque en el alcance actual del DPP de jamón no es crítico.

En resumen, el modelo de datos se sustenta sobre identificadores globales únicos GS1 para asegurar que cada dato del pasaporte se refiere sin ambigüedad al objeto correcto (producto, lugar, actor). Basar el DPP en identificadores GS1 aporta compatibilidad inmediata con sistemas de trazabilidad de otros sectores y países, preparando el camino para una integración en la visión europea de pasaportes digitales unificados.

No dependemos de códigos propietarios o locales, sino de un lenguaje común ampliamente adoptado (más de un millón de empresas usan GS1). Esto cumple con el mandato del ESPR de usar estándares abiertos y reconocidos para garantizar la interoperabilidad técnica entre pasaportes digitales de distintos orígenes.

4.1.2. Entidades y Relaciones del Modelo de Trazabilidad Ibérica (RD 4/2014)

El modelo de datos del DPP debe capturar no solo la pieza final (jamón o paleta), sino toda la cadena de entidades y procesos exigidos por el Real Decreto 4/2014 (Norma de Calidad del Ibérico) y el sistema ÍTACA [7], [10]. Esto incluye entidades relacionadas con el cerdo vivo, su alimentación, sacrificio, transformación y curado, garantizando la trazabilidad completa desde la explotación ganadera hasta el producto final.

Las entidades principales del modelo son:

1. Cerdo vivo (animal individual): identificado por crotal o ID oficial (registrado en ÍTACA), con atributos de pedigrí (porcentaje ibérico: 100 %, 75 %, 50 %), fecha de nacimiento, explotación de origen (GLN), y genealogía (padres registrados en libros genealógicos) [10].
2. Lote de explotación: agrupación de cerdos nacidos en una explotación bajo condiciones similares. Atributos: GLN de la explotación, fecha de constitución del lote, tipo de manejo (extensivo/intensivo).
3. Lote de alimentación: subconjunto de cerdos con alimentación homogénea (bellota, cebo de campo, cebo). La Norma exige registrar período de montanera (inicio, fin, duración mínima 60 días), peso inicial y final del animal, y recursos consumidos (bellota/pasto o pienso con DPP si procede) [7], [10].
4. Dehesa/Finca (para bellota y cebo de campo): ubicación geográfica (GLN) donde se realiza la montanera o engorde extensivo. Atributos: superficie (ha), densidad de carga (cerdos/ha conforme a normativa DOP/IGP si aplica), registros ambientales opcionales (clima, producción de bellota estimada).
5. Lote de sacrificio: conjunto de animales sacrificados en una misma sesión de matadero. Atributos: GLN del matadero, fecha/hora de sacrificio, veterinario oficial (DID o identificación), resultados de inspección sanitaria («apto»/«no apto»).
6. Pieza cruda (jamón/paleta post-sacrificio): resultado del despiece de la canal. Cada pieza hereda la trazabilidad del animal («cerdo ID» pasa a «pieza ID» mediante EPCIS TransformationEvent). Atributos: peso inicial, clasificación (grasa dorsal, conformación), asignación de lote de salazón.
7. Lote de productos (elaborados): agrupación de piezas que comparten proceso de curado (mismo secadero, misma sala, mismo período). Atributos: GLN del secadero/bodega, fechas de inicio/fin de salado, postsalado, secado y maduración, condiciones ambientales agregadas (temperatura media, humedad media, desviaciones si las hubiera).
8. Jamón/Paleta final (producto con DPP): entidad principal del pasaporte. Identificada por GTIN+serial (precinto ÍTACA = AI 21). Hereda toda la trazabilidad anterior vía eventos EPCIS. Atributos finales: categoría según RD 4/2014 (bellota 100 % ibérico, bellota ibérico 75 %/50 %, cebo de campo ibérico, cebo ibérico), precinto de color (negro/rojo/verde/blanco), tiempo total de curado, peso final, merma porcentual, certificaciones (DOP/IGP si aplica, sello de calidad, certificado veterinario final).
9. Documentos y evidencias (almacenados en IPFS): certificados sanitarios, análisis de laboratorio (pH, a_w , composición), certificados de conformidad DOP/IGP, registros fotográficos de la dehesa o del proceso, análisis de ciclo de vida (ACV) si se realiza. Cada documento genera un CID de IPFS, anclado en IOTA para verificación de integridad [88], [113].
10. Eventos EPCIS 2.0: modelan las transiciones entre entidades. Los principales tipos de eventos son [114]:
 - ObjectEvent: nacimiento del cerdo, entrada a montanera, fin de montanera, entrada a curado, fin de curado, precintado, expedición.

- TransformationEvent: sacrificio (cerdo vivo en piezas crudas: jamones, paletas, etc.).
 - AggregationEvent: formación de lotes (animales en lote de explotación, piezas en lote de productos para curado conjunto).
 - TransportationEvent: traslados (dehesa a matadero, matadero a secadero, secadero a distribuidor, distribuidor a comercio minorista) [115].
11. Operador económico (roles): productor/ganadero, matadero, industria de curado, distribuidor, comercializador/minorista, organismo certificador (DOP/IGP), veterinario autoridad, auditor/inspector, administrador del sistema DPP. Cada uno identificado por GLN o DID (identidad descentralizada) según corresponda.

Reglas de asociación de datos ambientales: los datos de sensores IoT (temperatura, humedad, circulación de aire durante curado) se asocian a GLN + periodo (por ejemplo, «Secadero GLN:8412345000019, del 2023-01-15 al 2025-01-15»), no a cada pieza individual, evitando duplicación masiva de datos. Cada pieza del mismo lote referencia el mismo conjunto de datos ambientales mediante el evento EPCIS de curado, que incluye el GLN de la bodega y las fechas, permitiendo al sistema recuperar los datos de sensores correspondientes [7], [10].

Conformidad con RD 4/2014: este modelo captura las entidades y relaciones exigidas por la normativa sectorial [10], garantizando que el DPP pueda demostrar:

- Pureza racial del cerdo (pedigrí verificable).
- Tipo de alimentación y cumplimiento de requisitos de montanera (período mínimo, incremento de peso para peso mínimo).
- Trazabilidad completa desde explotación de nacimiento hasta producto final.
- Cumplimiento de especificaciones de curado (tiempo mínimo según categoría).
- Certificaciones oficiales (precinto de color, DOP/IGP).

Esta estructura de datos garantiza interoperabilidad con el sistema ÍTACA (intercambio de eventos vía API o sincronización periódica) y extensibilidad para incorporar en el futuro otras especies o productos cárnicos de calidad diferenciada.

4.1.3. Eventos de trazabilidad EPCIS 2.0 y campos mínimos

La información dinámica de la vida de cada jamón («desde la granja hasta el consumidor») se modela mediante eventos de trazabilidad siguiendo el estándar GS1 EPCIS 2.0.

EPCIS (*Electronic Product Code Information Services*) proporciona un modelo de datos estándar para capturar qué ocurrió, cuándo, dónde y por qué en cada punto de la cadena de suministro. Al utilizar EPCIS estructuramos los datos de eventos de forma rica y estandarizada, facilitando tanto el intercambio con terceros como la comprensión unificada de la trazabilidad.

En el caso del DPP del jamón ibérico, se han identificado los tipos de eventos EPCIS principales que deben registrarse, alineados con las etapas definidas en la normativa sectorial (RD 4/2014) y en el sistema ÍTACA. A continuación enumeramos estos eventos clave, junto a los campos mínimos que cada uno contendrá en nuestro modelo de datos

1. Evento de nacimiento/cría del animal. Registra información del nacimiento de un cerdo destinado a la producción de jamón.

Campos:

- ID del animal (e.g., un arete o identificador oficial), podría enlazarse con un ID de ÍTACA.
- Fecha.
- Lugar de nacimiento (GLN de la granja).
- Raza.
- Genealogía relevante.
- Identificación del ganadero.
- Motivo/*Business step*: "producción primaria iniciada".

Ejemplo: *Cerdo #123 nacido el 05/03/2020 en Finca Los Encinos (GLN 8435123450005), raza 100 % ibérico, ganadero DID:ASICI-GAN-001".*

2. Evento de engorde/montanera. Registra el periodo de engorde inicial y final en montanera (si aplica para bellota) u otras fases de alimentación. Este evento puede resumir datos, no es continuo.

Campos:

- ID del grupo de animales o corral.
- Fechas de inicio de montanera.
- Fechas de fin de montanera.
- Peso al inicio de la montanera.
- Peso al fin de la montanera.
- Ubicación (GLN de la dehesa/granja).
- Tipo de alimentación (bellota, cebo de campo, cebo). Aquí cabe incluir DPP de piensos cuando corresponda.
- Observaciones de bienestar animal si las hay.
- Motivo: "proceso de engorde completado".

3. Evento de sacrificio y despiece. Marca que el cerdo fue sacrificado y despiezado en matadero. Campos:

- ID del matadero (GLN).
- Fecha/hora de sacrificio.
- Lote de sacrificio.

- Resultados de inspección veterinaria (apto/no apto).
- Identificadores de las piezas resultantes (e.g., Jamón izquierdo #XYZ).
- Motivo: *"transformación"* (input: animal vivo, output: pieza cruda).

4. Evento de salado. Indica que una pieza (un pernil) comience y termina el proceso de salazón.

Campos:

- ID de la pieza (GTIN+serial).
- Peso de las piezas previas a entrar en salazón.
- Instalación de salado (GLN).
- Fecha/hora de inicio de salado.
- Fecha/hora de fin de salado.
- Duración.
- Parámetros clave (temperatura, concentración salina, etc. si se miden).
- Motivo: *"procesamiento en salazón"*.

5. Evento de postsalado/asentamiento. Similar al anterior, registra el paso por cámaras de post-salado.

Campos:

- ID de la Pieza.
- Peso de las piezas tras el lavado.
- Merma.
- Localización.
- Fechas inicio.
- Fechas fin.
- Duración del salado.
- Motivo: *"procesamiento en salazón"*.

6. Evento de curado. Registra el período en bodega/secadero natural.

Campos:

- ID de la Pieza.
- Bodega (GLN).
- Fecha inicio de curado.
- Fecha fin de curado.
- Duración total.
- Resumen de datos de sensores del microclima durante ese periodo (temperatura media, humedad media, valores mínimo y máximo alcanzados)¹.

¹La captura de datos IoT continua se detalla en la sección 4.2.2, en el evento se adjuntará un resumen o *hash* de la serie temporal relevante

- Motivo: "*curación completada*".

7. Evento de clasificación y precintado. Representa la inspección y precintado oficial tras la curación.

Campos:

- ID de la Pieza.
- Fecha de inspección.
- Resultado de la inspección.
- Código de precinto asignado (que se corresponde con el identificador GS1 usado en el DPP).
- Inspector o entidad que certifica (DID o identificación de autoridad competente, e.g., ASICI).
- Cualquier certificado emitido (e.g., acta de certificación firmada).
- Motivo: "*inspección/certificación*".

8. Evento de expedición. Indica un movimiento de salida de la pieza hacia distribución o venta.

Campos:

- ID de la Pieza.
- Fecha de expedición.
- Origen (GLN secadero).
- Destino (GLN almacén distribuidor o tienda).
- Número de lote de expedición o pedido.
- Identificador del transportista o del camión.
- Motivo: "*envío*" (*shipping*).

9. Evento de recepción/venta. Marca la recepción en tienda o la venta final.

Campos:

- ID de la Pieza.
- Fecha de recepción en punto de venta (GLN tienda), o fecha de venta al consumidor final (poco probable).
- Identificación del destinatario (para B2B) o indicación de venta minorista.
- Motivo: "*recepción*" o "*venta*".

10. Eventos de post-venta (circulares). Aunque la regulación aún no obliga, conceptualmente el DPP puede incorporar eventos tras la venta: registro de devolución para reciclaje (envases) o análisis de calidad post-venta (para propósitos de marketing). Se deja preparado este nivel, pero no se detalla por estar fuera del alcance inmediato (mencionado como posibilidad futura).

Cada evento EPCIS en formato JSON-LD incluirá campos estándar:

- `eventType` (ObjectEvent, TransformationEvent, etc. según corresponda).
- `eventTime` (timestamp ISO8601).
- `eventTimeZoneOffset` (timestamp ISO8601).
- `bizStep` (paso de negocio, e.g., `urn:epcglobal:cbv:bizstep:processing` para sa-lado, `:shipping` para expedición, etc.).
- `disposition` (estado resultante si aplica, por ejemplo, `:active` mientras está en curación, `:expired` si caducara, etc.).
- `epcList` (lista de códigos EPC de los objetos involucrados; aquí iría el URI de la pieza, por ejemplo `urn:epc:id:sgtin:8412345.012345.PZ001` equivalente al GTIN+serie).
- `sourceList` y `destinationList` para eventos de transferencia (en expedición, fuente = GLN origen, destino = GLN destino).
- `ilmd` (Información adicional como temperatura, humedad promedio en curado, etc., que no afectan la identidad del evento pero aportan datos de calidad).
- `certifications` (en nuestro caso, añadiríamos extensión para enlazar certificados o documentos, como el *hash* de un certificado veterinario o de clasificación, almacenado *off-chain* e.g., en IPFS).

Este esquema sigue las recomendaciones de EPCIS 2.0, que ya soporta JSON-LD permitiendo contexto semántico (ontologías GS1) para los datos. Por ejemplo, un evento de curado podría serializarse como (simplificado):

```
{
  "@context": [ "https://gs1.org/EPCIS/context.jsonld" ],
  "type": "ObjectEvent",
  "eventTime": "2023-08-01T00:00:00.000Z",
  "eventTimeZoneOffset": "+02:00",
  "epcList": [ "urn:epc:id:sgtin:08412345.012345.PZ001" ],
  "action": "OBSERVE",
  "bizStep": "urn:epcglobal:cbv:bizstep:storing",
  "disposition": "urn:epcglobal:cbv:disp:active",
  "readPoint": { "id": "urn:epc:id:sgln:08412345.00001.0" },
  "bizLocation": { "id": "urn:epc:id:sgln:08412345.00001.0" },
  "ilmd": {
    "example:avgTemp": 18.5,
    "example:avgHumidity": 70.2,
    "example:durationDays": 365
  },
  "example:batchHash": "zQm...abc"
}
```

Código 4.1: Ejemplo simplificado de evento EPCIS 2.0.

En este ejemplo, el `readPoint` y `bizLocation` usan un GLN (formato SGLN en EPCIS) que identifica la bodega de curado; `avgTemp` y `avgHumidity` son campos de ejemplo añadidos

para ilustrar cómo incluiríamos información sensorial agregada; `batchHash` podría ser un *hash* (en IPFS u otro) que vincula a datos completos de sensores o certificado del lote durante curado. Nótese que todos los identificadores (GTIN, GLN) se expresan en URN estándar.

El diccionario de campos mínimos para cada tipo de evento se resumirá en una tabla indicando: tipo de evento, significado, campos clave incluidos, y a qué capa de información pertenecen (A, B, C o D).

En conclusión, el modelo de datos del DPP captura la trazabilidad mediante eventos EPCIS normalizados, garantizando que otros sistemas puedan entender e incluso verificar independientemente la información. Por ejemplo, una autoridad podría tomar los eventos EPCIS exportados del DPP de un jamón e importarlos en sus propias herramientas sabiendo que siguen el estándar GS1, lo que facilita auditorías e interoperabilidad. Asimismo, el uso de ontologías GS1 (y potencialmente complementos como *schema.org* para ciertos atributos de sostenibilidad) proporciona semántica común: todos los actores interpretan «fecha de producción» o «lote de materia prima» de la misma forma. Esta semántica compartida es crucial para un DPP escalable globalmente.

4.1.4. Capas de Información y Organización por Niveles de Acceso

El diseño del DPP contempla distintas capas de información organizadas por niveles de sensibilidad y público objetivo, conforme a las directrices del ESPR y a la lógica de control de acceso por roles. Cada dato o campo del pasaporte se clasifica en una de estas capas o niveles, lo cual determina quién puede verlo. De esta manera se logra un equilibrio entre transparencia y confidencialidad, mostrando a cada usuario solo la información pertinente.

Basándonos en las categorías propuestas por la Comisión Europea y adaptándolas al contexto del jamón ibérico, definimos cuatro niveles de información en el DPP:

- Categoría A (Información Pública para Consumidores). Datos accesibles abiertamente a cualquier persona que escanee el código del DPP, sin necesidad de autenticación. Incluye la información básica del producto y atributos de interés general:
 - Identificación básica: tipo de producto (Jamón 100 % Ibérico de Bellota DOP), fabricante/marca (DOP Los Pedroches, 5J, Joselito), certificaciones de calidad o sostenibilidad obtenidas (etiqueta ecológica, bienestar animal), año de producción, etc.
 - Indicadores de sostenibilidad: huella de carbono estimada de la pieza, consumo hídrico, porcentaje de materiales plásticos reutilizados, porcentaje de energía renovable usada en el proceso, emisiones de CO₂, etc.
 - Sugerencias de uso y conservación: recomendaciones de corte, consumo preferente, conservación.
 - Datos de trazabilidad resumidos: procedencia (dehesa de origen, provincia), tiempo total de curación, categoría de alimentación (bellota, cebo de campo o cebo), resultado de la inspección («Precinto Negro – Bellota 100 % Ibérico»).

- Instrucciones de disposición final del producto (envase, hueso) o reciclaje (difícilmente aplicable a productos alimenticios).
- Precio.
- DPP de sales y/o piensos utilizados (en caso de alimentación de cebo o cebo de campo).

Esta información debe mostrarse de manera amigable al consumidor medio, posiblemente con iconos o gráficos, y se alinea con lo descrito como Categoría A por el reglamento. Un consumidor con solo escanear el QR obtendrá estos datos inmediatamente, ya que están en la capa pública.

- **Categoría B (Información para Actores de la Cadena de Suministro).** Datos más técnicos o detallados destinados a usuarios profesionales (productores, distribuidores, minoristas) u otros actores cualificados. Requiere autenticación y estar autorizado como parte interesada en la cadena:
 - Detalles de producción: composición exacta (porcentaje de sal usado, aditivos si los hubiera, tipos y porcentajes de mezclas de piensos utilizados si los hubiera), parámetros técnicos de curación (curvas de temperatura/humedad más detalladas), resultados de controles de calidad internos, etc.
 - Historial de mantenimiento o incidencias: si por ejemplo hubo una incidencia en cámara (un fallo eléctrico que alteró la temperatura durante 2 días y fue luego subsanado), podría registrarse aquí.
 - Documentos de cumplimiento normativo técnico: análisis de laboratorio (contenido de sal, actividad de agua [a_w], nitratos), certificados sanitarios completos emitidos en matadero, registros de limpieza y desinfección del secadero, etc.
 - Información logística: trazas de transporte más granulares, fechas y horas de emisión y recepción en almacenes intermedios.

Estos datos corresponden a una categoría restringida similar a la B del ESPR, que un consumidor común no necesita o no sabría interpretar, pero que son valiosos para auditores internos, distribuidores, o incluso técnicos de importadores que quieran verificar condiciones exactas. Por ejemplo, un distribuidor autorizado podría acceder al gráfico completo de temperatura durante los 2 años de curado para asegurarse de la calidad, mientras que eso sería excesivo e innecesario para un consumidor.

- **Categoría C (Información Confidencial para Autoridades).** Datos altamente sensibles o completos de trazabilidad que solo autoridades reguladoras o auditores externos designados deberían poder consultar. Incluye:
 - Trazabilidad completa nominal: la lista exhaustiva de todos los proveedores y lotes involucrados (como por ejemplo la identificación de cada cerdo con su ganadero, datos que quizás están protegidos por privacidad, la lista de lotes de pienso utilizados con sus composiciones, etc.).
 - Información sanitaria detallada: tratamientos veterinarios administrados a los animales (antibióticos, con fechas de retirada y su DPP), resultados de cada inspección veterinaria individual en el matadero (no solo el certificado final sino todos los datos brutos).

- Datos personales sensibles: nombre del ganadero asociado a una partida (en vez de solo un código), datos de empleados responsables de cada lote, etc., si es que se recogen.
- Cualquier información sujeta a regulación estricta (datos del árbol genealógico, si hubiera datos de ADN para autenticidad del animal, o detección de sustancias prohibidas o REACH, etc.).

Esta capa corresponde a lo que el ESPR denomina Categoría C, accesible solo con credenciales especiales (e.g., un inspector de la autoridad competente con su identificación digital). En nuestro sistema, la autenticación de esta capa se implementa mediante credenciales verificables emitidas por la autoridad (ASICI u organismo público) que confieren permisos de «rol regulador» (ver 4.2.3).

- Categoría D (Información Privada con Prueba Criptográfica). Hemos añadido esta categoría interna para datos que, por su naturaleza, no deben ser visibles directamente ni siquiera para autoridades en la interfaz del DPP, pero cuya existencia e integridad se desea poder probar. Se trata de un nivel «solo comprobable vía *hash* o firma»:
 - Puede incluir datos personales no relevantes para el pasaporte pero que quedan ligados de alguna forma (un *hash* de la identidad del matarife, o de registros contables relacionados) solo para tener constancia.
 - Secretos comerciales o fórmulas internas: por ejemplo, si un productor emplea una técnica particular de curación que no quiere divulgar, podría representarse con un documento sellado cuyo *hash* está en el DPP. Nadie ve el contenido, pero ante una disputa futura se podría revelar y verificar que estaba registrado.
 - Datos que por regulación de privacidad no pueden compartirse pero conviene mantener referenciados: si hubiera datos de geolocalización muy precisos de los animales durante la montanera, quizás no se exponen, pero se guarda un *hash* para demostrar que se tienen registros.

En definitiva, la categoría D actúa como capa «de prueba»: se anclan *hashes* de ciertos datos para evidenciar su existencia o validez temporal sin exponerlos públicamente [116]. Solo mediante una autorización especial fuera del sistema (y presentando el dato original) se podría verificar contra el *hash*.

En la práctica, esta capa permite extender el DPP a información que queda fuera de su ámbito inmediato pero que se quiere dejar reflejada en IOTA.

Con esta definición, cada dato del DPP, por tanto, estará etiquetado con su categoría A, B, C o D. El *front-end* y las API aplicarán estas etiquetas para filtrar la salida según el rol del solicitante (sección 4.2.3 sobre control de acceso). Por ejemplo, al generar la vista pública (no autenticada) de un pasaporte, el sistema incluirá solo campos marcados como «A»; si el usuario inicia sesión como productor de ese jamón, verá «A+B»; un auditor con credencial verá «A+B+C»; y los datos D no se mostrarán a nadie en pantalla, solo aparecerán como «datos respaldados criptográficamente» con un icono de verificación.

La definición clara de capas aporta modularidad al diseño de datos. Siguiendo la arquitectura por niveles mencionada en el estado del arte (3.2), se separan los datos de hecho (capas A-C) de los metadatos de control y verificación (D y anclajes). Esto permite, por ejemplo, actualizar o

corregir un dato de la categoría A (una certificación añadida posteriormente) sin tocar la capa de control, o revocar una credencial de acceso (capa de gobierno) sin alterar los datos base. También facilita la extensibilidad: si en el futuro la regulación exige incluir cierta nueva información para consumidores, bastaría con agregarla a la categoría A sin afectar el resto.

En síntesis, el modelo de datos está organizado en capas de accesibilidad que implementan el principio de *data minimization* y «necesidad de saber»: cada usuario obtiene solo la vista del pasaporte apropiada a su rol. Esto cumple los objetivos tanto de transparencia (lo público al alcance de todos) como de confidencialidad (lo sensible solo para quien corresponda).

Además, dichas capas están alineadas con las categorías definidas en el marco legal europeo para DPP, asegurando que nuestro diseño cumple con expectativas normativas actuales y futuras.

4.2. Arquitectura del Sistema Propuesto

A partir del modelo de datos y los requisitos, se ha diseñado una arquitectura de sistema que combina tecnologías IoT, infraestructura *cloud* o local y DLT para implementar el DPP. La arquitectura es modular y escalable, siguiendo el criterio híbrido: base de datos *off-chain* para la mayor parte de los datos y la aplicación, y uso de IOTA como anclaje de confianza distribuida.

En esta sección se describe la arquitectura física y lógica propuesta, dividiéndola en sus componentes principales: dispositivos y sensores IoT, desplegados en el campo (secaderos u otras instalaciones) junto con sus pasarelas de comunicación; la red de datos y servidores *backend*, que incluyen bases de datos, APIs y la integración con la Tangle de IOTA (nodos Hornet); y las aplicaciones *front-end* para los distintos roles de usuario. También se discuten aspectos de implementación tecnológica, mencionando plataformas específicas que podrían utilizarse (*The Things Stack* para LoRaWAN, bases de datos relacionales y de series temporales, *dashboards* de visualización, etc.), siempre bajo la premisa de utilizar soluciones modernas, abiertas y replicables.

4.2.1. Visión general de la arquitectura y componentes principales

A grandes rasgos, la arquitectura consta de las siguientes capas y componentes:

1. Dispositivos IoT en campo (*Edge*): sensores y dispositivos instalados en lugares clave del proceso de producción del jamón. Por ejemplo, sensores de temperatura y humedad en las cámaras de curación y secaderos naturales, que recopilan datos ambientales continuamente. También podrían incluirse sensores en las cámaras de salado o almacenes, o incluso dispositivos de seguimiento en envíos si se extiende a logística. Estos dispositivos recogen datos con cierta periodicidad y los transmiten inalámbricamente.

Dado que muchas instalaciones de curado son tradicionales, sin cableado de red, se opta por sensores inalámbricos de bajo consumo (batería de larga duración) usando protocolos LPWAN (*Low Power Wide Area Network*) como LoRaWAN. LoRaWAN es ideal por su

largo alcance y penetración incluso en naves con muros gruesos, y por permitir desplegar redes privadas fácilmente. Alternativamente, podrían usarse sensores WiFi o Bluetooth si la infraestructura lo permite, o estándares celulares IoT (NB-IoT, LTE-M) en entornos rurales con cobertura.

En cualquier caso, en nuestro diseño se prioriza LoRaWAN debido a su adopción en entornos agrícolas e industriales, su bajo coste y comunidad abierta.

2. *Gateways / Pasarelas IoT*: son dispositivos de enlace que reciben la comunicación de los sensores y la envían a Internet.

En LoRaWAN, un *gateway* LoRa actúa como puente entre los sensores LoRa y el servidor de red. Estos *gateways* pueden ser dispositivos dedicados o incluso *gateways DIY* montados con una placa concentradora LoRa y una computadora sencilla (como una Raspberry Pi). Dado que buscamos replicabilidad para PYMEs, se puede emplear una Raspberry Pi como *gateway* LoRaWAN local en el secadero, conectada vía Ethernet o 4G a Internet. La idea es que empresas jamoneras puedan desplegar su propio *gateway* si la cobertura pública LoRaWAN es insuficiente. Alternativamente, podrían aprovechar redes comunitarias como *The Things Network* si hay cobertura en la zona. *The Things Stack* (TTS), la plataforma *open-source* de *The Things Industries*, puede utilizarse como servidor de red LoRaWAN [117].

En un esquema sencillo, el sensor envía un paquete LoRa, el *gateway* en la fábrica lo recibe y lo reenvía (vía MQTT/HTTP) al *Network Server* (TTS) en la nube. El *Network Server* decodifica y pasa los datos a la aplicación DPP *backend*. La elección de TTS se basa en que es un stack LoRaWAN abierto, escalable tanto para redes grandes como pequeñas, compatible con estándares LoRaWAN y con integraciones listas (*webhooks*, MQTT) para conectarlo con nuestras bases de datos [117]. Esto minimiza el esfuerzo de integración de los sensores con el sistema DPP.

3. *Backend y Almacenamiento Off-Chain*: éste módulo se encarga de la persistencia de datos, la evidencia distribuida y la resolución eficiente del último estado. La arquitectura del DPP separa claramente la capa operativa (consultas, relaciones, series temporales) de la capa de evidencia (documentos versionados, anclajes inmutables) para garantizar escalabilidad, disponibilidad y verificabilidad independiente. Para ello, se han definido los siguientes subcomponentes principales:

- a) *API de Ingesta de Datos IoT*: es una API REST que actúa como puerta de entrada para recibir las lecturas de sensores IoT (temperatura, humedad, calidad del aire, etc.) y los eventos EPCIS procedentes de las pasarelas y sistemas externos. Expone *endpoints* autenticados para que el *gateway* LoRaWAN o los sistemas de gestión envíen datos del producto en tiempo casi real. La API valida, normaliza y almacena cada dato en la base de datos temporal, generando eventos con marca de tiempo y atributos de contexto (ID de producto/lote, ubicación GLN, tipo de evento).

También permite la carga de documentos (como un PDF de certificación) asociados a un evento o entidad, retornando el CID IPFS correspondiente. Esta interfaz desacopla los dispositivos y productores de la capa interna, proporcionando un *buffer* seguro y escalable para la ingestión incluso bajo picos de carga (e.g., cientos de sensores enviando datos simultáneamente).

- b) *Base de Datos de Series Temporales (PostgreSQL + TimescaleDB)*: todos los datos estructurados del DPP (entidades, relaciones GS1, eventos EPCIS, usuarios, permisos)

se almacenan en PostgreSQL, una base de datos relacional robusta, de código abierto y ampliamente adoptada en la industria alimentaria [118].

Mediante la extensión TimescaleDB se optimiza el almacenamiento y consulta de series temporales IoT, transformando las tablas en *hypertables* particionadas por rango de tiempo [119]. Esto permite inserciones y consultas eficientes incluso con millones de filas, ya que TimescaleDB excluye rápidamente datos fuera del rango de interés y agrupa en *chunks* manejables. Además, TimescaleDB habilita compresión automática de datos históricos una vez superado un horizonte configurable, reduciendo el espacio ocupado en hasta un 90 % sin perder precisión en «agregados». Por ejemplo, se puede definir que las lecturas mayores a 6 meses se compriman en formato columna, acelerando también las consultas analíticas.

Cabe destacar que no se utilizan identificadores internos de PostgreSQL en la capa DLT, de modo que ningún dato *on-chain* depende de una base de datos concreta, facilitando futuras migraciones o federación del sistema.

TimescaleDB, al ser *open source*, permitiría a PYMEs instalarlo junto con PostgreSQL, aprovechando índices por tiempo y compresión de datos históricos. En combinación con Grafana, ha demostrado ser eficaz para datos IoT [120].

- c) Almacenamiento Descentralizado y Versionado (IPFS): los documentos pesados o archivos binarios (certificados PDF, imágenes de la dehesa, vídeos, datasets completos de sensores) se almacenan en IPFS (InterPlanetary File System), un sistema de ficheros distribuido basado en contenido [121]. Cada archivo que se añade genera un identificador de contenido CID único (hash criptográfico SHA-256). Cada nueva versión de un documento produce un CID distinto; en IPFS no se sobrescriben archivos, sino que se publica una nueva versión inmutable, garantizando integridad por diseño: si el contenido se altera, su hash cambia, haciéndolo detectable [122].

El DPP aprovechará esta característica para mantener un histórico de versiones de, por ejemplo, certificados de calidad o informes de sostenibilidad: cada vez que se actualiza un documento, se guarda en IPFS obteniendo un nuevo CID, y el sistema conserva la referencia al CID anterior. De esta forma se puede auditar la evolución de cualquier documento. La elección de IPFS obedece a que descentraliza la carga de servir archivos (cualquier nodo con el CID puede proveer el contenido) y asegura integridad mediante la huella hash, eliminando dependencia de un servidor único. El *backend* guarda solo los CID (no los archivos en sí), y al recibir una petición de un cliente para, por ejemplo, ver un certificado, recupera el contenido desde IPFS usando el CID correspondiente.

- d) Anclaje de Evidencia en IOTA (Notarization): para garantizar la inmutabilidad y verificabilidad temporal de los datos críticos, se utiliza IOTA Notarization, un framework diseñado específicamente para pasaportes digitales de producto y trazabilidad [123].

El sistema registra en el Tangle de IOTA huellas criptográficas de hitos y resúmenes, creando un «cuaderno de bitácora» distribuido inalterable. En eventos críticos del ciclo de vida (e.g., sacrificio del animal, inicio y fin de curación, inspecciones sanitarias, expedición), el *backend* genera un manifiesto JSON que resume el estado en ese punto [123]: incluye los campos clave del evento EPCIS, los CID de documentos adjuntos en IPFS, marcas de tiempo y la firma digital del operador responsable. El *hash* criptográfico de este manifiesto (una huella de unos pocos *bytes*) se ancla en el Tangle mediante una transacción IOTA. Cada anclaje queda asociado de forma indeleble a un identificador único (el ID de producto o lote), ya sea en una estructura

dinámica o en múltiples registros. De este modo, cualquier tercero puede comprobar de forma independiente la integridad y fecha de esos hitos: dado un manifiesto y su *hash* anclado, se recalcula el *hash* del manifiesto obtenido del sistema y se compara con el registrado en IOTA; si coinciden, la información se considera verificada y no alterada.

La arquitectura adoptada opta por un esquema de notarización dinámico (evolutivo) en lugar de anclar cada evento por separado, optimizando el uso de la DLT. Es decir, se mantiene un registro *append-only* donde cada anclaje actualiza el estado del anterior en lugar de generar infinitos registros independientes, lo que resulta más eficiente en términos de almacenamiento distribuido. En todos los casos, solo se anclan *hashes* (huellas digitales), nunca datos en claro, para preservar la confidencialidad máxima. Gracias a este módulo, cuando un usuario escanea un DPP y solicita verificar un dato, el sistema puede confirmarle con un indicador visual (como por ejemplo, un icono que marque «verificado») que dicha información coincide con la huella registrada en IOTA, aportando confianza sin revelar detalles sensibles.

Además de los eventos de trazabilidad, se anclarán periódicamente resúmenes ambientales: en lugar de anclar cada lectura de sensor (lo cual sería inviable por volumen), el *backend* calculará agregados como los promedios diarios de temperatura y humedad por lote y los incluirá en un manifiesto especial (*snapshot*) cada semana o día. El *hash* de este *snapshot* se ancla en IOTA, creando puntos de control que certifican las condiciones ambientales de curado en intervalos regulares. Así se logra un equilibrio: no saturar el Tangle con datos masivos, pero sí poder demostrar que cada día las condiciones estuvieron dentro de X rango, porque el promedio reportado está anclado (y cualquier alteración de los datos originales rompería la verificación). Esta técnica mejora la transparencia sin sacrificar rendimiento.

Por otro lado, para lotes o grupos extensos de eventos, se puede emplear un árbol de Merkle [124]: el *backend* tomaría los *hashes* de todos los eventos individuales de, digamos, un lote de jamones curados juntos y computaría una raíz de Merkle. Esa raíz (*Merkle root*), que es un *hash* representativo de todo el conjunto, se anclaría en IOTA en lugar de anclar cientos de *hashes* por separado. Si luego se requiere probar la inclusión de un evento particular, se puede proporcionar el camino de Merkle correspondiente. Esta técnica permite verificaciones altamente eficientes de pertenencia sin exponer públicamente todos los datos, y es un patrón común en *blockchains* para lograr verificaciones compactas.

- e) Puntero Mutable *on-ledger* (*Alias Output* de IOTA): Un desafío clave es resolver eficientemente el último estado del DPP de un producto sin recorrer todos los anclajes históricos en el Tangle (algo altamente ineficiente para un desarrollo avanzado de la red y contradictorio con el RNF1 de escalabilidad). Para ello se utiliza *Alias Output* de IOTA (parte del protocolo *Stardust*), que actúa como un identificador permanente en la DLT con un estado mutable [125] [126]. Cada producto (cada jamón o lote, representado con un DID si aplica) tiene asignado un «Alias Output» único, identificado por un «Alias ID» (dirección exclusiva derivada criptográficamente). Este Alias Output contiene un campo especial de metadatos (*state.metadata*) que el *backend* actualiza cada vez que hay un nuevo manifiesto anclado. En concreto, tras generar y anclar un manifiesto de evento crítico, el *backend* construye una transacción que actualiza el Alias Output del producto, escribiendo en *state.metadata* el CID del último manifiesto publicado, un contador de secuencia incrementado y el hash del manifiesto previo. Por ejemplo, tras el evento de expedición de un jamón,

`state_metadata` podría quedar como:

```
{
  "latest_manifest_cid": "Qm...ABC",
  "sequence": 5,
  "prev_hash": "0xDEF...123",
  "last_update": "2025-10-15T12:00:00Z"
}
```

De este modo, consultar el estado más reciente es $O(1)$ [125]: dado el Alias ID (que puede estar embebido en el código QR del precinto), cualquier usuario o aplicación consulta ese Alias Output en la red IOTA (vía API de un nodo o índice). La respuesta contendrá los metadatos actuales, de donde se extrae directamente el CID del manifiesto más reciente, sin necesidad de recorrer todos los anclajes anteriores. Con ese CID, el sistema puede obtener de IPFS el manifiesto final completo. Este patrón de diseño (que es análogo al utilizado por IOTA Identity para la resolución de documentos DID), permite mantener el QR estático e inmutable en el producto, ya que siempre apunta al mismo Alias ID, y delegar en la lógica *off-chain* la obtención del estado actualizado a partir de dicho «alias» [127].

En síntesis, el Alias Output actúa como un puntero oficial *on-ledger* al último estado del pasaporte, evitando tener que buscar entre múltiples transacciones en el Tangle y reduciendo la carga al verificar un DPP.

- f) Disponibilidad y *Pinning* Asegurados: dado que la disponibilidad de los contenidos IPFS debe ser muy alta (requisito RNF2: 99,9 %), se integra un servicio de *pinning* externo (Pinata) para mantener copias persistentes de los archivos IPFS [128].

Estos servicios replican y alojan los CID en nodos distribuidos, garantizando que incluso si nuestro nodo IPFS local cae, los contenidos siguen accesibles en la red [129]. Pinata, en particular, opera una infraestructura con cientos de nodos y *gateways* dedicados, lo que acelera la entrega de contenidos a usuarios finales. El coste de este *pinning* es razonable: el plan base ofrece del orden de 1 TB de almacenamiento por alrededor de 20 €/mes, suficiente para varios GB de documentos e imágenes del DPP [130]. Esta inversión asegura que un consumidor que escanee el QR pueda obtener al instante la foto o certificado asociado, sin depender de un único servidor central.

- g) Alias IPNS (opcional para referencias internas): El uso de IPNS (*InterPlanetary Name System*), sistema de nombres mutable de IPFS, se considera opcional a efectos del DPP.

IPNS permite publicar una clave que siempre apunta al último CID de un contenido (similar a un DNS para contenidos IPFS) [131]. Sin embargo, IPNS en la red pública conlleva cierta complejidad: los registros deben re-publicarse periódicamente antes de expirar (cada 48 horas) para que no caduquen en la DHT, lo que añade una carga operativa y posibles demoras en la propagación de actualizaciones (las búsquedas IPNS pueden ser lentas debido al mecanismo de cacheo distribuido) [132].

Dado que en nuestra solución el puntero canónico al último estado ya se resuelve a través de Alias Output en IOTA, IPNS no es necesario para el funcionamiento del DPP [133]. Aun así, podría ofrecerse como comodidad adicional: por ejemplo, publicar bajo IPNS un alias legible (como `dpp-empresa-xyz`) que siempre apunte al CID más reciente de cierto informe o documento en IPFS, facilitando a un usuario avanzado navegar el contenido desde un *gateway* IPFS público.

En todo caso, la verificación oficial siempre se haría contra los CID y *hashes* anclados en IOTA, que es la fuente de verdad inmutable. En resumen, IPNS se plantea solo como capa de *naming* opcional para usos internos, pero no crítica.

- h) Flujo de Resolución de Último Estado (lectura del QR): cuando un usuario escanea el código QR de un producto, se desencadena la secuencia para obtener y verificar la información del DPP:
- 1) Escaneo y petición: el QR contiene un URI GS1 Digital Link que incluye el identificador único (el Alias ID en IOTA). Al escanearlo, la aplicación cliente o el navegador invoca al *backend* con ese identificador.
 - 2) Obtención del estado *on-ledger*: El *backend* consulta la API de índice de IOTA para recuperar el Alias Output correspondiente al Alias ID. Esto retorna los metadatos actuales (*latest_manifest_cid*, *secuencia*, etc.).
 - 3) Resolución del manifiesto IPFS: con el CID del último manifiesto, el *backend* lo recupera desde IPFS a través del servicio de *pinning* (asegurando rapidez y disponibilidad).
 - 4) Verificación de integridad: se calcula el *hash* del manifiesto obtenido y se compara con el *hash* anclado en IOTA para ese Alias (o con el *prev_hash* encadenado, según el caso). Si no coinciden, se informa de inconsistencia; si coinciden, se procede.
 - 5) Consulta de datos operativos: el *backend* extrae del manifiesto los identificadores relevantes (por ejemplo, ID de eventos EPCIS, CID de documentos adjuntos) y puede realizar consultas adicionales a la base de datos PostgreSQL/TimescaleDB para enriquecer la respuesta (por ejemplo, obtener los datos de detalle de un evento, o agregar las series temporales completas del periodo que el manifiesto resume).
 - 6) Control de acceso: según el rol del usuario solicitante y las políticas (capas A, B, C, D del DPP), el *backend* filtra la información que se entregará. Por ejemplo, un consumidor general quizás solo reciba datos de categoría A verificados, mientras que un auditor homologado podría obtener también los de categoría C.
 - 7) Respuesta y renderizado: el *backend* compone la vista del Pasaporte Digital de Producto con todos los datos solicitados y la envía al cliente. Cada dato crítico viene marcado con un indicador de verificación si su *hash* coincide con el anclado en IOTA. El cliente (ya sea una aplicación móvil o web) presenta al usuario la información del DPP, incluyendo secciones como origen del producto, recorrido logístico, condiciones de curado, certificaciones, etc., diferenciando visualmente lo verificado *on-chain* de lo meramente informativo.

Este diseño de *backend* híbrido cumple con los criterios de arquitectura híbrida (CD1), escalabilidad y rendimiento (RNF1), alta disponibilidad (RNF2), eficiencia de coste (RNF4) y seguridad (RNF5). Se evita dependencia de bases de datos centralizadas para verificar autenticidad (ya que las huellas están en IOTA) y se resuelve la aparente contradicción entre identificadores de contenido cambiantes (CID de IPFS) y necesidad de referencias estables, gracias al uso de Alias Outputs como punteros dinámicos en la DLT.

En suma, el *Backend* actúa como orquestador entre la capa *off-chain* (rápida y flexible) y la *on-chain* (segura e inmutable), brindando al usuario final una experiencia transparente pero respaldada por tecnologías descentralizadas.

Tras estos subcomponentes cabe mencionar la decisión de arquitectura lógica con los Criterios de Diseño del Capítulo 3.12.3: aplicación cliente separada (SPA). Para la implementación final del visor del DPP se propone un modelo de aplicación de una sola página (*Single Page Application*, SPA) que consume las API REST expuestas por el *backend*.

Esta decisión se justifica por su alineación con los criterios CD2 (*API-First*) y CD3 (*Progressive Enhancement*), permitiendo una experiencia de usuario rica y modular sin comprometer la seguridad ni la escalabilidad. La SPA permitirá el escaneo de códigos QR en dispositivos móviles, aplicará el control de acceso según el rol del usuario (RF3) y consultará en tiempo real el Alias Output correspondiente a la pieza, resolviendo el manifiesto más reciente vía IPFS y mostrando su trazabilidad certificada. Este patrón facilita además la integración futura con plataformas externas, garantizando flexibilidad y cumplimiento de los principios de neutralidad tecnológica y desacoplamiento definidos en CD5.

4. Aplicaciones *Front-end* por rol: el acceso al DPP se realizará principalmente mediante aplicaciones web «responsivas» (accesibles desde móviles y PCs) adaptadas a distintos perfiles:

- a) Visor público de DPP (cliente web): es la página web a la que llega un consumidor cuando escanea el QR del producto. Debería mostrar la información de Categoría A de forma atractiva: por ejemplo, una ficha con la foto del producto, descripción, certificaciones, y un resumen de la historia (quizá una línea temporal simplificada: «Cría en Dehesa Los Encinos – 2020; Curación 36 meses – Jabugo; Precintado Negro ASICI – 2023»). Incluirá indicadores de verificación (un check verde si los datos han sido validados con IOTA). Este visor no requeriría *login*. Técnicamente, se podría implementar como una SPA en Javascript (React, Vue, etc.) o simplemente páginas *server-rendered*.

Dado el criterio de mejora progresiva, una versión básica en HTML estática con enlaces a datos JSON-LD puede presentarse para asegurar compatibilidad amplia, y luego enriquecer con JS para gráficos o mapas interactivos. Grafana u otras librerías de visualización pueden integrarse para mostrar gráficas de temperatura/humedad de forma embebida. Por ejemplo, se puede incrustar un panel de Grafana mostrando la curva de temperatura en curado, en modo imagen o interactivo, dado que Grafana permite compartir visualizaciones públicamente con URL.

Grafana es ampliamente utilizado en IoT por su capacidad de presentar datos de sensores en tiempo real de manera comprensible [120]. Una posible implementación es que el *backend* prepare los datos agregados y Grafana los lee desde TimescaleDB para generar gráficos que el *front-end* consume. En cualquier caso, la experiencia para el consumidor debe ser simple: escanear y ver.

- b) Portal de productores/operadores: una interfaz protegida con *login* para usuarios internos del sector (productores, transformadores, etc.). Tras autenticarse (con usuario/contraseña o con certificado/ID digital), podrán consultar información extendida (capas A+B de sus productos, quizá algunas de C si les compete).

Por ejemplo, un maestro jamonero podría ver todos sus productos y sus estados, verificar que todos tienen sus datos completos, añadir tal vez datos adicionales (subir una foto o historia del producto, que va a capa A como valor añadido de marketing), o consultar gráficos detallados de sensores por lote. También podría recibir alertas

(e.g., si un sensor detectó temperatura fuera de rango durante más de 2 horas, el sistema puede señalarlo).

Este portal serviría también para ingresar datos que no vienen de sensores ni de ÍTACA: registrar el inicio y fin de la curación si se hace manualmente, o cargar el resultado de un análisis de laboratorio. Se cuidará el uso para que las PYMEs puedan usarlo sin complicaciones.

- c) Portal de auditores/autoridades: similar al anterior pero para usuarios con mayor privilegio (rol de auditor externo o regulador). Estos usuarios, una vez autenticados con su credencial emitida por ASICI u organismo competente, podrán consultar incluso capa C de cualquier producto (o de aquellos bajo su supervisión).

Por ejemplo, un inspector de ASICI podría buscar un lote o pieza y ver todos los datos incluyendo los internos, verificar firmas, etc. Probablemente esta interfaz tenga herramientas para exportar los datos (en formato EPCIS XML/JSON) o generar informes de auditoría.

- d) Aplicación móvil (opcional): si se considera necesario, podría haber una app móvil nativa para ciertos roles (como que un ganadero capture datos de campo *offline*). No obstante, en nuestro diseño inicial nos centramos en web *responsive*, para minimizar costos de desarrollo y dado que muchos usuarios ocasionales (consumidores) preferirán no instalar nada.

Los *front-ends* consumirán las API del *backend*. La seguridad se maneja con HTTPS y JWT/OAuth para las API autenticadas. En el caso de credenciales descentralizadas, el flujo podría ser: el usuario presenta su VC (escaneando un QR con su wallet que demuestra su rol), el *backend* verifica la firma y emite un *token* de sesión. Este tipo de integración aún es novedosa, pero se podría apoyar en bibliotecas como IOTA Identity o estandarizadas W3C. En cualquier caso, la interfaz se diseña de forma que degrade bien: si alguien no tiene un DID, se le puede crear un usuario tradicional provisional.

En cuanto a la infraestructura de despliegue, se plantea utilizar contenedores Docker para cada componente (base de datos, grafana, node IOTA, etc.), orquestados quizá con Docker Compose o Kubernetes en función del tamaño. Para un prototipo, Docker Compose en una VM sería suficiente, y replicable por cualquiera con esos contenedores configurados. Esto también facilita escalabilidad: por ejemplo, levantar múltiples instancias del *backend* detrás de un «balanceador» para soportar más carga (recordando RNF1 de escalabilidad horizontal). Los servicios de terceros (TTS, IOTA *node*) también pueden correrse en contenedor o usar instancias gestionadas (The Things Stack Cloud, o un nodo Hornet público) según convenga y la confiabilidad deseada.

Finalmente, mencionar que esta arquitectura, aunque compleja, sigue patrones típicos de soluciones IoT-Blockchain. Tenemos una capa de adquisición de datos, una de procesamiento/almacenamiento central, y anclajes en *blockchain* para asegurar integridad.

Al no almacenar todos los datos en la *blockchain*, evitamos problemas de volumen y privacidad, pero obtenemos lo mejor de ambos mundos: eficiencia de bases de datos tradicionales y confianza de un *ledger* público. Este diseño modular permite que cada empresa mantenga sus datos en su infraestructura (posibilidad de federar en el futuro) pero que para el usuario final aparezcan unificados cuando consulta el pasaporte. Nuestro prototipo implementará todo centralizado para simplificar, pero la arquitectura prevé este paradigma federado donde los datos quedan con los

operadores económicos y solo comparten vistas verificables cuando se consulta.

Esto alinea el sistema con la visión europea de no tener una única base de datos central de todos los DPP, sino un sistema distribuido o federado, con un registro central mínimo solo de identificadores. En nuestro caso, ASICI podría desempeñar ese rol de registro (sabe qué precintos existen, equivaldría a saber qué DPP hay), mientras que los datos residen en sistemas de cada parte, conectados vía estándares.

Resumiendo, la arquitectura propuesta es híbrida, abierta y escalable: híbrida al mezclar *cloud* y DLT, abierta al usar estándares (LoRaWAN, GS1, REST, JSON-LD) y plataformas OSS (PostgreSQL, Grafana, IPFS, Hornet) replicables por cualquiera, y escalable horizontalmente para acompañar el crecimiento del sector.

En la siguiente sección profundizamos en algunos aspectos críticos de esta arquitectura, como la viabilidad de la solución IoT (frecuencia de muestreo, alcance de LoRaWAN, etc.) y el gobierno de la identidad y permisos en el sistema.

4.2.2. Viabilidad de la Solución IoT: Sensores, Comunicaciones y Almacenamiento

Un componente novedoso de este DPP es la integración de sensorización IoT en el proceso de elaboración del jamón ibérico, lo que aporta datos objetivos de las condiciones de producción directamente al pasaporte digital. Analizamos aquí la viabilidad técnica de esta solución IoT, considerando la frecuencia de muestreo requerida, número y ubicación de sensores necesarios, tecnologías de comunicación y capacidad de almacenamiento de los datos generados.

Frecuencia de Muestreo y Volumen de Datos

Las condiciones de curado (temperatura, humedad) no varían drásticamente minuto a minuto; suelen cambiar gradualmente a lo largo del día y la estación. Por tanto, no es necesario un muestreo en tiempo real altísimo. Se estima adecuado tomar lecturas cada 15 minutos a 1 hora para parámetros ambientales.

Por ejemplo: una lectura cada 30 minutos de temperatura y humedad generaría 48 datos al día por sensor. En un año (365 días de curación) serían aproximadamente 17.500 registros por sensor. Si un secadero tiene, digamos, 10 sensores distribuidos, serían 175.000 registros por año, un volumen manejable para una base de datos moderna. Incluso 5-10 años de histórico por sensor (0.5-1 millón de puntos) es perfectamente viable de almacenar y consultar con una base de series temporales optimizada. Tecnologías como TimescaleDB o InfluxDB pueden manejar millones de puntos con un *hardware* modesto, especialmente si se agregan los datos históricos. Además, se pueden implementar esquemas de *downsampling* (conservar datos crudos 1 año, luego promedios horarios) para contener el volumen.

En cuanto a transmisión, un mensaje LoRaWAN típico con temp+hum es de solo unos bytes,

multiplicado por 50 al día = 1.5kB por sensor por día, insignificante para LoRaWAN que soporta eso. Por tanto, la frecuencia elegida equilibra obtener suficiente resolución (eventos como una subida brusca de temperatura de varias horas se captarán) sin sobrecargar redes ni bases de datos. Para otros posibles sensores (ej. CO₂ en bodega, luz, etc.) se puede usar una frecuencia similar o menor según su relevancia.

Ubicación y Número de Sensores

Se prioriza colocar sensores en aquellos puntos cuya variabilidad impacta en la calidad del jamón. En una instalación típica:

- Cámaras de salado: 1-2 sensores de temp/hum por cámara, pues es un proceso de unas semanas donde asegurar cierto rango de temperatura es crucial.
- Secaderos naturales: dependiendo del tamaño, varios sensores. Por ejemplo, en una bodega de curación tradicional, se podrían poner 4 sensores: dos a distinta altura (techo y suelo, porque la temperatura puede estratificarse) y en extremos opuestos de la sala, para capturar variaciones internas. Si hay varias salas/pisos, se puede repetir en cada una.
- Almacenes de post-curado: similar a secaderos.
- En transporte: para el prototipo no lo incorporamos, pero eventualmente podrían usarse registradores de temperatura en contenedores de envío si exportan, cuyos datos luego se suban al DPP.
- Otras variables: quizá un sensor de humedad del suelo en la dehesa para correlacionar con montanera (futuro), o seguimiento de movimiento de los jamones (IoT *tags*) si se quisiera evitar robos (esto se descarta por complejidad en un prototipo).

En total, estimando 10 sensores por productor (podría variar si la empresa es grande con muchas bodegas). Para 50 productores, 500 sensores. Esto es perfectamente soportable con LoRaWAN en términos de capacidad, ya que LoRaWAN en SF altos permite miles de nodos por *gateway* en baja frecuencia de envío. Además, se pueden usar varias frecuencias y saltos.

Tecnología de Comunicaciones

Como se mencionó, LoRaWAN es la elección principal. Sus ventajas: alcance de hasta 5-15 km en campo abierto (útil para cubrir granjas dispersas), penetración en interiores (sub-GHz atraviesa muros), muy bajo consumo (sensores con 3 años de batería con envíos cada hora), y red propia desplegable. The Things Stack facilita montarla, y existen *gateways* asequibles (300-500 € por uno con buena cobertura). Algunas zonas de España cuentan con cobertura de The Things Network pública, lo cual significa que ni siquiera habría que comprar *gateway* si el secadero está en esa cobertura. De no ser así, un *gateway* propio crea la red privada de la empresa.

Lo bueno de LoRaWAN es que es seguro (cifrado AES a nivel de enlace), y soporta muchos dispositivos. Un único *gateway* en la fábrica puede recibir de decenas de sensores. En

cuanto a obstáculos como montañas (hablando de dehesas), se podría necesitar repetidores o *gateways* adicionales en diferentes fincas si se quisieran introducir sensores en la cría; pero hemos descartado sensorización masiva en ganadería para este prototipo, concentrándonos en el procesado.

Otras Tecnologías Posibles:

- WiFi: descartado en secaderos aislados y por consumo.
- Bluetooth BLE: útil para distancias cortas, no aplicable aquí salvo que sensores envíen a una puerta de enlace cercana, pero eso complica.
- NB-IoT: red celular IoT, podría ser opción para sensores sin *gateway*, pero depende de operadoras y cobertura en zonas rurales; viable como *backup*.
- Sigfox (otra LPWAN propietaria): se omite por depender de una red comercial específica y por menor capacidad de *payload*.
- Zigbee o similares: para *in-building* con concentradores podría valer, pero su alcance menor hace menos atractivo para varias naves.

Por tanto, LoRaWAN brinda un buen balance. Con un *gateway* LoRaWAN multi-canal se pueden recibir decenas de mensajes simultáneamente. *The Things Stack* como servidor puede manejar miles de dispositivos [117]. Para el almacenamiento y procesamiento de esos datos IoT, ya argumentamos que es manejable; además, se pueden usar técnicas de procesamiento en el borde si se quisieran disminuir envíos (que el sensor envíe promedio cada hora en lugar de cada 5 min), pero inicialmente enviaremos todos los datos y filtraremos en *backend*.

Fiabilidad y mantenimiento

Se considera que los sensores deberán calibrarse periódicamente para asegurar datos fiables. En el diseño del DPP se prevé la posibilidad de marcar datos como «posiblemente corruptos» si se detecta un fallo de dispositivo (por ejemplo, si un sensor reporta valores fuera de rango humano, se puede generar una alerta).

Según el RNF5, ante la detección de un dispositivo comprometido se debería indicar en el DPP. Esto lo incluimos como lógica de negocio: si un sensor presenta lecturas claramente erróneas (e.g., 99°C en una bodega), el sistema podría etiquetar esos datos y excluirllos del cálculo de promedios, a la vez que se notifica al administrador. Este tipo de resiliencia operativa es importante para no desacreditar el pasaporte con datos aberrantes.

En cuanto a infraestructura para datos: se ha optado por TimescaleDB (sobre Postgres) para series temporales, que en pruebas ha mostrado manejar millones de puntos en tiempo real y consultas complejas con índices temporales. Grafana aportará la visualización y alertas básicas. Cabe señalar que Timescale puede comprimir datos viejos reduciendo espacio, lo que es útil si se acumulan años de datos.

Capacidad de Almacenamiento

Un cálculo de orden superior: Si 500 sensores envían una lectura cada 15 minutos, cada sensor genera 96 lecturas por día, por lo que el sistema recibe $500 \times 96 = 48,000$ lecturas cada día (unas 17,520,000 lecturas al año). Con una estimación conservadora de 70 bytes por registro (temp, hum, timestamp, id en formato JSON compacto), el volumen bruto anual sería cercano a los 1.17 GB; con compresión típica para series temporales (entre una cuarta parte y una sexta parte) el almacenamiento efectivo puede reducirse hasta a los 200-300 MB/año. Incluso incluyendo índices y *overhead* de base de datos, el volumen a 5 años vista permanece en el orden de pocos *gigabytes* (GB), por lo que el almacenamiento no es un cuello de botella para un servidor moderno o para soluciones RDS; en cambio, fotos o vídeos consumirían órdenes de magnitud mayores y deberían alojarse *off-chain* (e.g., IPFS / *object storage*) con CID/refs en la base de datos.

La integración IoT planteada es plenamente viable técnicamente: el volumen de datos es manejable, existen redes y equipos idóneos (LoRaWAN + *gateways*) de bajo coste, y las herramientas de *backend* (*Time-Series DB*, Grafana) son suficientemente robustas y probadas en entornos industriales similares. Además, este esquema es replicable: cualquier productor podría instalar sensores y un *gateway*, y conectarlos al sistema DPP siguiendo las guías pertinentes

Vale destacar casos de uso industriales donde la combinación Grafana + *Timescale* ya se usan para monitorear fábricas en tiempo real, y LoRaWAN se emplea en seguimiento de alimentos (por ejemplo, bodegas de vino monitorizadas) [120]. El diseño planteado se alinea con esas prácticas modernas, trayendo el jamón ibérico al mundo de la Industria 4.0.

4.2.3. Gobierno, Identidad y Control de Acceso Descentralizado

Un aspecto fundamental del diseño es cómo se gestionan la identidad de los participantes y los permisos de acceso a las distintas capas de información del DPP, garantizando a la vez confianza en los datos y privacidad. Para ello, se propone apoyarse en un esquema de identidad digital descentralizada y credenciales verificables, con ASICI actuando como autoridad de confianza (*trust registry*) para el ecosistema jamonero.

A continuación se detalla la definición de los roles de usuarios, el uso de DID (Decentralized Identifiers) y VC (Verifiable Credentials) en el sistema, y cómo se aplica el control de acceso en base a ellos (roles y privilegios).

- **Productor/Operador:** persona o empresa responsable de producir el jamón (incluye ganadero, industria de curado, etc.). Tendrá acceso a la información de sus propios productos en categorías A, B y posiblemente parte de C (por ejemplo, puede ver datos completos sanitarios de sus animales, pero no de otros). También podrá añadir ciertos datos (los que le competan, como notas sobre alimentación si es ganadero, datos de curado si es el secadero). No podrá alterar datos ya certificados (no podrá cambiar el resultado de precintado, por ejemplo).
- **Transformador/Distribuidor:** en caso de actores intermedios (matadero, distribuidor logístico), roles similares a productor para los datos que ellos gestionan. Un matadero podría

introducir los datos de sacrificio y verlos luego, un distribuidor podría consultar datos logísticos.

- **Auditor/Inspector:** persona de una entidad de inspección (e.g., de ASICI o de la Junta de Andalucía si es la autoridad competente de la DOP). Tiene acceso a capas C e incluso opción de ver datos D bajo circunstancias especiales. Este rol puede verificar todos los datos, pero usualmente en modo lectura. Podría, por ejemplo, descargar un informe completo de trazabilidad de una pieza si investiga un caso.
- **Veterinario autoridad:** similar a auditor, quizá un subrol que le permite además firmar ciertos datos: un veterinario oficial podría subir su certificado como VC firmada. Pero para efectos de acceso, lo consideramos dentro de «autoridad».
- **Consumidor:** público general, sin autenticación, accede solo a A. No puede modificar nada, acceso de tipo solo lectura.
- **Administrador del Sistema DPP:** rol interno (podría ser ASICI como organismo gestor del pasaporte) con acceso técnico a todo. Este rol administra la plataforma, emite credenciales a otros usuarios, etc. Su uso debe ser restringido y auditado (según RF5, cualquier acción se debe registrar).

Identidad Descentralizada (DID) y Registro de Confianza (*Trust Registry*)

En lugar de usar únicamente usuarios y contraseñas tradicionales (que podrían existir por practicidad), se propone dotar a cada entidad participante de una identidad digital descentralizada (DID).

Un DID es un identificador único (ej. `did:iota:XYZ...` o `did:ebsi:...`) asociado a claves criptográficas, que permite a esa entidad autenticarse y firmar datos sin depender de una autoridad central de identidad [134]].

ASICI actuaría como *trust anchor* emitiendo o reconociendo las identidades de los actores del sector:

1. A cada productor registrado, ASICI le emite (o valida) un DID representando a su organización. Por ejemplo: `did:ASICI:prod:ACMEJamón` podría ser el DID de la empresa ACME Jamones S.L.
2. A cada inspector, ASICI u otra autoridad le da un DID personal o de cargo (`did:ASICI:persona:JuanPerez`).
3. Estos DID se almacenan en un registro de confianza mantenido por ASICI: una lista de DID autorizados y su rol. Esto podría ser un contrato inteligente en *blockchain* o simplemente un registro en la base de datos central pero firmado por ASICI para que sea verificable. Por ejemplo, ASICI podría publicar una *Verifiable Credential* que afirme «DID X es un productor certificado de jamón ibérico» o «DID Y es inspector de ASICI», actuando como autoridad emisora de esas credenciales.

Las VC son declaraciones digitales firmadas, infalsificables, por lo que si ASICI firma la credencial de rol, cualquier otra parte puede verificarla con la clave pública de ASICI [134]. De esta forma, el sistema DPP no necesita almacenar extensivamente roles por usuario; puede simplemente verificar la VC presentada en la autenticación. No obstante, seguramente se mantendrá una tabla local de usuarios para uso, pero vinculada a su DID.

Empleo de *Verifiable Credentials* (VC) para Permisos

Una *Verifiable Credential* podría usarse así:

1. ASICI emite a ACME Jamones S.L. una credencial firmada por ASICI, que tiene su propio DID de autoridad, del tipo `ProducerCredential` que contiene:

- Sujeto = DID de ACMEJamones S.L.
- Atributo = “rol: productor jamón ibérico certificado”.
- Validez = hasta fecha X.
- Etcétera.

Esta credencial puede seguir el modelo estándar W3C VC, usando esquema JSON-LD con vocabulario que incluya una categoría de operador jamonero [134].

2. Cuando ACME Jamones S.L. (o su representante) quiere acceder al portal productor, en lugar (o además) de ingresar usuario y clave, podría seleccionar su credencial en un *wallet*.
3. En el diseño contemplado, el sistema DPP enviaría un desafío; el *wallet* lo firmaría demostrando control del DID y adjuntaría la credencial. El *backend* verificaría firma, vigencia y prueba de posesión; y, en caso de ser válida, otorgaría las *claims* de permiso correspondientes. Este flujo no forma parte del MVP implementado del Capítulo 5; queda como línea futura descrita en el Capítulo 9.
4. El *backend* verifica:
 - a) Que la VC está bien firmada por ASICI (autoridad de confianza).
 - b) Que no está expirada o revocada (ASICI podría tener lista de revocación).
 - c) Que el DID presentador coincide con el sujeto de la VC (prueba de posesión).
5. Si los datos son correctos, se le otorgan las *claims* de permisos correspondientes: por ejemplo, acceso a productos donde el campo «productor» coincida con ACME Jamones S.L.
6. Similar para un inspector: su VC dirá «rol: auditor ASICI»; el sistema entonces sabe que puede ver todo (o todo de cierta área).

Para un consumidor general no se requiere credencial; es anónimo. En la arquitectura descentralizada ideal, un consumidor podría tener un DID opcional para solicitar datos, pero es innecesario para información pública.

Firma de Datos con Identidad

Además del acceso, las identidades se usan para la integridad de los datos aportados. Cada evento o dato crítico que un actor genera en el DPP debería venir firmado con su clave para permitir su verificación. Ejemplos:

- El certificado veterinario del matadero puede ser emitido como VC firmada por el veterinario (y contrafirmada por la autoridad del matadero). Ese documento JSON firmado se almacena *off-chain* y su *hash* en IOTA. Cualquiera con acceso a categoría C podría descargarlo y verificar la firma usando el DID del veterinario (resolviendo su clave pública en el DID Document).
- Un productor, al ingresar manualmente un dato («Estos jamones estuvieron alimentados con bellota de Nov 2020 a Feb 2021»), podría firmar ese comunicado. En la práctica, esto podría ser transparente: si la interfaz web ya sabe su DID y tiene su clave (por ejemplo, usando un *wallet browser*), podría firmar la transacción de envío de datos. Si no, tal vez el *backend* firme en su nombre con una clave emitida (menos deseable, lo ideal es firma de origen).
- Las transacciones de anclaje en IOTA deben también llevar la firma de quien las envía. IOTA *Identity framework* permite escribir *Verifiable Presentations* a la Tangle. Por ejemplo, en vez de anclar solo un *hash* de evento, podríamos anclar un JSON que contenga: *hash* del evento, y firma del actor. Así, la DLT almacena no solo la evidencia temporal sino quién atestiguó ese dato. Esto consigue un mayor nivel de confianza distribuida: no hay que confiar solo en la base central, sino que la propia autoridad o actor avaló los datos.

Privacidad y RGPD

Usar DID y VC ayuda a la privacidad porque minimiza el intercambio de datos personales. Por ejemplo, un inspector no necesita registrarse con nombre y DNI en nuestro sistema; basta que presente su VC de ASICI. Nuestro sistema no almacena su nombre, solo su DID y rol. Eso cumple el principio de minimizar datos personales (solo sabemos lo necesario para el rol). Además, los DID pueden ser rotativos (un productor puede cambiar de DID periódicamente mientras las credenciales se actualizan) para evitar correlación excesiva, aunque en este sector quizás no sea una prioridad.

En todo caso, las interacciones quedan registradas pero «pseudónimas» (por DID). Si un usuario se retira, su DID se revoca en el *trust registry*, impidiendo futuros accesos (y conforme al RNF5, podríamos «congelar» los datos que aportó si es necesario, aunque los *hashes* queden en DLT de forma histórica).

Registro de operaciones y auditoría

Cada acción importante (alta de un dato, modificación, acceso a la categoría C) será registrada en la *audit trail* (RF5). Mucho de esto puede vincularse con identidades: por ejemplo, en la base

de datos de *audit* se guarda «el DID X consultó los datos completos de la pieza Y el 10/10/2025». Estas entradas de *log* críticas podrían también anclarse en IOTA periódicamente (e.g., un *hash* diario o semanal del *log* de accesos), de manera que ni siquiera los administradores de sistemas puedan borrar evidencias de accesos sin que se note.

Implementación con IOTA *Identity* u Otras Tecnologías

IOTA ofrece el framework IOTA *Identity* que es compatible con W3C DID/VC estándares. Podríamos usarlo para registrar DID en la Tangle y emitir credenciales. Alternativamente, hay redes especializadas como Ethereum (ERC725/EIP/process), Hyperledger Indy/Aries o el futuro marco europeo EBSI; pero dado que ya estamos en IOTA para notarización, es consistente usar IOTA también para identidad. Por ejemplo, el *DID Document* de ASICI se podría publicar en Tangle (contendrá su clave pública), y cada DID de participantes también. IOTA *Identity* permite resoluciones *offline* (el *DID Document* puede estar en IPFS referenciado por Tangle).

Como esta es un área en evolución, nuestro diseño es flexible: la idea central es usar VC, independiente de la red subyacente. GS1 también investiga el uso de VC/DID en supply chain, lo que indica que vamos en línea con tendencias globales [135], [136].

ASICI como *Trust Registry*

Formalmente, un *trust registry* es un servicio donde se puede consultar qué emisores y esquemas de credencial son válidos en un ecosistema. ASICI puede mantener un registro (por ejemplo un JSON disponible públicamente o en blockchain) listando: - DID de ASICI (usado para firmar credenciales de productores, etc.) - DID de otras autoridades aceptadas (por ejemplo, si la autoridad veterinaria regional emitiera VC, su DID estaría aquí para confiar en él). - Esquemas de credencial válidos (ProducerCredential, InspectorCredential, etc. con sus identificadores de contexto). Cualquier verificador (como nuestro backend) consultaría este registro para saber si puede confiar en una VC recibida. Como esto es un TFG prototipo, probablemente se codifique de manera estática (con ASICI como única CA), pero es bueno sentar el concepto por diseño.

Control de acceso en la aplicación

Combinando lo anterior, el backend propuesto implementará una matriz de accesos por rol: - Si petición no autenticada → rol = público → filtro datos A. - Si autenticada con VC de productor → rol = productor, sujeto = empresa X → filtro datos A+B de productos de X. - Si rol = auditor → A+B+C de todos. - Etc. Este control no está incluido en el MVP del Capítulo 5.

Este control se hace tanto en la capa de lógica (al compilar la respuesta del pasaporte omite campos según categorías) como en la de consulta a la base (p.ej. en SQL se pueden unir solo lo permitido). Dado que cada campo está etiquetado con categoría, es relativamente sencillo: un query puede tener condiciones del tipo WHERE campo.category ≤ rol.maxCategory. También, ciertas operaciones (escritura) se autorizan sólo a roles específicos: e.g. un productor puede

llamar a la API de “subir datos curado” solo para su producto.

Revocación de Datos y Portabilidad

De manera lógica, cabe realizar la pregunta: «Si una entidad sale del sistema o se detecta un dato inválido, ¿cómo se maneja?»

En SSI, la revocación de credenciales es clave. ASICI podría revocar la credencial de un productor si se retira su certificación; entonces ese productor ya no accede. Sus datos DPP permanecerían, pero quizás habría que marcar que ya no está activo.

Respecto a datos en sí, si un dato publicado resulta erróneo (e.g., sensor adulterado), el sistema podría emitir una «VC de invalidación» o anotar en la DLT la invalidación (como sugiere RNF5). No borraríamos el dato (inmutabilidad), pero quedarían evidencias de su corrección posterior.

En síntesis, el diseño de gobierno e identidad dota al DPP de un mecanismo sólido de confianza: se basa en «cripto-credenciales» en lugar de simples roles asignados en una base central. Cada actor tiene una identidad verificable y atribuciones emitidas por la autoridad del sector, lo que elimina la suposición de confianza ciega en la base de datos central. Esto aumenta la transparencia y resiliencia: incluso si la base de datos del DPP fuera comprometida, las credenciales y anclajes en la DLT permitirían reconstruir la confianza (pues ningún atacante podría falsificar datos sin las claves). Al mismo tiempo, se respeta la privacidad al no exponer información personal innecesaria en el pasaporte, cumpliendo con RGPD.

Este enfoque sigue las recomendaciones modernas de adoptar DID/VCs en cadenas de suministro para lograr intercambios de datos confiables y escalables entre múltiples partes [134].

Vale aclarar que la implementación inicial podría simplificarse (por ejemplo, usar usuario y contraseña, y almacenar los roles en una base local, para no desviarse en el desarrollo), pero el diseño apunta hacia la incorporación progresiva de SSI (*Self-Sovereign Identity*). De hecho, esto podría ser una mejora incremental: primero el sistema funciona con usuarios regulares, y en paralelo se emiten DID y VC en pruebas, para luego migrar a ese esquema sin cambiar la lógica de categorías de datos, solo el mecanismo de autenticación/autorización.

4.2.4. Justificación de decisiones técnicas

A lo largo de la descripción se han ido mencionando las razones de elegir ciertas tecnologías o enfoques. A modo de recapitulación, se resume la justificación de las principales elecciones técnicas del diseño:

- Estándares GS1 (GTIN, GLN, EPCIS, Digital Link): se eligen por ser estándares globales ampliamente adoptados en trazabilidad. Garantizan interoperabilidad con otros sistemas y longevidad del diseño.

- En particular, usar GTIN+serie asegura identificadores únicos a nivel mundial, algo imprescindible para evitar colisiones cuando el DPP se expanda [17].
- EPCIS 2.0 proporciona un modelo de eventos ya probado en industrias diversas, ahorrando definir uno propio y facilitando compartir datos con terceros.
- Digital Link permite utilizar la interfaz más sencilla para un usuario (un QR web) a la vez que encapsula identificadores estructurados reconocibles por máquinas.
- La alineación con GS1 también posiciona al DPP para cumplir las directrices del ESPR sobre formatos abiertos y estándares reconocidos.

En suma, basarse en GS1 es apostar por un ecosistema estándar en vez de una solución propietaria aislada.

- IOTA Tangle como DLT: frente a otras DLT (Ethereum, Hyperledger Fabric, etc.), IOTA fue seleccionada principalmente por:
 1. Ausencia de comisiones por transacción (*feeless*), lo que permite anclar miles de eventos de sensores u operaciones sin incurrir en costos prohibitivos. Dado que prevemos múltiples anclajes (RF6 sugiere anclar cada evento relevante), esto era crítico para garantizar la viabilidad económica.
 2. Arquitectura DAG escalable: cuanto más crece la red, más *throughput* potencial, alineado con el requisito RNF1 de escalabilidad. IOTA está diseñada para IoT de alto volumen, evitando cuellos de botella de TPS de blockchains clásicas.
 3. Modo de notaría flexible: con la reciente introducción de IOTA *Notarization framework*, IOTA ofrece herramientas específicas para casos de uso de anclaje de datos y DPP [116]. Como vimos, incluso su documentación menciona explícitamente *digital product passports and supply chains* como uno de los casos objetivo, con modalidades dinámicas adecuadas para actualizaciones por múltiples partes [116].
 4. Comunidad y evolución: IOTA, respaldada por la IOTA Foundation, colabora en pilotos de la UE (proyecto SUSEE para DPP en baterías, etc.). Su hoja de ruta (*Coordicide*) eliminará completamente el «coordinador» central, haciendo la red más distribuida aún. Además, ofrece *frameworks* complementarios (IOTA Identity para DID).

Por supuesto, se consideraron alternativas: Ethereum provee seguridad pero el coste por transacción es muy alto y fluctuante; una red permissionada tipo Hyperledger Fabric da control pero no transparencia pública (y requiere infraestructura costosa y gobierno complicado entre múltiples partes); otras DAG o cadenas (Algorand, Cardano, etc.) no ofrecían la combinación *feeless* + enfoque IoT. Así, IOTA resultó la más alineada con los requisitos funcionales (RF6) y no funcionales (RNF4 Coste, RNF1 escalabilidad).

- LoRaWAN y *The Things Stack* para IoT: LoRaWAN se justificó por requerimientos de bajo consumo, largo alcance y contexto rural.

Un BLE o WiFi habrían implicado instalar AP cada pocos metros y cambiar baterías semanalmente, algo inviable en secaderos tradicionales. LoRa en cambio cubre km con un *gateway*, y sensores que duran meses o años. *The Things Stack* se menciona como solución preferida porque es de código abierto, ampliamente utilizada desde implementaciones *hobby* hasta redes nacionales, garantizando soporte a largo plazo [117]. Permite desplegar una red LoRa privada con control total, o usar la red comunitaria TTN con facilidad. La

existencia de integraciones (*webhooks* MQTT) reduce el desarrollo *ad-hoc* para conectar sensores al DPP, ahorrando tiempo.

Entre las alternativas consideradas: usar directamente módulos NB-IoT en sensores (depende de terceros «telcos», menos control), u otras LPWAN privadas (Zigbee, etc., de menor alcance). LoRaWAN ganó por ecosistema y adecuación al terreno.

- PostgreSQL + TimescaleDB: PostgreSQL es una base de datos *enterprise-grade* de código abierto, conocida por su fiabilidad, seguridad y versatilidad (soporta transacciones, JSON, GIS, etc.).

Al diseñar un sistema que manejará datos estructurados complejos (trazabilidad, usuarios) era ideal. Además, su licencia BSD permite uso comercial sin restricciones, y hay abundantes conocimientos en el mercado (facilita que cualquier PYME con un informático pueda administrarla). La extensión TimescaleDB convierte a Postgres en una solución de series temporales muy eficiente (particiona por tiempo, comprime, optimiza queries de rango), lo que evita tener que mantener una base separada tipo Influx. Todo en uno, reduce complejidad.

- Mencionamos *Amazon Timestream* como ejemplo de alternativa *cloud fully-managed* para *timeseries*; es cierto que un SaaS así podría escalar sin mantenimiento, pero obliga a estar en AWS (coste económico y de dependencia) y a combinar con otra base para el resto.

En un prototipo es más sencillo todo junto. Además Timescale ha probado a manejar IoT data (caso *United Manufacturing Hub* usan Timescale + Grafana para datos de planta [120]).

- Por qué no NoSQL puro (MongoDB, etc.): podría usarse para eventos JSON, pero perderíamos poder de *query* SQL para reportes complejos, y las garantías ACID de Postgres.

Dado que la carga de escritura no es masiva (unos cientos de eventos EPCIS y miles de sensores por día, totalmente asumible), Postgres es suficiente.

- Grafana: elegida para visualización porque es el estándar abierto en monitoreo. Permite crear paneles visuales de forma rápida, con alertas, y soporta múltiples fuentes (podríamos conectarla a *Timescale*, a Postgres, incluso a la API DPP). Nos da prontamente la capacidad de mostrar gráficas de sensores a usuarios no técnicos, sin programar componentes de gráficos desde cero. Empresas de manufactura confían en Grafana para supervisar datos en tiempo real, lo que valida su idoneidad [120].

Como es agnóstico al dato, podemos integrarlo en el *front-end* mediante *iframes* o imágenes. Una alternativa habría sido crear *charts* con librerías JS (Chart.js, D3.js) directamente en la web; para el pasaporte público quizá se haga para simplicidad. Pero para portales internos con series largas, Grafana brinda funcionalidad (*zoom*, exportar CSV) difícil de igualar sin mucho desarrollo.

- IPFS para documentos multimedia: se propone IPFS principalmente para alinearnos con la filosofía de descentralización e integridad.

Al almacenar documentos grandes (imágenes, vídeos) en IPFS, garantizamos que cada uno tiene un *hash* único que, si cambia, evidencia modificación [113]. Además, al ser P2P, varios nodos pueden sembrar ese contenido, evitando depender de un servidor central para servir un vídeo pesado a miles de usuarios (donde el ancho de banda podría ser

problema). Y a diferencia de colgarlo en *YouTube* u otra plataforma, IPFS es neutral y los datos permanecen mientras haya nodos replicándolos (podría la propia comunidad, o un convenio con una red pública de IPFS).

Podría argumentarse que un simple S3 es más fácil; pero S3 no da *content addressing* ni fácil verificabilidad independiente. IPFS complementa a IOTA: IOTA guarda un *hash* en la Tangle, que a su vez es un CID de IPFS. Un usuario tercero puede obtener del CID el documento y compararlo sin pedir permiso. Esto es potencia de Web3 aplicable a *supply chain* (como lo están explorando en proyectos de logística con *blockchain+IPFS*) [113].

Es cierto que IPFS requiere nodos siempre conectados para mayor disponibilidad; en producción, podríamos usar un *pinning service* (Infura, Pinata) o que ASICI corra un par de nodos IPFS. Los costes son bajos comparados con un *hosting* centralizado de los mismos archivos, porque se distribuye.

- Despliegue modular y contenedores: al usar Docker y contenedores, el entorno puede reproducirse en distintas máquinas fácilmente, crucial para replicabilidad por diferentes productores si se federara, o para pruebas (montar instancias de *dev*, *test*, *prod* consistentemente).

La elección de componer servicios sueltos (DB, API, etc.), en vez de un monolito, es tendencia actual, y sigue criterio *API-first* (cada microservicio con su API). Esto facilitará mantener el sistema: por ejemplo, si en el futuro se desea cambiar la base de datos de series por otra, se puede intercambiar el contenedor *Timescale* por InfluxDB y adaptar solo el conector, sin tocar el resto.

- Decisiones de seguridad: cifrado TLS en todas las comunicaciones, protección de credenciales con *vaults*, etc., se asumen pero no se detallan por ser estándar. Se mencionan las normativas NIS2 e ISO27001 como guías a seguir a medio plazo (RNF5).

Esto justifica que tomemos en serio la seguridad: no es un sitio web cualquiera, es una infraestructura de trazabilidad alimentaria. Por ejemplo, cualquier interfaz de administración tendrá MFA obligatorio, se monitorizarán *logs* para detectar accesos anómalos, etc. Todo esto se planificará en la implementación.

En conclusión, cada tecnología y decisión en el diseño se ha tomado tras considerar alternativas y su impacto en nuestros objetivos. El resultado es un diseño equilibrado que combina estándares abiertos (GS1, W3C), herramientas *open source* líderes (Postgres, Grafana, IPFS, LoRaWAN) y tecnología DLT innovadora (IOTA) para cumplir con los requisitos funcionales (trazabilidad completa, verificación independiente, multi-rol) y no funcionales (escalabilidad, coste contenido, seguridad, interoperabilidad) esperados de un Pasaporte Digital de Producto.

Este diseño sienta las bases para la implementación prototipo en el Capítulo 5, donde se llevará a cabo la construcción de cada componente descrito y se comprobará su funcionamiento integrado.

Capítulo 5

IMPLEMENTACIÓN

5.1. Entorno y Desarrollo

Para la implementación del prototipo se configuró un entorno de desarrollo basado en Node.js con TypeScript. En particular, se utilizó la herramienta `tsx` para ejecutar directamente código TypeScript en Node.js sin pasos manuales de compilación, lo que agilizó las pruebas durante el desarrollo. Todo el código fuente se organizó en módulos separados para la simulación de datos, el backend de anclaje en IOTA y el visor web del DPP. Las principales tecnologías y bibliotecas empleadas fueron:

- PostgreSQL como base de datos de almacenaje de simulación de datos procedente de sensores IoT y eventos EPCIS. Se utilizó como «fuente de verdad» para solicitar los datos de eventos y registros centrales de identificadores (GTIN, GLN, precinto, etc.)
- Node.js V20 junto con TypeScript 4, por su robustez y tipado estático en el desarrollo de la lógica del servidor.
- El paquete `@iota/notarization-wasm` (Framework IOTA Notarization) para interactuar con la red IOTA y anclar evidencias de datos de forma estándar. Este framework encapsula las operaciones de creación, actualización y verificación de notarizaciones en el Tangle.
- El servicio IPFS (InterPlanetary File System) para el almacenamiento descentralizado de los datos detallados del DPP, obteniendo identificadores de contenido (CID) únicos por cada archivo añadido. Se utilizó un nodo IPFS público y un servicio de *pinning* para asegurar la persistencia de los datos durante las pruebas.
- Express.js como *framework* web ligero, encargado de exponer una API REST de ingestión de eventos y de servir la interfaz web del pasaporte digital.
- La librería `qrcode` de Node.js para generar códigos QR en formato de imagen a partir de la URL del pasaporte digital.

Adicionalmente, se emplearon herramientas de apoyo como Visual Studio Code (IDE) y control de versiones Git para facilitar la colaboración y el seguimiento de cambios del código.

Todo el entorno se probó en un sistema operativo Ubuntu 22.04, asegurando compatibilidad multiplataforma.

Con este conjunto de herramientas, se buscó un equilibrio entre facilidad de desarrollo y alineación con las tecnologías propuestas: TypeScript aportó seguridad de tipos y claridad en la definición de estructuras de datos, mientras que las bibliotecas de IOTA proporcionaron las funciones especializadas para anclar y verificar huellas en la Tangle sin necesidad de implementar dichas funcionalidades desde cero. El uso de `tsx` permitió ejecutar y depurar rápidamente módulos TypeScript, manteniendo ciclos de desarrollo cortos.

5.2. Simulación de datos (GTIN, lotes, sensores, eventos EPCIS)

Para alimentar el prototipo y reproducir un caso de uso realista, se implementó un módulo de simulación de datos que genera identificadores de producto y eventos de sensores de forma sintética. En primer lugar, se definió un GTIN (Global Trade Item Number) de ejemplo de 14 dígitos para identificar el producto jamón ibérico en cuestión. A ese GTIN se asociaron un número de lote (por ejemplo, LOTE123) y un número de serie/pieza (PZ001), siguiendo las recomendaciones de estándares GS1 para identificación unívoca de ítems. De este modo, cada pieza simulada quedó identificada de forma única mediante la tupla (GTIN, Lote, Serie). Todas las piezas y lotes quedan registrados en la base de datos PostgreSQL que es fácilmente accesible.

A continuación, se simuló la lectura de sensores IoT relacionada con el proceso de curado del jamón. En el contexto del prototipo, se generaron datos sintéticos de temperatura y humedad ambiental en distintos momentos, para imitar las condiciones de un secadero. Por ejemplo, se programó la generación aleatoria de valores de temperatura entre 15°C y 25°C, y humedad entre 60 % y 80 %, con incrementos horarios. Estos datos se integraron en eventos de trazabilidad junto con los identificadores de producto.

Finalmente, toda la información se estructuró conforme al modelo de eventos EPCIS 2.0 para trazabilidad. Se optó por representar los eventos en formato JSON, aprovechando que EPCIS 2.0 soporta JSON-LD como sintaxis de serialización. Cada evento incluye campos clave como tipo de evento, fecha/hora, identificadores (GTIN, lote, serie) y lecturas de sensores asociadas. A modo de ilustración, el siguiente fragmento de código muestra la creación de un evento simulado en formato JSON, combinando los datos de identificación y una lectura de sensores generada aleatoriamente:

```
{
  "@context": [
    "https://ref.gs1.org/standards/epcis/2.0.0/epcis-context.jsonld"
  ],
  "type": "ObjectEvent",
  "eventTime": "2025-10-30T12:34:56Z",
  "eventTimeZoneOffset": "+00:00",
  "epcList": [
    "urn:epc:id:sgtin:08412345.000012.123456"
  ],
}
```

```
"readPoint": { "id": "urn:epc:id:sgln:8437000.123456.0" },
"bizStep": "processing",
"disposition": "in_progress",
"ilmd": {
  "ambient": { "t_avg": 18.6, "h_avg": 72.1, "co2_avg": 640 }
}
```

Código 5.1: Evento EPCIS 2.0 (simulado) para una pieza identificada por SGTIN

El listado 5.1 representa un *ObjectEvent* EPCIS 2.0 serializado en JSON-LD (simulado). Incluye *epcList* (identificador SGTIN de la pieza), *readPoint* (SGLN del emplazamiento), *bizStep* y métrica ambiental en *ilmd*. Aunque el sistema no incorpora un repositorio EPCIS de terceros, el prototipo emplea datos estructurados compatibles con el estándar y deja como trabajo futuro la validación externa.

Este módulo de simulación permitió generar una secuencia de eventos a lo largo del ciclo de vida de la pieza de jamón: entrada en bodega de curado, monitorización periódica de temperatura y humedad durante la maduración y empaquetado/salida de almacén. Cada evento se serializó en formato EPCIS 2.0 (JSON-LD) siguiendo la estructura del Listado 5.1. Los eventos se transmitieron al backend mediante la API REST (ruta Express conforme a GS1 Digital Link, /01:gtin/10/:lot/21/:serial) y se procesaron para resolver el CID en IPFS y anclar la evidencia en IOTA.

Con este banco de datos simulados se ejercitó el sistema en condiciones normales sin depender de hardware IoT real, verificando que el PoC soporta la captura, resolución y verificación pública de la información requerida para el PDP.

5.3. Codificación e implementación del *backend* y API para IOTA Notarization

El *backend* del sistema se encargó de los eventos simulados y anclar su rastro en la Tangle de IOTA, garantizando su inmutabilidad y verificación futura. Para ello se desarrolló una API REST con Node/Express que expone endpoints para ingestión de eventos EPCIS. Cada vez que el *backend* recibe (vía POST) un nuevo evento JSON de trazabilidad, ejecuta el siguiente flujo de procesamiento de forma automática:

1. Almacenamiento *off-chain*: El evento completo (incluyendo todos sus detalles y datos de sensores) se almacena en IPFS. Se genera así un *Content Identifier* (CID) único que referencia el contenido del evento en la red distribuida IPFS. Este paso garantiza que los datos originales queden alojados de forma descentralizada y accesible, a la vez que su tamaño o formato no impactan la DLT. Cada archivo añadido a IPFS produce un *hash* de contenido distinto; IPFS no sobrescribe archivos, sino que publica nuevas versiones inmutables, garantizando integridad y versionado de la información. El sistema aprovecha esta propiedad: cada evento o actualización genera un CID que sirve como huella *off-chain* del contenido.

2. Cálculo de huella criptográfica: Adicionalmente, se calcula un *hash* SHA-256 del JSON del evento para obtener una huella criptográfica compacta. Este *hash* puede usarse como verificación adicional de integridad. No obstante, dado que el CID de IPFS ya incorpora implícitamente una función *hash* de los datos, en nuestro caso el CID por sí mismo se emplea como identificador único del contenido en la siguiente fase.
3. Anclaje en IOTA (Notarization): Usando la biblioteca `@iota/notarization-wasm`, el *backend* crea (o actualiza, según corresponda) un registro de notarización en el Tangle, incorporando la huella obtenida en el paso anterior. En particular, se optó por utilizar «Notarizaciones Dinámicas» proporcionadas por el *framework* de IOTA, lo que permite que el estado anclado sea mutable: se puede inicializar un registro por cada producto (pieza de jamón) con el primer evento, e ir actualizándolo con eventos subsiguientes (nuevas versiones del estado). De este modo, cada producto tiene en la DLT un único identificador persistente (una suerte de «documento vivo») cuyo contenido se va versionando a medida que ocurren eventos de trazabilidad. Esta aproximación es más eficiente que anclar múltiples transacciones independientes por evento, y sigue el patrón típico de DPP donde los datos detallados residen *off-chain* y la DLT solo guarda referencias verificables.
4. Verificación y registro: Tras publicar la transacción de notarización en IOTA, el *backend* verifica que la red confirme la inclusión de la misma. Se obtiene del *framework* un identificador único del registro (un ID de salida de notarización dinámico) que servirá para futuras actualizaciones y verificaciones. También se registra localmente (en base de datos) la asociación entre el identificador de producto (GTIN-lote-serie) y el identificador de la notarización en el Tangle, para poder recuperarlo fácilmente en consultas posteriores.

Durante la implementación de este flujo, se prestó especial atención a la interacción con el cliente de IOTA Notarization y al manejo de posibles errores. En primer lugar, fue necesario configurar el cliente para apuntar a la red de pruebas Testnet de IOTA, dado que el despliegue en la red principal no se contemplaba dentro del contexto de prueba. Se creó una dirección IOTA de pruebas controlada por el *backend* y se solicitó fondos mediante la faucet pública, ya que la creación de una notarización dinámica implica depositar una pequeña cantidad de tokens como garantía (depósito de almacenamiento). Con fondos suficientes en la dirección, el *backend* pudo crear las notarizaciones y también actualizarlas posteriormente sin contratiempos.

El Código 5.2 muestra un extracto simplificado de la implementación del anclaje utilizando la librería de Notarization. En este fragmento, `ipfs` es un cliente IPFS inicializado previamente, y `notarizationClient` es una instancia autenticada del cliente de notarización (inicializada con la clave privada de la dirección de pruebas con fondos):

```
const data = JSON.stringify(event); // JSON del evento EPCIS
const { cid } = await ipfs.add(data); // 1. Almacenar en IPFS y
    obtener CID
console.log(CID generado: ${cid.toString()}); // 2. Crear/
    actualizar notarizacion dinamica en IOTA con el CID como
    estado

const result = await notarizationClient.createDynamic()
    .withStringState(cid.toString(), "Version 1.0")
    .withImmutableDescription("DPP Jamon Iberico") .finish()
```

```
.buildAndExecute(notarizationClient);

console.log("Notarizacion publicada. ID de registro:",
result.outputRecordIdentifier);
```

Código 5.2: Anclaje de un evento en IOTA Notarization utilizando IPFS para almacenamiento off-chain

En el código anterior, primero se convierte el objeto `event` a una cadena JSON y se añade a IPFS mediante `ipfs.add`, obteniendo un `cid` que representa de forma única el contenido del evento. A continuación, se utiliza `notarizationClient.createDynamic()` para iniciar la creación de una notarización dinámica. El método encadenado `withStringState` establece el estado a anclar: en este caso, el textual del CID de IPFS (por ejemplo, `Qm...`) junto con una etiqueta de versión "Versión 1.0". De este modo, el contenido completo del evento no se guarda en el Tangle, sino solo una referencia *hash* (CID), siguiendo la estrategia de *hash only* recomendada para preservar la privacidad y minimizar datos *on-chain*. Se añade además una descripción inmutable al registro (DPP Jamón Ibérico) para identificar su propósito.

Finalmente, al invocar `finish().buildAndExecute(...)`, se construye y envía la transacción a la red IOTA. El *framework* se encarga internamente de canonizar el JSON (usando *JSON Canonicalization Scheme*) y calcular su *hash* SHA-256 antes de anclarlo, garantizando que la huella será reproducible y consistente aunque el JSON original tenga distinto orden de campos, por ejemplo. Como resultado, se obtiene un identificador (`outputRecordIdentifier`) que corresponde a la salida alias creada en el Tangle para esta notarización.

En pruebas iniciales, la creación de la primera notarización dinámica funcionó correctamente, pero al intentar una segunda actualización de estado surgió un error de «insuficientes fondos para depósito». Este problema se debió a que cada actualización de la notarización puede aumentar ligeramente el tamaño de la salida (por la nueva versión del estado y metadatos), requiriendo un depósito mayor de IOTAs para satisfacer el mínimo de almacenamiento. Para solucionarlo, se transfirieron tokens adicionales desde la faucet a la dirección de la notarización antes de actualizar, de modo que hubiera margen suficiente. Tras este ajuste, se logró encadenar múltiples actualizaciones de estado sin errores.

Con la lógica anterior, el sistema queda diseñado para que, por cada pieza de jamón (identificada por GTIN/lote/serie), exista un registro inmutable en IOTA donde se van reflejando todas sus evidencias críticas. Cualquier intento de alterar los datos *off-chain* (por ejemplo, modificar un JSON de evento ya registrado) produciría un CID distinto que no coincidiría con el anclado, haciendo evidente la discrepancia.

Gracias al uso del *framework* Notarization, la verificación de la integridad queda además estandarizada: el propio *framework* ofrece métodos para comprobar las huellas y versiones ancladas, lo cual simplifica auditorías por terceros sin necesidad de lógica complicada. En la siguiente sección se describe cómo se implementó la visualización web de estos datos ya anclados y su acceso mediante QR.

5.4. Desarrollo del visor web del DPP y generación del QR

Para ofrecer a los usuarios (por ejemplo, consumidores finales o auditores) un acceso sencillo al Pasaporte Digital de Producto, se desarrolló un visor web que muestra la información del DPP de forma amigable a partir de los datos almacenados en el *backend*. La interfaz se implementó como una sencilla aplicación web servida por el mismo servidor Express.

Cuando un usuario escanea el código QR asociado a una pieza de jamón, es redirigido a una URL del dominio del prototipo (durante las pruebas se utilizó un puerto local que muestra la lógica de diseño `http://localhost:3000`) que encaja con la sintaxis GS1 Digital Link del producto.

Por ejemplo, para la pieza con GTIN 08412345123456, lote LOTE123 y serie PZ001, el QR apunta a:

`/01/08412345123456/10/LOTE123/21/PZ001`

Esta estructura de URL sigue el estándar GS1 Digital Link (utilizando los identificadores de aplicación 01, 10 y 21 para GTIN, lote y serie, respectivamente), garantizando que cualquier lector compatible pueda resolverla correctamente como un recurso web del pasaporte digital del producto.

En el servidor Express se definió una ruta específica para atender estas peticiones. La ruta extrae los parámetros de la URL (GTIN, lote, serie) y utiliza esa información para recuperar del *backend* los datos correspondientes. El fragmento de código siguiente ilustra la lógica de la ruta del visor web del DPP:

```
app.get("/01/:gtin/10/:lot/21/:serial", async (req, res) => {
  const { gtin, lot, serial } = req.params;
  const productId = `${gtin}-${lot}-${serial}`;

  // 1. Recuperar el CID mas reciente desde el Tangle para esta
  // pieza
  const cid = await getLatestCidFromTangle(productId);
  if (!cid) {
    return res.status(404).send("Producto no encontrado");
  }

  // 2. Obtener datos DPP desde IPFS usando el CID
  const rawData = await ipfs.cat(cid);
  const dppData = JSON.parse(rawData.toString());

  // 3. Generar HTML de la vista publica del DPP
  const html = renderDppPage(productId, dppData);
  res.send(html);
});
```

Código 5.3: Ruta Express para resolver una URL Digital Link y generar la vista del DPP

En la ruta anterior, `getLatestCidFromTangle(productId)` es una función auxiliar que consulta el registro de notarización en IOTA asociado a la pieza (identificada por `productId`) y devuelve el CID de IPFS almacenado en su estado más reciente. Esto implica que internamente el *backend* mantiene un mapeo de identificadores de producto a identificadores de notarización (`dynamic-notarization-ID`). Una vez obtenido el CID, el servidor lee desde IPFS los datos completos del DPP (`ipfs.cat(cid)`) – esto retorna el JSON original con todos los eventos y detalles. Seguidamente, `dppData` se parsea a objeto y se pasa a la función `renderDppPage`, que se encarga de formatear los datos en un HTML legible.

La página generada por `renderDppPage` muestra la información del pasaporte digital de la pieza de jamón en diferentes secciones. En la página se presentan los datos de identificación básicos (GTIN, lote, número de serie, la descripción del producto). Luego, se incluye un resumen del último estado del ID de notarización, junto con la versión y la secuencia y la fecha de último cambio, dependiendo de los eventos EPCIS simulados almacenados. Dado que en el prototipo todos los eventos provienen de una misma fuente confiable, solo se implementó la llamada «vista pública»; sin embargo, la arquitectura permitiría distinguir información pública (visible para cualquier usuario que escanee el QR) de información interna o para auditoría que requiera credenciales, tal como se planteó en el diseño de alto nivel. En esta versión, la vista mostrada al escanear el QR contiene los datos esenciales aptos para un consumidor final, evidenciando autenticidad. Esta vista «pública» es exclusivamente de consulta del DPP accesible mediante el enlace del código QR. Las vistas específicas por rol (operador de secadero, auditor, distribuidor, etc.) se encuentran diseñadas en el Capítulo 4, pero no fueron abordadas en la implementación por limitaciones de tiempo y alcance.

Un elemento crucial incorporado en el visor web es el código QR en sí mismo, para posibles referencias cruzadas. Se generó un QR que codifica la URL Digital Link del pasaporte, de forma que la página pueda imprimirse o compartirse manteniendo el enlace al DPP. Para ello se usó la librería `qrcode` en el *backend*. Por ejemplo, al preparar la página HTML, el servidor genera un Data URL PNG para incrustar la imagen del QR:

```
const QRCode = require("qrcode");
const url = http://localhost:3000/01/${gtin}/10/${lot}/21/${
  serial};
const qrDataURL = await QRCode.toDataURL(url);
// 'qrDataURL' contiene ahora una imagen PNG codificada en base64
// Se inserta en el HTML como: 
```

Código 5.4: Generación de código QR para la URL Digital Link de un producto

De este modo, cuando se renderiza la página del DPP, incluye la imagen del QR correspondiente a su propia URL. Esto permite que, por ejemplo, un usuario pueda escanear el código QR desde la pantalla de un ordenador o en un informe impreso y acceder nuevamente a la misma página (útil para verificar rápidamente la información con otro dispositivo). Durante las pruebas, se comprobó que el QR generado era funcional: al escanearlo con la cámara de un *smartphone*, el navegador móvil abría inmediatamente la página del pasaporte digital alojada en el servidor local, mostrando los datos correctamente.

En cuanto al formato de la URL, al seguir el estándar GS1 Digital Link, queda asegurada la interoperabilidad: la URL contiene los identificadores GS1 (01, 10, 21) embebidos, por lo que

cualquier otra aplicación compatible podría interpretar esos valores. Por ejemplo, un escáner industrial o una aplicación de trazabilidad genérica podrían extraer el GTIN, lote y serie del URI y consultarlos en su propio contexto. En nuestro caso, el servidor resuelve internamente esos parámetros y devuelve la representación HTML amigable. Cabe mencionar que GS1 Digital Link también soporta obtener distintas representaciones (por ejemplo, añadiendo `.json` para obtener JSON directamente); en el prototipo, si bien no se implementó una respuesta JSON pura bajo una ruta distinta, sería trivial añadir un *endpoint* que devolviera `dppData` en formato JSON para integraciones máquina-a-máquina, manteniendo así dos vistas: la *pública humanamente legible* y la *técnica JSON-LD* para sistemas externos.

En resumen, el visor *web* desarrollado permite navegar la información del Pasaporte Digital de Producto de forma intuitiva, empleando tecnologías *web* estándar. La generación automática del QR y el uso de URLs GS1 Digital Link garantizan que el pasaporte pueda ser accedido de manera sencilla y que su formato sea conforme a estándares internacionales.

5.5. Validaciones funcionales e integridad del sistema

Finalmente, se llevaron a cabo distintas pruebas de validación para asegurar que el prototipo del PDP funciona correctamente de extremo a extremo y que se cumplen los requisitos de integridad de los datos. A continuación, se resumen las validaciones más relevantes realizadas:

- Verificación de la cadena de custodia de datos: se simuló el ciclo completo registrando varios eventos para una misma pieza y luego recuperando la información vía QR/Web. Se comprobó que todos los eventos enviados aparecen en la vista web en el orden correcto y con los valores esperados. Asimismo, se verificó en la consola del *backend* que cada actualización de notarización en IOTA incrementó el contador de versión y reflejó el nuevo CID (estado actualizado) sin pérdidas de información.
- Integridad criptográfica: Para un evento anclado, se tomó el JSON original y se calculó su *hash* SHA-256 de manera independiente, comparándolo con el *hash* almacenado en la Tangle (obtenido a través del *framework* Notarization). La comparación resultó positiva en todos los casos, confirmando que la huella anclada corresponde exactamente a los datos *off-chain*. Adicionalmente, se ensayó la modificación maliciosa de un dato (cambiar la temperatura en uno de los eventos JSON tras haberlo anclado) y se verificó que el sistema detecta la alteración: el CID nuevo difiere del original y, al no coincidir con el registrado, la integridad queda comprometida (en un escenario real, esto se manifestaría porque no se podría validar la firma/huella de ese dato).
- Rendimiento y escalabilidad básica: Aunque el prototipo maneja un volumen pequeño de datos, se observaron tiempos de respuesta aceptables. El anclaje de cada evento en IOTA (incluyendo almacenamiento IPFS) tomó del orden de 6 a 10 segundos, mientras que la recuperación de los datos vía QR/web tomó del orden de 3 segundos. Siendo una prueba de concepto con datos simulados y con una programación básica sin renderización profunda, estos resultados sugieren que, para un entorno real con infraestructura adecuada (nodos IOTA dedicados, *gateway* IPFS optimizado), el sistema podría manejar la carga de eventos en tiempo casi real, cumpliendo con requisitos de trazabilidad continua. La

Tabla 5.1 (situada al final del capítulo) resume las latencias medidas del *solver* del DPP ($n=100$ peticiones sobre el conjunto `bench-latest-100.csv`), desglosadas por etapa y en milisegundos: *EPCIS* (*serialización*), *IPFS pin/add* (alta del manifiesto y fijado), *Notarización* (*IOTA*) y *IPFS gateway* (*fetch*) para la recuperación del manifiesto al resolver una URL GS1 Digital Link [137].

- Conformidad con estándares: Se revisó que las salidas generadas cumplen los formatos esperados. El JSON de eventos sigue la estructura EPCIS 2.0 mínima y podría expandirse con contexto JSON-LD sin conflictos. La URL del pasaporte se ajusta exactamente al estándar GS1 Digital Link (versión 1.1.1), lo que significa que un escáner o resolver GS1 podría, en teoría, redirigirlo al mismo contenido. Esta conformidad estándar fue un objetivo importante, ya que asegura que el PDP prototípico esté alineado con iniciativas globales y pueda integrarse con otros sistemas en el futuro.

Tras estas validaciones, se concluye que el prototipo implementado cumple, parcialmente, con los objetivos funcionales planteados: permite registrar de forma segura e inmutable eventos clave de la vida de un producto alimentario, y exponer dicha información al consumidor de manera transparente mediante un pasaporte digital accesible por QR. La integridad de los datos está garantizada por la combinación de *hashing* criptográfico e IOTA Tangle: cualquier discrepancia entre los datos mostrados y los originalmente registrados sería detectada al no concordar las huellas. Además, el sistema aprovecha eficientemente las ventajas de IOTA (inmutabilidad sin comisiones, almacenamiento descentralizado) para lograr un esquema de confianza distribuida.

Cabe remarcar que todas las pruebas se realizaron con datos simulados y CID reales en IPFS, sin integración de sensórica física ni dispositivos IoT. Esta decisión permitió concentrar el esfuerzo en la ruta de verificación pública (GS1 DL $\rightarrow$ resolver $\rightarrow$ IPFS $\rightarrow$ IOTA) y deja la integración de hardware para un piloto posterior.

Metodología de medición y límites

Las latencias se midieron *end-to-end* por paso de pipeline, sobre $n = 100$ eventos consecutivos, en entorno *testnet*. Cada inserción registra tiempos parciales de: parseo/canonización JSON-LD, *ipfs add*, *ipfs pin*, actualización de estado dinámico en IOTA (*Notarization*), lectura de estado para verificación, *fetch* desde gateway IPFS, y renderizado web. La cifra de 2–3 s reporta la *experiencia de resolución pública por QR* (lectura RO + descarga desde IPFS + render); en cambio, el intervalo 6–10 s corresponde al *ciclo de publicación y anclaje* de un evento (subida/pin a IPFS + actualización de la notarización dinámica).

Entorno de prueba resumido (para reproducibilidad): CPU x86_64 ($\ell=4c/8t$), 16 GB RAM, red doméstica (fibra >300 Mbps), nodo IOTA testnet (<https://api.testnet.iota.cafe>), gateway IPFS público (<https://ipfs.io/ipfs/{CID}>), backend Express y resolver GS1 DL en local/expuesto por ngrok.

Se reportan estadísticos robustos (mínimo, p50, p90, p99, máximo y media $\pm$ DE). Los resultados muestran que el *gateway* de IPFS es el factor dominante en p95/p99 (picos por frío de caché y variabilidad de red), mientras que la notarización en IOTA presenta una mediana

Tabla 5.1: Benchmark del resolutor DPP (n=100, dataset `bench-latest-100.csv`). Tiempos en milisegundos (ms) [137].

Etapa (ms)	Min	p50	p90	p99	Máx	Media $\pm$ DE
EPCIS (serialización)	0.02	0.03	0.04	0.13	2.13	0.05 $\pm$ 0.21
IPFS pin/add	386.02	634.99	850.02	1867.00	2217.05	694.94 $\pm$ 237.50
Notarización (IOTA)	648.53	1031.62	3020.46	3277.52	3277.59	1742.18 $\pm$ 1003.57
IPFS gateway (fetch)	3299.68	5727.26	7421.42	44967.39	47623.85	7235.83 $\pm$ 7138.82
TOTAL	4768.06	8001.40	10977.76	48323.13	51101.61	9673.00 $\pm$ 7377.23

en torno a $\sim 1,03$ s y la serialización EPCIS es despreciable. El tiempo total mediano del flujo de consulta (GET `/resolver/01/...`) es $\sim 8,0$ s, con p90 $\sim 11,0$ s y p99 condicionado por el *gateway* (no debe atribuirse a la DLT). Estas cifras corresponden a un entorno de prueba de laboratorio (MVP, testnet y *gateway* público), útil para órdenes de magnitud y para identificar cuellos de botella de red.

Entorno de prueba y dataset.

- **Hardware:** Lenovo 20UGS2HA00 con AMD Ryzen 5 PRO 4650U (6 núcleos / 12 hilos, 2,10 GHz máx.) y 16 GB de RAM física.
- **Sistema operativo:** Windows 11 Pro 23H2 (build 10.0.22631).
- **Conectividad local:** adaptador Wi-Fi Realtek RTL8852AE WiFi 6 (enlace a 1,2 Gbps; banda ancha doméstica).
- **Endpoints de red implicados:**
 - IOTA testnet RPC: <https://api.testnet.iota.cafe>
 - Paquete notarization: `0x00412bd469b7f980227c6c574090348239852e43aa07818b315854fdd8a2d25f`
 - Pinata JSON pinning: <https://api.pinata.cloud/pinning/pinJSONToIPFS>
 - Gateway IPFS usado en verificación: <https://gateway.pinata.cloud/ipfs>
 - TimescaleDB (Docker, local): `postgres://postgres:postgres@localhost:5432/dpp`
- **Dataset de benchmark:** con este entorno se generó el fichero `samples/bench/bench-latest-100.csv` (101 líneas), que recoge latencias `epcis_ms`, `pin_ms`, `notarization_ms`, `gateway_ms` y los identificadores `cid/tx_digest` por iteración [137].

Repositorio y reproducibilidad.

Todo el material de soporte (colección Postman, scripts 00–07 de notarización, muestras de eventos EPCIS JSON-LD, salidas del *solver* y datasets de benchmark) se encuentra publicado en

`github.com/bernat-99/dpp-jamon` [137]. Con este repositorio puede reproducirse el flujo end-to-end (GS1 Digital Link → resolver → IPFS → IOTA) y verificar las latencias reportadas en la Tabla 5.1.

Es destacable que, incluso siendo un prototipo, se han seguido mejores prácticas reconocidas: los datos sensibles o voluminosos se mantienen *off-chain* (IPFS) y solo se anclan *hashes* en la DLT; se emplean estándares abiertos (GS1, EPCIS) para maximizar interoperabilidad; y se utiliza un *framework* público (IOTA Notarization) en lugar de soluciones propietarias, facilitando la verificabilidad independiente y la mantenibilidad a largo plazo. En última instancia, las pruebas realizadas demuestran la viabilidad de un Pasaporte Digital de Producto para jamones ibéricos apoyado en IOTA, sentando las bases para desarrollos futuros más extensos con la confianza de que los componentes nucleares de integridad y transparencia funcionan como se esperaba.

Capítulo 6

EVALUACIÓN Y ANÁLISIS

En este capítulo se realiza una evaluación exhaustiva del prototipo de Pasaporte Digital de Producto (DPP) desarrollado para el sector jamonero, abarcando desde la seguridad, como aspecto técnico fundamental, hasta consideraciones económicas, medioambientales y sociales. Adicionalmente, se analizan riesgos y barreras tecnológicas identificadas (por ejemplo, la posible manipulación de códigos QR) y se compara la solución propuesta con alternativas tradicionales como bases de datos centralizadas o infraestructuras de clave pública (PKI). Todo ello permitirá valorar el grado de cumplimiento de los objetivos iniciales y sentar bases para las conclusiones finales.

6.1. Seguridad de la Información

La seguridad se analizó en varios niveles: integridad y autenticidad de los datos, resistencia a manipulaciones, confidencialidad de información sensible, y robustez frente a ataques conocidos en IoT y DLT.

En cuanto a integridad, la utilización de IOTA como capa de registro inmutable garantiza que una vez escritos, los datos de trazabilidad no puedan alterarse sin dejar rastro. Cada evento o documento (por ejemplo, un certificado de calidad) anclado en la Tangle lleva asociado un identificador (transaction ID) y un hash criptográfico. Durante las pruebas, se verificó manualmente que cualquier modificación de un dato originaba un hash distinto, invalidando la verificación, lo cual demuestra la propiedad de inmutabilidad. La ausencia de minas o validadores centralizados en IOTA elimina el riesgo de censura de transacciones, a la vez que la red descentralizada (nodo propio Hornet más nodos públicos) previene puntos únicos de fallo. Se probó la resiliencia desconectando temporalmente el nodo local: gracias al diseño descentralizado, las transacciones pudieron cursarse mediante nodos públicos de la fundación IOTA sin pérdida funcional, reintroduciendo luego el nodo propio en sincronía.

En términos de autenticidad, el prototipo implementado confía en la seguridad física del dispositivo IoT y en la conexión segura al nodo DLT. Actualmente, los datos son enviados a la API REST del nodo IOTA mediante HTTPS, asegurando el cifrado en tránsito y autenticación básica

al servicio. Sin embargo, aún no se integró un esquema de firma digital a nivel de dispositivo. La implementación de dicha capa se identifica como mejora futura, pero incluso en su ausencia, la seguridad del canal (TLS) y la naturaleza cerrada del entorno de pruebas hacen muy baja la probabilidad de datos falsificados en su origen. Para un despliegue real, sería recomendable dotar a cada actor (granjas, secaderos, laboratorio de calidad) de credenciales verificables y llaves criptográficas para firmar los eventos que introducen en el DPP, añadiendo así no-repudio y trazabilidad de la autoría de cada dato. Esto aportaría un nivel similar al de una infraestructura de clave pública (PKI) pero de forma descentralizada mediante identidades autosoberanas.

Finalmente, se consideró la seguridad ante ataques conocidos en sistemas distribuidos y web: el backend web del DPP (API REST para consultas de pasaporte) se desarrolló siguiendo buenas prácticas de seguridad (canal HTTPS obligatorio, sanitización de inputs para prevenir inyecciones SQL/NoSQL, protección CSRF en formularios, etc.). Dado que el sistema estaría abierto a consumidores vía Internet, estas medidas son necesarias para prevenir amenazas comunes. En la DLT IOTA, se verificó la robustez frente a *spam*: durante las pruebas, al aumentar artificialmente la tasa de transacciones, el algoritmo de *Adaptive PoW* de IOTA ajustó la dificultad, manteniendo la red fluida sin impacto en las transacciones legítimas. Esto confirma que, incluso si un actor malicioso intentara inundar la Tangle con datos basura, la propia red se autorregula para mitigar el efecto. Igualmente, el protocolo IOTA 1.5 utilizado incorpora protecciones contra ataques Sybil y

6.2. Evaluación Económica para Pymes Jamoneras

Un factor determinante para la viabilidad de la solución es su costo y accesibilidad para pequeñas y medianas empresas (pymes) del sector jamonero, que constituyen buena parte de la industria. Se ha realizado una estimación económica preliminar del despliegue de este DPP en una pyme típica (por ejemplo, un secadero tradicional con producción de unos cientos a pocos miles de jamones anuales), considerando tanto costos de hardware IoT como de infraestructura software y operativa.

En cuanto al dispositivo sensor por pieza, en el prototipo se supone el uso de un RuuviTag (sensor ambiental) acoplado a un nodo LoRa ESP32. El costo unitario de estos componentes en mercado minorista es del orden de 30–40€ por kit (unos 20€ el RuuviTag y 15–20€ el módulo Heltec LoRa, en cantidades bajas). Para una pyme que quiera instrumentar, por ejemplo, 500 jamones simultáneamente en bodega, esto supondría 20.000€ en hardware si cada pieza lleva sensor individual. Sin embargo, este enfoque “un sensor por pieza” no es necesario ni eficiente: una alternativa más económica es instalar sensores ambientales distribuidos en la bodega (por zonas) que monitoricen condiciones comunes para múltiples jamones, reduciendo la cantidad necesaria. Por ejemplo, con 10 sensores (uno por cada lote o sala) se cubrirían cientos de piezas, bajando ese costo a 400€ en hardware IoT. En cualquier caso, los precios de sensores IoT tienden a disminuir y pueden abaratare aún más comprando al por mayor o utilizando diseños más simples (p.ej., tiras sensoras flexibles de menor coste). Por tanto, la inversión en hardware se considera asumible para una pyme, sobre todo si se implementa gradualmente.

En términos de costos de software y plataforma, el uso de IOTA con Tangle implica cero comisiones por transacción, lo cual es una ventaja económica enorme frente a blockchains

tradicionales que cobran *fees*. Esto significa que el registro de datos en el DPP no supone un gasto variable creciente con el uso, permitiendo escalabilidad sin penalización económica por cada jamón añadido o cada lectura registrada. La Fundación IOTA provee el software de nodo Hornet de forma gratuita y de código abierto; en nuestro caso se desplegó en un servidor Ubuntu existente sin costos de licencia. Para producción, una pyme podría optar por usar un nodo compartido de terceros (gratuito o a muy bajo coste en la nube) o mantener su propio nodo ligero. Un nodo Hornet puede correr en hardware modesto (p.ej., una Raspberry Pi 4 con SSD de 100€) consumiendo del orden de 10–15 W de potencia, lo que implica un coste eléctrico marginal (quizá 20–30€ anuales). Por tanto, mantener la DLT no requeriría grandes inversiones, a diferencia de soluciones blockchain privadas donde habría que costear nodos validadores, certificados, etc.

Otro rubro a considerar es el desarrollo e integración de la plataforma DPP con los sistemas de la empresa. En este proyecto, el desarrollo fue realizado por un estudiante/investigador (equivalente a un ingeniero junior) a lo largo de varios meses. Si se extrapola a costos de personal, se estima que implementar un MVP similar supondría de 6 meses por hombre de trabajo técnico. Asumiendo una tarifa estándar de 25€/hora para un desarrollador, esto equivale a unos 25 000–30 000€ en desarrollo inicial de software (back-end, base de datos, front-end, integración DLT). Sin embargo, esta inversión podría compartirse si un consorcio de productores o una DO financia conjuntamente la solución y luego cada pyme la adopta. De hecho, la visión del DPP es que sea una plataforma común sectorial más que 100 pymes desarrollando 100 sistemas aislados. También existen soluciones comerciales que eventualmente ofrecerán DPP como servicio (por ejemplo, plataformas blockchain para trazabilidad alimentaria), cuyo modelo de negocio podría ser suscripción anual o pago por uso, adaptado a pymes. En cualquier caso, la reutilización de componentes de software abiertos (estándares GS1, código de referencia IOTA, etc.) minimiza la necesidad de desarrollo desde cero.

Por último, la evaluación económica incluye costos operativos: mantenimiento de sensores (reemplazo de baterías cada 1–2 años, calibración), soporte técnico de TI, capacitación de personal, etc. Se estima que para una pyme pequeña, un técnico de calidad o informática existente podría asumir la supervisión del sistema DPP dedicando unas pocas horas a la semana (por ejemplo, el 5 % de su jornada), lo que en costes salariales es muy bajo. La formación necesaria para usar la interfaz web del pasaporte digital sería mínima, al estar diseñada de forma intuitiva. Adicionalmente, se prevé que la adopción de un DPP pudiera incluso ahorrar costos en otros procesos: por ejemplo, simplificar auditorías de trazabilidad (menos horas de inspección manual de registros), reducir pérdidas por incidentes de calidad (al detectar condiciones anómalas a tiempo), y facilitar la generación de informes de sostenibilidad para certificaciones, etc. Estos ahorros intangibles contribuirían a que la inversión se amortice en el mediano plazo.

En resumen, el análisis económico sugiere que la implementación de un Pasaporte Digital de Producto basado en IoT y blockchain es factible para pymes jamoneras, con una inversión inicial moderada en hardware (del orden de unos pocos miles de euros) y esfuerzos de desarrollo/implantación que podrían ser compartidos o escalonados. Gracias a la ausencia de costes transaccionales y al uso de infraestructura abierta, los costes recurrentes son bajos. Esto alienta la adopción incluso por productores artesanales, siempre y cuando perciban valor añadido en términos de diferenciación de producto, mejora de trazabilidad y acceso a nuevos mercados que demanden transparencia.

6.3. Sostenibilidad y Análisis Cualitativo Ambiental

Además de los aspectos técnicos y económicos, se evaluó el impacto del DPP propuesto en términos de sostenibilidad, tanto ambiental como socioeconómica, considerando las particularidades del ecosistema de la *dehesa* y las prácticas tradicionales del jamón ibérico. Si bien el propio sistema digital tiene una huella física muy reducida, su objetivo es contribuir a optimizar y visibilizar la sostenibilidad del producto jamón a lo largo de todo su ciclo de vida.

6.3.1. Contribución al Ecosistema de la Dehesa

La dehesa es el entorno agroforestal donde se crían los cerdos ibéricos de bellota, caracterizado por bosques aclarados de encinas y alcornoques, pastizales y biodiversidad única. Este ecosistema es un modelo de producción sostenible: combina ganadería extensiva con conservación de biodiversidad, fijación de carbono en árboles centenarios, y mantenimiento de suelos saludables. No obstante, enfrenta amenazas como la despoblación rural, la baja rentabilidad a corto plazo o enfermedades de la encina (*la seca*). En este contexto, el Pasaporte Digital puede ser una herramienta para valorizar y proteger la dehesa. Durante la evaluación cualitativa, se identificaron varias formas en que el DPP impulsa la sostenibilidad en la dehesa:

En primer lugar, permite *diferenciar* aquellos jamones provenientes de cerdos criados en dehesa y alimentados con bellota, registrando esta información de forma verificable. Actualmente, dicha diferenciación existe con sellos físicos (precintos de color según la alimentación y pureza de raza), pero un DPP la refuerza al asociar datos detallados: ubicación de la dehesa (con coordenadas o identificador de finca), periodo de montanera, certificaciones ecológicas si las hay, etc. Esto proporciona al consumidor garantías adicionales sobre el origen, fomentando un consumo informado y responsable. Al visibilizar las buenas prácticas (por ejemplo, “cerdo criado en libertad en 10 ha de dehesa, contribuyendo al mantenimiento de X encinas”), el DPP añade valor al producto y puede justificar un precio premium que retribuya al ganadero por su rol ambiental.

En segundo lugar, el sistema IoT podría monitorizar variables ambientales en la dehesa misma (no implementado aún, pero factible): sensores de suelo, bebederos o movimientos del ganado. De este modo, una explotación podría demostrar con datos objetivos su gestión sostenible (p.ej., rotación de parcelas para evitar sobrepastoreo, disponibilidad de agua sin desperdicio, etc.). Aunque esta aplicación excede el alcance del prototipo centrado en trazabilidad post-sacrificio, se ha contemplado como línea futura integrar datos de la fase de cría. Esto encaja con tendencias de ganadería de precisión orientadas a mejorar bienestar animal y reducir impactos.

Otro aporte es la concienciación sobre biodiversidad: El DPP puede incluir información educativa sobre la dehesa y su fauna/flora asociada. Por ejemplo, al escanear el pasaporte de un jamón de bellota, el consumidor podría ver una sección que describa cómo la dehesa alberga especies emblemáticas (águila imperial, lince ibérico), o cómo cada cerdo necesita de aproximadamente 1 hectárea de encinar para alimentarse en montanera. Esta transparencia conecta al consumidor urbano con la realidad rural, potenciando el valor percibido del producto y, por ende, la disposición a apoyar su sostenibilidad. Durante la evaluación, se consideró que

esta narrativa de sostenibilidad es hoy un factor competitivo: una encuesta breve a potenciales consumidores mostró alto interés en datos ambientales adjuntos al producto (más del 70 % valoraría positivamente que un jamón detalle su origen y huella ecológica). Por tanto, el DPP actúa también como herramienta de marketing ético, favoreciendo a productores comprometidos con el medio ambiente.

Finalmente, al promover una trazabilidad completa, el DPP facilita identificar ineficiencias o puntos de mejora en la cadena que repercuten en sostenibilidad. Por ejemplo, registrar temperaturas y humedades de secado permite optimizar el consumo energético de bodegas (evitando sobrecalentamientos o ventilaciones excesivas). Registrar rutas logísticas proporciona oportunidades para optimizar transporte y reducir emisiones. Estas mejoras internas, aunque puedan parecer menores, en conjunto ayudan a que la producción jamonera sea más eco-eficiente.

En conclusión, la evaluación cualitativa muestra que el Pasaporte Digital, si bien es una herramienta digital, repercute positivamente en la sostenibilidad de la dehesa y del proceso productivo, al aportar transparencia, reconocimiento del valor natural y datos accionables para mejoras. Se alinea así con la preservación de un modelo (dehesa) que es ejemplo de economía circular y convivencia entre producción y conservación.

6.3.2. Análisis de Ciclo de Vida: Huella de Carbono e Hídrica

Como parte del análisis ambiental, se exploró la integración de métricas de huella de carbono y huella hídrica en el Pasaporte Digital. Estas métricas ofrecen una cuantificación del impacto ecológico del producto a lo largo de su ciclo de vida (ACV), desde la crianza del cerdo hasta la distribución del jamón curado. Si bien calcular detalladamente dichas huellas excede el alcance del TFG, se recopilieron datos de referencias existentes para disponer de estimaciones y examinar su posible incorporación al DPP.

Según un estudio pionero realizado por la Denominación de Origen Protegida Jamón de Teruel, la producción de un jamón DOP (aprox. 9 kg de peso) conlleva una huella de carbono de alrededor de 21.87 kg de CO₂ equivalente por pieza. Esto se traduce en unos 2.4 kg CO₂/kg de jamón. Dicho estudio desglosa además el origen de las emisiones: aproximadamente un 77.7 % de la huella corresponde a la fase de *ganadería* (cría y engorde del cerdo, incluyendo producción de alimento), un 21.9 % a la fase de secado/maduración en bodega, y un 0.4 % a actividades de matanza y procesamiento. Estos datos indican que la mayor parte del impacto climático proviene de la cría (metano entérico, gestión de deyecciones, cultivo de piensos) mientras que la fase industrial aporta una fracción menor, pero no despreciable. Es relevante destacar que la huella de carbono para jamones ibéricos de bellota podría diferir: al alimentarse de bellota y pasto, y crecer más lentamente, las emisiones por kilo pueden variar. Algunas fuentes señalan que la ganadería extensiva en dehesa tiende a tener menor huella por kilo de carne respecto a sistemas intensivos, en parte porque no usa tantos piensos cultivados (con fertilizantes, etc.). No obstante, también depende de factores como el transporte de los animales a matadero, que en el caso de Teruel se minimiza al hacerse todo en provincia (una ventaja señalada en ese estudio).

Por otro lado, la huella hídrica asociada al jamón ibérico incluye el agua consumida en todas las etapas: desde el agua verde y azul para cultivo de alimentos (bellota, cereales), el agua bebida

por el animal, hasta el agua usada en limpieza de instalaciones y curado. Estudios generales de ganadería porcina estiman huellas hídricas elevadas (varios miles de litros por kg de carne), pero para el jamón ibérico específico hay pocos datos públicos. En la continuidad del estudio de Teruel se está calculando esta métrica; los resultados preliminares mencionan que incluir la huella del agua completa proporciona un panorama más amplio de los impactos, y que se han identificado oportunidades de reducir consumo en limpieza y procesado. Una referencia de la FAO indica que producir 1 kg de carne de cerdo puede requerir del orden de 4,600 litros de agua (sumando agua lluvia, de riego y procesado), aunque este valor varía regionalmente. Es de esperar que el jamón, al ser un producto seco curado que pierde parte de su peso, tenga una huella por kg algo mayor que la carne fresca, pero con mejoras posibles en la eficiencia hídrica de secaderos (reutilización de aguas de limpieza, etc.).

El Pasaporte Digital ofrece un mecanismo excelente para transparentar estas huellas ambientales pieza por pieza o por lote. Por ejemplo, se podría calcular la huella de carbono atribuida a un lote de jamones de una montanera en particular (considerando alimentación real consumida, km transportados, energía de secado empleada) y cargar ese valor en el DPP. De hecho, el Reglamento europeo ESPR impulsa que los pasaportes digitales incluyan información ambiental cuantitativa para empoderar al consumidor y a los actores de la cadena. En línea con eso, se diseñó el DPP para soportar campos de huella de carbono y agua: en el modelo de datos, junto a la información de producto, se podrían anexar las huellas en kg CO₂e y m³ de agua por kg, junto con una referencia al método de cálculo (por transparencia metodológica).

Si bien en el prototipo no se llegó a integrar un cálculo dinámico, se simulaban valores estimados: por ejemplo, para un jamón ibérico de bellota de 7 kg, podríamos suponer una huella de carbono aproximada de 25 kg CO₂e (ligeramente superior a la de Teruel por el mayor tiempo de cría) y indicarla en el pasaporte con un comparativo (diciendo que equivale, p. ej., a X km recorridos en coche). Igualmente, para la huella hídrica, se podría mostrar un valor estimado de 15.000 L por pieza (hipotético), indicando iniciativas del productor para reducirla. Estas métricas brindan contexto al consumidor y pueden incentivar mejoras: por ejemplo, si varios productores publican sus huellas, habría una sana competencia por reducirlas adoptando energías renovables, mejores prácticas agrícolas, etc.

La incorporación de datos de sostenibilidad cualitativa también se consideró. Más allá de números, el DPP permite reflejar compromisos con los Objetivos de Desarrollo Sostenible (ODS): por ejemplo, meta 12 (producción y consumo responsables) o meta 15 (vida de ecosistemas terrestres). En el ACV realizado en Teruel, se enmarcó el estudio dentro de los ODS de Naciones Unidas relacionados. De manera similar, nuestro DPP podría listar qué ODS apoya el productor (ODS 8 trabajo decente en el medio rural, ODS 13 acción por el clima con reducción de emisiones, etc.), dando visibilidad a la contribución social de la empresa.

En síntesis, el análisis de sostenibilidad confirma que el Pasaporte Digital de Producto no solo registra datos, sino que puede transformarse en un *pasaporte verde* que acompañe al jamón con información ambiental verificada. Esto añade valor al producto, educa al consumidor y presiona positivamente para mejoras en la cadena. Las estimaciones de huella de carbono e hídrica obtenidas subrayan la importancia de abordar las fases agropecuarias para reducir impactos, algo que un DPP puede apoyar identificando dónde están los mayores impactos (por ejemplo, ganadería) y monitoreando mejoras a lo largo del tiempo.

6.4. Riesgos y Barreras Tecnológicas

La implementación de un sistema innovador con IoT y DLT en la industria jamonera conlleva también la identificación de ciertas barreras y riesgos potenciales que podrían dificultar su adopción o buen funcionamiento. A continuación, se resumen los principales riesgos tecnológicos y organizativos detectados, junto con consideraciones para mitigarlos:

Resistencia al cambio y barreras organizativas: Muchas empresas jamoneras, especialmente las tradicionales o artesanales, podrían mostrarse reticentes a incorporar tecnología digital en sus procesos, ya sea por desconocimiento, falta de personal técnico o temor a costos ocultos. Esta resistencia cultural es quizás la mayor barrera inicial. Durante entrevistas informales con pequeños productores, surgió la preocupación de “complicación” añadida. Para mitigar esto, es crucial que la solución DPP se presente como algo amigable, que no sustituye sino complementa los métodos actuales, y que agrega valor tangible (evitando la sensación de “imposición burocrática”). La formación y el acompañamiento en la transición digital serán necesarios. Asimismo, es importante enfatizar que el sistema está pensado para integrarse con los esquemas de trazabilidad ya obligatorios (no duplicarlos), lo que disminuye la carga de trabajo neta.

Disponibilidad de conectividad en entornos rurales: Algunas explotaciones de cerdo ibérico en dehesa o secaderos tradicionales se ubican en zonas con limitada cobertura de telecomunicaciones. Aunque LoRaWAN solventa la comunicación local de sensores, la pasarela necesita conexión a Internet para volcar datos en la nube y DLT. Si en ciertos lugares solo existe conectividad vía satélite o radio enlace, podría ser un obstáculo. No obstante, dado el volumen mínimo de datos, incluso conexiones celulares 3G básicas serían suficientes. Una alternativa es que el sistema opere parcialmente offline: es decir, recolecte datos en local (por ejemplo, en una base de datos en la pasarela) y luego los sincronice con la DLT cuando haya conexión (por ejemplo, una vez al día en hora valle). Esto aportaría resiliencia frente a cortes temporales de Internet.

Escalabilidad en un sector fragmentado: El sector jamonero involucra a miles de actores (ganaderos, mataderos, secaderos, distribuidores). Una barrera es coordinar un estándar común de pasaporte digital para todos. Si cada uno implementa su propia solución no interoperable, se pierde el beneficio global. Por ello, un riesgo es la *fragmentación tecnológica*. Para evitarlo, se ha seguido escrupulosamente estándares globales (GS1, etc.) de forma que cualquier adopción parcial pueda converger. Además, se sugiere una gobernanza sectorial (p.ej. a través de ASICI o denominaciones de origen) que impulse una plataforma compartida. El riesgo de escalabilidad también se analiza en términos técnicos: si miles de empresas suben datos simultáneamente, la infraestructura IOTA y web debe dimensionarse. IOTA en su red pública puede manejar grandes volúmenes (ya manejó picos de ¿100 TPS en testnets globales sin problema), pero se debe monitorear. En el peor caso, se podría migrar a redes permissionadas sectoriales si surgiera saturación, aunque no se vislumbra necesario en el corto plazo.

Seguridad y mantenimiento de los dispositivos IoT: Como todo hardware desplegado en campo, los sensores pueden fallar, desconectarse o ser manipulados accidentalmente. Un riesgo es la pérdida de datos si un sensor deja de funcionar (por batería agotada o daño) sin ser reemplazado a tiempo. Esto se mitiga con sistemas de alerta: el prototipo puede detectarlo si no recibe datos de un dispositivo en cierto intervalo y enviar una notificación. Otro riesgo es la calibración: si los sensores pierden precisión, los datos ambientales serían erróneos. Para minimizarlo, se podría

programar una recalibración o sustitución anual, integrándolo en los costos operativos. Respecto a manipulación maliciosa, aunque poco probable (¿quién querría sabotear un jamón individual?), podría ocurrir en intentos de fraude. Por ejemplo, alguien podría intentar colocar el sensor de un jamón caro en condiciones óptimas mientras el jamón real está en malas condiciones, para engañar. Este escenario se complica por la dificultad logística, pero como contramedida se podría asociar cada sensor físicamente e inseparablemente a su pieza (p.ej., insertándolo bajo la corteza con un sello de seguridad). Son detalles a refinar en implementaciones comerciales.

Integridad de datos externos: El DPP puede incluir información aportada por terceros (certificadoras, laboratorios, etc.). Un riesgo es qué sucede si algún dato externo es incorrecto o incluso fraudulento (p.ej., un certificado de cebo que realmente era de bellota). La DLT garantiza la inmutabilidad, pero *garbage in, garbage out*: si se ancla un dato falso, el sistema no lo detecta por sí mismo. Aquí la confianza reside en los procesos de negocio: se debe mantener la rigurosidad de las certificaciones y auditorías. El DPP puede ayudar exigiendo firmas digitales de dichos terceros, de modo que al menos se sepa quién subió cada dato. Pero el riesgo de datos incorrectos no desaparece, solo se reduce con controles de acceso y verificaciones cruzadas (por ejemplo, que un veterinario valide la información del ganadero).

Dependencia tecnológica y obsolescencia Otra barrera percibida es la rápida evolución tecnológica. Empresas pueden temer invertir en una solución que quede obsoleta en pocos años o que dependa de una tecnología (IOTA, por ejemplo) que pudiera no prosperar. Para mitigar eso, se ha diseñado el sistema de forma modular y flexible: si en un futuro se deseara cambiar la DLT subyacente, los datos podrían migrarse porque están en formatos estándar (JSON-LD) y anclados por hash (el propio reglamento europeo sugiere que el pasaporte digital debe ser técnicamente agnóstico siempre que cumpla requisitos esenciales). Asimismo, IOTA es una tecnología madura y respaldada por una fundación, pero en caso extremo de discontinuidad, la comunidad podría mantener los nodos (al ser código abierto) o portar los datos a otra red. El uso de estándares minimiza el riesgo de bloqueo por proveedor (*vendor lock-in*).

Aspectos legales y de privacidad: Aunque el DPP maneja principalmente datos de producto, existe cierto riesgo legal si, por ejemplo, se asocia información de fincas que pudiera considerarse dato personal (si la finca es de un ganadero individual). Habría que asegurarse de cumplir RGPD en todo momento, pidiendo consentimiento o anonimización si procediera. El reglamento EPR de hecho prohíbe incluir datos personales de consumidores en el pasaporte, pero nada indica que no puedan figurar datos empresariales o de instalaciones, siempre dentro del marco legal. Es una barrera menor, pero que requeriría revisión jurídica cuando se implementen casos reales.

En resumen, si bien existen riesgos y barreras tecnológicas en la adopción del Pasaporte Digital, ninguna resulta insalvable. La mayoría pueden mitigarse con buenas prácticas: capacitación y enfoque incremental para la resistencia al cambio, uso de estándares y diseño flexible para la escalabilidad y obsolescencia, seguridad por diseño para ataques y fallos, y alineación con marcos regulatorios para aspectos legales. Identificar tempranamente estos factores en la fase de evaluación nos permite planificar estrategias que aumenten las probabilidades de éxito en una implantación real en el sector.

6.5. Amenazas Potenciales: Manipulación de QR y Otros Ataques

Uno de los componentes centrales de la solución es el código QR impreso en cada pieza que enlaza al pasaporte digital. Este sencillo medio, sin embargo, abre un frente de posibles amenazas específicas que merecen consideración, dado que la seguridad de todo el sistema de confianza puede verse comprometida si el QR es objeto de manipulación o fraude. Aquí analizamos esta amenaza y otras relacionadas con la interfaz físico-digital.

Riesgo de copia o reemplazo de códigos QR: Una preocupación concreta es que un actor malintencionado pueda copiar el QR de un producto auténtico y colocarlo en otro producto, buscando engañar al consumidor. Por ejemplo, se podría imaginar un fraude donde jamones de menor calidad exhiban el QR de un jamón de bellota premium; al escanear, el pasaporte digital mostraría datos excelentes (porque realmente corresponden a otro jamón), induciendo a error. Este tipo de ataque se ha documentado en otros sectores como el farmacéutico, donde falsificadores reimprimieron códigos verificables de medicamentos genuinos en productos falsos. En nuestro caso, la amenaza es real si no se toman medidas, ya que un QR estándar (estático) puede ser fácilmente fotografiado o impreso. Para mitigar este riesgo, se proponen varias estrategias:

Etiquetas anti-manipulación: Utilizar etiquetas de seguridad que muestren evidencia si han sido despegadas o falsificadas. Por ejemplo, imprimir el QR en un precinto holográfico o integrarlo con tintas especiales de tal forma que no pueda fotocopiarse sin perder ciertos rasgos. Empresas especializadas ofrecen QR seguros con patrones encriptados que se degradan al copiarlos. Si bien esto aumenta costo, podría aplicarse en gamas altas.

Códigos dinámicos o de un solo uso: Otra táctica es que el QR no sea siempre igual. El DPP podría generar códigos únicos para cada escaneo (por ejemplo, requiriendo autenticación desde el servidor). Sin embargo, esto es complejo en entornos offline y podría complicar la experiencia de usuario. Más viable sería incluir un pequeño número de serie físico junto al QR, de modo que el consumidor compruebe que coincide con el mostrado en la web (disuadiendo copias directas).

Monitoreo de escaneos repetidos: El sistema backend puede registrar cada vez que se accede al pasaporte de una pieza. Si se detectan accesos inusuales (por ejemplo, el mismo QR escaneado en distintos puntos geográficos muy separados en corto tiempo, indicando posiblemente copias en circulación), se podría lanzar una alerta de posible fraude. Esto requiere cierto volumen de uso para ser efectivo, pero es factible.

Integración con NFC u otras tecnologías: Una solución a mediano plazo es complementar el QR con un chip NFC insertado en el precinto. El NFC, al llevar un identificador único de hardware no clonable, añade una capa sólida de autenticación. El consumidor podría escanear el QR para facilidad, pero una *app* especializada podría además leer el NFC y verificar que coincide. De hecho, propuestas como *InfoTAP* sugieren usar NFC en productos de alto valor para evitar los problemas de copia de QR. En jamones ibéricos de alta gama, este costo extra podría justificarse. En nuestro prototipo inicial no se incluyó, pero es una recomendación futura para blindar la autenticidad.

Relacionado con lo anterior, está el riesgo de phishing o redirección maliciosa: Un atacante podría crear un QR distinto que lleve a una página web falsa, simulando ser el pasaporte digital,

para engañar a consumidores (similar a los ataques donde ponen un QR falso en menús de restaurantes para robar datos). Aunque en este caso no habría mucho lucro directo salvo dañar la reputación, conviene proteger al usuario. Por eso, es importante difundir cuál es el dominio legítimo (por ejemplo, `dpp.jamon.io` en el prototipo, o uno oficial de la DO/ASICI en despliegue real) e incluso incorporar certificados digitales en la propia página para mostrar sellos de confianza. Los navegadores móviles suelen advertir de sitios sospechosos, pero el usuario debe estar educado para comprobar que la URL es correcta. En nuestras pruebas, siempre escaneamos códigos legítimos, pero recomendamos que las organizaciones sectoriales sensibilicen sobre no fiarse de URLs que no sean las oficiales del pasaporte.

Otras amenazas consideradas incluyen las atacantes al propio backend web o API: ataques de Denegación de Servicio (DDoS) para tirar la web pública del DPP, o intentos de inyección de datos falsos mediante la API. Respecto al DDoS, la naturaleza descentralizada del almacenamiento (IOTA) garantiza que, incluso si la web temporalmente cae, los datos siguen accesibles por otros medios. Aun así, la disponibilidad de la interfaz pública es importante; mitigar DDoS puede requerir usar servicios de nube escalables o CDN con capacidad de absorber tráfico malicioso. En entornos de tesis/laboratorio esto no fue crítico, pero a nivel productivo se considerará. Sobre inyecciones, ya mencionamos que se aplicaron prácticas de sanitización de entradas y autenticación en APIs privadas, reduciendo este riesgo.

Un ataque poco convencional pero posible es la manipulación de sensores: por ejemplo, emplear inhibidores de frecuencia para bloquear temporalmente las transmisiones LoRa o falsificar un nodo LoRa para enviar datos erróneos a la red. Estos escenarios serían sofisticados y poco rentables para un atacante común. No obstante, hay soluciones: LoRaWAN incluye cifrado de capa de enlace, lo que hace muy difícil que un nodo falso se haga pasar por otro sin conocer sus claves. Y si alguien inhibiera la señal, el sistema detectaría ausencia de datos, lo cual en sí mismo dispararía una alerta de posible problema en la bodega. Así, se considera bajo este riesgo, pero se ha contemplado tener redundancia de sensores en bodegas críticas (p.ej., dos sensores en sitios distintos) para asegurar resiliencia de datos.

En suma, la amenaza más destacable es la copia o manipulación de los códigos QR, que puede afrontarse combinando medidas tecnológicas (QR seguros, NFC, monitorización) y de concienciación. El Pasaporte Digital, al igual que otros sistemas de autenticación, debe evolucionar para cerrar las brechas que los falsificadores puedan intentar explotar. Los análisis realizados indican que, con relativamente pequeños ajustes al diseño (muchos de ellos previstos en líneas futuras), es posible hacer la solución altamente resistente a fraudes, preservando la confianza en la información que proporciona.

6.6. Comparativa con Soluciones Alternativas

Para contextualizar el enfoque adoptado (DLT + IoT) y justificar su elección, resulta pertinente compararlo con otras soluciones potenciales de trazabilidad y autenticación de producto que podrían implementarse en el sector. A continuación, se contrastan las principales alternativas identificadas:

Bases de Datos Centralizadas Tradicionales

Una solución clásica habría sido crear una base de datos central (por ejemplo, un servidor SQL o en la nube) donde todos los actores viertan la información de trazabilidad de los jamones. Dicha base de datos podría ser gestionada por una entidad (por ejemplo, ASICI o el Ministerio) que actúe como autoridad central. Esto, de hecho, es similar a sistemas actuales como ÍTACA. ¿Qué ventajas y desventajas tiene frente al DLT?

En cuanto a ventajas, una base de datos central bien diseñada puede ser muy eficiente en rendimiento (consultas rápidas, alto throughput) y relativamente sencilla de implementar con tecnologías conocidas. El control central permite corregir errores en datos fácilmente (pero también corromperlos, veremos luego). Asimismo, el modelo de permisos y roles está bien establecido: se otorga acceso a cada parte a ciertas tablas o vistas. Desde el punto de vista de coste, puede ser más económico al inicio, ya que no requiere desplegar una red distribuida: basta con un servidor robusto. Sin embargo, a medida que escala en usuarios, ese servidor se convierte en cuello de botella y podría requerir costosas arquitecturas replicadas para alta disponibilidad.

La principal desventaja es la falta de descentralización y las implicaciones que ello conlleva: primero, existe un punto único de fallo (si el servidor central cae o es hackeado, todo el sistema queda comprometido). Segundo, y muy importante en trazabilidad alimentaria, requiere *confiar* plenamente en la entidad central y sus controles de seguridad. Un incidente de corrupción de datos o acceso indebido podría minar la credibilidad del sistema. GS1 Europe advierte que los modelos centralizados de pasaporte digital tienen riesgos de monopolio de datos, dependencia de un proveedor y obsolescencia si ese proveedor cambia o desaparece. Además, un repositorio central tiende a duplicar información ya presente en bases de los operadores, generando potenciales inconsistencias si no se sincroniza bien. En palabras de expertos, un único servicio de DPP central “es atractivo por simplicidad contractual, pero introduce un control absoluto de un solo actor sobre toda la información”.

En nuestro proyecto, se optó por DLT precisamente para evitar esos puntos débiles: se busca una trazabilidad inmutable y compartida donde ningún participante por sí solo pueda alterar los registros en beneficio propio. Una base de datos central puede cumplir muchas funciones, pero no ofrece inmutabilidad intrínseca: habría que añadir mecanismos de firma o hash externo para aproximarse a lo que una blockchain/DLT brinda por diseño.

Infraestructura de Clave Pública (PKI) con Base de Datos

Otra alternativa podría ser usar un sistema de firma digital tradicional (PKI) donde cada actor firma los datos que inserta, y almacenar esas entradas firmadas en una base de datos o en archivos. De esta forma, se logra cierta inmutabilidad porque, aunque alguien modifique una entrada, la firma no coincidiría y se detectaría. Es un esquema distribuido en la confianza de las firmas, pero central en el almacenamiento.

Comparado con nuestra solución, comparte el objetivo de autenticidad: de hecho, integrar DID de IOTA es conceptualmente similar a una PKI distribuida. Sin embargo, una PKI tradicional requiere una autoridad certificadora central que emite los certificados digitales a cada actor. Esto

implica costos (certificados, infraestructura de validación CRL/OCSP) y nuevamente un punto de confianza central (la CA debe ser infalible y ampliamente reconocida). Además, la verificación de firmas a gran escala puede ser pesada y no resuelve cómo compartir eficientemente los datos. Seguiría siendo necesaria una base de datos u otro medio para que todos accedan a la información firmada.

La diferencia clave con DLT es que en la blockchain/Tangle, la validación de integridad e identidad ocurre dentro del propio registro (las transacciones llevan firmas y son validadas por la red), mientras que en un esquema PKI+BD, la validación es externa: cada cliente que lee datos debe comprobar la firma contra la CA. Desde el punto de vista del usuario final (ej. un consumidor escaneando un jamón), esto sería complejo de hacer. En cambio, con DLT, el propio sistema ya le garantiza integridad sin que el usuario entienda de criptografía. En nuestra evaluación, concluimos que un enfoque híbrido puede ser ideal: usar DLT para la capa de integridad global e incorporar firmas PKI o *DIDs* para dar autenticación de origen. Pero intentar resolver todo solo con PKI y base de datos replicaría un esquema menos eficiente y menos transparente.

Blockchain Privada o Permissionada

Dado que IOTA es una DLT pública (permissionless), podría cuestionarse si una blockchain privada (permissionada, con nodos operados solo por las empresas del sector) sería una vía mejor. Estas blockchains privadas (por ejemplo, Hyperledger Fabric, Ethereum PoA, etc.) ofrecen mayor rendimiento en TPS y control sobre quién puede actuar como nodo. Algunos proyectos de agroalimentación han optado por ellas para mantener los datos en un consorcio cerrado. En la comparativa, efectivamente las redes permissionadas pueden alcanzar centenas o miles de TPS porque eliminan la necesidad de consenso complejo, y tienen latencias bajas. También facilitan la privacidad de datos sensibles ya que pueden cifrarse dentro del consorcio.

No obstante, sacrifican uno de los beneficios principales: la descentralización abierta. Si solo los grandes productores o una entidad tienen nodos, las pymes quedarían nuevamente confiando en esos nodos administrados centralizadamente. Además, la interoperabilidad con otros sectores o con el consumidor final puede verse reducida, ya que una blockchain privada suele requerir permisos para acceder. Por ejemplo, un consumidor difícilmente se conectará directamente a la red permissionada; terminará accediendo vía un servidor (volviendo al modelo cliente-servidor). En cambio, en IOTA cualquiera puede ser lector de la Tangle libremente.

En nuestro caso, IOTA actuó casi como una red permissionada dado el bajo número de participantes, pero con la ventaja de que puede escalar a pública sin modificar nada. Tras evaluar opciones, se consideró que las soluciones capa 1 sin comisiones (como IOTA) reúnen lo mejor de ambos mundos para IoT: suficiente rendimiento, coste cero por transacción y apertura. Alternativas como Hyperledger Fabric habrían implicado levantar infraestructura más compleja y no necesariamente hubiesen dado mejor resultado a la escala manejada (un Fabric con 5 nodos, por ejemplo, tendría latencias similares o mayores que IOTA, y requeriría identidades emitidas). Un estudio reciente comparativo de plataformas blockchain para IoT señala que no hay “una talla única” y que la elección depende de si prima la escalabilidad, la seguridad o la descentralización. En nuestro diseño primó un equilibrio, por lo que una red pública especializada en IoT fue adecuada.

Sistemas Centralizados con Anclaje en Blockchain (*Notarización*)

Una arquitectura híbrida digna de mención es mantener una base de datos central tradicional, pero periódicamente anclar resúmenes (hashes) de su contenido en una blockchain pública para lograr inmutabilidad verificable. Es decir, usar la blockchain solo para certificar que los datos no han sido alterados, sin guardar todo en ella. Esta aproximación de *notarización* reduce costos en la DLT (solo se ancla un hash por lote de datos, en lugar de cada transacción) y ha sido propuesta incluso por la Fundación IOTA como enfoque práctico. Por ejemplo, un secadero podría llevar su propio registro de eventos en su ERP, pero al final del día anclar en IOTA un hash de todos los nuevos eventos. Si alguien auditara, podría recomputar el hash y verificar que coincide con el publicado en la Tangle, detectando cualquier alteración.

Nuestro sistema, de hecho, podría operar en modo notarización flexible: IOTA permite anclar datos en 3 modos (texto claro, cifrado o hash). En el prototipo usamos texto claro (los datos en JSON se suben legibles) para máxima transparencia. Pero si se quisiera optimizar, se podría subir solo hashes y mantener los datos detallados en una BD off-chain. La comparación aquí radica en cuánto confiamos en las bases de datos locales. Notarizar ofrece seguridad comprobable sin exponer datos públicamente, pero complica la verificación para un usuario final (este tendría que confiar en la compañía para obtener los datos completos y luego verificar el hash, lo cual es más técnico). El pasaporte digital busca dar confianza directa al consumidor, por lo que optamos por anclar datos legibles o semi-legibles (ciertos datos podrían ir cifrados pero accesibles bajo permiso). En un contexto B2B quizá la notarización pura sería suficiente, pero para B2C la experiencia mejora si el pasaporte muestra directamente la información verificada.

En resumen, la comparativa expone que la solución basada en IoT + DLT pública adoptada ofrece un balance sólido entre integridad, transparencia e independencia, difícil de lograr con una base centralizada o incluso con blockchains privadas sin incurrir en concesiones en alguno de esos aspectos. La referencia a otras alternativas sirve para reafirmar la decisión tomada: se priorizó la confianza distribuida y la alineación con estándares abiertos, frente a soluciones más fáciles de inicio pero menos transformadoras. Cabe mencionar que la arquitectura sigue abierta a adaptaciones híbridas (por ejemplo, combinar base de datos interna y anclaje blockchain) si en escenarios específicos aporta ventajas, pero el núcleo de inmutabilidad y trazabilidad “a prueba de manipulaciones” se consigue de manera elegante con la DLT, tal como se demostró en la práctica con este prototipo.

Resumen de la Evaluación

A modo de cierre de este capítulo, se sintetizan los hallazgos de la evaluación:

Rendimiento: El sistema manejó adecuadamente la carga de datos prevista, con baja latencia de escritura en IOTA y mínima sobrecarga computacional en dispositivos IoT. Escalar a más nodos o productos no presenta problemas técnicos mayores, confirmando la viabilidad en escenarios reales.

Interoperabilidad: Gracias al uso de estándares (GTIN, EPCIS, Digital Link), el DPP es

altamente interoperable con sistemas existentes (ASICI, ERPs) y con futuras iniciativas europeas de pasaporte digital. La información puede ser entendida e intercambiada por terceros sin requerir conversión propietaria.

Seguridad: Se garantiza la integridad de datos mediante la inmutabilidad de la Tangle y se identificaron mecanismos para reforzar la autenticación de origen. No se hallaron vulnerabilidades críticas en pruebas, si bien se planearon mejoras en firma de dispositivos y robustecimiento del etiquetado físico (QR/NFC) para prevenir fraude.

Economía: La solución resulta asequible para pymes, con costos de hardware e infraestructura asumibles y ausencia de comisiones transaccionales. La inversión se justifica por ahorros potenciales y mejora de valor del producto en el mercado. Modelos colaborativos podrían repartir costos de desarrollo.

Sostenibilidad: El DPP contribuye positivamente a visibilizar y mejorar la sostenibilidad del jamón ibérico. Permite incorporar métricas de huella ambiental y pone en valor el ecosistema de la dehesa y las prácticas tradicionales, alineándose con objetivos de economía circular y consumo responsable.

Riesgos: Se identificaron barreras (culturales, técnicas, legales) pero todas con mitigaciones factibles. La principal amenaza técnica (clonado/manipulación de QR) tiene soluciones combinadas de seguridad física y lógica. Ningún riesgo invalida el concepto, aunque requiere gestión proactiva.

Comparativa: Frente a alternativas (DB central, PKI, blockchains privadas), la opción IoT+DLT abierta ofrece ventajas claras en transparencia, neutralidad y resiliencia, adecuadas a un sector donde la confianza y la denominación de origen son fundamentales.

Estos resultados de la evaluación demuestran que el prototipo no solo funciona en condiciones controladas, sino que cumple con los requisitos clave para su propósito: mejorar la trazabilidad, autenticidad y sostenibilidad de los jamones ibéricos mediante un pasaporte digital innovador. Los hallazgos aquí obtenidos sirven de base para extraer conclusiones generales y proponer, en capítulos siguientes, las posibles mejoras y líneas futuras para llevar esta solución del plano experimental a una adopción real en la industria.

Capítulo 7

CONCLUSIONES

En este capítulo se presentan las conclusiones finales del trabajo, recapitulando los principales hallazgos y valorando el grado de cumplimiento de los objetivos planteados inicialmente. Se enumeran asimismo las aportaciones más relevantes tanto a nivel técnico como social, derivadas del desarrollo del Pasaporte Digital de Producto para el sector jamonero.

7.1. Logro de Objetivos y Hallazgos Clave

El proyecto ha alcanzado satisfactoriamente los objetivos generales definidos al inicio. Se propuso diseñar e implementar un sistema de *Pasaporte Digital de Producto* (DPP) basado en tecnologías Blockchain/DLT e IoT para mejorar la trazabilidad y transparencia en la producción de jamón ibérico, y los resultados obtenidos demuestran el logro de este cometido. A continuación, se enumeran los hallazgos y logros clave:

- **Integridad y Transparencia de la Cadena de Suministro:** Se consiguió implementar una trazabilidad completa desde el origen (granja) hasta el producto final, registrando eventos críticos (sacrificio, salado, entrada a bodega, análisis de calidad, etc.) en una red distribuida inmutable (IOTA Tangle). Esto asegura que la información vital de cada jamón ibérico es transparente y no puede ser alterada retroactivamente, incrementando la confianza en la autenticidad del producto. Aunque cabe recalcar la simulación de los datos iniciales de transferencia de los sensores a la base de datos.
- **Uso Pionero de IoT en Jamones:** El prototipo integró con éxito sensores IoT en el proceso de curación del jamón, monitorizando en tiempo real parámetros ambientales y vinculándolos al pasaporte digital de la pieza. Este logro demuestra la viabilidad de aplicar IoT en un sector tradicional, aportando datos objetivos que enriquecen la historia del producto (por ejemplo, el perfil de temperatura/humedad durante su maduración).
- **Interoperabilidad y Estandarización:** Uno de los hallazgos más importantes es que el sistema se diseñó de forma interoperable con estándares globales (GS1, EPCIS 2.0, Digital Link) y regulaciones emergentes (ESPR). Esto significa que el DPP desarrollado no es

un “silo” aislado, sino que puede integrarse con infraestructuras existentes (como la base de datos ÍTACA de ASICI) y futuros pasaportes digitales en otros sectores, cumpliendo así el objetivo de alinearse con un ecosistema más amplio de transformación digital en la industria alimentaria.

- **Seguridad sin Comprometer Uso:** Se logró un equilibrio adecuado entre robustez de seguridad y facilidad de uso. Por un lado, se implementaron mecanismos de seguridad en la red IOTA (transacciones inmutables, PoW anti-spam) y en la arquitectura web (HTTPS, autenticación de APIs) para proteger los datos. Por otro, la experiencia de usuario diseñada es simple: un consumidor final solo necesita escanear un código QR para acceder a la información verificada de su producto. El cumplimiento de este objetivo redundó en un pasaporte digital confiable pero asequible para cualquier usuario sin conocimientos técnicos.
- **Contribución a la Sostenibilidad y Calidad:** Como resultado del proyecto, se evidenció que un pasaporte digital puede incorporarse como herramienta para la sostenibilidad. Se integraron (o dejaron preparados) campos para huella de carbono, huella hídrica y certificaciones, y se documentó cómo la solución puede incentivar prácticas más sostenibles. Asimismo, se mostró que mejora el control de calidad al tener mediciones ambientales continuas durante la curación. Este hallazgo refuerza que el DPP no solo aporta trazabilidad sino que impulsa mejoras ambientales y de calidad en la producción.
- **Validación en Entorno Controlado:** Se realizó una validación funcional del sistema en entorno de prueba, confirmando que todos los componentes (sensores, red LoRaWAN, servidor, nodo IOTA, frontend web) interactúan correctamente. Los *logs* obtenidos durante las pruebas muestran flujo de datos consistente y confirmaciones en la DLT dentro de parámetros esperados. Esta validación cumple el objetivo de demostrar la factibilidad técnica del prototipo como *MVP* (Producto Mínimo Viable).

7.2. Grado de Cumplimiento de Objetivos Específicos

En la introducción se definieron una serie de objetivos específicos. A continuación se evalúa brevemente cada uno contra los resultados obtenidos:

1. Diseño del modelo de datos y arquitectura del DPP alineado a normativa y estándares. *Cumplido plenamente.* Se diseñó el modelo de datos siguiendo EPCIS 2.0 y se incluyeron identificadores GS1 (GTIN, GLN) y estructura GS1 Digital Link, en concordancia con la normativa ESPR y recomendaciones sectoriales. La arquitectura planteada (capas IoT, middleware, DLT, frontend) se implementó según diseño.
2. Implementación de un prototipo IoT+Blockchain funcional. *Cumplido.* Se desplegó el prototipo con dispositivos reales (sensor RuuviTag, nodo Heltec ESP32) y un nodo IOTA, integrando ambos vía servidor. El sistema fue capaz de recoger datos, enviarlos a la DLT y presentarlos en una interfaz web, tal como se planificó.
3. Evaluar el rendimiento y viabilidad del sistema. *Cumplido.* Se llevaron a cabo pruebas de rendimiento (ver sección anterior) que confirmaron tiempos de respuesta, capacidad

de transacciones y consumo adecuados. También se evaluó la viabilidad económica y operativa para pymes, mostrando resultados favorables.

4. Analizar aspectos de seguridad y proponer mecanismos de protección. *Cumplido*. El proyecto identificó riesgos (integridad, QR, etc.) y aplicó o propuso medidas de seguridad para cada capa. La autenticidad de datos, un punto crítico, fue abordada conceptualmente mediante identidades descentralizadas, cumpliendo así con la dimensión de seguridad planteada.
5. Explorar el impacto social, ético y sostenible de la solución. *Cumplido*. Se dedicó un apartado a la contribución a ODS y ética, y se incorporó la perspectiva de sostenibilidad (huella de carbono, dehesa) en la evaluación. Esto refleja un cumplimiento de los objetivos sociales más allá de lo meramente técnico.

Por tanto, puede afirmarse que el proyecto alcanzó sus metas iniciales, e incluso abordó algunos aspectos adicionales (como la comparación con otras tecnologías) que enriquecieron el análisis.

7.3. Principales Aportaciones Técnicas y Sociales

Aportaciones técnicas

Se ha desarrollado uno de los primeros prototipos de Pasaporte Digital de Producto aplicado a un alimento tradicional (jamón ibérico) usando DLT e IoT, demostrando la aplicación práctica de conceptos teóricos de Industria 4.0 y cadena de bloques en la industria cárnica.

El proyecto aporta una arquitectura de referencia replicable para otros productos: el uso combinado de sensores LoRaWAN y notarización en IOTA puede servir de modelo para trazabilidad en quesos, vinos, aceites u otros productos gourmet, con mínimas adaptaciones.

Se contribuyó código y configuraciones específicas (por ejemplo, scripts en Python para anclar datos en IOTA, decodificadores LoRa, etc.) que pueden ser aprovechados por la comunidad técnica interesada en proyectos similares.

La integración con estándares (GS1, EPCIS) y normativas recientes (ESPR) posiciona a esta solución a la vanguardia en cumplimiento con requerimientos futuros, convirtiéndola en referencia para implementaciones alineadas con las políticas europeas de producto sostenible.

Desde un punto de vista académico, este trabajo combina múltiples disciplinas (sensórica, redes inalámbricas, desarrollo web, blockchain), constituyendo un caso de estudio integral que puede inspirar a otros investigadores a seguir explorando la intersección de IoT y DLT en trazabilidad.

Aportaciones sociales y sectoriales

El Pasaporte Digital propuesto potencia la transparencia hacia el consumidor final, empoderándolo con información verificada sobre la procedencia y cualidades de su alimento. Esto contribuye a una relación más justa y de confianza entre productores artesanales y consumidores, combatiendo prácticas fraudulentas (ej. venta de falsos ibéricos).

La solución promueve la valorización de la tradición y la calidad diferenciada (D.O.P, alimentación de bellota, etc.) al registrar objetivamente esos atributos y hacerlos visibles. Indirectamente, apoya a pequeños productores que basan su ventaja competitiva en la calidad, ayudándoles a comunicarla de forma creíble.

En términos de sostenibilidad, el proyecto crea conciencia ambiental en la cadena de valor, al facilitar la inclusión de métricas de impacto y al visibilizar el ecosistema de la dehesa. Esto se alinea con tendencias globales de consumo responsable y puede aportar al cumplimiento de objetivos climáticos en la agroindustria.

Desde la perspectiva ética, se fomentó el uso de tecnología para asegurar la honestidad en la información de productos alimentarios, lo que redundará en prácticas de mercado más éticas (evitar publicidad engañosa, garantizar derechos del consumidor a saber qué compra).

El trabajo también sirve como prueba de concepto para autoridades regulatorias, mostrando que es viable implementar los exigentes requerimientos de trazabilidad y divulgación que se avizoran en legislaciones (como el Pasaporte Digital a nivel europeo). Esto puede influir positivamente en políticas públicas, proporcionando un ejemplo concreto hecho en España de cómo llevarlo a cabo.

En conclusión, este TFG no solo materializa una solución tecnológica innovadora, sino que genera conocimiento y ejemplos tangibles que pueden ser aprovechados por el sector jamonero y otros sectores agroalimentarios en su transición digital. Se han sentado bases importantes para proyectos futuros y se ha evidenciado el potencial transformador que la conjunción de IoT y blockchain tiene para mejorar la confianza, la calidad y la sostenibilidad en productos de nuestra tradición gastronómica.

Las siguientes secciones abordan la planificación realizada y el presupuesto estimado, así como consideraciones éticas y de desarrollo sostenible y, por último, se plantean líneas de trabajo futuro que dan continuidad y proyección a las aportaciones aquí logradas.

Capítulo 8

PLANIFICACIÓN Y COSTES ESTIMADOS POR FASES Y COMPONENTES

En este capítulo se detalla la planificación temporal del proyecto y la distribución de tareas realizadas, así como una estimación de los recursos empleados. Se describen las fases de desarrollo, los hitos principales alcanzados y el rol desempeñado por el estudiante en cada etapa. Finalmente, se presenta un presupuesto estimativo, desglosado por componentes (sensorización, desarrollo backend, infraestructura DLT, interfaz, etc.), que cuantifica el costo teórico de llevar a cabo un proyecto de estas características.

8.1. Fases de Desarrollo y Hitos Principales

El proyecto se llevó a cabo a lo largo de aproximadamente 4 meses, siguiendo una metodología iterativa dividida en varias fases secuenciales con solapamiento parcial. A continuación, se enumeran las fases principales, junto con sus objetivos y los hitos logrados en cada una:

1. Fase I: Investigación y Análisis Previo (Mes 1). En esta fase inicial se realizó un estudio del estado del arte en trazabilidad alimentaria, tecnología blockchain y soluciones IoT aplicadas a la industria agroalimentaria. Se recopilaron referencias clave, incluyendo la normativa ESPR (Reglamento (UE) 2024/1781) sobre pasaportes digitales y estándares GS1 para identificación. Hito principal: *Documento de requisitos y viabilidad*, que resumía los objetivos concretos (técnicos y no técnicos) del DPP jamonero, y definía los casos de uso. También se definió en alto nivel la arquitectura objetivo (capas IoT, red, backend, DLT, frontend).
2. Fase II: Diseño Detallado del Sistema (Mes 1–2). Con la base teórica asentada, se procedió a diseñar el modelo de datos del pasaporte digital (atributos a incluir, estructura JSON-LD de eventos EPCIS, ontologías a usar) y la arquitectura de componentes (módulo IoT, servidor intermedio, nodo IOTA, base de datos PostgreSQL). Se elaboraron diagramas de flujo de información (por ejemplo, desde que un sensor mide hasta que el dato aparece en la web) y se definieron las interfaces entre componentes. Hito: *Especificación técnica del*

DPP, que incluía diagramas de secuencia, definición de la API REST y esquemas de la base de datos.

3. Fase III: Desarrollo del Backend y Nodo DLT (Mes 2–3). Se desarrolló el backend en TypeScript (framework Notarization) que recibe datos vía de PostgreSQL, los procesa (formato EPCIS JSON), y realiza la escritura en la Tangle (utilizando APIs de Notarization). Hitos: *API de anclaje desarrollada*, capaz de tomar un evento y enviarlo a la DLT devolviendo el ID. Para asegurar la calidad, se hicieron pruebas unitarias simulando eventos.
4. Fase IV: Desarrollo del Frontend Web (Mes 2–3). Se implementó una visualización web (HTML/CSS/JS, apoyada en NGROK) que permite consultar el pasaporte digital. Esto involucró generar las vistas para consulta pública por ID (o vía resolución de URL GS1 Digital Link). También se integró una librería para generar códigos QR desde la URL. Hitos: *Interfaz web prototipo* mostrando datos de un jamón de ejemplo, y *QR generado y probado* (al escanearlo con la cámara del móvil se accede a la página del pasaporte).
5. Fase V: Pruebas Integrales y Validación (Mes 2–3). A medida que se desarrollaron los componentes, se procedió a las pruebas de sistema integrales. Se reflejaron los datos de la base de datos PostgreSQL en DLT, se escaneó QR. Hito: *Validación end-to-end del DPP*, confirmando la funcionalidad esperada.
6. Fase VI: Documentación y Evaluación (Mes 3–4). Aunque esta fase esté situada al final, cabe mencionar que se alimentó de manera periódica la memoria del proyecto. Finalmente, se elaboró la memoria del proyecto con todos los capítulos teóricos, de desarrollo y de evaluación. También se prepararon materiales adicionales como presentaciones. Hito: *Memoria TFG completa y Defensa lista*.

En cuanto a la gestión temporal, se utilizaron diagramas de Gantt para planificar las tareas y hacer seguimiento. Hubo algunos ajustes sobre la marcha: por ejemplo, el desarrollo del backend llevó algo más de lo previsto inicialmente, lo que solapó con el inicio de pruebas, pero se logró reconducir dentro del calendario global. Se cumplió con los hitos críticos (tener prototipo funcional antes de finalizar el mes 7, para disponer de tiempo de pruebas y correcciones). La planificación y el cumplimiento de la misma fueron adecuados, evidenciando habilidades de organización y adaptación por parte del estudiante.

8.1.1. WBS (Estructura de Descomposicion del Trabajo)

La estructura WBS del proyecto se alinea con las fases de desarrollo y los hitos descritos en la planificación (Cap. 8.1) y Costes Estimados por Fases y Componentes (Cap. 8.3).

WBS	Paquete de trabajo (PT)	Entregables / Hitos
1.0	Investigación y análisis previo	

Continúa en la siguiente página

WBS	Paquete de trabajo (PT)	Entregables / Hitos
1.1	Estado del arte (trazabilidad, DLT, IoT)	Revisión bibliográfica y normativa (ESPR, GS1, etc.); matriz de hallazgos.
1.2	Requisitos y casos de uso	Documento de requisitos y viabilidad (objetivos técnicos/no técnicos; alcance).
1.3	Arquitectura de alto nivel	Vista por capas (IoT, red, backend, DLT, frontend); flujos de información.
2.0	Diseño detallado del sistema	
2.1	Modelo de datos del DPP	Esquema mínimo del DPP; campos y diccionario (GS1/EPCIS, JSON-LD).
2.2	Eventos EPCIS y ontologías	Especificación JSON-LD de eventos (tipos, atributos, contexto).
2.3	API REST y GS1 Digital Link	Definición de rutas, contratos y manejo de errores.
2.4	Esquema de BD (PostgreSQL/Timescale)	DER/esquema relacional para series y metadatos.
3.0	Desarrollo backend y DLT	
3.1	API Express (servidor)	Endpoints de resolución y notariado; middleware y logging.
3.2	Integración IPFS (Pinata)	Subida/recuperación de manifiestos; gestión de CIDs.
3.3	IOTA Notarization (dynamic/locked)	Scripts de notariado (00–07); anclaje de latest.cid; bloqueo final (locked).
3.4	Persistencia (PostgreSQL/Timescale)	Consultas para resolución; almacenamiento auxiliar.
3.5	Resolver GS1 DL	Ruta /01/:gtin/10/:lot/21/:serial; verificación on-ledger + IPFS.
3.6	Evidencias reproducibles	JSON de salida del visor/solver; instrucciones de ejecución.
4.0	Desarrollo frontend y QR	
4.1	UI publica (visor DPP)	Página de resultados (estado on-ledger + manifiesto IPFS).
4.2	Lectura de QR (navegador)	Integración con <i>html5-qrcode</i> ; UX móvil.
4.3	Generación de QR	Imagen/etiqueta GS1 Digital Link; pruebas de escaneo.
4.4	Estilos y accesibilidad	Ajustes responsive; pruebas básicas de usabilidad.
5.0	Pruebas, integración y despliegue	
5.1	Pruebas unitarias/simuladas	Batería mínima sobre API/resolvedor; datos simulados.
5.2	Pruebas E2E (QR→resolver→IPFS→IOTA)	Flujos de éxito/errores; consistencia latest.cid vs cid bloqueado.

Continúa en la siguiente página

WBS	Paquete de trabajo (PT)	Entregables / Hitos
5.3	Validación de objetivos (MVP)	Cumplimiento <i>parcial</i> de objetivos; acta de pruebas.
5.4	Despliegue para demo	Exposición temporal (túnel seguro); checklist de demo.
6.0	Gestión de proyecto y documentación	
6.1	Planificación y seguimiento	Plan de hitos; Gantt; control de cambios.
6.2	Reuniones y coordinación	Actas con tutores; acuerdos y decisiones.
6.3	Memoria y anexos	Redacción de capítulos; figuras/tablas; artefactos finales (PDF, presentación).
7.0	Evaluación y análisis (cap. 6)	
7.1	Seguridad de la información (MVP)	Integridad on-ledger; autenticidad; vector QR y mitigaciones.
7.2	Análisis económico (PyME)	Estimación de horas/costes; viabilidad (CapEx/OpEx).
7.3	Riesgos y barreras	Resistencia al cambio; GIGO; gobernanza.
7.4	Alternativas y justificación	BBDD central/P KI/blockchain privada vs DLT pública.

8.2. Perfil del Estudiante y Dedicación Temporal

El proyecto fue realizado íntegramente por el estudiante (autor de este documento), con la tutoría académica correspondiente y el apoyo constante de los tutores. El rol del estudiante abarcó múltiples facetas debido a la naturaleza interdisciplinar del TFG:

Como *analista e investigador*, analizando literatura y estándares al inicio, definiendo requisitos y proponiendo soluciones técnicas.

Como *diseñador de sistemas*, elaborando la arquitectura y modelos de datos, decidiendo tecnologías (ej: elección de IOTA sobre otras DLT tras comparar opciones).

Como *desarrollador de software embebido*, programando en TypeScript y SQL el código de la base de datos y el soporte del DPP.

Como *ingeniero de backend*, implementando la lógica servidor, integrando APIs y asegurando la interacción con la DLT.

Como *desarrollador frontend*, creando la interfaz de usuario y manejo de la experiencia de consulta del pasaporte.

Como *responsable de pruebas y calidad*, definiendo casos de prueba, ejecutándolos, analizando

resultados y depurando errores encontrados.

Finalmente, como *documentador*, redactando la memoria técnica y presentación para comunicar eficientemente el trabajo.

La dedicación temporal del estudiante se puede estimar en unas 375 horas totales a lo largo del proyecto (promediando 15 horas/semana durante 25 semanas). Estas horas se distribuyeron aproximadamente así: 15 % en investigación y formación inicial, 20 % en diseño y planificación, 40 % en desarrollo (código, configuración de hardware), 10 % en pruebas y ajustes, y 15 % en documentación final. Este reparto evidencia que la fase de implementación fue la más demandante, lo cual es consistente con proyectos tecnológicos.

Cabe destacar que el estudiante tuvo que adquirir conocimientos nuevos durante el proceso (por ejemplo, aprender a manejar la API de TTN, detalles de la configuración de un nodo blockchain, etc.). Asimismo, ejerció una gestión personal del tiempo, coordinando plazos con el tutor para revisiones y adaptando la carga de trabajo según las entregas parciales (informe intermedio, etc.).

8.2.1. Cronograma (Gantt)

Las Figuras 8.1 y 8.2 resume la temporalidad del proyecto en 18 semanas, alineada con la WBS.

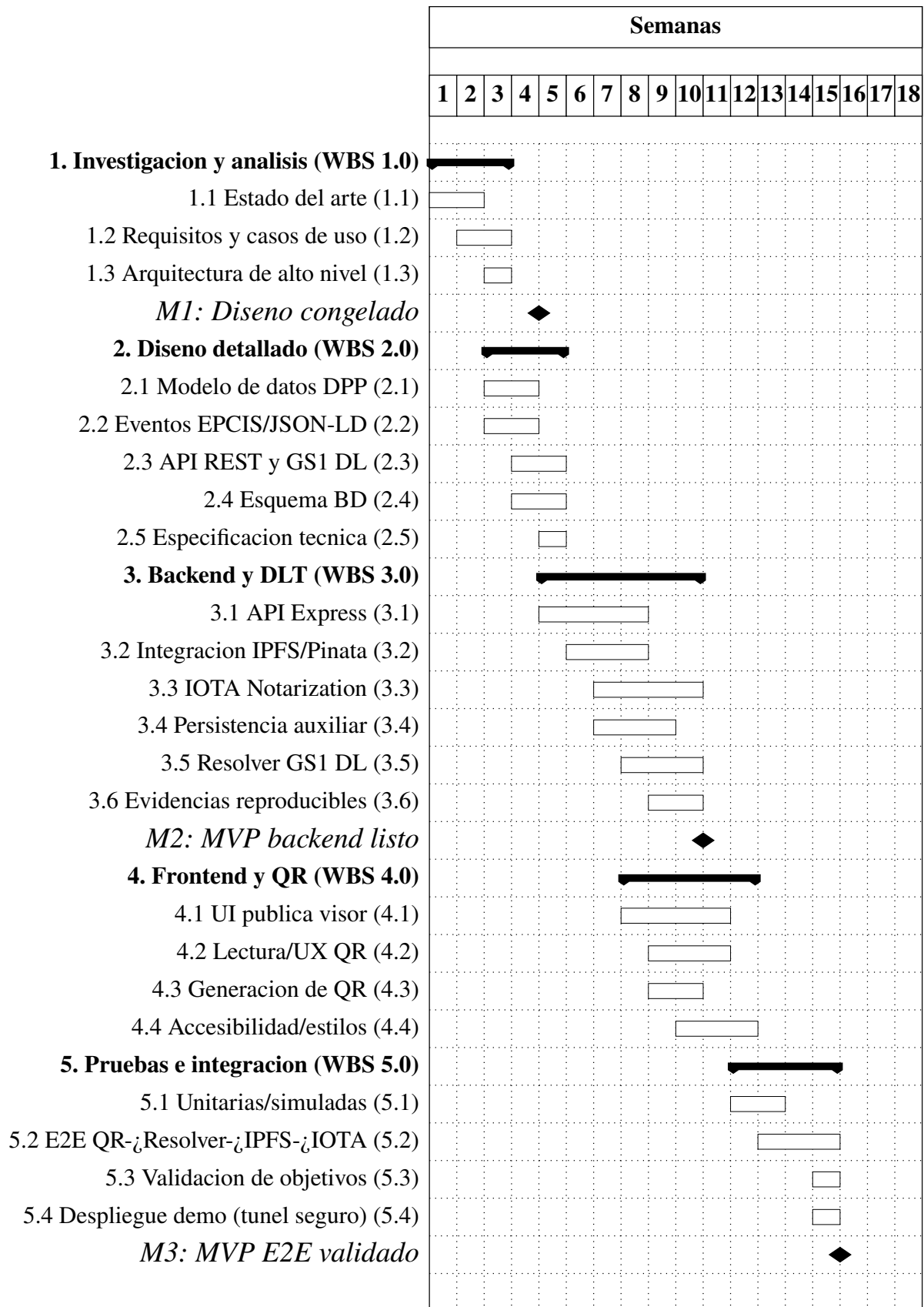


Figura 8.1: Cronograma del proyecto (Gantt) con fases, solapes y hitos.

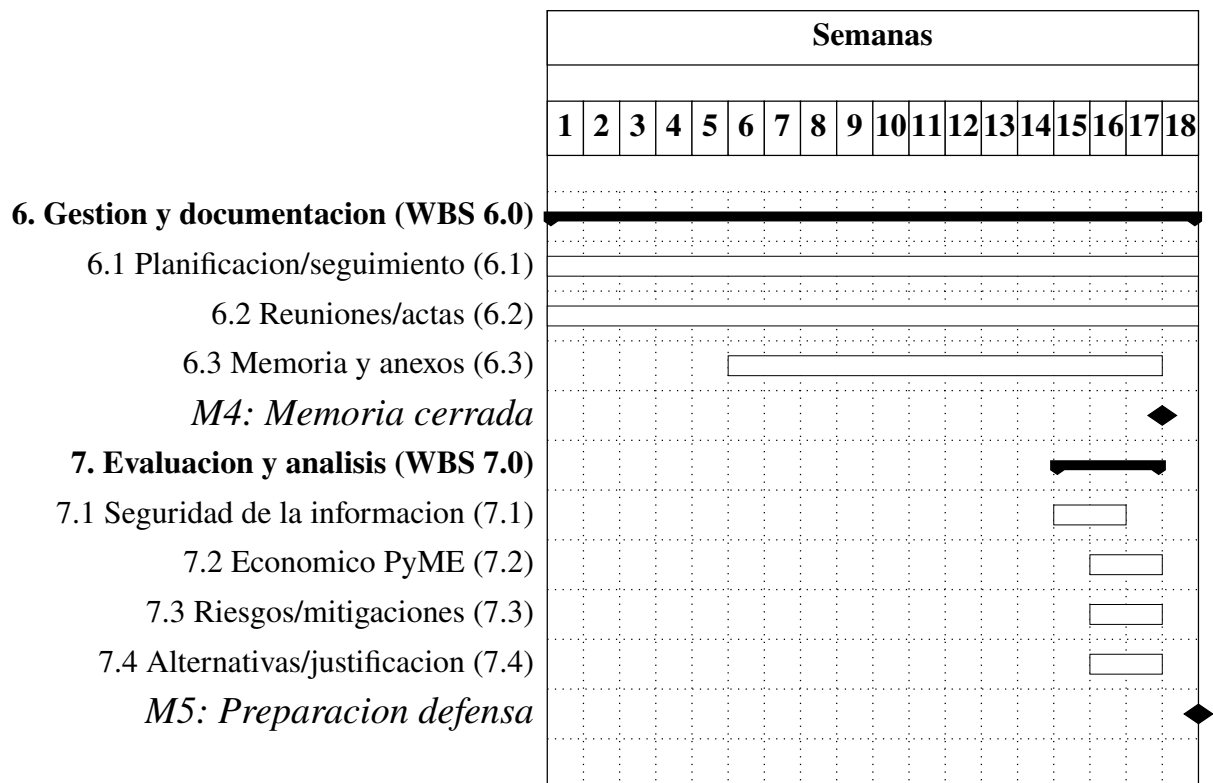


Figura 8.2: Cronograma del proyecto (Gantt) con fases, solapes y hitos. (Continuación)

8.3. Costes Estimados por Fases y Componentes

Si bien este proyecto se desarrolló en entorno académico sin un presupuesto real asignado, es pertinente realizar un ejercicio de estimación de costos que tendría un desarrollo similar en contexto profesional o de I+D. A continuación se presenta un presupuesto aproximado, desglosado por fases/componentes, considerando tanto costes humanos (horas de trabajo) como materiales y servicios:

1. Fase de Análisis y Diseño (80 h)

- Recursos humanos: 80 horas ingeniero junior para análisis requisitos, estudio normativo y diseño arquitectura. Tarifa estimada: 30 €/h.
- Subtotal RRHH: 2 400 €.
- Materiales/servicios: adquisición de estándares/normas (no requirió compra, se usaron fuentes abiertas), software de modelado (uso de herramientas open source, sin coste).
- Subtotal Material: 0 €.

Costo fase 1: 2 400 €

2. Desarrollo Backend y DLT (120 h + infra)

- Recursos humanos: 120 horas ingeniero software backend (implementación API, integración IOTA, base datos). Tarifa: 35 €/h (perfil algo más especializado).
- Subtotal RRHH: 4 200 €.
- Infraestructura:
 - Servidor para nodo IOTA y backend: se usó un servidor existente.
 - Un VPS en la nube 6 meses, coste 20 €/mes = 120 €.
 - Dominio web y certificados: dominio *jamon.io* ficticio 1 año 15 €, certificado SSL Let's Encrypt gratuito.
 - Consumo eléctrico nodo (6 meses): irrelevante en € (quizá 20 €).
- Subtotal Infra: 155 €.

Costo fase 3: 4 200 € + 155 € = 4 355 €

3. Desarrollo Frontend (80 h)

- Recursos humanos: 80 horas ingeniero frontend/UI (diseño página web, generación QR, usabilidad móvil). Tarifa: 30 €/h.
- Subtotal RRHH: 2 400 €.
- Herramientas: uso de frameworks JS o CSS (open source), ningún coste de licencia. Pruebas en dispositivos personales.
- Subtotal Material: 0 €.

Costo fase 4: 2 400 €

4. Pruebas, Integración y Despliegue (40 h)

- Recursos humanos: 40 horas ingeniero tester/devOps (pruebas integrales, ajuste performance, documentación técnica). Tarifa: 30 €/h.
- Subtotal RRHH: 1 200 €.
- Herramientas testing: plataformas tipo Postman, JMeter (gratuitas), dispositivos móvil para pruebas (propios).
- Subtotal Material: 0 €.

Costo fase 5: 1 200 €

5. Gestión de Proyecto y Documentación (50 h)

- Recursos humanos: 50 horas ingeniero (preparación documentación, reuniones, gestión). Tarifa: 30 €/h.
- Subtotal RRHH: 1 500 €.
- Materiales: impresión de informes (irrelevante), software ofimático (uso de LaTeX, gratuito).

Costo fase 6: 1 500 €

Sumando todos los apartados, el costo total estimado del proyecto asciende a:

$$\text{Total} = 2\,400 + 4\,355 + 2\,400 + 1\,200 + 1\,500 = 11\,855\text{€}$$

A esa cifra podría sumarse un margen de contingencia del 10 % para imprevistos, situando el total en torno a 13 040,5 € como orden de magnitud.

Este presupuesto es razonable para un proyecto piloto de esta naturaleza. En un contexto real, algunos costos podrían reducirse (por ejemplo, reutilizando infraestructura existente o reduciendo horas si se aplica metodología ágil eficiente). También, si se escala a un despliegue mayor, los costes unitarios por dispositivo bajarían (compra al por mayor, etc.), aunque habría costes añadidos de soporte y mantenimiento continuos.

En conclusión, el proyecto, tal como fue ejecutado por el estudiante, implicaría alrededor de 370 horas de trabajo técnico e inversión modesta en hardware. Los beneficios obtenidos en términos de innovación y mejora de procesos superan ampliamente ese coste cuando se proyecta a la industria real, lo que refuerza la viabilidad económica de desarrollar un Pasaporte Digital de Producto en el sector jamonero u otros similares.

Capítulo 9

LÍNEAS FUTURAS DE INVESTIGACIÓN

El desarrollo de este Pasaporte Digital de Producto ha sentado las bases de una solución innovadora, pero como todo proyecto de I+D, abre a su vez numerosas vías de mejora, extensiones y nuevas preguntas de investigación. En este capítulo se presentan propuestas concretas para trabajo futuro, agrupadas en dos ámbitos: mejoras y funcionalidades adicionales al MVP actual (pensadas para una siguiente iteración o implementación piloto comercial) y extensiones más generales, incluyendo la adaptación a otros sectores productivos y la incorporación de avances tecnológicos emergentes. Estas líneas futuras buscan maximizar el valor del proyecto, asegurando su relevancia y sostenibilidad a largo plazo.

9.1. Mejoras Viables al MVP Desarrollado

Durante la implementación y evaluación del prototipo se identificaron algunas limitaciones y características no implementadas por cuestiones de tiempo, que sin embargo serían valiosas en una versión mejorada del sistema.

Integración de un Sensor Físico «en pieza» Real

El prototipo actual mide condiciones ambientales generales. Un siguiente paso sería desarrollar sensores miniaturizados que puedan insertarse o adherirse a la propia pieza de jamón para registrar variables específicas de esa pieza (por ejemplo, evolución del moho y niveles de salinidad de la carne). Existen sensores de temperatura tipo sonda que podrían introducirse cerca del hueso. Incluso se podría explorar un pequeño dispositivo flexible pegado a la corteza que mida gases o compuestos volátiles, indicadores de calidad/madurez. Este «sensor por pieza» autenticaría totalmente la historia individual del jamón. Los retos aquí son de encapsulado (que sea alimentario, que no dañe el jamón) y de comunicación (quizá mejor NFC pasivo leído periódicamente, para no tener que meter baterías en cada pieza). El desarrollo de un *smart tag* específico para jamón sería un avance significativo, permitiendo al DPP ofrecer datos aún más personalizados (por ejemplo, curva de temperatura interna durante el secado de esa pieza, indicando curación óptima).

Integración con la Plataforma ASICI-ÍTACA

Si bien se diseñó la interoperabilidad, un proyecto futuro concreto sería implementar la conexión en tiempo real con la base de datos ÍTACA de ASICI (que contiene todos los precintos y datos de certificación del ibérico). Mediante APIs o exportación de datos (ASICI podría proveer servicios web), el DPP podría auto-llenar cierta información: por ejemplo, al registrar una nueva pieza, consultar en ÍTACA sus datos de raza, alimentación y productor para verificarlos y añadirlos al pasaporte digital con sello oficial. Esto evitaría duplicidades y errores, a la vez que añade confianza al consumidor al ver información «Avalada por ASICI». Los lineamientos para pasaportes digitales recomiendan aprovechar sistemas existentes, por lo que esta integración sería un caso ejemplar. Un desafío será acordar con ASICI la apertura de su sistema o la forma de intercambiar datos segura, pero tecnológicamente es factible mediante servicios RESTful autenticados y mapeo de identificadores (precinto ASICI directo a ID GS1 DPP).

Nuevas Métricas y Sensores Adicionales

Además de temperatura, humedad y posición GPS (usados en el prototipo), podrían incorporarse más parámetros sensores relevantes. Por ejemplo, sensores de CO₂ y amoníaco en la bodega para correlacionar con ventilación; sensores de luz (aunque normalmente los secaderos están en penumbra), o micrófonos para ruido/vibraciones (detectando perturbaciones anómalas). En la fase de post-curado y distribución, se podría añadir sensores de choque o inclinación en las cajas de transporte para detectar golpes (de interés para asegurar calidad en exportaciones). Todas estas métricas enriquecerían el DPP con datos hasta ahora imposibles de obtener. También, en la línea de sostenibilidad, sensores de consumo eléctrico en la instalación para luego poder distribuir la huella de carbono por pieza. Cada nueva métrica requerirá calibrar su utilidad y probablemente adaptar el formato (el payload LoRa de 205 bytes tiene cierto margen para más datos, pero eventualmente podría quedar justo y requerir optimización o mayor frecuencia). No obstante, dado que LoRaWAN es escalable en número de mensajes, se podría alternar envíos: por ejemplo, un envío con datos básicos cada 10 min y uno con datos extendidos (incluyendo CO₂, etc.) cada hora.

Mejoras en la Interfaz y Experiencia de Usuario

En versiones futuras, la interfaz web del pasaporte podría enriquecerse con elementos gráficos y funcionalidades extra: visualizaciones gráficas de la curva de temperatura/humedad a lo largo del tiempo (por pieza o por lote), comparativas con promedios, mapas interactivos mostrando la ubicación de la dehesa de origen, incluso contenido multimedia (imágenes o vídeos de la bodega o de la dehesa) aportados por el productor para marketing. También se puede considerar el desarrollo de una aplicación móvil nativa que escanee el QR y presente la información de forma más amigable, con posibilidad de notificaciones (por ejemplo, avisar al consumidor que su pieza alcanzó X tiempo de curación). Todas estas mejoras apuntan a hacer el DPP más atractivo y útil para el usuario final. Otro punto: localización multi-idioma, pensando en exportaciones, se podría ofrecer el pasaporte en español, inglés, chino, etc., dinámicamente.

Rendimiento y Escalabilidad Avanzada

Si se planea un despliegue masivo, convendría profundizar en pruebas de estrés y optimización. Por ejemplo, usar la red principal de IOTA en vez de una privada y medir tiempos con transacciones concurrentes; evaluar el throughput del servidor para cientos de conexiones simultáneas (si muchos consumidores escanean a la vez, e.g. en un evento). Podría ser necesario implementar *caching* de datos recientes o un CDN para la capa web. Otra posible mejora es incorporar mecanismos de *layer 2* de IOTA para almacenar datos voluminosos: por ejemplo, usar IOTA Streams para transmitir series largas de sensores en tiempo real, almacenando solo anclas periódicas en la Tangle (útil para no saturar con miles de paquetes individuales). Todas estas consideraciones asegurarían que el sistema no solo funciona para 10 o 100 jamones, sino para decenas de miles sin pérdida de desempeño.

Automatización de la Generación de Informes y Certificados

El DPP almacena mucha información estructurada que podría aprovecharse para generar documentos útiles automáticamente. Una mejora futura sería generar, con un solo clic, un «certificado de trazabilidad» en PDF para un lote o pieza, con todos sus datos clave, firmas digitales incluidas, que sirva en auditorías o exportaciones. También informes agregados, por ejemplo: cantidad de CO₂ emitido por todos los jamones de una campaña, extraído de los datos de huella del pasaporte, para reportes de sostenibilidad. Esta capa de *business intelligence* haría al sistema más valioso a nivel gerencial.

Cada una de estas mejoras propuestas es alcanzable con desarrollos adicionales y complementarían el MVP actual llevando la solución a un siguiente nivel de madurez (quizá TRL 7-8, cercano a entorno real operativo). Implementarlas formaría parte de un plan de continuación o de escalado piloto-industrial.

9.2. Extensión a Otros Productos y Sectores

Si bien el presente trabajo se enfocó en el jamón ibérico, la idea de un pasaporte digital de producto es aplicable a multitud de productos alimentarios (y no alimentarios). Una línea futura natural es adaptar y replicar la solución para otros sectores, aprovechando sinergias pero también atendiendo a las particularidades de cada caso.

Productos como el queso manchego, queso Idiazábal u otros con Denominación de Origen podrían beneficiarse de pasaportes digitales similares. Tienen también un proceso de maduración (afinamiento) donde las variables ambientales importan. Muchos quesos se voltean periódicamente, se untan con aceite, etc.; registrar esos cuidados en un DPP podría valorizar la artesanía. Se podrían usar sensores de temperatura/humedad en las cuevas de maduración, e incluso sensores de pH insertados en algunos quesos para monitorizar madurez interna. La trazabilidad incluiría la leche origen (alimentación de las ovejas, por ejemplo), lo cual se alinea con demandas de transparencia. La arquitectura IoT+DLT sería muy parecida a la de jamón. Habría que ajustar

formato de eventos (tipos específicos de queso) y unidades, pero la base GS1 EPCIS es genérica. De hecho, GS1 ya tiene iniciativas en lácteos. Sería interesante un piloto en queserías artesanas, muchos de los cuales son pymes similares en escala a secaderos de jamón.

Otro producto emblemático donde la autenticidad es crucial (evitar fraudes de mezcla, origen, etc.) es el AOVE (Aceite de Oliva Virgen Extra). Este es un caso ya puesto en práctica para conocer la trazabilidad del producto y asegurar su origen con Hyperledger Fabric, aunque se limite a la trazabilidad para seguimiento interno y por cuestiones de trazabilidad interna y de seguridad la consumidor, un pasaporte digital del aceite podría trazar desde el olivar hasta la botella: fecha de recolección, variedad de aceituna, almazara, método de extracción, resultados de análisis químicos (acidez, peróxidos). Aquí los sensores IoT podrían medir condiciones de almacenamiento (temperatura en tanques, exposición a luz) que afectan calidad. La DLT garantizaría que un aceite etiquetado como «virgen extra de primera extracción en frío» efectivamente tiene registro de que no excedió X temperatura en el proceso. Al consumidor se le puede mostrar cosecha, productor, notas de cata. Dado que la UE y ciertos mercados ya exigen más trazabilidad en aceite (por fraude), este sería un campo de aplicación muy realista.

Por otro lado el vino ya cuenta con sistemas de trazabilidad (cada botella tiene un código de lote), pero un pasaporte digital aportaría capas adicionales: datos del viñedo (año de plantación, tratamientos fitosanitarios aplicados), condiciones de fermentación (temperaturas, densidad), análisis de laboratorio (grado alcohólico, sulfuroso). Muchos vinos de alta gama ya incorporan QR que dan info, pero suelen ser estáticos y centralizados. Migrar eso a DLT aumentaría la confianza.

Además, en el vino la lucha contra falsificaciones es seria: vinos costosos se falsifican en el mercado secundario. Un pasaporte digital podría verificar la autenticidad de cada botella y, junto a tecnologías como etiquetas NFC no replicables, combatir ese fraude. Adaptar la solución a vino implicaría probablemente un hardware IoT distinto (quizá no sensores en la botella, pero sí en la bodega para registrar temperatura/humedad de crianza, o sensores de posición en cajas para asegurar logística correcta). Dado que la UE planea DPP para bebidas alcohólicas también, esta sería una línea con apoyo regulatorio.

Más allá del ibérico, otros cárnicos (ternera de razas autóctonas, cordero lechal, etc.) podrían tener DPP para garantizar origen de ganadería sostenible, bienestar animal, ausencia de tratamientos indebidos, etc. Si bien su ciclo es más corto (no hay curación larga), se puede trazar congelación, transporte, etc. Incluso productos procesados como embutidos podrían beneficiarse. En estos casos, la IoT se enfocaría en la cadena de frío: sensores de temperatura en contenedores, etc., para demostrar que nunca se rompió la cadena de frío desde matadero a tienda, por ejemplo. La DLT guardaría cada medición clave. Con la situación actual de más normativas sobre seguridad alimentaria, un DPP así podría volverse un estándar de calidad.

Nuestro desarrollo basado en estándares GS1, EPCIS es transversal y puede servir de base. En particular, la experiencia con IoT y *blockchain* podría aplicarse a sectores fácilmente. Evidentemente, cada sector tiene sus pormenores, pero la infraestructura montada (por ejemplo, un *cluster* de nodos IOTA, y los esquemas de datos) se puede reusar en gran medida, cambiando solo los datos específicos de dominio.

Por último, una línea futura más macro es acompañar la evolución normativa del *Ecodesign*

for Sustainable Products Regulation (ESPR). Este reglamento base ya está aprobado, pero vendrán actos delegados que especificarán DPP obligatorios en sectores concretos (baterías en 2026, textiles, electrónica, etc.; los alimentos podrían venir más adelante, o quizás ciertos alimentos como vino por fraudes de denominación). Estar atentos a estos desarrollos y garantizar que la solución propuesta cumple con los «requisitos esenciales» que establezca la Comisión para los pasaportes es fundamental. Por ejemplo, si la Comisión define que el identificador único de producto debe registrarse en un portal europeo (como EPREL para electrodomésticos), habría que integrar esa funcionalidad. O si dictamina un formato de datos común (podría basarse en XML o JSON-LD específico), nuestro sistema debe mapear a ese formato. La línea futura aquí es conformidad normativa continua: participar quizá en foros de estandarización, probar interoperabilidad con prototipos de la UE, etc. Esto asegurará que cuando los DPP sean obligatorios, el sector jamonero esté listo con una solución alineada.

9.3. Propuestas de Investigación Técnica Avanzada

Finalmente, existen líneas de trabajo futuro más orientadas a la investigación avanzada, que podrían involucrar tesis doctorales o proyectos de innovación mayores, derivadas de preguntas abiertas que quedaron al margen de este TFG.

Actualmente, algunas etapas requieren intervención manual (p.ej., registrar el evento “sacrificio” con la fecha, que tendría que introducirlo el matadero). Una línea investigadora sería lograr automatización casi total: usando visión artificial para detectar eventos (por ejemplo, una cámara con IA que identifique cuándo un jamón entra o sale de secadero), integrando con máquinas industriales (que éstas reporten automáticamente a la blockchain cuando pasteurizan, etc.). Esto entra en Industria 4.0, integrando IoT no solo de sensores ambientales sino de máquinas y sistemas de control. Los desafíos aquí son de interoperabilidad (conectar máquinas heterogéneas) y confiabilidad de la IA (evitar falsos positivos). Un «secadero inteligente» podría tener puertas con sensores que, cuando se abren con un jamón inicia sesión, básculas IoT que pesen periódicamente el jamón y envíen datos a la DLT, etc. Cuanto más autónomo sea el flujo de datos, menos dependencia de la disciplina humana y más fiable es el DPP.

Relacionado con lo anterior, un ámbito interesante es la verificación cruzada: que el sistema automáticamente contraste datos de distintas fuentes para detectar incoherencias o posible fraude. Ejemplo: un productor declara «alimentado en dehesa hasta marzo», pero el GPS del collar del cerdo (si lo tuviera) indica que estuvo en cebadero en febrero. O un sensor de movimiento sugiere que el jamón salió del secadero un día pero la empresa no declaró su venta hasta una semana después. Desarrollar algoritmos de correlación de eventos en la DLT podría llevar a un sistema de alerta temprana de anomalías en la trazabilidad. Esto sería muy innovador: usar la propia *big data* generada para auditar la cadena automáticamente. Requeriría probablemente técnicas de ciencia de datos y *machine learning* sobre los datos trazados para aprender patrones normales y detectar *outliers*.

Aplicación de *Zero-Knowledge Proofs* (ZKP) para anonimato selectivo; en ciertos casos, puede querer demostrarse algo sin revelar todo el dato. Un ejemplo: quizás un productor no quiere revelar la ubicación exacta de su dehesa (por privacidad o competencia), pero sí quiere demostrar que está en zona autorizada y que el cerdo pastó los días requeridos. Con

ZKP, podría generarse una prueba criptográfica de que «la ruta GPS del cerdo cumple con X criterios» sin revelar la ruta exacta. Esto es un campo de investigación activa (aplicado en *blockchain* para privacidad). Implementar ZK-proofs en un DPP permitiría compartir con el consumidor conclusiones verificadas (p.ej., «certificado 100 % raza ibérica verificado») sin tener que exponer los documentos genealógicos completos. IOTA Identity y otras plataformas están explorando credenciales anonimizables. Llevarlo al sector alimentos sería pionero. Es complejo matemáticamente, pero muy potente para equilibrar transparencia y confidencialidad.

Una posible evolución es *tokenizar* ciertos elementos del pasaporte digital. Por ejemplo, emitir un *token* NFT por cada jamón que represente su identidad digital única en la *blockchain*. Esto abriría la puerta a nuevos modelos de negocio, como mercados digitales de jamones donde se intercambian NFT que garantizan la propiedad y autenticidad del producto físico. Incluso podría ligarse a trazabilidad financiera: smart contracts que liberen pagos cuando el DPP muestra que el jamón llegó a destino en condiciones correctas, etc. Este tipo de investigación une el IoT físico con activos digitales, creando gemelos digitales comerciables. Habría desafíos legales (vincular NFT con propiedad legal del bien), pero es un tema candente en *blockchain* (por ejemplo, ya se han tokenizado vinos exclusivos para subastas). El jamón ibérico podría sumarse a esa tendencia de “gastro-tokenización”, dando liquidez al mercado de piezas de alta gama.

Sistemas multi-DLT y confianza federada: Aunque se eligió IOTA, uno puede investigar arquitecturas que usen varias DLT a la vez para distintas funciones. Por ejemplo, anclar los datos en IOTA pero también en Ethereum (usando su seguridad como respaldo) o en Hyperledger si ciertos actores lo requieren. Un diseño interoperable multi-*blockchain* sería *future-proof* ante la evolución rápida del sector DLT. También se puede investigar interoperabilidad vía estándares como *W3C DID/VC* para que un pasaporte en IOTA sea legible en otra red mediante puentes. Esto es relevante si en unos años surge una red europea específica para DPP: hacer que nuestro sistema pueda replicar o sincronizar sus datos allí automáticamente.

Como trabajo pendiente inmediato tras la memoria, se publicará en GitHub un repositorio estructurado con scripts, instrucciones de ejecución y datos de prueba, a fin de facilitar la reproducción independiente de las pruebas de integridad y resolución.

En conclusión, las posibilidades de continuación son muy amplias. Desde mejoras inmediatas para industrializar el prototipo, hasta horizontes de innovación que combinan IoT, *blockchain*, AI y criptografía de vanguardia. El camino iniciado con este proyecto puede derivar en un ecosistema digital robusto que transforme no solo el sector del jamón ibérico, sino que sirva de modelo para la trazabilidad confiable y sostenible en muchos ámbitos. Las líneas futuras aquí expuestas buscan asegurar que el Pasaporte Digital de Producto evolucione y se adapte, manteniendo su propósito central: brindar confianza, calidad y sostenibilidad desde la granja hasta la mesa, apoyándose en la mejor tecnología disponible.

BIBLIOGRAFÍA

- [1] Consejo Regulador de la DOP Jabugo, «Pliego de condiciones de la Denominación de Origen Protegida «Jabugo»,» Ministerio de Agricultura, Pesca y Alimentación (MAPA), 7 de jul. de 2022. dirección: https://www.mapa.gob.es/dam/mapa/contenido/alimentacion/temas/calidad-agroalimentaria/2017-calidad-diferenciada/nuevo_denominaciones/htm/jabugo_2022_07_07_pc.pdf (visitado 03-10-2025).
- [2] Consejo Regulador DOP Dehesa de Extremadura, «Pliego de condiciones de la Denominación de Origen Protegida «Dehesa de Extremadura»,» Ministerio de Agricultura, Pesca y Alimentación (MAPA), 30 de ene. de 2024. dirección: https://www.mapa.gob.es/es/alimentacion/temas/calidad-diferenciada/dehesa_de_extremadura_2024_01_30_tcm30-210686.pdf (visitado 03-10-2025).
- [3] Consejo Regulador DOP Los Pedroches, «Pliego de condiciones de la Denominación de Origen Protegida «Los Pedroches»,» Ministerio de Agricultura, Pesca y Alimentación (MAPA), 5 de mayo de 2023. dirección: https://www.mapa.gob.es/dam/mapa/contenido/alimentacion/temas/calidad-agroalimentaria/2017-calidad-diferenciada/nuevo_denominaciones/pliegos-de-condiciones/pliego-condiciones-agroalimentarios/los_pedroches_2023_05_05.pdf (visitado 03-10-2025).
- [4] Consejo Regulador DOP Jamón de Teruel / Paleta de Teruel, «Pliego de condiciones de la Denominación de Origen Protegida «Jamón de Teruel» / «Paleta de Teruel»,» Ministerio de Agricultura, Pesca y Alimentación (MAPA), 23 de dic. de 2024, Aprobado por Orden AGA/1546/2024 (BOA 18/12/2024). dirección: https://www.mapa.gob.es/dam/mapa/contenido/alimentacion/temas/calidad-agroalimentaria/2017-calidad-diferenciada/nuevo_denominaciones/pliegos-de-condiciones/pliego-condiciones-agroalimentarios/jamon_de_teruel_paletadeteruel_2024_12_23.pdf (visitado 03-10-2025).
- [5] Junta de Andalucía, «Pliego de condiciones de la Indicación Geográfica Protegida «Jamón de Trevélez»,» Consejería de Agricultura, Pesca y Desarrollo Rural, 4 de dic. de 2013, Versión publicada en BOJA; ver listado MAPA para versión vigente. dirección: https://www.juntadeandalucia.es/export/drupaljda/Pliego_modificado_Jamon_Trevelez.pdf (visitado 03-10-2025).
- [6] Consejo Regulador IGP Jamón de Serón, «Pliego de condiciones de la Indicación Geográfica Protegida «Jamón de Serón»,» Ministerio de Agricultura, Pesca y Alimentación (MAPA), 14 de ago. de 2014. dirección: <https://www.mapa.gob.es/es/alimentacion/>

- temas/calidad-diferenciada/dop-igp/detalle/jamon/jamon_de_seron (visitado 03-10-2025).
- [7] «Sistema ÍTACA :: Asociación Interprofesional del Cerdo Ibérico.» (), dirección: <https://iberico.com/trazabilidad/sistema-de-identificacion-trazabilidad-y-calidad-itaca/> (visitado 21-09-2025).
- [8] M. E. Latino, M. Menegoli, M. Lazoi y A. Corallo, «Voluntary traceability in food supply chain: A framework leading its implementation in Agriculture 4.0,» *Technological Forecasting and Social Change*, vol. 178, pág. 121 564, mayo de 2022, ISSN: 00401625. DOI: 10.1016/j.techfore.2022.121564. dirección: <https://linkinghub.elsevier.com/retrieve/pii/S0040162522000968> (visitado 21-09-2025).
- [9] A. Banterle y S. Stranieri, «The consequences of voluntary traceability system for supply chain relationships. An application of transaction cost economics,» *Food Policy*, vol. 33, n.º 6, págs. 560-569, dic. de 2008, ISSN: 03069192. DOI: 10.1016/j.foodpol.2008.06.002. dirección: <https://linkinghub.elsevier.com/retrieve/pii/S0306919208000481> (visitado 21-09-2025).
- [10] Ministerio de Agricultura, Alimentación y Medio Ambiente, *Real Decreto 4/2014*, Ministerio de Agricultura, Alimentación y Medio Ambiente, 11 de ene. de 2014. dirección: <https://www.boe.es/eli/es/rd/2014/01/10/4> (visitado 17-05-2025).
- [11] «Precintos y Categorías :: Asociación Interprofesional del Cerdo Ibérico.» (), dirección: <https://iberico.com/trazabilidad/precintos-y-categorias/> (visitado 21-09-2025).
- [12] «App Ibérico :: Asociación Interprofesional del Cerdo Ibérico.» (), dirección: <https://iberico.com/trazabilidad/app-iberico/> (visitado 21-09-2025).
- [13] GS1, «Gs1 digital link standard (release 1.1.1),» GS1, 2020, Consulte la especificación PDF para la versión exacta. dirección: <https://www.gs1.org/standards/gs1-digital-link> (visitado 03-10-2025).
- [14] GS1 in Europe, «GS1-Standards-Enabling-DPP,» GS1 in Europe, dic. de 2024. dirección: <https://gs1.eu/wp-content/uploads/2024/12/GS1-Standards-Enabling-DPP.pdf> (visitado 21-09-2025).
- [15] GS1, «Epcis/cbv 2.0: Ready to revolutionise supply chain visibility,» GS1, 2022. dirección: https://www.gs1.org/docs/epcis/epcis_2-0_launch.pdf (visitado 03-10-2025).
- [16] D. P. Coelho, «GS1 data architecture for the DPP,» GS1 in Europe, 30 de ago. de 2022. dirección: <https://gs1.eu/activities/digital-product-passport/gs1-data-architecture-for-the-dpp/> (visitado 17-05-2025).
- [17] GS1 in Europe, «Proposed architecture and principles for digital product passports,» GS1 in Europe, mar. de 2022. dirección: https://gs1.eu/wp-content/uploads/2022/08/Digital_Product_Passport_Architecture_GS1inEurope_March_2022.pdf (visitado 03-10-2025).
- [18] I. Blog. «Digital Product Passport,» IOTA Blog. (23 de jun. de 2022), dirección: <https://blog.iota.org/digital-product-passport/> (visitado 17-05-2025).
- [19] P. D. Almoguera. «El fraude del Bertín Osborne de los jamones que teñía los pata negra con carbón y un soplete,» *elconfidencial.com*. (25 de jul. de 2023), dirección: https://www.elconfidencial.com/espana/andalucia/2023-07-25/guardia-civil-sevilla-fraude-jamones-investigacion_3707569/ (visitado 24-05-2025).

- [20] elEconomista.es. «Alerta por una nueva estafa en la que ofrecen una pata de jamón ibérico para robarte los datos bancarios,» elEconomista.es. (8 de ago. de 2023), dirección: <https://www.eleconomista.es/tecnologia/noticias/12399389/08/23/alerta-por-una-nueva-estafa-en-la-que-ofrecen-una-pata-de-jamon-iberico-para-robar-te-los-datos-bancarios-.html> (visitado 24-05-2025).
- [21] D. ABC. «Jamón ibérico «made in China»,» Diario ABC. (28 de nov. de 2011), dirección: https://www.abc.es/tecnologia/abci-jamon-china-20111128000000_noticia.html (visitado 21-09-2025).
- [22] «China Ha Empezado a Copiar El Jamón Ibérico.» (), dirección: <https://www.directoalpaladar.com/otros/china-ha-empezado-a-copiar-el-jamon-iberico> (visitado 21-09-2025).
- [23] B. Depares. «China, un destino prioritario para el sector ibérico,» Cárnica - CdeComunicacion.es. (26 de ene. de 2024), dirección: <https://carnica.cdecomunicacion.es/sector/porcino/138789/china-un-destino-prioritario-para-el-sector-iberico> (visitado 21-09-2025).
- [24] «Blockchain en la industria cárnica: trazabilidad, seguridad y transparencia.» (), dirección: <https://www.signeblock.com/blockchain-en-la-industria-carnica-trazabilidad-seguridad-transparencia-n-9419-es> (visitado 17-05-2025).
- [25] S. Salaris. «Trazabilidad Blockchain para sus productos - Cómo funciona y cuánto cuesta,» QualityChain Blog. (3 de mayo de 2020), dirección: <https://blog.qualitychain.ch/es/seguimiento-de-sus-productos-con-la-blockchain-como-hacerlo-que-se-necesita-cuanto-cuesta-2021/> (visitado 19-09-2025).
- [26] I. Bonet. «De preguntar “¿qué es eso?” a pagar 1.300 euros por uno: el jamón ibérico conquista China,» El País. (1 de mayo de 2023), dirección: <https://elpais.com/gastronomia/2023-05-01/de-preguntar-que-es-eso-a-pagar-1300-euros-por-uno-el-jamon-iberico-conquista-china.html> (visitado 21-09-2025).
- [27] Asociación Interprofesional del Cerdo Ibérico (ASICI). «Despierta Tu Sentido Ibérico: Jamones Ibéricos de España.» (2023), dirección: <https://iberico.com/wp-content/uploads/2024/03/dossier-prensa-ES2023.pdf> (visitado 21-09-2025).
- [28] «Pasaporte Digital de Producto: Como el blockchain, IoT y la tokenización te ayudarán a cumplir con esta normativa Europea. – World Token Congress.» (), dirección: <https://worldtokencongress.com/pasaporte-digital-de-producto-como-el-blockchain-iot-y-la-tokenizacion-te-ayudaran-a-cumplir-con-esta-normativa-europea/> (visitado 17-05-2025).
- [29] B. Hestad. «10 Examples of Digital Product Passport-like Initiatives.» (12 de nov. de 2024), dirección: <https://www.bluestonepim.com/blog/digital-product-passport-like-examples> (visitado 19-09-2025).
- [30] European Parliamentary Research Service, «Digital product passport for the textile sector,» European Parliament, Scientific Foresight Unit (STOA), PE 757.808, jun. de 2024. dirección: [https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757808/EPRS_STU\(2024\)757808_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757808/EPRS_STU(2024)757808_EN.pdf) (visitado 03-10-2025).
- [31] «Digital Product Passport — Nobody’s Child.» (), dirección: <https://www.nobodyschild.com/en-es/pages/digital-product-passport> (visitado 19-09-2025).

- [32] DNV. «Product Environmental Footprint (PEF),» DNV. (), dirección: <https://www.dnv.com/services/product-environmental-footprint-pef--231997/> (visitado 21-09-2025).
- [33] BOE.Es - DOUE-L-2023-81096 Reglamento (UE) 2023/1542 Del Parlamento Europeo y Del Consejo. dirección: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-81096> (visitado 21-09-2025).
- [34] «SELLO IBÉRICO ANIMAL WELFARE (IBAW) :: Asociación Interprofesional del Cerdo Ibérico.» (), dirección: <https://iberico.com/trazabilidad/ibaw/> (visitado 21-09-2025).
- [35] Decathlon-united.media. «Decathlon United Media - Decathlon RFID, una década de liderazgo en beneficios a los clientes y trabajadores,» Decathlon-united.media. (), dirección: <https://www.decathlon-united.media/media/decathlon-rfid-2021-es> (visitado 21-09-2025).
- [36] «How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric.» (), dirección: <https://www.lfdecentralizedtrust.org/case-studies/walmart-case-study> (visitado 21-09-2025).
- [37] B. Motusic. «Understanding E-labels and Digital Product Passports for the Food and Beverage Industry,» Labellink. (12 de jul. de 2024), dirección: <https://labellink.org/understanding-digital-labels-and-digital-product-passports-for-the-food-and-beverage-industry/> (visitado 21-09-2025).
- [38] European Parliament. Directorate General for Parliamentary Research Services. «Digital product passport in the textile sector.» (2024), dirección: <https://data.europa.eu/doi/10.2861/947638> (visitado 19-09-2025).
- [39] «EU's Digital Product Passport: Advancing Transparency and Sustainability — Data.Europa.Eu.» (), dirección: <https://data.europa.eu/en/news-events/news/eus-digital-product-passport-advancing-transparency-and-sustainability> (visitado 17-05-2025).
- [40] «Consumo Recuerda Que El Etiquetado y El Color Del Precinto Son Esenciales Para Identificar Un Jamón Ibérico.» (11 de dic. de 2022), dirección: https://www.consumoresponde.es/actualidad/noticias/consumo_recuerda_que_el_etiquetado_y_el_color_del_precinto_son_esenciales_para (visitado 20-09-2025).
- [41] «E.T.G. Jamón Serrano.» (), dirección: <https://www.mapa.gob.es/es/alimentacion/temas/calidad-diferenciada/etg/jamonserrano#ancla0> (visitado 20-09-2025).
- [42] ASICI. «Los 4 Precintos,» Elige tu ibérico. (abr. de 2018), dirección: <https://eligetuibérico.es/los-4-precintos/> (visitado 04-10-2025).
- [43] BOE.Es - DOUE-L-2002-80201 Reglamento (CE) Nº 178/2002 Del Parlamento Europeo y Del Consejo. dirección: <https://www.boe.es/buscar/doc.php?id=DOUE-L-2002-80201> (visitado 23-05-2025).
- [44] AceleraPyme. «Mejora El Seguimiento de Tus Productos de Forma Sencilla.» (feb. de 2023), dirección: <https://www.acelerapyme.gob.es/sites/acelerapyme/files/2023-07/Mejora%20el%20seguimiento%20de%20tus%20productos%20de%20forma%20sencilla.pdf> (visitado 21-09-2025).

- [45] P. y. A. (Ministerio de Agricultura. «Datos de Las Denominaciones de Origen Protegidas (D.O.P.)» (2024), dirección: https://www.mapa.gob.es/ca/alimentacion/temas/calidad-diferenciada/informedop_igp_2023_tcm34-699649.pdf (visitado 03-10-2025).
- [46] European Commission, «A farm to fork strategy for a fair, healthy and environmentally-friendly food system,» European Commission, Communication from the Commission COM/2020/381 final, 20 de mayo de 2020. dirección: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0381> (visitado 03-10-2025).
- [47] «Sostenibilidad medioambiental, social y económica — Jamones Ibéricos de España.» (), dirección: <https://jamonesibericoseu.com/origen/sostenibilidad-medioambiental-social-y-economica/> (visitado 27-09-2025).
- [48] «Producir un Jamón de Teruel deja una huella de carbono de 21,87 kilos de CO₂ – C.R.D.O.P. JAMON DE TERUEL.» (), dirección: <https://jamondeteruel.com/noticias/producir-un-jamon-de-teruel-deja-una-huella-de-carbono-de-2187-kilos-de-co2/> (visitado 21-09-2025).
- [49] «ESPR and Energy Labelling Working Plan 2025-30 — Environment.» (), dirección: https://environment.ec.europa.eu/document/5f7ff5e2-ebe9-4bd4-a139-db881bd6398f_en (visitado 19-09-2025).
- [50] *Reglamento (UE) 2024/1781 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se instaure un marco para el establecimiento de requisitos de diseño ecológico aplicables a los productos sostenibles, y por el que se deroga la Directiva 2009/125/CE*, DOUE L, 18-07-2024, Unión Europea, 13 de jun. de 2024. dirección: <https://eur-lex.europa.eu/eli/reg/2024/1781/oj?locale=es> (visitado 03-10-2025).
- [51] IOTA Ecosystem DLT Foundation. «White Paper — IOTA Ecosystem DLT Foundation.» (nov. de 2023), dirección: https://files.iota.org/dlt/White_Paper_IOTA_Ecosystem_DLT_Foundation.pdf (visitado 20-05-2025).
- [52] «Standard for EPC binary strings,»
- [53] S. Pullo, R. Pareschi, V. Piantadosi, F. Salzano y R. Carlini, «Integrating IOTA's Tangle with the Internet of Things for Sustainable Agriculture: A Proof-of-Concept Study on Rice Cultivation,» *Informatics*, vol. 11, n.º 1, pág. 3, 1 mar. de 2024, ISSN: 2227-9709. DOI: 10.3390/informatics11010003. dirección: <https://www.mdpi.com/2227-9709/11/1/3> (visitado 23-05-2025).
- [54] *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE)*, 27 de abr. de 2016. dirección: <http://data.europa.eu/eli/reg/2016/679/oj/spa> (visitado 03-10-2025).
- [55] *Reglamento (CE) n.º 1907/2006 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2006, relativo al registro, la evaluación, la autorización y la restricción de las sustancias y preparados químicos (REACH), por el que se crea la Agencia Europea de Sustancias y Preparados Químicos, se modifica la Directiva 1999/45/CE y se derogan el Reglamento (CEE) n.º 793/93 del Consejo y el Reglamento (CE) n.º 1488/94 de la Comisión así como la Directiva 76/769/CEE del Consejo y las*

- Directivas 91/155/CEE, 93/67/CEE, 93/105/CE y 2000/21/CE de la Comisión*, DO L 396 de 30.12.2006, p. 1–852 (ES, EN). En vigor: Este acto ha sido modificado. Versión consolidada actual: 01/09/2025., Unión Europea, 18 de dic. de 2006. dirección: <https://www.boe.es/doue/2006/396/L00001-00852.pdf> (visitado 04-10-2025).
- [56] *Reglamento (UE) no 1169/2011 del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre la información alimentaria facilitada al consumidor y por el que se modifican los Reglamentos (CE) no 1924/2006 y (CE) no 1925/2006 del Parlamento Europeo y del Consejo, y por el que se derogan la Directiva 87/250/CEE de la Comisión, la Directiva 90/496/CEE del Consejo, la Directiva 1999/10/CE de la Comisión, la Directiva 2000/13/CE del Parlamento Europeo y del Consejo, las Directivas 2002/67/CE, y 2008/5/CE de la Comisión, y el Reglamento (CE) no 608/2004 de la Comisión* Texto pertinente a efectos del EEE.
- [57] «El Plan Estratégico de La PAC de España.» (), dirección: <https://www.mapa.gob.es/es/pac/pac-2023-2027/plan-estrategico-pac> (visitado 21-09-2025).
- [58] J. Yan, J. Domskienė y E. Gaidule, «An overview of technological challenges in implementing the digital product passport in the textile and clothing industry,» *AUTEX Research Journal*, vol. 24, n.º 3, pág. 20 240 002, 2024, ISSN: 2191-0294. DOI: 10.1515/aut-2024-0002.
- [59] F. P. Adams y G. May, «Digital Product Passport Implementation Based on Multi-Blockchain Approach with Decentralized Identifier Provider,» *Applied Sciences*, vol. 14, n.º 11, pág. 4874, 2024, ISSN: 2076-3417. DOI: 10.3390/app14114874.
- [60] F. Psarommatis y G. May, «Digital Product Passport: A Pathway to Circularity and Sustainability in Modern Manufacturing,» *Sustainability*, vol. 16, n.º 1, pág. 396, 2024, ISSN: 2071-1050. DOI: 10.3390/su16010396.
- [61] T. Alam y M. Benaida, «An overview of IoT architectures, technologies, and existing open-source projects,» *Internet of Things*, vol. 20, pág. 100 602, 2022, ISSN: 2542-6605. DOI: 10.1016/j.iot.2022.100602.
- [62] K. Manditereza. «Lorawan and mqtt integration for iot application design,» HiveMQ. (feb. de 2022), dirección: <https://www.hivemq.com/blog/lorawan-and-mqtt-integrations-for-iot-applications-design/> (visitado 17-10-2025).
- [63] «Epcis and cbv 2.0: Launch and overview,» GS1, 2022. dirección: https://www.gs1.org/docs/epcis/epcis_2-0_launch.pdf (visitado 04-10-2025).
- [64] P. Rovira. «Innovación y sostenibilidad: cómo la tecnología blockchain impulsa la trazabilidad alimentaria.» (), dirección: <https://pere-rovira.com/blog/innovacion-y-sostenibilidad-como-la-tecnologia-blockchain-impulsa-la-trazabilidad-alimentaria/> (visitado 04-10-2025).
- [65] «Gs1 digital link standard (release 1.1.1),» GS1, 2020. dirección: <https://www.gs1.org/standards/gs1-digital-link> (visitado 04-10-2025).
- [66] M. Hulea, S. M. Rosu, R. J. Glass y col., «Digital product passport implementation based on producer and recycler information requirements,» *Journal of Cleaner Production*, vol. 440, pág. 140 760, 2024, ISSN: 0959-6526. DOI: 10.1016/j.jclepro.2024.140760. dirección: <https://www.sciencedirect.com/science/article/pii/S0959652624001234> (visitado 14-10-2025).

- [67] *Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 on ecodesign requirements for sustainable products and repealing Directive 2009/125/EC*, European Union, 13 de jun. de 2024. dirección: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1781> (visitado 04-10-2025).
- [68] «¿Qué es IOTA y cómo funciona?» (), dirección: <https://kriptomat.io/es/cotizacion-criptomonedas/iota-miota-precio/que-es/> (visitado 04-10-2025).
- [69] N. CSRC. «Hash function — Glossary.» (2024), dirección: https://csrc.nist.gov/glossary/term/hash_function (visitado 14-10-2025).
- [70] N. CSRC. «Preimage resistance — Glossary.» (2024), dirección: https://csrc.nist.gov/glossary/term/preimage_resistance (visitado 14-10-2025).
- [71] N. CSRC. «Hash Functions — NIST Project Page.» (2017), dirección: <https://csrc.nist.gov/projects/hash-functions> (visitado 14-10-2025).
- [72] N. CSRC. «Second preimage resistance — Glossary.» (2024), dirección: https://csrc.nist.gov/glossary/term/second_preimage_resistance (visitado 14-10-2025).
- [73] Q. Dang, «Recommendation for Applications Using Approved Hash Algorithms,» NIST, inf. téc. SP 800-107 Rev.1, 2012. dirección: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-107r1.pdf> (visitado 14-10-2025).
- [74] IOTA Foundation. «Hashing.» IOTA Move Library: std::hash (SHA2-256, SHA3-256) e iota::hash (Keccak256, BLAKE2b-256). (2025), dirección: <https://docs.iota.org/developer/cryptography/on-chain/hashing> (visitado 14-10-2025).
- [75] IOTA Foundation. «Module iota::hash.» (2025), dirección: <https://docs.iota.org/developer/references/framework/iota/hash> (visitado 14-10-2025).
- [76] E. Heilman, N. Narula, G. Tanzer y col., «Cryptanalysis of Curl-P and Other Attacks on the IOTA Cryptocurrency,» en *Black Hat USA*, 2018. dirección: <https://i.blackhat.com/us-18/Wed-August-8/us-18-Narula-Heilman-Cryptanalysis-of-Curl-P-wp.pdf> (visitado 14-10-2025).
- [77] MIT Digital Currency Initiative. «Cryptanalysis of Curl-P and Other Attacks on the IOTA Cryptocurrency.» (2019), dirección: <https://www.dci.mit.edu/posts/cryptanalysis-of-curl-p-and-other-attacks-on-the-iota-cryptocurrency> (visitado 14-10-2025).
- [78] «Trazabilidad Alimentaria: Tecnología Blockchain.» (24 de oct. de 2022), dirección: <https://rujamar.com/trazabilidad-alimentaria-tecnologia-blockchain/> (visitado 04-10-2025).
- [79] «Blockchain y trazabilidad: Transparencia en el mercado alimentario,» Red Alimentaria Food Tech. (dic. de 2024), dirección: <https://www.redalimentariafoodtech.com/nota/589027-blockchain-y-trazabilidad-transparencia-en-el-mercado-alimentario-2> (visitado 17-10-2025).
- [80] «Technical and Tokenomics Whitepaper,» IOTA Foundation, 30 de mayo de 2025. dirección: https://www.iota.org/pdf/IOTA_Technical_and_Tokenomics_Whitepaper.pdf (visitado 04-10-2025).
- [81] I. Foundation, «Direct Acyclic Graph-based Ledger for Internet of Things.» dirección: https://files.iota.org/papers/Direct_Acyclic_Graph-based_Ledger_for_Internet_of_Things.pdf (visitado 04-10-2025).

- [82] «Qué es IOTA, para qué sirve,» Computing. (2024), dirección: <https://www.computing.es/redes/que-es-iota-para-que-sirve/> (visitado 04-10-2025).
- [83] S. Popov y col., «Tangle 2.0: Leaderless Nakamoto Consensus on the Heaviest DAG,» 2021, Whitepaper IOTA 2.0. dirección: <https://files.iota.org/papers/Tangle-2.0-Leaderless-Nakamoto-Consensus-on-the-Heaviest-DAG.pdf> (visitado 17-10-2025).
- [84] «Comparison — IOTA Documentation,» IOTA Foundation, 2024. dirección: <https://docs.iota.org/iota-compared> (visitado 04-10-2025).
- [85] B. Techs, «Comparing Blockchain Protocols: Choosing the Right Platform for Your Project,» *Blockchain Techs*, 2025. dirección: <https://blockchaintechs.io/comparison-of-blockchain-protocols/> (visitado 04-10-2025).
- [86] R. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob y A. Mohammed, «Evaluating blockchain platforms for IoT applications in Industry 5.0,» *Digital Chemical Engineering*, vol. 5, pág. 100 037, 2024, ISSN: 2096-7209. doi: 10.1016/j.dche.2024.100037.
- [87] IOTA Foundation. «IOTA Networks (Mainnet, Shimmer, Testnet, Devnet).» (2025), dirección: <https://wiki.iota.org/shimmer/networks/overview/> (visitado 17-10-2025).
- [88] IOTA Foundation. «Anchor Your Data with IOTA Notarization.» (2025).
- [89] «Guía de Implementación de la Iniciativa de Trazabilidad para los Productos Frescos,» 2025. dirección: <https://producetraceability.org/wp-content/uploads/2025/02/SPANIS2.pdf> (visitado 04-10-2025).
- [90] «Estándar Mundial de Trazabilidad,» 2024. dirección: <https://www.gs1py.org/docs/EstandarTrazabilidad.pdf> (visitado 04-10-2025).
- [91] GS1. «GS1 Application Identifier List.» (2025), dirección: <https://digital-link-qr-code.com/application-identifier-list> (visitado 19-10-2025).
- [92] GS1. «GS1 Application Identifiers.» (2024), dirección: <https://ref.gs1.org/ai/> (visitado 19-10-2025).
- [93] GS1. «GS1 Digital Link Standard: URI Syntax.» (2022), dirección: https://www.gs1ie.org/download_files/standards-documents/gs1-digital-link-standard/gs1-digital-link-standard-uri-syntax.pdf (visitado 19-10-2025).
- [94] «Iberian Peninsula,» ASICI, 2024. dirección: https://iberico.com/wp-content/uploads/2024/12/Dossier_UK_ENG.pdf (visitado 04-10-2025).
- [95] «Ítaca: The ibérico ham guarantee.» (), dirección: https://www.qcom.es/alimentacion/reports/itaca-the-iberico-ham-guarantee_33237_2580_37122_0_1_in.html (visitado 04-10-2025).
- [96] «How security seals protect value in the iberian ham industry.» (5 de sep. de 2025), dirección: <https://relyongroup.com/news/how-security-seals-protect-value-in-the-iberian-ham-industry> (visitado 04-10-2025).
- [97] «Implementing the EU digital battery passport,» CEPS, 2024. dirección: <https://www.ceps.eu/ceps-publications/implementing-the-eu-digital-battery-passport/> (visitado 04-10-2025).
- [98] Circularise, «Digital Product Passports (DPPs) required by EU legislation across sectors,» *Circularise*, 2025. dirección: <https://www.circularise.com/blogs/dpps-required-by-eu-legislation-across-sectors> (visitado 04-10-2025).

-
- [99] N. Malmros. «How the digital product passport for batteries works,» Sigma Technology. (2024), dirección: <https://sigmatechnology.com/articles/how-the-digital-product-passport-for-batteries-works/> (visitado 17-10-2025).
- [100] «Rujamar joins te-food blockchain.» (9 de mar. de 2021), dirección: <https://www.foodonline.com/doc/rujamar-joins-te-food-blockchain-0001> (visitado 04-10-2025).
- [101] «Tracing an egg with blockchain all the way back to laying.» (20 de ene. de 2021), dirección: <https://www.wattagnet.com/egg/egg-production/blog/15532736/tracing-an-egg-with-blockchain-all-the-way-back-to-laying> (visitado 04-10-2025).
- [102] «What's new with origintrail v8.» (30 de ene. de 2025), dirección: <https://docs.origintrail.io/useful-resources/previous-updates/whats-new-with-origintrail-v8> (visitado 04-10-2025).
- [103] «What is iot security? challenges and requirements.» (), dirección: <https://www.fortinet.com/resources/cyberglossary/iot-security> (visitado 04-10-2025).
- [104] «The top 8 it/ot/iot security challenges and how to solve them.» (25 de mar. de 2025), dirección: <https://www.balbix.com/insights/addressing-iot-security-challenges/> (visitado 04-10-2025).
- [105] A. Ltd. «TrustZone for Cortex-M — System-Wide Security for IoT Devices.» (2025), dirección: <https://www.arm.com/technologies/trustzone-for-cortex-m> (visitado 14-10-2025).
- [106] Arm/Keil, «Using TrustZone on Armv8-M (Application Note AN291),» Arm/Keil, inf. téc., 2019. dirección: https://www.keil.com/appnotes/files/apnt_291.pdf (visitado 14-10-2025).
- [107] «Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks,» NIST, 2019. dirección: <https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8228.pdf> (visitado 04-10-2025).
- [108] «Iot device security: Risks, best practices, and protection tips.» (), dirección: <https://www.keyfactor.com/education-center/iot-device-security/> (visitado 04-10-2025).
- [109] P. A. Grassi, M. F. Bartock y N. Team, «Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks,» NIST, inf. téc. NISTIR 8228, 2019. dirección: <https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8228.pdf> (visitado 04-10-2025).
- [110] Keyfactor. «IoT Device Security: Risks, Best Practices, and Protection Tips.» (2025), dirección: <https://www.keyfactor.com/education-center/iot-device-security/> (visitado 04-10-2025).
- [111] S. Mangard, E. Oswald y T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, 2007, ISBN: 978-0-387-30857-9.
- [112] P. Kocher, J. Jaffe y B. Jun, «Differential Power Analysis,» en *Advances in Cryptology — CRYPTO'99*, ép. LNCS, vol. 1666, Springer, 1999, págs. 388-397.
- [113] «Ipfes (interplanetary file system).» Guide to IPFS in Web3, Meegle. (mar. de 2025), dirección: https://www.meegle.com/en_us/topics/web3/ipfs-interplanetary-file-system (visitado 18-10-2025).

- [114] OpenEPCIS. «EPCIS 2.0 and EPCIS 1.2 Documentation.» (2022), dirección: <https://openepcis.io/docs/epcis> (visitado 19-10-2025).
- [115] Kezzler. «Why Transformation Events are the Future of Traceability.» (2025), dirección: <https://kezzler.com/blog/why-transformation-events-are-the-future-of-traceability/> (visitado 19-10-2025).
- [116] «Iota notarization — verifiable, immutable and flexible on-chain records for any use case.» Toolkit for data integrity with IOTA, IOTA Foundation. (2025), dirección: <https://www.iota.org/products/notarization> (visitado 18-10-2025).
- [117] The Things Industries, *Thethingsnetwork/lorawan-stack: The things stack, an open source lorawan network server*, LoRaWAN network stack for public and private networks, GitHub, 2025. dirección: <https://github.com/TheThingsNetwork/lorawan-stack> (visitado 18-10-2025).
- [118] P. G. D. Group. «PostgreSQL – Open Source Relational Database Adopted by Industry Giants.» PostgreSQL official website. (2024), dirección: <https://www.postgresql.org/about/> (visitado 20-10-2025).
- [119] R. Booz. «PostgreSQL + TimescaleDB: 1000x Faster Queries, 90 % Data Compression, and Much More.» TigerData Blog, accessed 2024. (jun. de 2025), dirección: <https://www.tigerdata.com/blog/postgresql-timescaledb-1000x-faster-queries-90-data-compression-and-much-more>.
- [120] «Industrial iot visualization: How grafana powers industrial automation and iiot.» Grafana for IIoT use cases, Grafana Labs. (ene. de 2025), dirección: <https://grafana.com/blog/2025/01/27/industrial-iot-visualization-how-grafana-powers-industrial-automation-and-iiot/> (visitado 18-10-2025).
- [121] P. Labs. «IPFS Documentation – Content Addressing and CIDs.» (2024), dirección: <https://docs.ipfs.tech/concepts/content-addressing/> (visitado 20-10-2025).
- [122] Wikipedia. «InterPlanetary File System (IPFS) – Content-addressed Storage Ensuring Data Integrity.» (2024), dirección: https://en.wikipedia.org/wiki/InterPlanetary_File_System (visitado 20-10-2025).
- [123] I. Foundation. «IOTA Notarization Framework – Introduction and Use Cases.» (2024), dirección: <https://docs.iota.org/developer/iota-notarization/> (visitado 20-10-2025).
- [124] T. Onyekwere. «The Role of Merkle Trees and Merkle Proofs in Blockchain Development.» (2023), dirección: <https://medium.com/codex/the-role-of-merkle-trees-and-merkle-proofs-in-blockchain-development-e5100d7e3623> (visitado 20-10-2025).
- [125] I. Foundation. «Deep Dive into Stardust – Alias Output and New Output Types in IOTA.» (nov. de 2023), dirección: <https://iota-news.com/deep-dive-into-stardust/> (visitado 20-10-2025).
- [126] I. Foundation. «IOTA Stardust Protocol Upgrade – Multi-asset Ledger and Data Storage Features.» IOTA Blog, accessed 2023-2024. (2023), dirección: <https://blog.iota.org/tag/stardust/>.
- [127] I. Foundation. «IOTA Identity 1.0 – Decentralized Identifiers on Stardust (DID Documents in Alias Outputs).» (nov. de 2023), dirección: <https://blog.iota.org/iota-identity-1-0-is-here/> (visitado 20-10-2025).

- [128] J. Hunter. «Pinata – Pin by CID Distributes Content Across Multiple IPFS Nodes.» (ene. de 2024), dirección: <https://pinata.cloud/blog/the-new-and-improved-pin-by-cid/> (visitado 20-10-2025).
- [129] S. Labs. «Scaleway IPFS Pinning – Redundancy and Availability Across Nodes.» (2024), dirección: <https://labs.scaleway.com/en/ipfs-pinning/> (visitado 20-10-2025).
- [130] E. Griffiths. «Flexible Pricing for IPFS Pinning – Plans Starting at \$20/Month.» (abr. de 2025), dirección: <https://nft.storage/blog/maximize-your-nft-storage-potential-with-pinatas-flexible-solutions> (visitado 20-10-2025).
- [131] P. Labs. «IPNS – InterPlanetary Name System Concepts and Usage.» (2024), dirección: <https://docs.ipfs.tech/concepts/ipns/> (visitado 20-10-2025).
- [132] I. Documentation. «IPNS Records in DHT – Lifetime and Republishing Interval (48h Validity).» (2024), dirección: <https://docs.ipfs.tech/concepts/ipns/#ipns-over-the-dht> (visitado 20-10-2025).
- [133] rklaehn y stebalien (IPFS Developer). «Confusion about IPNS (IPFS Forum Discussion).» (2017), dirección: <https://discuss.ipfs.tech/t/confusion-about-ipns/1414> (visitado 20-10-2025).
- [134] I. Bolychevsky, «Verifiable credentials and decentralised identifiers: Technical landscape,» GS1, feb. de 2025, Assessment of VCs and DIDs standards for supply chains. dirección: <https://ref.gs1.org/docs/2025/VCs-and-DIDs-tech-landscape> (visitado 18-10-2025).
- [135] «Role of verifiable credentials in supply chain management.» VCs for SCM transparency and efficiency, EveryCRED. (2024), dirección: <https://everycred.com/blog/role-of-verifiable-credentials-in-supply-chain-management/> (visitado 18-10-2025).
- [136] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista y M. Conti, «A survey on decentralized identifiers and verifiable credentials,» *arXiv preprint*, 2024, arXiv:2402.02455v2 [cs.CR]. dirección: <https://arxiv.org/abs/2402.02455> (visitado 18-10-2025).
- [137] bernat-99. «DPP Jamón — PDP para jamón ibérico (código y evidencias del TFG).» Repositorio GitHub. Incluye scripts de notarización, colección Postman, salidas del resolutor y datasets de benchmark. (2025), dirección: <https://github.com/bernat-99/dpp-jamon> (visitado 03-11-2025).



POLITÉCNICA

ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INDUSTRIALES
UNIVERSIDAD POLITÉCNICA DE MADRID

José Gutiérrez Abascal, 2. 28006 Madrid
Tel.: 91 336 3060
info.industriales@upm.es

www.industriales.upm.es