ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

MÁSTER EN INGENIERÍA INDUSTRIAL

BLOCKCHAIN APLICADO A SUPPLY CHAIN. PROPUESTA DE APLICACIÓN AL SECTOR ALIMENTARIO

Autor: Borja Calvo Gallego
Director: Cristina Domínguez Soto

Madrid

Julio 2018

AUTORIZACIÓN PARA LA DIGITALIZACIÓN, DEPÓSITO Y DIVULGACIÓN EN RED DE PROYECTOS FIN DE GRADO, FIN DE MÁSTER, TESINAS O MEMORIAS DE BACHILLERATO

1º. Declaración de la autoría y acreditación de la misma.

El autor D. Borja Calvo Gallego_____

DECLARA ser el titular de los derechos de propiedad intelectual de la obra: Blockchain en supply chain. Propuesta de aplicación al sector alimentario_____, que ésta es una obra original, y que ostenta la condición de autor en el sentido que otorga la Ley de Propiedad Intelectual.

2º. Objeto y fines de la cesión.

Con el fin de dar la máxima difusión a la obra citada a través del Repositorio institucional de la Universidad, el autor **CEDE** a la Universidad Pontificia Comillas, de forma gratuita y no exclusiva, por el máximo plazo legal y con ámbito universal, los derechos de digitalización, de archivo, de reproducción, de distribución y de comunicación pública, incluido el derecho de puesta a disposición electrónica, tal y como se describen en la Ley de Propiedad Intelectual. El derecho de transformación se cede a los únicos efectos de lo dispuesto en la letra a) del apartado siguiente.

3º. Condiciones de la cesión y acceso

Sin perjuicio de la titularidad de la obra, que sigue correspondiendo a su autor, la cesión de derechos contemplada en esta licencia habilita para:

a) Transformarla con el fin de adaptarla a cualquier tecnología que permita incorporarla a internet y hacerla accesible; incorporar metadatos para realizar el registro de la obra e incorporar "marcas de agua" o cualquier otro sistema de seguridad o de protección.
b) Reproducirla en un soporte digital para su incorporación a una base de datos electrónica, incluyendo el derecho de reproducir y almacenar la obra en servidores, a los efectos de garantizar su seguridad, conservación y preservar el formato.
c) Comunicarla, por defecto, a través de un archivo institucional abierto, accesible de modo libre y gratuito a través de internet.
d) Cualquier otra forma de acceso (restringido, embargado, cerrado) deberá solicitarse expresamente y obedecer a causas justificadas.
e) Asignar por defecto a estos trabajos una licencia Creative Commons.
f) Asignar por defecto a estos trabajos un HANDLE (URL *persistente)*.

4º. Derechos del autor.

El autor, en tanto que titular de una obra tiene derecho a:

a) Que la Universidad identifique claramente su nombre como autor de la misma
b) Comunicar y dar publicidad a la obra en la versión que ceda y en otras posteriores a través de cualquier medio.
c) Solicitar la retirada de la obra del repositorio por causa justificada.
d) Recibir notificación fehaciente de cualquier reclamación que puedan formular terceras personas en relación con la obra y, en particular, de reclamaciones relativas a los derechos de propiedad intelectual sobre ella.

5º. Deberes del autor.

El autor se compromete a:

a) Garantizar que el compromiso que adquiere mediante el presente escrito no infringe ningún derecho de terceros, ya sean de propiedad industrial, intelectual o cualquier otro.
b) Garantizar que el contenido de las obras no atenta contra los derechos al honor, a la intimidad y a la imagen de terceros.
c) Asumir toda reclamación o responsabilidad, incluyendo las indemnizaciones por daños, que

pudieran ejercitarse contra la Universidad por terceros que vieran infringidos sus derechos e intereses a causa de la cesión.

d) Asumir la responsabilidad en el caso de que las instituciones fueran condenadas por infracción de derechos derivada de las obras objeto de la cesión.

6º. Fines y funcionamiento del Repositorio Institucional.

La obra se pondrá a disposición de los usuarios para que hagan de ella un uso justo y respetuoso con los derechos del autor, según lo permitido por la legislación aplicable, y con fines de estudio, investigación, o cualquier otro fin lícito. Con dicha finalidad, la Universidad asume los siguientes deberes y se reserva las siguientes facultades:

- La Universidad informará a los usuarios del archivo sobre los usos permitidos, y no garantiza ni asume responsabilidad alguna por otras formas en que los usuarios hagan un uso posterior de las obras no conforme con la legislación vigente. El uso posterior, más allá de la copia privada, requerirá que se cite la fuente y se reconozca la autoría, que no se obtenga beneficio comercial, y que no se realicen obras derivadas.
- La Universidad no revisará el contenido de las obras, que en todo caso permanecerá bajo la responsabilidad exclusive del autor y no estará obligada a ejercitar acciones legales en nombre del autor en el supuesto de infracciones a derechos de propiedad intelectual derivados del depósito y archivo de las obras. El autor renuncia a cualquier reclamación frente a la Universidad por las formas no ajustadas a la legislación vigente en que los usuarios hagan uso de las obras.
- La Universidad adoptará las medidas necesarias para la preservación de la obra en un futuro.
- La Universidad se reserva la facultad de retirar la obra, previa notificación al autor, en supuestos suficientemente justificados, o en caso de reclamaciones de terceros.

Madrid, a 4 de Julio de 2018

ACEPTA 

Fdo.: Borja Calvo Gallego

Motivos para solicitar el acceso restringido, cerrado o embargado del trabajo en el Repositorio Institucional:

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título .Blockchain en supply chain. Propuesta de aplicación al sector alimentario en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico 2017/2018 es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos. El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido tomada

de otros documentos está debidamente referenciada.

Fdo.: Borja Calvo Gallego Fecha: 10/07/2018

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Fdo.: Cristina Domínguez Soto Fecha: 10/ 07/ 2018

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA (ICAI)

MÁSTER EN INGENIERÍA INDUSTRIAL

BLOCKCHAIN APLICADO A SUPPLY CHAIN. PROPUESTA DE APLICACIÓN AL SECTOR ALIMENTARIO

Autor: Borja Calvo Gallego
Director: Cristina Domínguez Soto

Madrid

Julio 2018

BLOCKCHAIN EN SUPPLY CHAIN. PROPUESTA DE APLICACIÓN AL SECTOR ALIMENTARIO.

Autor: Calvo Gallego, Borja.
Director: Domínguez Soto, Cristina.
Entidad Colaboradora: ICAI – Universidad Pontificia Comillas.

RESUMEN DEL PROYECTO

El presente trabajo de fin de máster consiste en la propuesta teórica de implantación de un sistema de gestión de la cadena de suministro basado en blockchain, utilizando como caso práctico la cadena de suministro del jamón ibérico. Para ello, en el trabajo se pueden diferenciar tres bloques principales:

- Estado del arte de supply chain, recopilando los modelos existentes en el mundo empresarial

- Estado del arte de blockchain, recogiendo información sobre su funcionamiento técnico y sus aplicaciones

- Caso práctico de aplicación, centrado en la cadena de suministro del jamón ibérico en España, donde se detallan las recomendaciones para una implantación de la tecnología blockchain

1. Supply chain

Supply chain puede definirse informalmente como el conjunto de etapas que sigue un producto desde el proveedor de materia prima hasta el consumidor final. Es un concepto que ha sufrido una gran evolución en los últimos años y cuya evolución conlleva asociadas unas técnicas de gestión adecuadas. Estas técnicas de gestión de la cadena de suministro se han desarrollado intensamente en los últimos años, adquiriendo gran relevancia en las empresas de la mayoría de sectores.

El sector alimentario en particular presenta una serie de retos (productos perecederos y salud pública) que hacen que mejorar la transparencia y trazabilidad de la cadena de suministro sea una prioridad para las empresas del sector.

La necesidad de identificar cada uno de los productos de consumo propició la creación del estándar del código de barras, ampliamente utilizado en la actualidad,

aunque cuenta con considerables desventajas, ya que debe existir una colocación frente al lector, puede deteriorarse fácilmente, etc. Para paliar estas desventajas, se introdujo el RFID (*Radio Frequency Identification*), que funciona sin fuente de alimentación externa, es complicado de dañar y además admite la lectura y escritura dinámica de datos a lo largo de la cadena, lo que lo convierte en ideal para exprimir las capacidades computacionales y de análisis existentes en la actualidad y hacer más segura, fiable y eficiente la cadena de suministro.

2. Blockchain

Blockchain es la tecnología que sustenta bitcoin, su aplicación más conocida y presentada en 2008. Blockchain es una base de datos descentralizada, protegida mediante criptografía y organizada mediante bloques de transacciones relacionados entre si matemáticamente. Sin embargo, lo que hace única a esta tecnología es la imposibilidad de alteración de los registros, lo que permite a las partes establecer confianza de forma directa, sin una tercera entidad que la aporte.

El funcionamiento a nivel técnico de blockchain es complejo, pero de forma resumida es el siguiente:

1. *Registro de la transacción*: Tras realizarse una transacción (Juan le compra una moto a Luis, una empresa compra de su proveedor, se vende una entrada para un concierto, etc), se registran los datos asociados a la transacción.

2. *Creación del bloque*: Una vez en la red, el registro de información se combina con la información de otras transacciones en un bloque ordenado cronológicamente. Cuando se completa el bloque, se le asigna información horaria para que toda la información almacenada en la cadena sea secuencial.

3. *Incorporación de los bloques*: Una vez se ha completado el bloque, se envía a la red, añadiéndose a la cadena. Cabría la posibilidad de que todos los participantes enviasen bloques a la vez, pero la información horaria recogida en los bloques rompería esa simultaneidad, asegurando su incorporación en el orden correcto y la copia actualizada de la cadena para todos los participantes.

4. *Protección de la cadena*: La cadena es encriptada mediante criptografía, generando un hash (secuencia única de caracteres alfanuméricos). Para realizar la unión de los bloques, el hash del bloque anterior (n) es añadido como dato al bloque n+1, de forma que al hashear el bloque n+1, se incluye la

información del bloque n. Al ser el hash único, cualquier modificación de un dato en un bloque n provocará un desajuste en el hash del bloque n+1 y siguientes, denotando una alteración.

Cabe destacar la diferenciación entre dos tipos de blockchains, las públicas y las privadas:

- *Blockchains públicas*: Cualquier persona, usuario o no, puede acceder y consultar las transacciones realizadas. Además, cualquier persona puede acceder, convertirse en usuario y ser partícipe de la red. Aunque los propietarios de las transacciones no pueden ser identificados, sus direcciones si que son trazables, por lo que excepto en el caso de que sean expresamente diseñadas para ser anónimas, las cadenas de bloques son pseudoanónimas.

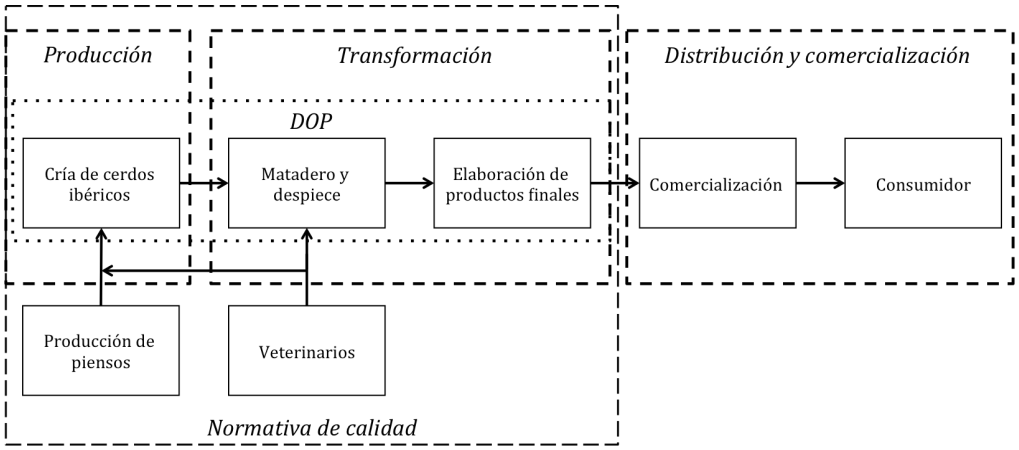
- *Blockchains privadas*: Las blockchains privadas surgen a raíz de la imposibilidad de compartir, por confidencialidad, todos los registros de forma abierta. Por lo tanto, estas cadenas de bloques solo son accesibles a los usuarios de la cadena, que deben ser invitados a serlo. Además los usuarios podrán solo consultar la cadena o consultar y modificarla, según los intereses y diseño de cada cadena privada. La desventaja es que todos los nodos se conocen y tienden a ser menos numerosos que en una blockchain pública, por lo que la posibilidad de un ataque exitoso se multiplica. En cuanto al anonimato, en las blockchains privadas, se puede establecer el nivel de anonimato que la entidad responsable desee.

La tecnología blockchain ha suscitado el interés de la industria tecnológica y, aunque no se ha logrado implantar de forma masiva más allá del ámbito financiero, existen pilotos de aplicación en sectores diversos, como el energético o el de los seguros. Es una tecnología llamada a ser protagonista de la próxima revolución, siendo la base del IoT (*Internet of Things*).

3. Caso de aplicación en el sector alimentario. El jamón ibérico.

Además de los retos anteriormente comentados, en el sector alimentario existen ciertos productos que por su exclusividad o precio, son objeto de fraude (atún rojo, caviar o jamón ibérico entre otros). En el presente trabajo se presenta una propuesta de implantación de un sistema basado en blockchain para el jamón ibérico.

El sector del jamón ibérico en España es un sector altamente tradicional y opaco, con productos diferenciados (jamón de cebo, de cebo de campo o de bellota) y que aún constando de un etiquetado estricto, es objeto de fraude. Actualmente, la cadena de suministro del jamón ibérico se puede ilustrar de la siguiente manera:



Actualmente (AS-IS) las empresas que participan en la cadena de suministro gestionan la trazabilidad a través del etiquetado, que es en forma de códigos de barras. Además, cada empresa lo realiza de forma individual, sin interconexiones y muchas veces utilizando registros en papel, de forma que en caso de necesidad de retirada de un producto o lote, esta se realiza de forma ineficaz e ineficiente.

La implantación de un sistema basado en blockchain permitiría:

i. Certificar el origen del jamón
ii. Trazabilidad total integrada en la cadena de suministro
iii. Información totalmente disponible y accesible al consumidor mediante código QR.

El funcionamiento del sistema se basaría en el etiquetado con tecnología RFID que recogiese datos de entrada/salida de cada etapa así como parámetros críticos dentro de las mismas (humedad relativa y temperatura). Estos datos serían registrados utilizando la cadena de bloques privada accesible mediante el proyecto hyperledger y accesibles al consumidor final mediante un código QR con toda la información que sería generado por el distribuidor.

En el análisis económico propuesto, se han elaborado tres escenarios (optimista, neutro y pesimista), analizando el neutro y obteniendo los siguientes resultados:

VAN	3.635 €
Tasa de descuento	10%
TIR	11%
Payback (años)	5,87

Como resultado de un VAN>0, se considera el proyecto económicamente viable.

Durante la elaboración del presente trabajo, se han encontrado las siguientes conclusiones principales:

1. Blockchain aportaría la seguridad y confianza extra al consumidor de que el producto que adquiere es el que el etiquetado dice ser, además, lo hace a un coste no excesivamente alto, por lo que se genera la posibilidad de utilización de los sistemas por las explotaciones más pequeñas.

2. Incluso con la implantación de blockchain, quedan remanentes pequeños riesgos de fraude, principalmente ligados a las acciones humanas, pues una automatización total no es posible en el sector.

3. Las ventajas de implantar un sistema de gestión basado en blockchain en el sector alimentario son numerosas, sin embargo, el gran número de partícipes de estas cadenas y la diseminación en ellas hace que las soluciones basadas en blockchain tengan una implementación compleja que requiere un horizonte temporal significativo.

Finalmente, se sugieren una serie de recomendaciones para el sector, resumidas en la tabla siguiente y sobre las que podría proponerse más adelante un estándar de gestión.

Ítem	***Detalles***
Blockchain privada	Inscripción en el proyecto hyperledger
Etiquetas RFID con sensor de humedad y temperatura integrado	
Registros en blockchain	Entrada y salida de cada etapa y parámetros de control oportunos
Control continuo de temperatura y humedad relativa durante elaboración	Junto al tiempo de procesado (obtenido por los registros de entrada y salida) son parámetros críticos para asegurar la calidad
Control de origen y destino en transporte	
Acceso del consumidor	Una vez el distribuidor da de alta el jamón en su sistema, genera un código QR que contiene toda la información

BLOCKCHAIN IN SUPPLY CHAIN. AN APPLICATION IN THE FOOD INDUSTRY.

Author: Calvo Gallego, Borja.
Director: Domínguez Soto, Cristina.
Collaborative Entity: ICAI – Universidad Pontificia Comillas.

PROJECT SUMMARY

The present document consists on the theoretical proposal for the application of a blockchain-based supply chain management system, using as a practical guide to implantation Spanish dry-cured ham. Within the project, three contents blocks can be found:

- Supply chain state of the art, reviewing the existing models within the corporate world
- Blockchain state of the art, gathering information about how it works and its applications
- Application case, focused on the Spanish dry-cured ham supply chain, and where the recommendations for a blockchain-based system are stated

1. Supply chain

Supply chain can be defined as the set of stages that a product follows, from the producer until it reaches the final consumer. It is a concept that has greatly evolved over the last years, hand-to-hand with associated management techniques. These management techniques have strongly developed over the last few decades, gaining great relevance within the companies, no matter the economic sector.

Food industry in particular presents a series of challenges (perishable products and public health) that strongly push towards the development of supply chain transparency and traceability.

Barcode was propitiated by the necessity of individually identifying each product, and is now a standard widely use through the industry although it has numerous disadvantages such as the in-front colocation towards the lector, the easy deterioration it can suffer, etc. To ease these, RFID (Radio Frequency Identification) was

introduced. It works without an external power supply, it is difficult to harm and admits writing and reading of dynamic data along the supply chain, what makes it perfect to exploit the computational and analysis capabilities that are available nowadays, making the supply chain safer, more reliable and efficient.

2. Blockchain

Blockchain is the technology behind bitcoin, the most widely known application, presented in 2008. Blockchain is a decentralized database, protected by cryptography and organized using transaction blocks connected between them mathematically. However, what makes this technology unique is the impossibility of modifying the registers, what allows different parties to establish direct confidence, without the need for a third entity that adds trust.

How blockchain works at a technical level is complex, but in summary its main steps are:

1. *Transaction registration:* When a transaction is done (John buys a motorcycle from Ben, a company buys to its provider, a concert ticket is sold, etc.) data associated with the transactions are registered.

2. *Block creation:* Register gets combined with others transactions in a block that is chronologically organized. When the block is completed, time information is added so the chain is also ordered.

3. *Block aggregation:* Once the block is completed, it is sent to the network, adding it to the chain. It could happen that all participants sent blocks simultaneously, but the time information within the blocks would break that simultaneousness, assuring that block aggregation is done in the correct way.

4. *Chain protection:* The chain is encrypted using cryptography, generating a hash (unique sequence of alphanumeric characters). For making the blocks connections, last block hash (n), is added as a data to the n+1 block, so that when block n+1 is hashed, information from block n is included. Being the hash unique, any modification of a data in block n will result in a hash modification of block n+1 and the next ones, indicating an alteration.

There are two different types of blockchains, public and private:

- *Public blockchains*: Any person, user or not, can access the database and check the transactions. Furthermore, any person can access, become a user and be part of the network. Even though the users that register each transaction are not identifiable, the directions they use are, so except the blockchain is design as anonymous, public blockchains are pseudo-anonymous.

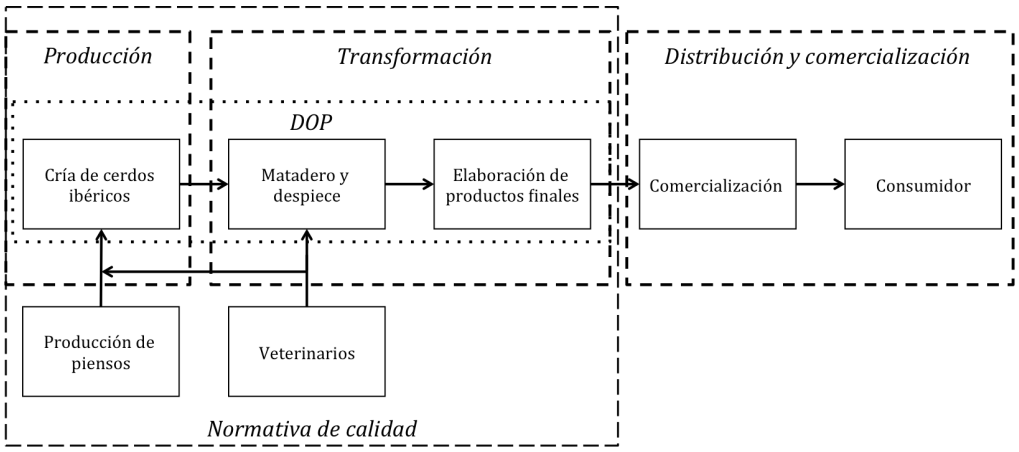
- *Private blockchain*: Private blockchains arise from the impossibility to share all the register openly for confidentiality reasons. This blockchains are only accessible for the users, which have to be invited to gain access. Users could only check or check and modify the blockchain according to the design of each private blockchain. The disadvantage is that all the nodes are known and tend to be less numerous than in a public blockchain, multiplying the probability of a successful attack. Regarding anonymity, in private blockchains, the anonymity level can de design according to the interests of the responsible entity.

Blockchain technology have gained the interest of the tech industry and although its only massive application has been in the financial sector, pilot projects exist within a variety of industries such as energy or insurance. It is a tech called to play a leading role in the next revolution, being the base of IoT (Internet of things).

3. Application case in the food industry. Spanish dry-cured ham.

In addition to the challenges formerly named, within the food industry, there are some products that because of its exclusivity or price are fraud targets (red tuna, caviar or Spanish dry-cured ham among others). In this document a theoretical proposal is presented for the implementation of a blockchain-based system for the Spanish dry-cured ham.

Spanish dry-cured ham industry is highly traditional and opaque, with product differentiation regarding the animals' diet and although there is a strict label system, fraud is present in the industry. Nowadays, Spanish dry-cured ham supply chain can be illustrated as follows:



Nowadays (AS-IS) companies that participate in the supply chain manage traceability through the label system, using mainly a barcode. In addition, each company keeps the record individually, there are not connections and paper-based registers are used sometimes. This way, in the case that a product has to be withdrawn, this withdrawal would be inefficient.

The implementation of a blockchain-based system would allow to:

i. Certify the dry-cured ham origin
ii. Global traceability integrated along the whole supply chain
iii. Product information available and accessible to the consumer via QR code

The system would be based in a RFID label that would record input and output data in each stage as well as critical parameters (relative humidity and temperature). This data would be recorded using a private blockchain accessible using the hyperledger project and the access to the consumer will be provided using a QR code generated by the distributor.

There has been an economic analysis, defining three different scenarios (optimist, neutral and pessimist). The neutral scenario has been analyzed and the results are shown in the following table:

NPV	3.635 €
Discount rate	10%
TIR	11%
Payback (years)	5,87

NPV value is greater tan zero, so the project generates value and the project is considered economically viable.

During the elaboration of this project, the following main conclusions have been found:

1. Blockchain would provide the consumer with the extra security and confidence that the product that is buying is what the label says. In addition, the blockchain-based system makes this possible at a reserved cost, generating a new differentiation possibility for small companies.

2. Even with the implementation of the blockchain-based system, small fraud risks still exist. These are mainly related to human actions, because a full automation is not possible in the industry.

3. Advantages of implementing a blockchain-based system in the food industry are numerous, however, the large amount of parties involved in the supply chain and their dissemination make the implementation of blockchain-based systems a complex project, requiring a long timeline.

Finally, a series of recommendations are given for the industry, gathered in the following table, could be the base for an industry standard.

Item	***Details***
Private blockchain	Hyperledger project registration
RFID labels with humidity and temperature sensors embedded	
Blockchain registers	Input/output at each stage and opportune parameters
Continuous control of humidity and temperature during elaboration	Alongside with time of processes (obtained with input/output data) are the critical parameters to assure quality
Origin and destination control in transport	
Consumer access	Using a QR code generated by the distributor once the product has been registered into its system

I. Índice General

II. Lista de figuras

III. Lista de tablas

1. Introducción

1.1. Contexto y Motivación

En el contexto competitivo del ecosistema empresarial actual, las empresas deben evolucionar continuamente a través de la innovación, buscando la eficiencia, reduciendo costes y manteniendo o incrementando el nivel de servicio a sus clientes, cada vez más exigentes.

En este entorno, con un mercado cada vez más volátil y cambiante, muchas empresas han optado por mejorar la gestión de la cadena de suministro, lo que ha supuesto una gran evolución del sector.

En concreto, las empresas alimentarias cuentan posiblemente con las cadenas de suministro más complejas y fragmentadas de toda la industria, plagadas de intermediarios, con localizaciones productivas a lo largo de todo el mundo y rutas logísticas por tierra, mar y aire. Todo esto dificulta la posibilidad de mantener un control sobre las mismas, incrementando la incertidumbre y el riesgo.

La imposibilidad de tener un control estricto sobre los productos a lo largo de la cadena se materializa en dos aspectos principales, la poca eficacia a la hora de retirar productos o identificar el origen de una contaminación junto al fraude. Pueden parecer aspectos menores, pero tienen graves impactos potenciales, tanto económicos como sobre la seguridad y la salud pública.

La tecnología aplicada durante los últimos años ha mejorado la gestión de la cadena de suministro, pero se basa en sistemas centralizados, donde los datos se ceden a una empresa, y cuya integración entre empresas a lo largo de la cadena no es, en muchas ocasiones viable y siempre difícil.

Además, la custodia de los datos por parte de un solo agente presenta debilidades como la posibilidad de ataques cibernéticos o la dependencia de sistemas de terceros sobre los que no existe control.

Aún así, cabe destacar que la trazabilidad de productos es posible con los sistemas existentes, y se ha realizado con éxito en numerosas ocasiones aunque estas ocasiones han sido motivadas en su mayor parte por exigencias de las autoridades y se ha realizado de forma rudimental e ineficiente.

Así, un sistema de gestión de la cadena de suministro basado en blockchain no posibilitaría la trazabilidad *per se*, pero aportaría tres grandes beneficios:

1. Los datos registrados no se pueden modificar

2. La trazabilidad se asegura de manera integral sin necesidad de ceder los datos a terceros

3. Se genera una confianza que permite la entrada a otros participantes en la cadena, sobretodo en sectores alimentarios tradicionales, donde la confianza proveedor-empresa se sitúa en la base de los contratos

Blockchain o cadena de bloques es la tecnología detrás de Bitcoin, y llamada a ser la revolución de internet. Desde 2008, se ha implementado en el sector financiero en multitud de proyectos, sin embargo, el salto al resto de sectores ha sucedido más recientemente a través de pilotos. La cadena de suministro es uno de estos sectores en los que se ha implementado en algunos pilotos, pero para ser efectivo, se necesita la adaptación de todos los partícipes de la cadena de suministros de cada producto y se requiere tiempo.

El sector alimentario, a diferencia del financiero, se basa en productos físicos, activos tangibles y por tanto, la conexión entre el mundo físico y el digital debe ser correctamente gestionada, suponiendo, junto al económico, uno de los obstáculos principales para la implantación de esta clase de sistemas.

1.2. Objetivos

El trabajo consta de tres objetivos principales:

1. Realizar un estado del arte de los sistemas de trazabilidad y transparencia de la cadena de suministro en el sector alimentario.

Conocer la evolución histórica, las mejoras y el impacto de las mismas, así como la situación actual de los sistemas de trazabilidad y transparencia de la cadena de suministro en uno de los sectores en los que más importancia cobra.

2. Describir de forma teórica, un modelo de gestión de supply chain basado en la tecnología blockchain

Conocer las aplicaciones de blockchain en supply chain y las aplicaciones de esta tecnología en el sector alimentario.

3. Proponer un caso práctico de aplicación de un sistema de gestión basado en blockchain y unas recomendaciones para la industria

Realizar en un contexto práctico, una propuesta de funcionamiento de un sistema de gestión de la cadena de suministro basado en blockchain y unas recomendaciones para la industria.

1.3. Metodología y recursos empleados

En este punto se expone la metodología seguida que ha dado lugar al presente trabajo. Al tratarse de un proyecto con una propuesta teórica, no se sigue ninguna metodología definida en concreto, sino que se aborda de la manera descrita a continuación.

Tras la aceptación de la propuesta del trabajo, se realizó una primera aproximación a la tecnología blockchain y al mundo de la cadena de suministro con el fin de poder plantear el contenido necesario y razonable para el trabajo.

Tras la aprobación del contenido, se dividió el trabajo en dos etapas:

1. *Investigación*: Etapa inicial, informativa en la que realizar un estado actual (AS-IS) del sector de la cadena de suministro y llegar a comprender la tecnología blockchain. Para esta etapa se utilizaron los siguientes recursos:

    - Acceso a base de datos científicas disponibles desde la universidad, donde se pueden consultar diversos *papers* de investigación sobre la historia, evolución y tendencias de la cadena de suministro en el sector de interés

    - Contacto (conferencias o contacto directo) con asociaciones y profesionales del sector, con el fin de conocer qué grupos de trabajo existen en la industria sobre la optimización de cadena de suministro, si se baraja la implementación de blockchain a gran escala, etc.

    - Consulta de diversas fuentes y referencias (libros, páginas web, contacto con profesionales) con la finalidad de entender con precisión

la tecnología blockchain, las posibilidades que tiene y sus posibles aplicaciones en el campo de interés.

2. *Aplicación*: Etapa de definición del caso práctico de aplicación y de propuesta de estándar. De nuevo, se contactaron personas cercanas al sector de interés, en este caso el sector porcino y se realizó una propuesta de implantación del sistema de gestión basado en blockchain en dicho sector (TO-BE)

1.4. Estructura del documento

El presente trabajo comienza con una contextualización del problema y el establecimiento de los objetivos perseguidos.

En el capítulo dos se aborda un repaso al sector de la cadena de suministro, desde la definición, la evolución hasta los sistemas actuales utilizados en la industria.

El capítulo tres se dedica a la descripción de la tecnología blockchain, desde su nacimiento hasta sus usos más innovadores, pasando por su funcionamiento técnico básico.

El capítulo cuatro pretende ser una agregación de los dos anteriores y elaborar sobre la implementación de sistemas blockchain en supply chain. Este capítulo es una introducción al capítulo siguiente, el cinco, donde se detalla un caso práctico de aplicación en el sector porcino.

El capítulo seis se dedica a la planificación del proyecto, incluyendo la estructura de descomposición y el diagrama de Gantt, que sitúa temporalmente el proyecto.

El documento finaliza además de las referencias con un capítulo dedicado a las conclusiones, los impactos (económicos, sociales y medioambientales) generados y los futuros desarrollos que podrían realizarse tomando como base este proyecto.

2. Supply chain

2.1. Introducción

¿Cómo llega al supermercado un *brik* de leche fresca? ¿Cómo es posible que haya disponibilidad de todo tipo de verduras y frutas a lo largo de todo el año? Todos los productos que consumimos, desde comida hasta ropa pasan por un largo proceso desde la granja o la fábrica donde se producen hasta que se encuentran a disposición del cliente. Este proceso por el que circulan los productos entre el productor y el consumidor final es lo que se conoce como cadena de suministro (término que deriva del inglés *supply chain* , y que, en adelante, se utilizan indiferentemente).

2.1.1. ¿Qué es supply chain?

Supply chain es un concepto que nace en la década de 1980, y que desde entonces, no ha parado de evolucionar. Tal ha sido esta evolución que la propia definición de supply chain puede resultar sombría y confundirse con logística. Según el Consejo de Profesionales de Gestión de la Cadena de Suministro (CSMP por sus siglas en inglés), supply chain se define como:

"El intercambio de información y material en los procesos logísticos desde la adquisición de las materias primas hasta la entrega de productos al usuario final. Todos los vendedores, proveedores de servicios y clientes son nexos en la supply chain" [1]

Así pues, la cadena de suministro cumple una función de integración, que liga todos los eslabones necesarios para que el consumidor final vea satisfechas sus necesidades. Una cadena de suministro incluye todas las etapas por las que pasa un producto, desde el proveedor inicial hasta el consumidor final.

En la Figura 1 puede apreciarse una red de cadenas de suministro, donde cada producto individual fluirá a través de diferentes partícipes conformando su propia cadena de suministro.

Es importante señalar que tradicionalmente se ha dividido la cadena de suministro en distintos ciclos correspondientes a cada una de las etapas que la componen. Las razones para ello son múltiples, entre las que destacan:

[1] Traducción libre de la definición extraída del glosario de términos proporcionado por el CSMP.

- Independencia de cada etapa para evitar la transmisión de problemas de unas a otras

- Definición de los dueños de cada proceso y sus responsabilidades, intentando evitar duplicidades

Sin embargo, esta aproximación de división de la cadena de suministro tiene contrapartidas, elevando los costes totales de la misma debido a la cantidad de inventario necesario para satisfacer un determinado nivel de servicio. [VORS09]

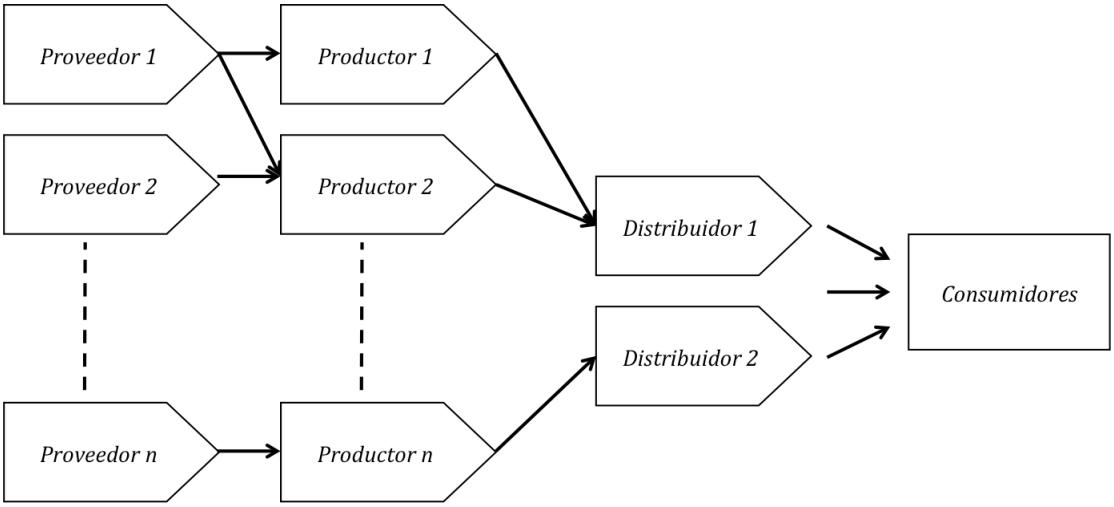


Figura 1. Cadena de suministro

La función de la cadena de suministro no podría llevarse a cabo sin la aplicación de unas técnicas de gestión adecuadas, pues toda cadena de suministro es dinámica e implica un flujo constante de información, datos y productos. Nace así la gestión de la cadena de suministro o *supply chain management* (SCM), como el conjunto de técnicas, herramientas y procesos que permiten administrar de forma adecuada la supply chain de una empresa. La definición proporcionada por el CSMP es la siguiente:

"La gestión de la cadena de suministro abarca la planificación y administración de todas las actividades involucradas en la obtención de materias primas, conversión y todas las actividades logísticas. También incluye la coordinación y colaboración con terceros, que pueden ser proveedores, intermediarios y clientes. En esencia, la gestión de la cadena de suministro integra la gestión de la oferta y la demanda interna y externa de la compañía"[2]

[2] Traducción libre de la definición extraída del glosario de términos proporcionado por el CSMP

Desde su implementación en las empresas, la gestión de la cadena de suministro ha visto como su importancia aumentaba, siendo actualmente uno de los principales *drivers* del éxito de una empresa. Este aumento de la importancia ha evolucionado de la mano de:

- Desarrollo de técnicas de gestión en todos los ámbitos que engloba la cadena de suministro (e.g. lean y six sigma, just in time, métodos heurísticos, etc.)

- Impacto económico, social y medioambiental creciente de la cadena de suministro en un mundo cada vez más globalizado

La gestión de la cadena de suministro ha evolucionado mucho durante los últimos años, sin perder el foco en el concepto de valor. Se entiende por valor la cantidad que un consumidor está dispuesto a pagar por un producto, así, una actividad será considerada como aportadora de valor cuando el incremento de lo que está dispuesto a pagar un consumidor tras dicha actividad sea mayor que el coste de llevarla a cabo.

Durante los últimos años, este concepto de valor se ha expandido, pasando de una perspectiva totalmente económica a una perspectiva más amplia, evaluando también las consecuencias sociales y medioambientales de las actividades.

Tal y como se ha comentado anteriormente, la cadena de suministro o su gestión pueden confundirse con logística, esta confusión resulta muy común debido a la evolución sufrida por el sector. Sin embargo, en la actualidad, logística, según el *Council of Logistics Management* (CLM) se define como:

"Logística es la parte de la cadena de suministro que planea, implementa y controla que el flujo y almacenaje de bienes, servicios o información desde el punto de origen hasta el consumidor sea eficaz y eficiente."[3]

Aunque a nivel general, en todo tipo de empresas e industrias la importancia de la cadena de suministro es, como se ha comentado, creciente, existen algunos sectores en los que su importancia y complejidad es especialmente relevante. Un claro ejemplo de este tipo de sectores es el sector agroalimentario, que cuenta con unas características y unos retos muy interesantes para la gestión de la cadena de suministro. Esto hace que sea el centro del presente trabajo.

[3] Traducción libre de la definición proporcionada por el CLM

La principal característica que hace que la cadena de suministro en la industria alimentaria tenga especial relevancia es la caducidad de los productos. Dentro de esta industria se pueden distinguir principalmente dos tipos de cadenas de suministro:

a. Cadenas de suministro para productos frescos
b. Cadenas de suministro para productos procesados

En ambas cadenas, la materia prima es de gran importancia, sin embargo, existe una gran diferencia entre ambas. La cadena de productos procesados añade valor a una materia prima mediante algún cambio significativo (e.g. nueces peladas) mientras que la de productos frescos añade valor por el hecho de no implementar cambios en el producto.

Así, a pesar de algunas diferencias, en los dos tipos de cadenas de suministro, todos los participantes en el proceso (agricultores, intermediarios, fabricas de procesado, comerciantes, etc.) comprenden que la calidad de la materia prima es esencial, y que una brecha en la cadena podría ocasionar la pérdida del producto (e.g. rotura de la cadena de frio en un producto congelado). Otro aspecto significativo que se debe tener en cuenta es la coordinación entre todas las partes, pues no puede existir un stock de producto durante mucho tiempo en ninguna etapa del proceso.

Además, dentro de la industria alimentaria, existen productos que por su procedencia, exclusividad o alguna otra característica propia diferencial son objeto de fraude. Estos productos, además de contar con las características propias de un producto alimentario, suponen un reto extra, pues la integración y confianza entre los partícipes de la cadena debe ser máxima para asegurar que el producto original llega al consumidor y evitar falsificaciones o fraudes que dañen el sector. Ejemplo de estos productos podrían ser el atún rojo, el caviar, las angulas o el jamón ibérico. Este último se ha seleccionado como caso práctico de aplicación en el presente trabajo.

Finalmente, es importante señalar los aspectos críticos que a menudo definen el éxito en la gestión de la cadena de suministro. La selección de los partícipes dentro de la cadena, que no dejan de ser socios comerciales de la empresa es de vital importancia, por ello, la recomendación de diferentes organismos, GS1 entre otros, es elegir estos socios teniendo en cuenta las metas estratégicas y la compatibilidad cultural. Además, la implementación exitosa de un sistema de gestión de cadena de suministro se basa principalmente en confianza y tecnología.

2.2. Sistemas de identificación

Una vez se ha introducido el sector en el que se centra el trabajo se procede en este apartado a describir brevemente las tecnologías implantadas en las cadenas de suministro que han posibilitado una mejora sustancial en la transparencia y la trazabilidad de las mismas.

2.2.1. Código de barras: El inicio de la revolución

El código de barras fue el primer sistema de gran implementación de identificación de productos a lo largo de la cadena de suministro. Aunque nació en la década de 1950, la adopción masiva no se hizo realidad hasta la década de 1980.

El código de barras esta formado por un conjunto de barras, espacios y números (Figura 2) que mediante su lectura, permiten identificar inequívocamente el producto al que ha sido previamente asignado. Mediante su lectura a lo largo de la cadena, permite realizar inventario de forma automatizada así como la consulta de características del producto.

Existen varios tipos, el más utilizado es el EAN-13 cuyos dígitos indican el tipo de producto, el código del productor, el código de producto y finalmente un dígito de control para verificar que la lectura del escáner está bien hecha. También son muy utilizados el EAN-128 o el EAN-8, teniendo todos ellos en común que siempre existe un dígito de control para chequear la integridad de los datos. [GS116].

Figura 2. Ejemplo de código de barras

El código de barras permite verificar que el producto ha llegado o salido de un eslabón de la cadena de suministro, siendo muy eficaz en el control de inventarios.

Sin embargo, presenta ciertas desventajas, [LING12] entre las cuales destacan:

- Es necesaria una colocación delante del lector, sin que pueda existir nada entre producto y lector

- Las etiquetas pueden deteriorarse dificultando o impidiendo la identificación

- Pueden existir errores de asignación de códigos de barras a productos, haciendo que la identificación sea errónea

- Permite la identificación de productos en entrada/salida de una etapa, pero su sistema de gestión de la información no permite trazabilidad o si la permite es de manera muy engorrosa

Una evolución del código de barras es el código QR (Figura 3), basado en una matriz bidimensional y de funcionamiento similar al anterior. Sin embargo, no ha conseguido una adopción significativa en el mercado.

Figura 3. Código QR

2.2.2. Tecnología RFID

Radio Frequency Identifcation (Identificación por radiofrecuencia) es un sistema de identificación capaz de transmitir información sin contacto entre un chip y un escáner.

Figura 4. Ejemplo de etiqueta RFID

El RFID funciona sin fuente de alimentación externa, siendo capaz de alimentarse de la energía de las ondas recibidas del escáner para luego enviar la información que contiene al mismo. [UPS05].

Durante los últimos años ha sido el mayor avance en cuanto a sistemas de identificación en la cadena de suministro, pues entre otras ventajas; permite almacenar gran cantidad de datos, permite la lectura automática y sin contacto, al transmitirse la información por ondas, no es necesaria una visión directa entre escáner y RFID y además es complicado de dañar.

La gran contrapartida del RFID ha sido hasta ahora su elevado precio. No solo de los sistemas a instalar (lectores, servidores, etc.) sino también de las etiquetas en si mismas. Sin embargo, el desarrollo de la tecnología y una adopción cada vez mayor (pasando de 3.000 millones de etiquetas vendidas en 2014 a 8.000 millones en 2017), ha hecho que el coste disminuya considerablemente. Actualmente, se pueden encontrar etiquetas RFID desde 10 centavos de dólar aproximadamente. [UPS05]

Aplicando reconocimiento RFID y con un sistema de gestión de datos en tiempo real, el uso de RFID permite conocer los movimientos de los productos etiquetados [LING12]. Así, la implantación a gran escala de RFID esta permitiendo mejorar la trazabilidad de la cadena de suministro, reducir problemas con stocks, aumentando la precisión de la gestión de stock e impactando positivamente en las ventas como resultado de ello.

La contrapartida actual de la tecnología RFID es la falta de homogeneidad, de una estandarización debido a la gran cantidad de información que es posible almacenar en cada etiqueta y los distintos datos que son útiles para las cadenas de suministro de cada sector. Sin embargo, y aunque no ha tenido el impacto deseado, desde el *MIT Auto-ID Center,* se ha desarrollado y propuesto una iniciativa de estandarización de las infraestructuras RFID.

2.3. Trazabilidad y transparencia

La trazabilidad de la cadena de suministro se ha tratado históricamente como un complemento a esta. Sin embargo y aunque la aproximación tradicional implica el funcionamiento de cada eslabón de la cadena de forma independiente, el planteamiento de un sistema de trazabilidad a lo largo de la cadena implica un replanteamiento de la cadena y su funcionamiento.

Debido a la novedad del concepto de trazabilidad en su aplicación a la cadena de suministro, y a su evolución en diferentes sectores, la definición conceptual de trazabilidad no se encuentra consensuada. La definición más generalista se encuentra en la norma ISO 8000 como: "*Capacidad para rastrear historia, aplicación o*

ubicación de una entidad mediante indicaciones registradas", en el resto de la literatura las definiciones se vuelven más amplias.

En cualquier caso, sea cual sea la definición tomada, se refiere a la capacidad de garantizar que los productos que se encuentran en movimiento en la cadena o que han llegado al final pueden ser seguidos (*tracking*) y son rastreables (*tracing*). *Tracking* es la capacidad de seguir un producto aguas abajo en la cadena de suministro, mientras que *tracing* es la capacidad de determinar el origen y características de un producto que ha llegado al final de la cadena. En el presente documento se trabaja sobre la definición proporcionada por AECOC[4] bajo los estándares de GS1:

"Se entiende trazabilidad como el conjunto de aquellos procedimientos preestablecidos y autosuficientes que permiten conocer el histórico, la ubicación y la trayectoria de un producto o lote de productos a lo largo de la cadena de suministros en un momento dado, a través de unas herramientas determinadas"

El concepto de trazabilidad ha adquirido relevancia en los últimos años debido principalmente a los escándalos alimentarios. La trazabilidad se ha reconocido como una herramienta para garantizar la seguridad alimentaria, centrándose en la prevención de riesgos y mitigando los impactos y la magnitud en caso de intoxicación.

La implantación de un sistema de trazabilidad en un producto supone un impacto en la cadena de valor de la organización desde distintos puntos de vista. Para el consumidor implica una mayor confianza y percepción de calidad, mientras que para el productor supone la posibilidad de garantizar su producto y el cumplimiento con las regulaciones existentes.

La implantación de un sistema de trazabilidad no depende solo de una empresa. Dentro de un sistema de trazabilidad son muchos los partícipes, pues todos los implicados en la cadena de suministro deben participar, y la falta de integración de una empresa participante en un eslabón supone la ineficiencia y el funcionamiento incorrecto de la totalidad del sistema.

Una de las claves en todo sistema de trazabilidad es la identificación de cada unidad de producto dentro de la cadena. En el apartado 2.2 se han descrito dos de las soluciones más utilizadas a día de hoy; el código de barras y los sistemas RFID. La

[4] Asociación Española de Codificación Comercial

evolución en este tipo de tecnología ha conseguido que se abran nuevas puertas para fortalecer y mejorar la trazabilidad de los productos.

A lo largo de la cadena de suministro, cada vez que un proceso relevante para la trazabilidad tiene lugar, se generan una serie de datos que deben ser almacenados. Estos datos, recogidos de forma diversa (normalmente en forma de códigos), deben contemplar según GS1, cinco dimensiones conocidas como las 5 W [GS116]:

- *Who* (quién): Distingue unívocamente a los partícipes involucrados en el proceso

- *What* (qué)*:* Define el producto que esta siendo trazado

- *Where* (dónde): Define el lugar en el que un evento ha tenido lugar (e.g. almacén, fábrica, etc.)

- *When* (cuándo): Define la fecha, hora en la que tuvo lugar el evento

- *Why* (por qué): Responde al porqué se realizo un proceso a un producto en el lugar y hora determinados

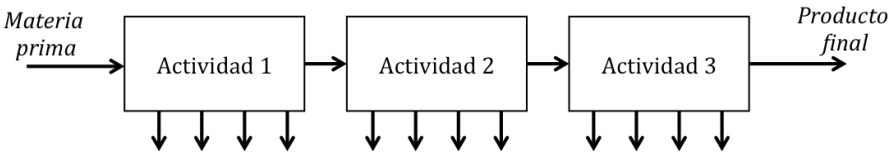
Teniendo esto en cuenta, en la Figura 5 se puede observar como cada partícipe de la cadena genera y gestiona sus propios datos, por lo que para un correcto funcionamiento del sistema de trazabilidad que se alimenta de dichos datos, es necesario que exista un modelo para compartir los datos a lo largo de la cadena.

Con el fin de intentar una estandarización, GS1 propone una serie de códigos para la gestión de estos datos a lo largo de la cadena de suministro. Estos códigos cubren la base necesaria en cuanto a identificaciones en la cadena de suministro, dejando otros posibles datos a incluir a decisión de la organización. Los códigos principales que se incluyen son [GS116]:

- GLN: *Global location number*
- GTIN: *Global trade item number*
- SSCC: *Serial shipping container code*
- GRAI: *Global returnable asset identifier*
- GIAI*: Global individual asset identifier*
- GSRN: *Global service relocation number*

En la Figura 5 se incluye un resumen de estos códigos y su relación con los eventos o actividades sobre el producto. Como puede observarse, cada actividad que se realiza sobre el producto (evento) viene descrito por los datos correspondientes.

Los diferentes modelos actuales bajo los cuales se comparten estos datos y el funcionamiento de una cadena alimentaria actual haciendo uso de los estándares aquí definidos puede encontrarse en el apartado 4.2



	Evento 1	*Evento 2*	*Evento 3*
Quién	GLN	GLN	GLN
Qué	GTIN+LOT	GTIN+LOT	SSCC
Cuándo	Fecha y hora	Fecha y hora	Fecha y hora
Dónde	GLN	GLN	GLN
Porqué	Proceso evento 1	Proceso evento 2	Proceso evento 3

Figura 5. Códigos de gestión de datos de trazabilidad. Detalle para un participante de la cadena con tres actividades sobre el producto

Además de los datos indicados, un sistema de trazabilidad será juzgado según las siguientes características [BOSO13]:

- *Amplitud*: Cantidad de información relacionada con un producto
- *Profundidad*: Información relevante para que pase entre eslabones
- *Precisión*: Grado de seguridad con el que se permite identificar un producto
- *Acceso*: Velocidad con la que la información se comunica en la cadena

Otros autores consideran otras características, sin embargo, esas son las más generales y aplicables al sector alimentario, foco de este proyecto.

En cuanto a la implantación de un sistema de trazabilidad es muy importante el aspecto económico. Los beneficios tal y como se ha comentado anteriormente se distribuyen e impactan a toda la cadena, por lo que los costes también deben estar distribuido a lo largo de toda la cadena.

Además de la trazabilidad, la transparencia de una cadena de suministro es una característica a definir por la o las empresas interesadas. La transparencia de una

cadena de suministro viene determinada por la cantidad de información sobre la misma que está disponible para el consumidor y los partícipes.

La transparencia de una cadena de suministro puede ser considerada como un catalizador para la adopción de practicas responsables a lo largo de la misma y esto puede llegar a tener influencia en las decisiones de compra de los consumidores. En general, se puede decir que una cadena de suministro es:

- *Opaca:* no hay ningún tipo de transmisión de información entre los participantes y no se encuentra disponible para el cliente final

- *Translúcida:* Solo se comparte cierta información entre los partícipes en la cadena. Con el cliente final no suele compartirse.

- *Transparente:* Toda la información es compartida con todos los participantes, incluyendo el cliente final.

2.4. Gestión de datos en la cadena de suministro

Una vez que se ha conseguido implantar un sistema de trazabilidad y se verifica que se generan de forma correcta todos los datos necesarios y deseados, se necesita un sistema que sea eficaz gestionando dichos datos.

Con los productos ya identificados de la manera que se ha descrito a lo largo de apartados anteriores, es necesario definir el modo en que esa información es asociada a cada producto y qué información es transmitida de un eslabón de la cadena a otro. Todavía existen en la actualidad, sobretodo en los eslabones de producción registros en papel, que no permiten llevar a cabo una trazabilidad completa a lo largo de toda la cadena de suministro al no conseguir la integración de los datos en el sistema. Así, la automatización y el registro electrónico de los datos es la única manera de asegurar la completa trazabilidad, pues esta viene dada por la fiabilidad de los datos recogidos y registrados en el sistema, siendo el sistema RFID el más recomendado en la literatura consultada.

Para el caso alimentario, es importante distinguir entre identificación primaria, que la realiza el primer eslabón de la cadena (normalmente el ganadero) y se refiere a la identificación del animal. Identificación secundaria es la realizada al llegar el producto a un eslabón (normalmente matadero), de forma que queda registrado y

preparado para añadir la información necesaria de las actividades realizadas en ese eslabón.

2.5. Trazabilidad en el sector alimentario

La trazabilidad en el sector alimentario es esencial desde el punto de vista de la seguridad y la salud pública. Es por ello que existen mecanismos de actuación para determinadas situaciones que se describen a continuación.

2.5.1. Gestión de intoxicaciones alimenticias

La posibilidad de intoxicaciones alimenticias disparó la necesidad y el desarrollo de la trazabilidad en la cadena de suministro alimentaria. En el caso de que exista una intoxicación debido a una contaminación o un lote de productos deba ser retirado a petición del productor o del regulador, el sistema de trazabilidad debe proveer con la informaciónnecesaria para hacerlo de la forma más rápida y eficiente posible.

Las nuevas regulaciones, cada vez más estrictas en materia alimenticia, la evolución de las tecnologías utilizadas para el análisis de los productos y el aumento de las importaciones de países en vías de desarrollo, con regulaciones más laxas, hacen que cada año sean más numerosos los casos en los que hay que retirar lotes de productos del mercado. Las causas para ello son múltiples, desde etiquetado incorrecto hasta la contaminación química o biológica.

En caso de necesidad de sacar un lote de productos del mercado, es de vital importancia para la correcta identificación del mismo la existencia de un sistema de trazabilidad automatizado, con datos compartidos entre los participantes de la cadena.
La retirada de un lote de productos tiene consecuencias negativas para la empresa tanto en imagen de marca como económicas. La retirada de un producto se explica con detalle en el apartado 4.2 de este documento, consiste en identificar aguas arriba el punto de contaminación o causante de la deficiencia para luego identificar aguas abajo el destino de todos los lotes potencialmente defectuosos.

Esto tiene un coste que se conoce como coste de retirada de producto (RC o *Recall Cost),* que depende de (i) el tamaño de los lotes a retirar, (ii) el mix de los lotes si estos no son el producto final y (iii) del nivel de dispersión de los lotes. Este coste se plantea como [RESE10]:

$$RC = \alpha \Pr Qr$$

Donde α es un factor de seguridad mayor que uno para incluir los costes asociados a la logística, perdida de ventas, etc. Pr es el valor de mercado del producto y Qr es la cantidad de producto a retirar. Cabe mencionar que existen otros modelos de costes, pero escapan al interés del proyecto.

2.5.2. Calidad e identidad

El desarrollo de la tecnología RFID, que es capaz de obtener datos relativos al producto (e.g. temperatura, humedad, etc.) mediante sensores específicos supone que el sistema de trazabilidad puede recoger de forma automatizada todo tipo de datos que ayuden a definir el estado actual y pasado del producto. Esto abre la puerta a la posibilidad de realizar planificaciones dinámicas en las fechas de caducidad de los productos.

La calidad de los productos no viene determinada por el sistema de trazabilidad en sí mismo, pero si que este sistema es capaz de recopilar datos de determinadas características que sí tienen influencia en la calidad (procesos, temperaturas, tiempo de vida, etc.).

Otra de las grandes ventajas de un sistema de trazabilidad completo es la preservación de identidad de un producto. Este concepto se aplica haciendo referencia a los atributos que no mejoran la calidad del producto pero que sí suponen un valor añadido para el consumidor (e.g. país de origen, orgánico, comercio justo, etc.). En estos caso, el consumidor no puede verificar estos atributos, por lo que la trazabilidad de estos productos debe ser completa, transparente y confiable a lo largo de toda la cadena de suministro, con certificaciones de los atributos deseados.

2.5.3. Prevención de fraude y falsificaciones

En el sector alimentario existen, como se ha comentado anteriormente, productos que son objeto de falsificaciones y fraudes. Son productos de alto coste y con una gran percepción de exclusividad (e.g. caviar, vino, jamón, etc.). Los fraudes y las falsificaciones tienen como resultado un gran daño económico por la imagen del producto y la marca así como por la pérdida de confianza del consumidor.

Para poder asegurar la originalidad de estos productos, el sistema de suministro debe ser capaz de conocer los procesos, localizaciones y condiciones de operación de los productos así como asegurar que la identificación de cada producto individual es única y veraz, evitando que se pueda mezclar o confundir con otros productos.

Existen tecnologías anti-fraude visibles e invisibles, pero la más importante es de nuevo, la tecnología RFID. Esta tecnología permite la automatización de las identificaciones y su verificación en un servidor central.
El sistema de trazabilidad podría ser utilizado para crear un "pedigree de producto", que podría ser implementado manteniendo la integridad de la cadena de suministro de los productos deseados [CHEU01].

Además, cabe destacar que sea cual sea el sistema anti-fraude utilizado puede ser compartido por socios comerciales del sector e incluso competidores para ayudar a limitar el impacto en el producto distribuido.

En la Figura 6 se ilustra el proceso seguido en general para la autentificación de producto y la verificación del mismo.

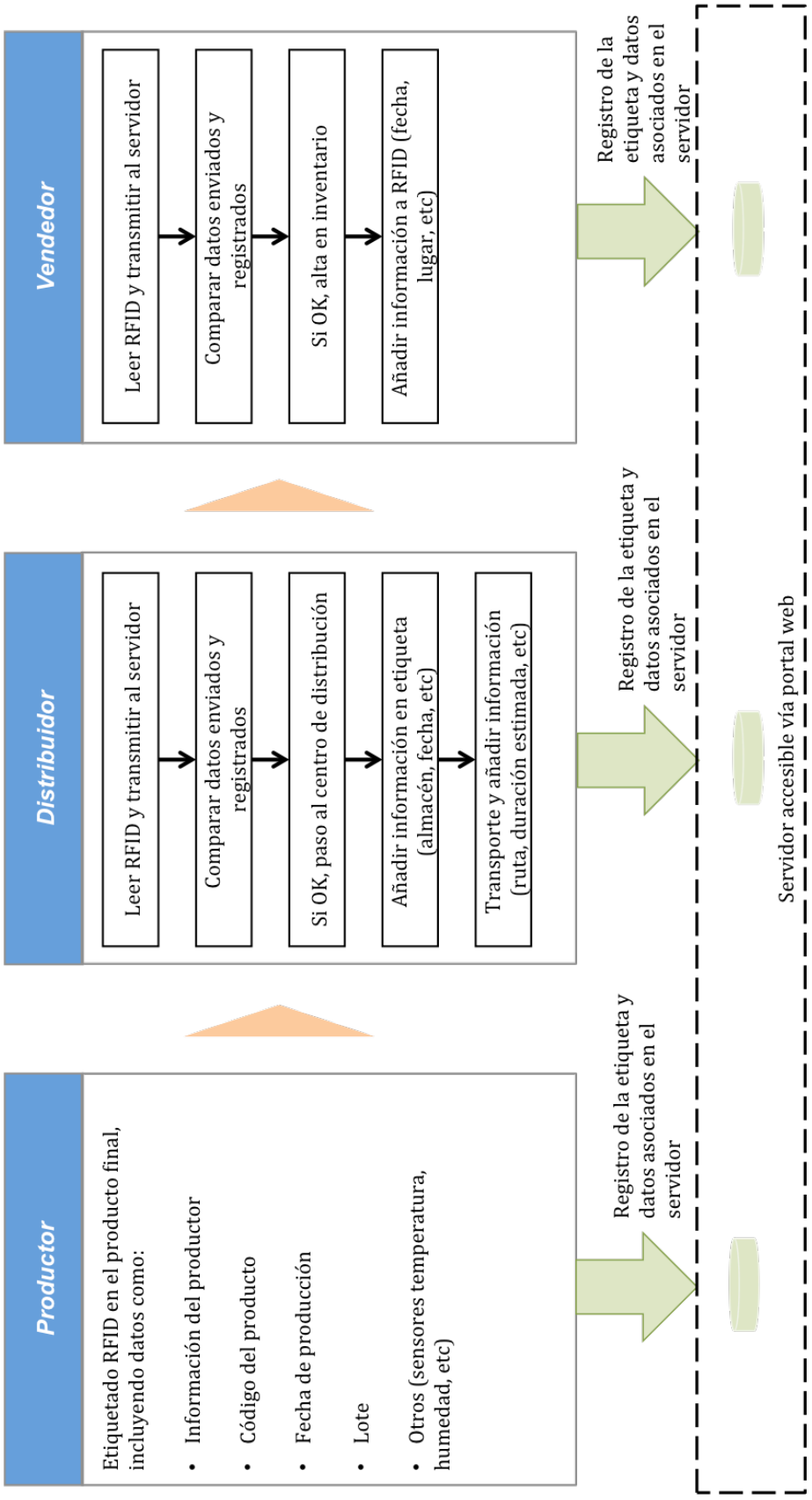


Figura 6. Funcionamiento esquemático de una cadena de suministro anti-fraude con RFID

3. Blockchain

En este capítulo se va a realizar una introducción teórica a la tecnología blockchain, aportando definiciones, el funcionamiento y aplicaciones. El objetivo del apartado no es el de ser un estado del arte exhaustivo, sino el de introducir los conceptos básicos de la tecnología que serán posteriormente aplicados en la gestión de sistemas de supply chain.

Cabe destacar que a lo largo del capítulo, se explica el funcionamiento de blockchain haciendo referencia a bitcoin y basando muchas explicaciones en él. Esto sucede porque bitcoin es la primera gran aplicación práctica de blockchain y permite la visualización y explicación de conceptos de forma clara.

3.1. ¿Qué es blockchain?

El 31 de octubre de 2008, en la web criptográfica *metzdowd.com* un usuario bajo el pseudónimo de Satoshi Nakamoto pública un *paper* llamado *Bitcoin P2P e-cash paper*. En él describe un sistema de pagos protegido mediante criptografía asimétrica y validado mediante consenso en una base de datos descentralizada, eliminando la necesidad de incluir un tercero de confianza que ratifique la transacción y la propiedad. Era el nacimiento de bitcoin, la aplicación más conocida de la tecnología blockchain.

Para poder comprender qué es blockchain, el potencial que tiene y lo que se esconde tras esta tecnología, es necesario analizar la evolución de internet y las necesidades existentes.

El internet que se utiliza actualmente irrumpió para facilitar el intercambio de información. Hoy en día, la información y las comunicaciones son inentendibles sin hacer referencia a internet. Se podría decir que el internet mundialmente conocido puede denominarse internet de la información [PREU17]. El potencial que esta tecnología tenía en 1995 se ha hecho hoy realidad, con la practica totalidad de industrias revolucionadas por modelos de negocio disruptivos de empresas surgidas de la nada en pocos años gracias a las posibilidades ofrecidas por internet (Facebook, Amazon, Google, etc.)

El siguiente paso en esta revolución, sería el internet del valor. Esta red, posible gracias a la tecnología blockchain sería una suerte de red en la que se pueda compartir valor (certificados, registros, archivos, etc.) de forma digital, descentralizada y segura,

eliminando la necesidad de una tercera entidad de confianza que haga posible la transacción.

Así pues, blockchain no es más que una base de datos descentralizada (que registra transacciones que pueden ser desde movimientos de dinero a la compra de bienes), protegida mediante criptografía y organizada mediante bloques de transacciones relacionados entre si matemáticamente. Pero lo que hace única a esta tecnología es la imposibilidad de alteración. Gracias a este factor, esta tecnología permite a partes que no confían entre ellas realizar transacciones de diversa índole sin necesidad de que exista un tercer participante que aporte la confianza, es la propia tecnología la que aporta dicha confianza entre participantes.

3.2. ¿Cómo funciona Blockchain?

En este apartado se va a introducir de forma general y sencilla el funcionamiento de la tecnología blockchain. Se van a utilizar conceptos que se encuentran explicados más detalladamente en los apartados 3.3 y siguientes.

Para funcionar, una cadena de bloques necesita recolectar datos, ordenarlos y luego archivarlos (cifrados mediante criptografía) de forma sucesiva en bloques. Esta es la base de esta tecnología, simplemente almacenar transacciones de forma segura y descentralizada. En la Figura 7 [SACH18] se muestran de forma esquemática las etapas necesarias para que el proceso de registro sea exitoso.

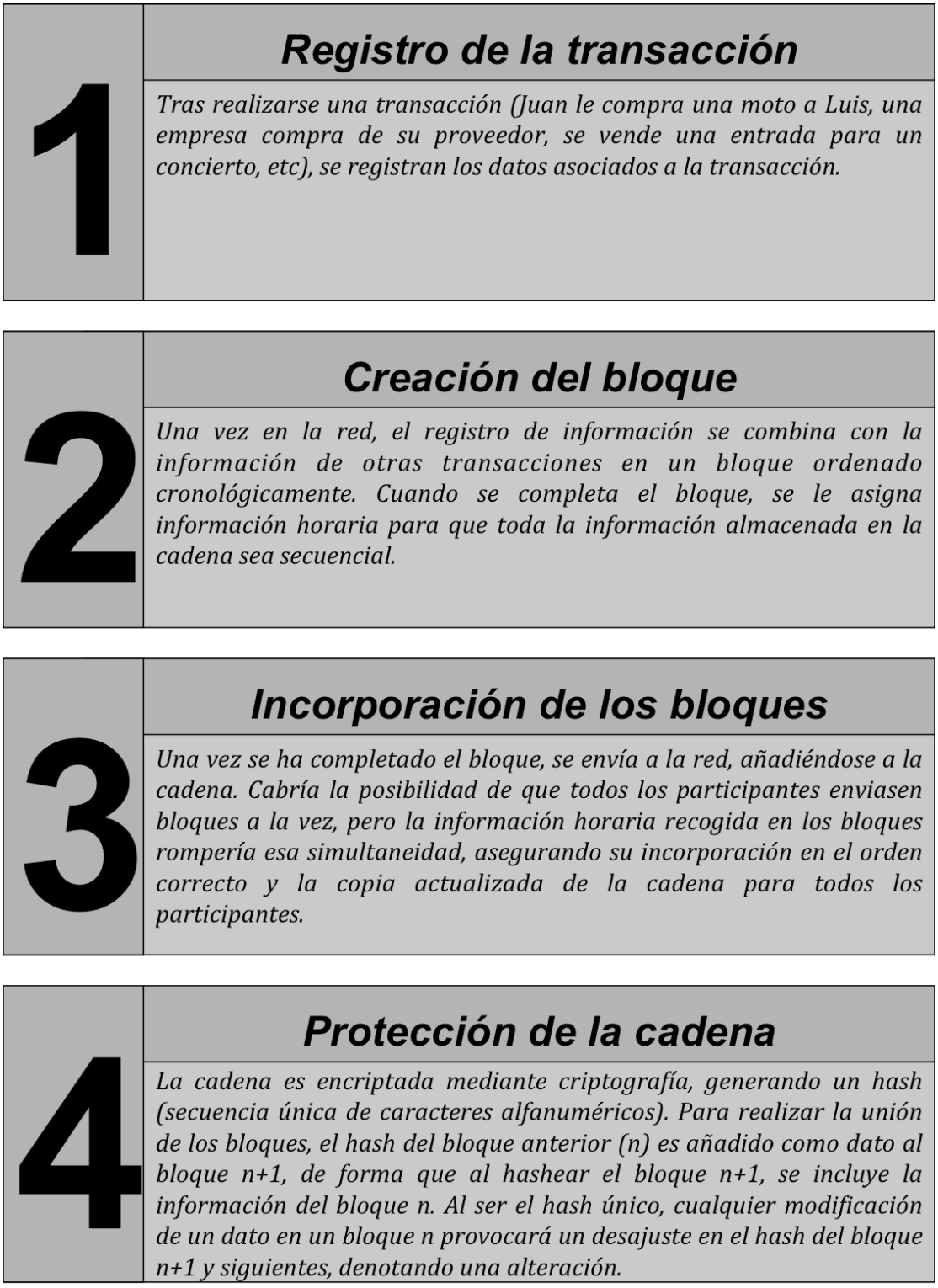


Figura 7. Explicación esquemática del funcionamiento de blockchain

Siguiendo este proceso, y como cada participante (nodo) tiene un duplicado actualizado de la cadena, se puede detectar cualquier intento de modificación y la cadena pasará a ser de confianza cuando todos los hashes presentes en ella se encuentren ajustados.

3.3. Aspectos técnicos básicos de blockchain

3.3.1. Conceptos y definiciones

Técnicamente, la tecnología blockchain se construye a través de una red global de ordenadores que gestionan una base de datos. Para ser esto posible, hace falta definir una serie de elementos básicos que componen dicha tecnología:

Nodos: Son los "puntos de unión" de la red. Son los ordenadores conectados a la cadena de bloques, pueden ser completamente distintos entre sí, pero deben poseer el mismo protocolo de comunicación.

Protocolo estándar: Software informático que hace posible la comunicación entre los distintos nodos de la red. Es simplemente un estándar común para usar entre todos los ordenadores que integran la red.

Red P2P (peer to peer): red de nodos que actúan como iguales entre sí, no hay clientes ni servidores, si no que los integrantes de la red actúan como servidores y clientes, sin jerarquías. El ejemplo más conocido es la red de descargas BitTorrent.

Sistema descentralizado: No existe jerarquía entre los nodos, los ordenadores conectados a la red actúan como iguales (salvo en sistemas descentralizados privados en los que pueden existir excepciones). Es la contraposición a un sistema centralizado, donde una entidad centraliza y controla al resto de participantes de la red.

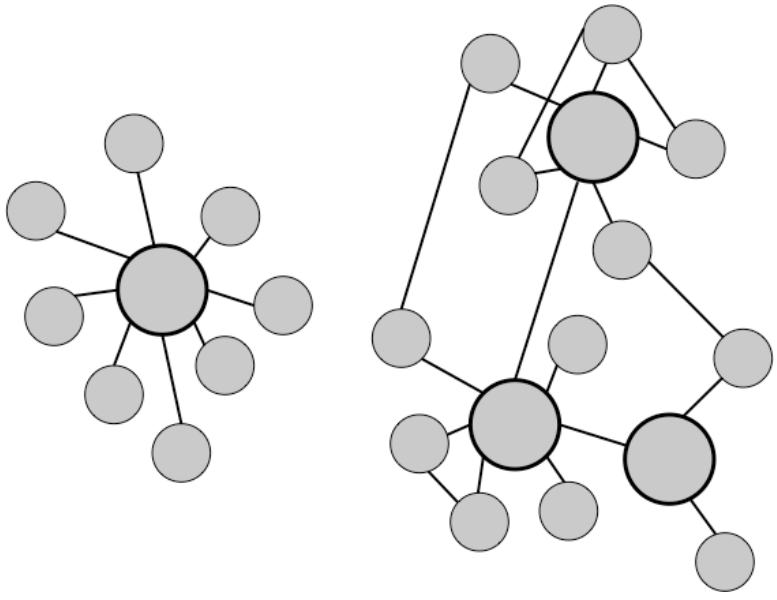


Figura 8. Sistema centralizado (izq.) y descentralizado (drcha.)

Criptografía: procedimiento mediante el cual un mensaje se cifra utilizando una clave, sin atender a su estructura, por lo que sea incomprensible para toda persona que no tenga la clave del algoritmo utilizado para realizar el cifrado. En blockchain se utiliza para evita la manipulación y garantizar la inalterabilidad, evitando introducir información errónea en la cadena.

Bloque: Base de datos que agrupa la información de varias transacciones ordenadas cronológicamente. Los bloques se agrupan y se añaden a la blockchain o cadena de bloques.

Cadena de bloques (blockchain): es la base de datos propiamente dicha, basada en bloques que almacenan los registros de los usuarios siguiendo procedimientos para darles validez e incorporarlos a la cadena. Una vez incorporado un bloque, se inicia la emisión de otro, permaneciendo la información del bloque anterior almacenada y totalmente inalterable mediante criptografía.

Consenso: Sustentado por el protocolo común, verifica y confirma las transacciones que se han llevado a cabo, así como su irreversibilidad. Es el encargado de proporcionar a los usuarios una copia inalterable y actualizada de la cadena de bloques.

Una vez definidos los diferentes componentes de la blockchain, se puede realizar una clasificación entre blockchains públicas y privadas. La base tecnológica de ambas es idéntica, la diferenciación viene dada por el acceso a cada una [PREU17].

3.3.2. Blockchains públicas

Cualquier persona usuario o no, puede acceder y consultar las transacciones realizadas. Además, cualquier persona puede acceder, convertirse en usuario y ser partícipe de la red. Aunque los propietarios de las transacciones no pueden ser identificables, sus direcciones si que son trazables, por lo que excepto en el caso de que sean expresamente diseñadas para ser anónimas, las cadenas de bloques son pseudoanónimas.

Las primeras redes blockchain diseñadas eran públicas y cumplían con estas características.

En las blockchain públicas, puesto que cualquier usuario puede realizar registros en el libro mayor o ledger y estos registros una vez verificados son inalterables, se utilizan unidades de cuenta denominadas tokens.

Un token es una serie de dígitos que representan un registro dentro de la cadena de bloques. Una cadena alfanumérica (e.g. ny8QRR2SwDXotjQ0VG4b) que represente un registro dentro de la cadena de bloques pública es un token (Aunque token y hash sean cadenas alfanuméricas, no deben confundirse, pues uno representa un registro de datos (token) mientras que otro es la base de la encriptación que aporta la seguridad propia de la cadena de bloques (hash))

3.3.3. Blockchains privadas

Las blockchains privadas surgen a raíz de la imposibilidad de compartir por confidencialidad todos los registros de forma abierta. Por lo tanto, estas cadenas de bloques solo son accesibles a los usuarios de la cadena, que deben ser invitados a serlo. Además los usuarios podrán solo consultar la cadena o consultar y modificarla, según los intereses y diseño de cada cadena privada. La desventaja es que todos los nodos se conocen y tienden a ser menos numerosos que en una blockchain pública, por lo que la posibilidad de un ataque exitoso se multiplica. En cuanto al anonimato, en las blockchains privadas, se puede establecer el nivel de anonimato que la entidad responsable desee.

La que probablemente sea la mayor diferencia entre ellas es que la blockchain pública es descentralizada, no se controla a quien participa en la red y todos los nodos están al mismo nivel. Mientras que una blockchain privada es distribuida, pues es una base de datos repartida en diferentes nodos, pero estos nodos deben ser invitados para formar parte de la red y pueden tener distintos permisos dentro de la cadena.

3.3.4. Funcionamiento técnico de blockchain (basado en bitcoin)

Este apartado no pretende ser una guía exhaustiva del núcleo de la tecnología blockchain, busca simplemente aportar una idea básica del funcionamiento interno de la tecnología.

Para comprender adecuadamente la técnica detrás de la tecnología blockchain hace falta introducir una serie de conceptos básicos de criptografía. La criptografía se basa en la transformación de un mensaje legible a otro ilegible mediante una clave (cifrado). En el mundo blockchain se utilizan tres tipos principales de criptografía; criptografía simétrica, criptografía asimétrica y hashing.

3.3.4.1. Criptografía simétrica

La criptografía simétrica es considerada la primera forma criptográfica moderna. Se basa en la utilización de una clave, con la que el emisor cifra el mensaje y el receptor lo descifra. Por ello, cualquiera que conozca la clave puede descifrar el mensaje. El principal problema que presenta es por tanto la distribución de claves, pues ha de realizarse mediante un canal seguro, evitando que un tercero pueda interceptarla.

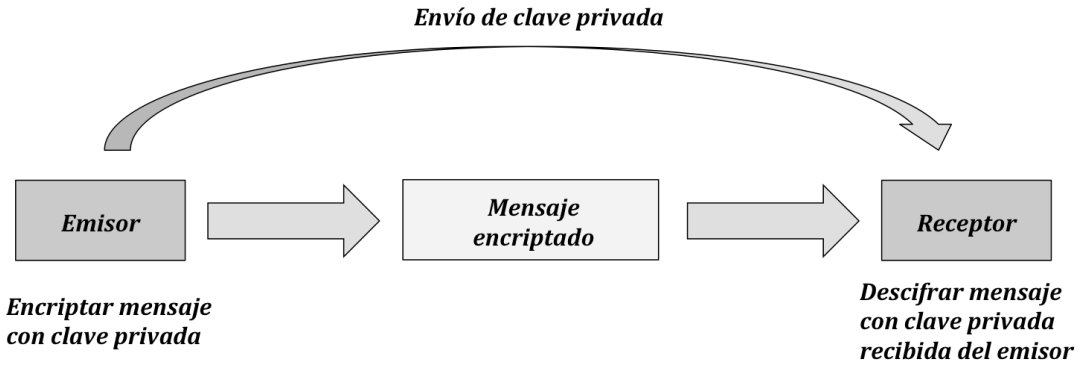


Figura 9. Diagrama de funcionamiento de la criptografía simétrica

Este tipo de criptografía se hizo famosa durante la segunda guerra mundial, ya que era el principio de funcionamiento de la máquina Enigma, con la que los alemanes cifraban sus comunicaciones.

En sus aplicaciones informáticas, la clave suele ser tan larga y complicada de recordar que se suele almacenar encriptada y protegida mediante una contraseña (que el usuario si pueda recordar). El tipo de claves utilizado es muy variado, pero el algoritmo más famoso es AES (Advanced Encryption Standard), que emplea 128 o incluso 256 bits (ordena aleatoriamente 256 posiciones de unos y ceros) esto implica tener 2^{128} o 2^{256} posibles combinaciones de ceros y unos (claves).

Para llegar a tener una idea de la seguridad de este sistema, solamente hace falta observar que para romper mediante fuerza bruta (probando claves) un archivo encriptado con AES-128 harían falta 10^{28} años utilizando el ordenador más potente que existe. O lo que es equivalente, si cada persona de los 7.000 millones de personas que habitan del planeta pudiese probar 10.000 millones de claves por segundo, y consideramos que se da con la clave correcta al haber probado el 50% de las combinaciones, harían falta 77.000.000.000.000.000.000.000.000 de años para descifrar la clave. [AURO12].

3.3.4.2. Criptografía asimétrica

La criptografía asimétrica puede considerarse una evolución de la criptografía simétrica, ya que surge para eliminar la debilidad de la criptografía simétrica de ponerse de acuerdo emisor y receptor en la clave a utilizar.

El principio de funcionamiento de la criptografía asimétrica es similar al de la simétrica, pero cuenta con pares de claves; una pública y otra privada. Esta pareja pertenece a una persona y está vinculada mediante una función unidireccional, de forma que conociendo la clave privada se puede averiguar la clave pública, pero no viceversa. Además, la clave privada suele ser una cadena de caracteres hexadecimal tan grande que es probabilísticamente imposible obtener otra igual.

El primer algoritmo utilizado para la generación de claves públicas y privadas es el conocido como RSA (por las siglas de sus creadores, Rivest, Shamir y Adleman) desarrollado en 1977. Se basa en la factorización de números enteros, mas concretamente en la multiplicación de dos números primos. En términos sencillos, la clave pública podría ser 120 y la clave privada, un numero primo tal que la multiplicación de sus cifras resultase en la clave pública; 835 por ejemplo. Conocida la clave pública (120) no se podría obtener la clave privada, puesto que los números 456, 645 o 2345 por ejemplo, arrojan el mismo resultado que 835. Teniendo en cuenta que los números utilizados son del orden de 10^{200}, se puede llegar a entender la enorme importancia que ha tenido este sistema.

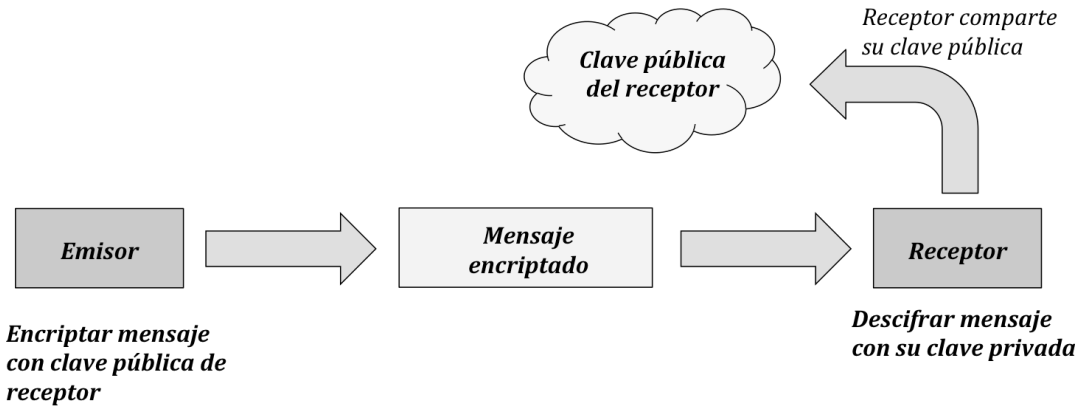


Figura 10. Diagrama de funcionamiento de la criptografía asimétrica

Tal y como se puede observar en la Figura 10, el principio de funcionamiento de la criptografía asimétrica para enviar un mensaje entre emisor y receptor es el siguiente: El receptor genera una pareja público-privada de claves, hace una pública y guarda la privada para sí mismo. El emisor que desea enviarle un mensaje, cifra el mensaje con

la clave pública del receptor y le manda el mensaje, que al recibirlo, el receptor descifra con su clave privada.

La gran aplicación de este tipo de criptografía fue la creación de firmas digitales, pues si el emisor firma digitalmente el mensaje con su clave privada, el receptor podría comprobar que el remitente es el correcto con la clave pública.

En el contexto bitcoin se utiliza un algoritmo denominado ECDSA (*Elliptic Curve Digital Secure Algorithm*) para el calculo de la clave pública.

3.3.4.3. Hashing

La criptografía basada en hash consiste en generar una secuencia de caracteres de longitud fija, una huella digital de un mensaje. El hash (la cadena de caracteres) se obtiene aplicando una función matemática sobre unos datos (mensaje), de esta forma, si se aplica la misma función a los mismos datos, se obtendrá siempre el mismo hash. Así, cualquier posible alteración que sufra el mensaje, hará que cambie el hash, siendo muy útil este sistema para garantizar la validez de los datos.

Por ejemplo, utilizando la herramienta online de creación de hash disponible en la web md5hashgenerator.com, que aplica la función hash conocida como md5 al mensaje deseado, se obtienen los resultados de la Tabla 1.

Mensaje	Web	Hash (MD5)
ingeniería	md5hashgenerator.com miraclesalad.com	01bf897db0326f3ad5bdeff53a54f2e6 01bf897db0326f3ad5bdeff53a54f2e6
Ingeniería Industrial	md5hashgenerator.com miraclesalad.com	89e187ea23afc6dc39ae9f3ef5b455e1 89e187ea23afc6dc39ae9f3ef5b455e1

Tabla 1. Detalle de hash con distintas herramientas

Asimismo, se ha realizado la misma operación pero utilizando la herramienta disponible en la pagina web miraclesalad.com. Tal y como puede observarse en la Tabla 1, el resultado no depende de la herramienta utilizada, si no del algoritmo (función) aplicada al mensaje, en este caso, md5.

Se puede comprobar, que modificando el mensaje, se modifica completamente el hash. Esto implica la identificación única y por tanto inequívoca de un dato. Esta característica no tiene el objetivo meramente criptográfico de cifrar un mensaje o actuar como clave para descifrarlo, si no que su aplicación práctica va más allá y permite comprobar que un archivo no ha sido alterado o corrompido. Una aplicación

sencilla, directa e importante de esto es la verificación de la legitimidad de código. Si un programador genera y pública un hash asociado al código de un software, el usuario al descargar el software puede generar de nuevo el hash y comprobar que coincide con el públicado con el programador. De no ser así, el software habría sufrido alguna modificación o alteración no deseada.

El protocolo md5 mostrado anteriormente lleva presente desde finales del siglo XX y se encuentra actualmente amenazado, no constituyendo un algoritmo criptográfico seguro. Por ello, se utiliza en blockchain el algoritmo SHA-256. Diseñado por la NSA estadounidense, se utiliza en la red bitcoin y para maximizar la seguridad, se utiliza doblemente la función hash a los mensajes (aplicar SHA-256 al hash resultante de la primera aplicación). En la Tabla 2 se muestra el resultado de aplicación de diferentes algoritmos a un mismo mensaje.

Mensaje	MD5
ingeniería	01bf897db0326f3ad5bdeff53a54f2e6
Ingeniería Industrial	89e187ea23afc6dc39ae9f3ef5b455e1

Mensaje	SHA-256
ingeniería	cb48e7551258441cfa95de07a38bdbe49cfd056f465a7af2cc6dc65802fbb57f
Ingeniería Industrial	a1e382b1c3d3c0a545b40fcac2ef4efbab3b93574a6b7421c2639e4bce609681

Mensaje	Doble SHA-256
ingeniería	61fea4ba6df94cc7a25d686b84fade18d82b2504d11d8b082b7c13e6e1e85b0a
Ingeniería Industrial	081b4a811b8283d71e39e6cb2f49d5fbf70be161e8c025b3e69eb0a30bdf591d

Tabla 2. Ejemplo de hashes con distintos protocolos

Para funcionar, blockchain, utiliza una mezcla de toda esta tecnología, tal y como se describe en el apartado 3.2. En la Figura 11 (extraída de la públicación original de Satoshi [NAKA08]) se ilustra el funcionamiento de la criptografía en la cadena de bloques (en este caso de bitcoin, al ser el planteamiento propuesto por Satoshi).

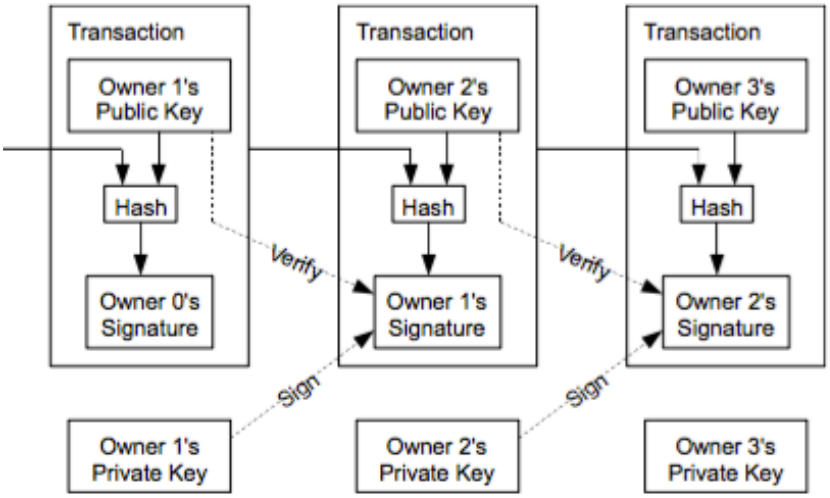


Figura 11. Propuesta de Satoshi para la interrelación de transacciones mediante criptografía

3.3.4.4. Árbol de Merkle

El árbol de Merkle es la forma en la que en la cadena de bloques se registran las transacciones dentro del bloque. Propuesto por Ralph Merkle en 1979, el árbol de Merkle es una forma de agrupación en forma de árbol de hashes que permite verificar de forma eficiente y segura la integración de los datos. En las aplicación empresariales de blockchain, el hash raíz (detallado a continuación) se puede firmar digitalmente, añadiendo una capa más de protección y seguridad.

El Árbol de Merkle va agrupando hashes hasta llegar a un hash raíz, que es, por lo general, el que se incluye en la cabecera del bloque. De esta forma, cualquier intento de modificación de los datos, cambiará, como se puede apreciar en la Figura 12 todos los hashes que se encuentren por encima, hasta llegar al hash raíz, lo que generaría un desajuste en la cadena de bloques.

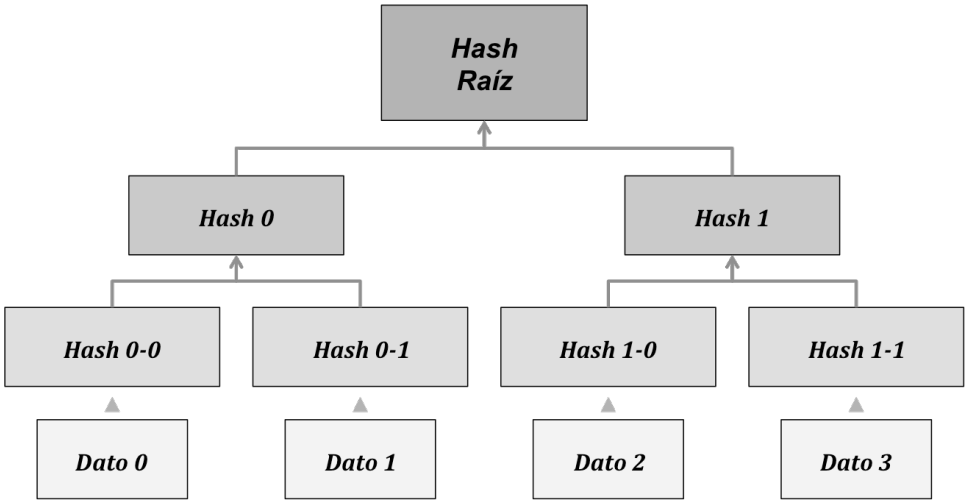


Figura 12. Detalle de ejemplo de Árbol de Merkle

3.3.5. Amenazas a la tecnología blockchain

3.3.5.1. Problema del doble gasto

El doble gasto es un problema que afecta a cualquier forma de dinero digital y potencialmente a cualquier aplicación de blockchain. En un sistema centralizado existe un tercero que coordina las transacciones, sin embargo, en un sistema descentralizado, hace falta un método para poder llegar a un acuerdo sobre el orden en el que se registran las transacciones.

Este problema se ilustra utilizando el conocido como problema de los generales bizantinos descrito a continuación, y cuya primera solución práctica surge con el planteamiento de Satoshi Nakamoto para el bitcoin, siendo este uno de los grandes logros de la moneda [PERE14].

El problema de los generales bizantinos es un dilema clásico en seguridad para sistemas descentralizados. Su formulación clásica es la siguiente:

Existe un grupo disperso de generales del antiguo imperio, y que deben ponerse de acuerdo en atacar una ciudad o retirarse, teniendo el plan éxito sólo si la mayoría ataca o se retira. Además, existen varias condiciones:

i) Solo se pueden comunicar entre ellos mediante mensajes

ii) No hay ninguna autoridad que los coordine (es un sistema descentralizado)

iii) Podría darse el caso de que alguno de ellos fuese un traidor e intente sabotear el plan

Para comprender la resolución propuesta por Satoshi, es necesario introducir previamente el concepto de hashcash, inventado en 2002 por Adam Black, un criptógrafo inglés [BACK02].

Hashcash surge como freno a los correos de spam no deseados. Adam Black formuló un sistema para imponer un coste no directamente monetario a los envíos de correo. Para ello, propuso incorporar la prueba de que el ordenador que enviaba los correos había dedicado tiempo y recursos para realizar el envío. Así, el coste en electricidad (consumida por la CPU) de esa prueba sería irrelevante para un e-mail individual, pero si se pretendían enviar mails de forma masiva, se imponía un coste.

Para poder hacer que el envío de un mail requiriese el consumo de recursos, se planteaba para cada correo que se quisiese enviar una prueba de trabajo (PoW por sus siglas en inglés). Una prueba de trabajo no es más que la resolución de un problema complejo que consume ciertos recursos computacionales. El problema planteado por Black consistía en hashear el mensaje una y otra vez hasta dar con un hash que comenzase por cuatro ceros. Para que el hash pudiese variar, se modificaba un pequeño dato denominado nonce (*number used once*), que no es más que un contador que cambia aleatoriamente para poder así generar un hash distinto en cada intento.

Así, al no poder predecir la forma de un hash, para obtener un hash que comience por cuatro ceros, se deberán probar combinaciones de mensaje y nonce, consumiendo recursos. Estableciendo la dificultad de encontrar un hash (aumentando las condiciones que debe cumplir), se aumenta la complejidad del problema y con ella, los recursos necesarios para poder llevar a cabo la actividad deseada (en sus orígenes, mandar un mail). Cabe destacar que el sistema hashcash no se llego a utilizar para su cometido inicial nunca.

Volviendo al problema de los generales bizantinos, a la resolución propuesta por Satoshi. Antes de plantear la solución, existen una serie de consideraciones previas:

- Cada general tiene un ordenador capaz de enviar, recibir mensajes y calcular hashes

- Cualquier general puede proponer una hora para el ataque, y el primer plan enviado será el primer plan a seguir

Con estas consideraciones, varios generales podrían enviar planes al mismo tiempo y por las posibles inestabilidades de la red unos generales podrían recibir primero el plan A y otros el B sin saber cual fue lanzado primero y por tanto cual es el verdadero.

Para superar este problema, Satoshi propone el uso de la cadena de bloques junto a pruebas de trabajo (PoW por sus siglas en inglés). Así, los generales podrán añadir votos a la cadena para llegar al consenso y que el ataque tenga éxito.

La resolución se basa en el funcionamiento de blockchain descrito de forma esquemática en el apartado 3.3. Se detalla aquí el funcionamiento de blockchain utilizando el problema de los generales como ejemplo.

El general que lanza el primer plan, lo hace buscando un hash con una dificultad determinada (utilizando un nonce junto al mensaje, de forma análoga a hashcash). La dificultad del hash a encontrar es un acuerdo previo de los generales, por ejemplo, igual que en hashcash, el hash del mensaje deberá comenzar por cuatro ceros. Dependiendo de la potencia computacional de la que dispongan los generales, se tardará un tiempo determinado en encontrarlo, de forma que una vez transcurrido un tiempo acordado (por ejemplo, tres horas), el plan (cadena) con mas votos (bloques) será el que se lleve a cabo.

Una vez el primer general consigue un hash, se constituye el primer bloque, que se distribuye al resto de generales, los cuales comienzan a buscar el segundo bloque. En este segundo bloque (y siguientes), el hash del bloque anterior se utiliza como contenido a hashear, de forma que el contenido de la cadena quede enlazada y asegurada. Con el segundo bloque enlazado, la cadena se volverá a actualizar para todos los generales y seguirán buscando nuevos votos [PREU17].

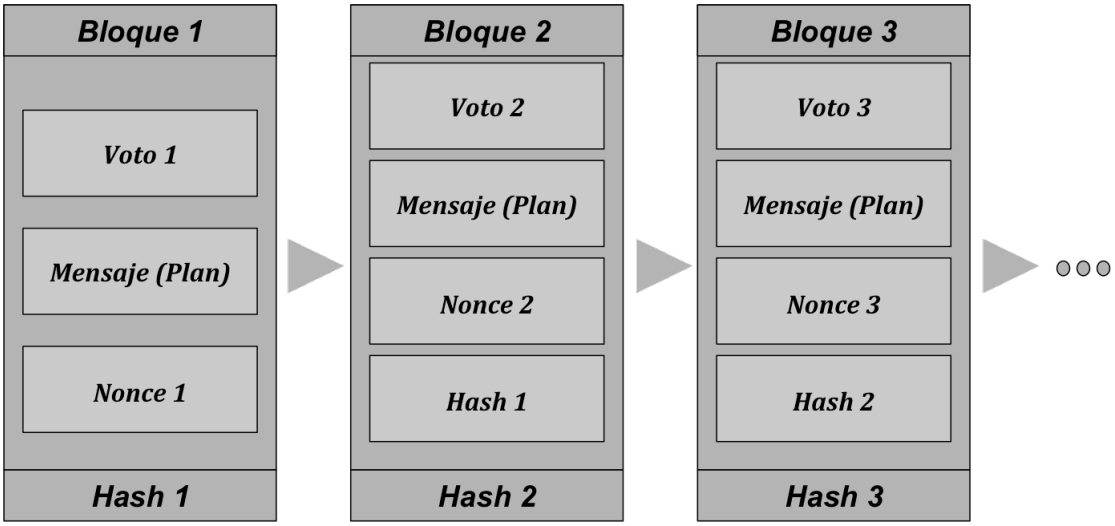


Figura 13. Esquema de estructura de los datos dentro del bloque

Al recibir un nuevo bloque, los generales, antes de aceptarlo, realizarán una serie de comprobaciones:

i) El nuevo hash debe comenzar con cuatro ceros (condición acordada)

ii) El hash es el resultante de los registros del bloque (numero de bloque, mensaje, hash anterior y nonce). Esta condición asegura la imposibilidad de modificación de contenidos registrados en la cadena

iii) Es el mensaje el mismo que en el bloque anterior (Esta condición asegura que un general traidor no podría cambiar el mensaje recibido)

Podrían existir dos problemas:

- *Generales traidores:* Si un general traidor quisiese modificar el mensaje recibido o lanzar otro erróneo, la composición de la cadena lo detectaría, ya que el nuevo plan no coincidiría con el del bloque anterior (comprobación iii) o bien la modificación del bloque anterior habría cambiado el hash de dicho bloque (comprobación ii).

- *Lanzamiento de dos planes simultáneamente:* Como se ha comentado, dos generales podrían lanzar el primer plan a la vez, y el resto de generales no sabrían discernir entre ambos. Según la propuesta de Satoshi, cada plan lanzado sería el inicio de una cadena de bloques, existiendo dos cadenas entre las cuales el resto de generales tendría que elegir. La cadena con más bloques sería el plan que tendría el consenso y el llevado a cabo con éxito.

Este sistema de consenso en sistemas descentralizados es lo que se denominó en el caso de bitcoin cadena de prueba de trabajo. Mediante el registro consensuado y cronológico de las transacciones, Blockchain impide el doble gasto. Esta propuesta es de vital importancia para la tecnología blockchain, pues no solo bitcoin necesita de una Prueba de trabajo, sino que cualquier implementación de blockchain necesitará el diseño de una prueba de trabajo acorde a las necesidades y exigencias del sistema, para poder asegurar con ello, la inviolabilidad y por tanto confianza de la cadena.

3.3.5.2. Otros problemas potenciales

Además del problema de los generales bizantinos, existen dos potenciales ataques clásicos contra blockchain y que pueden llegar a suponer un problema según la blockchain concreta que se este gestionando:

- *El ataque del 51%:* La cadena de bloques se basa en el consenso y la confianza, este ataque potencial consiste en poner de acuerdo al 51% de los participantes de la cadena de bloques para alterar algún contenido, i.e. llegar a falsear la cadena de bloques. Con este ataque, se podrían revertir transacciones o realizar dobles gastos, ya que los atacantes tendrían mayor poder computacional y por tanto la capacidad de generar bloques falsos, verificarlos y anexionarlos la cadena.

- *La maleabilidad de las transacciones:* Ataque ya superado, fue una debilidad inicial de bitcoin. Se basaba en la alteración del valor del hash de una transacción cuando no ha sido verificada, de modo que se verificase y anexionase a la cadena de bloques una transacción alterada.

3.4. Aplicaciones de Blockchain

En este apartado se va a realizar una pequeña introducción de algunas de las aplicaciones de blockchain que mayor repercusión han tenido o que mayor potencial tienen. No se pretende realizar una descripción exhaustiva y detallada de todas las aplicaciones, si no ilustrar el potencial de blockchain en tres sectores[5]; financiero, seguros y energía.

3.4.1. Blockchain en el sector financiero: Banca y criptomonedas

Desde el nacimiento de internet a finales del s. XX, ha existido un proyecto de revolución del mundo financiero, aprovechando el potencial que oferta la red. Los conocidos como cypherpunks[6], responsables de muchos de los avances en criptografía [LEVY93] y privacidad en la red desde finales de la década de los 80, quisieron crear un sistema financiero sin reguladores centrales, totalmente transparente y anónimo.

Fue una primera visión de lo que no llego hasta 2008; bitcoin. Desde que a principios de 2009 Satoshi realizase la primera transferencia en la cadena de bloques de bitcoin, han sido innumerables las aplicaciones de la descentralización y la tecnología blockchain en el mundo financiero. El surgimiento de bitcoin como medio de pago, supuso el primer caso de uso de blockchain, pues supuso la eliminación de un intermediario tradicional (banco) como tercero que aportase confianza entre dos partes.

El surgimiento de bitcoin en 2008 va acompañado de la mayor crisis financiera y bancaria en un siglo, lo que aumenta la desconfianza de la gente en los bancos tradicionales, a la vez que estos intentan pivotar su modelo de negocio, invirtiendo grandes cantidades de dinero en innovación. Uno de los focos de estas inversiones se encuentra en la tecnología blockchain. La revolución blockchain en el mundo bancario se sustenta principalmente en rentabilidad y regulación. Desde el inicio de la

[5] Al centrarse el resto del documento en supply chain, no se incluye en este apartado
[6] Cypherpunks es el término utilizado para describir a la comunidad de internet cuya lucha se basa en el mantenimiento de la privacidad del usuario y que se hayan en contra de la regulación de la red y la intervención gubernamental su manifiesto, puede encontrarse en www.activism.net/cypherpunk/manifesto

crisis, la rentabilidad de los bancos ha sido menor. La tecnología blockchain permite reducir los costes, a la vez que aporta transparencia, eficiencia, flexibilidad, y automatización, todas ellas características necesarias de la oferta al cliente en el nuevo paradigma bancario

Además de la revolución bancaria, que se encuentra en una fase semilla o como mucho, de testeo de proyectos, la gran revolución financiera de blockchain ha sido el surgimiento de las criptomonedas. Como se ha comentado a lo largo del capítulo, bitcoin fue la primera gran aplicación de blockchain, y la primera criptomoneda. A partir de ella, han surgido incontables criptomonedas, cada una con un propósito, una característica diferencial, pero todas basadas en blockchain. Las ventajas principales de las criptomonedas, que no son más que un medio digital de intercambio son:

- Reducción de costes con la eliminación de intermediarios
- Reducción de tiempos de realización de las transacciones
- Emisión limitada, controlando la inflación (e.g. Bitcoin tiene un máximo de 21 millones en circulación[7])
- Seguridad y transparencia

Tal ha sido la fiebre de las criptomonedas que según la web especializada cryptocurrencyfacts.com, existen más de 1.000 criptomonedas distintas. Sin embargo, solo unas pocas han adquirido relevancia (por ejemplo, solo 25 criptomonedas tienen una capitalización mayor de 1.000 millones de dólares). En la Tabla 3 se muestran las cinco criptomonedas con mayor capitalización[8]

Nombre	***Símbolo***	***Capitalización (Miles de millones)***
Bitcoin	BTC	$166
Ethereum	ETH	$82
Ripple	XRP	$37
Bitcoin Cash	BCH	$20
Litecoin	LTC	$11

Tabla 3. Capitalización de las cinco principales criptomonedas

Sin embargo, las criptomonedas han ido, a lo largo de su breve historia, acompañadas de polémica. El anonimato que garantizan es para muchos, una fuente potencial de blanqueamiento de capitales y financiación de actividades ilegales. Por esta razón, en algunos países (e.g. Bolivia [BCB17]) se ha prohibido su uso.

[7] bitcoin.org/en/faq#wont-the-finite-amount-of-bitcoins-be-a-limitation
[8] Febrero 2018

Además de esa característica, los grandes financieros han criticado las criptomonedas. Una de las mayores criticas la ha realizado Howard Marks (Fundador y gestor de Oaktree Capital, con 101.000 millones de dólares bajo gestión). En su carta a inversores *There they go…again* [MARK17] realiza una profunda reflexión sobre el valor intrínseco de las criptomonedas y se puede leer lo siguiente[9]:

"La gente me dice que estas criptomonedas son solidas porque (a) son seguras contra el hacking y la falsificación y (b) la emisión de monedas está limitada por el código que las crea. Pero… ¡no son reales! […] Se pueden utilizar monedas imaginarias para comprar otras monedas imaginarias o para invertir en compañías que creen nuevas monedas imaginarias.

Bajo mi punto de vista, las criptomonedas no son más que una moda (o quizá incluso una estafa piramidal) basada en asignar valor intrínseco a algo que carece de ello más allá de lo que la gente este dispuesta a pagar. Es completamente irracional comprar (o aceptar un pago) algo con bitcoin, El precio de bitcoin se ha duplicado desde inicio de año, ¿puede ser considerado como un medio de intercambio o almacén de valor –como debería ser una divisa- en lugar de simple especulación?

Juntas, bitcoin y ethereum tienen más valor que Paypal y prácticamente el mismo que Goldman Sachs, que preferirías, ¿poseer todas las monedas o una de esas dos compañías? En otras palabras, ¿es el valor de estas monedas real?"

La historia juzgará si las criptomonedas terminan convirtiéndose en divisas o si no han sido más que una fiebre de especulación, una burbuja similar a los tulipanes holandeses de 1637. Cualquiera que sea el resultado, de lo que no cabe duda es de que las criptomonedas han sido la primera gran aplicación de blockchain, han puesto esta tecnología en el foco mundial, centrando inversión en ella y posibilitando la su implantación y la potencial revolución en muchos otros sectores.

3.4.2. Blockchain en el sector de los seguros

El sector de los seguros ha sufrido una evolución similar a la banca, viendo como su rentabilidad ha ido disminuyendo y como la aprobación de nuevas regulaciones expande la competencia, haciendo que nuevas startups de base tecnológica se abran camino dentro de un sector gobernado por las grandes aseguradoras tradicionales.

[9]Traducción libre

La respuesta del sector a los cambios y a las nuevas exigencias de los clientes no se hizo esperar, y cinco grandes aseguradoras (Aegon, Allianz, Munich RE, Swiss RE y Zurich) crean en 2016 un consorcio de blockchain denominado Blockchain Insurance Industry Initiative – B3i[10], con el fin de compartir experiencias y conocimiento y revolucionar la industria de los seguros. A finales de 2017, más de 20 aseguradoras formaban parte de esta plataforma. El mayor cambio potencial que pueden obtener las empresas aseguradoras se sustenta en los contratos inteligentes (Smart Contracts), que se encuentran descritos en el apartado 3.4 de este documento.

Gracias a la utilización de esta tecnología, las empresas aseguradoras conseguirán un aumento de la seguridad, pues al estar toda la información dentro de la cadena de bloques, es sencillo evitar el fraude. Además, este tipo de soluciones, suponen un tipo de producto ideal para la nueva economía colaborativa. Sin embargo, la mayor ventaja del uso de blockchain en las aseguradoras podría llegar de la mano de contratos *ad-hoc* (e.g. La póliza del seguro del coche podrá incluir información mucho más detallada, siendo personalizada, y con posibilidades de actualización totalmente transparente). Sin embargo, el impacto de blockchain en el sector no se limita a eso, si no que es transversal a toda la cadena de valor [MACK17] de las compañías aseguradoras, desde el diseño de productos hasta la gestión de riesgos y de reclamaciones.

¿Es posible cuantificar el impacto? Existen estudios [CANT17] que prevén unos ahorros de 21.000 millones de dólares anuales (solo en seguros de automóviles), así como menores tarifas para los clientes.

3.4.3. Blockchain en el sector de la energía

El sector energético, uno de los sectores estratégicos más críticos de un país comenzó hace unos años su propia revolución: la descentralización. Tradicionalmente, la demanda energética se cubría con producción en las centrales, alejadas de los consumidores finales. Sin embargo, de un tiempo a esta parte, el modelo comenzó a cambiar, y la implementación de instalaciones capaces de generar energía en los propios centros de consumo (e.g. paneles solares en los tejados de las casas particulares). Esta descentralización no ha hecho más que comenzar, pues todo indica que esta descentralización va a ser la tendencia dominante en el futuro.

Así, los consumidores tradicionales se convertirán en consumidores con su propia fuente de generación energética. Pero, ¿dónde entra blockchain en este esquema? La

[10] https://b3i.tech/about-us.html

tecnología base para llevar a cabo esta transición ya existe y esta implementada, desde contadores inteligentes a paneles fotovoltaicos conectado. Sin embargo, blockchain es el catalizador necesario y esperado para que este sector acelere el cambio.

Actualmente existe un proyecto piloto en este ámbito que ha tenido bastante relevancia es la colaboración entre Siemens y la startup americana LO3, en el *Brooklyn Microgrid Project*[11]. Este proyecto ha supuesto la posibilidad de intercambio vecinal de la energía generada en unas placas solares instaladas en un tejado mediante blockchain. Además, permite al usuario que ha realizado la instalación que sus contadores "vayan al revés" los días en los que produce un exceso de energía y la vuelca a la red, convirtiéndose además de consumidor en productor.

3.4.4. Contratos Inteligentes (Smart Contracts)

Antes de comenzar este apartado, cabe destacar que el objetivo del apartado es el de aportar una visión general sobre lo que son y las ventajas que tienen los contratos inteligentes. En ningún momento se pretende aportar un enfoque técnico de los mismos ni de las aplicaciones concretas que tienen, pues se pueden utilizar potencialmente en cualquier sector y sus aplicaciones son prácticamente infinitas.

Descritos mucho antes que blockchain, un contrato inteligente es un acuerdo entre partes con la capacidad de autoejecutarse. Un código informático define las condiciones del contrato y se ejecuta cuando se cumple alguna premisa anteriormente definida. Vitalik Buterin (creador de ethereum, una criptomoneda en cuya blockchain se pueden programar y ejecutar contratos inteligentes) describe los contratos inteligentes como[12]:

"[En el contexto de un contrato inteligente] un bien es transferido y el programa corre el código hasta que en algún punto encuentra valida alguna de las condiciones previamente establecidas, por lo que automáticamente ejecuta el contrato y decide a que parte debe ir el bien"

Un contrato tradicional es un acuerdo entre partes cuya confianza puede ser intrínseca a la otra parte (Existen problemas si por ejemplo hay en juego una cantidad elevada de dinero). Los contratos tradicionales que tienen relevancia (e.g. compra de una casa) se firman ante notario. Esta figura aporta un registro público y aporta a (al menos una

[11] www.siemens.com/innovation/en/home/pictures-of-the-future/energy-and-efficiency/smart-grids-and-energy-storage-microgrid-in-brooklyn.html
[12] Traducción libre de la descripción de V. Bulterin en una conferencia en DC blockchain Summit 2016 (digitalchamber.org/events)

de) las partes el derecho a cobrar. Sin embargo, existe la figura de la deuda, y quizá la inversión necesaria para ejecutar el derecho a cobrar sea más cuantiosa que la deuda en sí misma.

La última manera de generación de confianza entre partes es someter el contrato a una tercera parte de confianza y someterse a su dictamen, pero este método también tiene debilidades; la tercera parte podría no aparecer o estar aliado con una de las partes.

Utilizando blockchain junto a contratos inteligentes se resuelven todas estas debilidades, se genera confianza (pues la cadena de bloques queda como registro público inalterable)entre partes - o mejor, elimina la necesidad de que exista confianza entre las partes - y el contrato se ejecuta siempre. En el contrato inteligente están definidas todas las condiciones que las partes deseen de forma muy concreta, evitando que puedan existir confusiones y evitando reclamaciones.

Para ilustrar el funcionamiento, se detalla un ejemplo de posible aplicación de un contrato inteligente. En la venta de una entrada online anticipada para cualquier espectáculo (e.g. un concierto), se suele permitir pagar una cuota que da derecho a la devolución del precio de la entrada en varios supuestos (anulación del espectáculo, imposibilidad de asistir, etc.) es un seguro de asistencia. Si llegado el momento del espectáculo, se cumplen algunas de las condiciones previamente estipuladas y se decide hacer uso del seguro, habrá que realizar algunas gestiones para reclamar la devolución del importe, esperar a que un agente realice una validación del caso y se apruebe la devolución y luego esperar días o incluso meses a que se reintegre el precio de la entrada.

Utilizando este mismo ejemplo pero aplicando un contrato inteligente en una cadena de bloques, la historia sería diferente. Al contratar el seguro, se rellenarían los datos personales y de reembolso del pago. En el espectáculo, si se ha dado alguna de las condiciones, el contrato se ejecutará y se devolverá el dinero, sin esperar a validación y aprobación del caso. El reembolso sería prácticamente instantáneo haciendo uso de criptomonedas y de tres a cinco días (tiempo aproximado para operaciones comerciales bancarias) en caso de pago en divisa. Para poder llevar esto a cabo, el contrato utilizó la información proporcionada con una base de datos (por ejemplo, las lecturas de las entradas en la entrada del espectáculo), la información enviada por el cliente y al no haber asistido, se ejecuta. El contrato entonces se destruye (estando la destrucción programada con anterioridad, ya que no se puede destruir información de la cadena de bloques) o se almacena en la blockchain.

Las ventajas principales de los contratos inteligentes frente a los tradicionales son:

- *Autonomía*: Pues no hace falta una tercera parte.
- *Confianza*: El contrato se almacena en una cadena de bloques inviolable e imperdible.
- *Rapidez*: La ejecución es instantánea cuando se detecta el cumplimiento de cierta condición.
- *Precisión*: En el momento en el que se cumpla una condición, el contrato se ejecuta. No existen interpretaciones.

Las aplicaciones de estos contratos en todo tipo de sectores son muy altas, y uno de los sectores en los que más potencial (tal y como se detalla en el apartado 3.4 del presente documento) existe es el logístico.

Sin embargo, los contratos inteligentes no se hayan libres de problemas. Según plantea el prestigioso bufete Linklaters en un documento que recoge las preocupaciones legales [LINK17], uno de los mayores problemas es el supuesto en el que el código se redacta de forma incorrecta. Un contrato tradicional podría anularse, pero un contrato inteligente se ejecutará.

3.5. Críticas y problemas de blockchain

A pesar de todas las bondades de blockchain descritas, como con cualquier tecnología disruptiva, no faltan las críticas. Muchas de las críticas se centran en bitcoin, al ser, como ya se ha comentado, la aplicación más conocida de la tecnología.

Una de las críticas más duras a bitcoin (y en el trasfondo a blockchain) la expuso Mike Hearn en un post [HEAR16] dentro de su blog en la web tecnológica medium.com.

Hearn, uno de los desarrolles mas notables de código de la comunidad bitcoin destaca que el desarrollo de bitcoin ha sido un experimento y que como muchos experimentos, ha fracasado. Esgrime dos razones principales; el fallo de la comunidad bitcoin y la limitación de bitcoin en cuanto a transacciones por segundo. Por ser general y ser una critica a blockchain, se va a detallar la segunda critica.

Hearn argumenta que el límite de transacciones que blockchain puede registrar en su aplicación para bitcoin es de siete por segundo (en 2011, actualmente, mucho menor por el aumento de la complejidad). Hearn argumenta que los registros en la cadena de

bloques pueden tardar entre minutos y horas, y nadie quiere esperar horas para verificar una transacción.

Esta crítica, ha sido también soportada por diversos expertos, cabe destacar en especial el artículo de la web bussinesinsider.com *Here's a key reason Bitcoin will struggle as a payments system*. Basado en un informe de BAML[13] en el que analistas analizaron el porqué del fracaso de bitcoin como sistema de pago. Una de las razones más importantes es precisamente el límite de transacciones por segundo. La media de verificación de una transacción en el análisis fue de unos 10 minutos, y en ese momento, se realizaban 300.000 transacciones al día en la red bitcoin. Esto implica que la velocidad de registro de las transacciones en la blockchain de bitcoin constituye un cuello de botella y debe ser tomado como precaución para el resto de aplicaciones potenciales. Para terminar de ilustrar este ejemplo, nótese que las compañías de crédito como Visa o Mastercard verifican unas 2.000 transacciones por segundo y cuentan con una capacidad para soportar picos de hasta 60.000. Además, según Kai Stinchcombe [STIN17], la energía consumida por la red bitcoin para procesar las 7 transacciones es 35 veces mayor que la consumida por Visa. Esto supone un gran problema potencial, ya que la solución no pasa exclusivamente por aumentar la capacidad de procesado de la red bitcoin si no de reducir a la vez la energía que consume.

Otra crítica que ha tenido mucho eco dentro de la comunidad blockchain es la llevada a cabo por Aengus Collins, recogida en el articulo *Four reasons to question the hype around blockchain* públicado en WEF (World Economic Forum). En el citado artículo, Collins recoge cuatro razones por las que cuestionar las expectativas puestas en blockchain:

- El *gap* existente entre las aplicaciones potenciales de blockchain y los proyectos de blockchain que se han no ya implementado, si no simplemente testado.
- ¿Es necesaria (y deseada) una solución tecnológica para la disminución de la confianza?

- Existen límites a la confianza que aporta blockchain, pues confiar en blockchain no es solo confiar en su tecnología si no en la implementación de la misma que las compañías lleven a cabo.

[13] Bank of America Merril Lynch

- ¿Cuáles serían las consecuencias imprevisibles de reemplazar los sistemas sociales de generación de confianza por métodos basados en tecnología y descentralización?

3.6. Adopción y expansión de blockchain

A pesar de todo el potencial y los usos factibles descritos en capítulo, lo cierto es que la cadena de bloques constituye una tecnología novedosa y que aunque cuenta con el potencial necesario para hacerlo, deberá demostrar que es revolucionaria.

Las grandes empresas de muchos sectores están realizando grandes inversiones en proyectos piloto y pruebas de todo tipo para probar la tecnología. Una nueva tecnología supone riesgos nuevos y unos costes potenciales que la mayoría de las empresas no pueden soportar. Por ello, es importante que las grandes empresas multinacionales testeen las posibilidades de uso de la tecnología y la sitúen al alcance de todas las empresas.

4. Blockchain en Supply Chain

En este capítulo se va a realizar una descripción de la implementación de sistemas de gestión de datos de supply chain en el sector alimentario. El objetivo del apartado no es realizar un análisis en profundidad para un caso de implantación en concreto, sino explorar las ventajas y desventajas de la supply chain tradicional y la gestionada mediante blockchain.

4.1. Blockchain como sistema de gestión de datos

En el capítulo anterior se ha descrito el funcionamiento de la tecnología blockchain de forma teórica, apoyándose en la primera y gran aplicación; bitcoin. En este capítulo, se pretende realizar un aplicación practica de las posibilidades de la tecnología blockchain en la cadena de suministro.

Actualmente, una persona puede pedir mediante un click prácticamente cualquier cosa y recibirlo en su casa al día siguiente, todo está al alcance de todos en un tiempo record, así que cabe preguntarse, ¿Qué falta hace cambiar algo que funciona, por qué evolucionar? La respuesta es muy amplia, pero en lo que respecta a este trabajo, no se trata solo de la comodidad del usuario, también de la eficiencia, de ser capaces de hacer lo mismo a un coste menor. De la seguridad, de solucionar los problemas existentes, sobretodo en materia de transparencia y trazabilidad a lo largo de la cadena de suministro. La tecnología blockchain aplicada a supply chain permitiría crear una base de datos distribuida, asegurada con la ultima tecnología criptográfica, que permitiese almacenar todos los movimientos de productos a lo largo de toda la cadena de suministro, desde su producción hasta su venta al consumidor final.

4.1.1. Sistema tradicional vs sistema distribuido

Los sistemas utilizados en la mayoría de empresas para la gestión de la cadena de suministro son los denominados ERP (*Enterprise Resource Planning*). Programas de gestión de los datos necesarios para gestionar la cadena de suministro de forma correcta. Son sistemas centralizados, implantados en las empresas a raíz de la expansión de los ordenadores a finales de la década de los 90, y que desde entonces hasta hoy, han supuesto una grandísima inversión en digitalización.

Sin embargo, y a pesar de los miles de millones de dólares invertidos por las diferentes industrias, la mayoría de las empresas solo tienen visibilidad parcial sobre

dónde se encuentran sus productos en un momento determinado. Además, en el caso en el que en una misma cadena existan diferentes participantes (un proveedor y un distribuidor distinto de la empresa fabricante por ejemplo), la integración de los sistemas, de ser factible, es compleja y laboriosa.

Otro de los grandes problemas es la sincronización, llegando en muchos casos a parecer que el inventario se encuentra duplicado en dos lugares al mismo tiempo. Estos sistemas de gestión se concibieron hace dos o tres décadas, cuando existían empresas con enormes cadenas de suministro verticalmente integradas, pero estáticas, y es esta ultima parte la que más ha evolucionado. Las cadenas de suministro actuales han dejado de ser estáticas para ser entes dinámicos.

Hoy en día, la cadena de suministro de una empresa ha dejado de ser el modelo tradicional de proveedor – productor – distribuidor para convertirse en un entramado con muchos proveedores, productores y distribuidores, usualmente cada uno en una localización geográfica diferente. Además, con el acortamiento del ciclo de vida de los productos y la demanda de los consumidores que exigen mejoras en los productos, rapidez y eficacia, la cadena de suministro ha ido dinamizándose, lo que dificulta obtener una visión global con un sistema de gestión como los ERP.

Una de las aproximaciones para la gestión de este nuevo ecosistema se encuentra en la tecnología blockchain. Tal y como se ha detallado en el capítulo 3 esta tecnología permite la confianza total entre las partes, algo fundamental en la cadena de suministro.

El núcleo de la tecnología blockchain, es decir, la descentralización, permite solucionar el problema de la sincronización, pues las transacciones (e.g. la materia prima entra en producción) se actualizan para todos los participantes en minutos, obteniendo una visión completa de la cadena, con una trazabilidad imposible hasta ahora y evitando la duplicación de los inventarios.

La mayor aportación de la gestión mediante blockchain es el aumento de la transparencia y la trazabilidad, ofreciendo información en tiempo cuasi-real, a todos los implicados en la cadena de suministro de dónde se encuentra un producto en un momento determinado así como sobre dónde ha estado. Con esto, se maximiza la eficiencia de los procesos de la cadena de suministro y por tanto, del negocio.

La gestión de la cadena de suministro mediante blockchain tiene gran impacto en la relación con proveedores, debido a que la mejora de los datos, tanto en cantidad como

en análisis, hace posible una mejor gestión del inventario, aprovechando las sinergias y los descuentos por volumen cuando sea posible, evitando stock innecesario (con un coste asociado estimado entre el 10 y el 40% anual del valor del producto según la industria), pero manteniendo el mismo nivel de servicio.

Otro de los grandes impactos de la implantación de un sistema descentralizado, gestionado mediante blockchain, sería la reducción del tiempo de pago. Pues la incorporación de los *Smart Contracts* (ver apartado 3.4) podría llevar a realizar los pagos a proveedores en los días establecidos por contrato, sin posibilidad de retrasos o incumplimientos por ninguna de las dos partes.

4.1.2. Errores humanos

En la gestión de la cadena de suministro, la recopilación, análisis y uso de los datos disponibles es clave, utilizando blockchain en lugar de los sistemas de gestión tradicionales, se podría realizar el tracking de cualquier producto en cualquier etapa de la cadena, asegurando que los registros no han sido alterados y que por tanto son confiables.

Sin embargo, la promesa de esta tecnología para revolucionar las cadenas de suministro se ha visto limitada por varias cuestiones, pero una de las mayores criticas esta basada en la inmutabilidad de blockchain. La inmutabilidad de blockchain es una de sus mayores ventajas, porque asegura la veracidad de las transacciones y la imposibilidad de falsificaciones por parte de terceros. Sin embargo, cualquier sistema es gestionado por seres humanos, y cualquier persona puede cometer un error e introducir en la cadena de bloques información incorrecta, que de no ser modificable, puede tener graves consecuencias económicas y sociales. Estos errores potenciales no obstante, también están presentes en otros sistemas de gestión y no son intrínsecos a blockchain. La automatización y la limitación de la cantidad de datos modificables manualmente por un ser humano pueden ser los caminos indicados para reducir la probabilidad y el potencial impacto de estos errores.

4.1.3. Desventajas de la implantación de los sistemas

Las mayores desventajas a la implantación de un sistema distribuido en la cadena de suministro de una empresa son:

- Los trabajadores con el conocimiento necesario para llevarlo a cabo son escasos y caros

- No existe un estándar en la industria para la implantación de los sistemas

- Para tener éxito, necesita ser adoptado no solo por una empresa sino por todas las empresas integrantes de una cadena de suministro, algo complicado teniendo en cuenta la compleja estructura de las cadenas de suministro actuales

4.2. Blockchain en supply chain. Caso del sector alimentario.

Resulta sorprendente como en el mundo totalmente digitalizado del s. XXI, en el que casi cualquier información es accesible instantáneamente y en cualquier lugar, se sepa tan poco sobre los productos que se consumen.

Cada uno de los productos que se compran, ha pasado por una serie de etapas, desde la producción hasta la distribución final. Estas etapas son generalmente desconocidas o ignoradas para el público que consume dicho producto. No deja de resultar sorprendente como en los productos alimentarios, el consumidor confía plenamente en el establecimiento al que compra, e inherentemente en sus empleados, instalaciones, proveedores, productores, etc.

Sin embargo, esta tendencia está cambiando en los últimos años, impulsados por escándalos alimentarios (e.g. carne de caballo en Reino Unido o el fraude del atún rojo en España) cada vez son más los consumidores que desean conocer las fuentes de origen de los productos que adquieren. Además, debido a estos escándalos, las autoridades, los distribuidores y los consumidores, quieren poder identificar, en caso de contaminación, la fuente de un producto y la reconstrucción de todas las etapas por las que ha pasado.

Este cambio de paradigma supone la necesidad de que el producto pueda ser trazado desde el punto de venta al origen de producción. La tecnología existente hoy en día en la mayoría de las cadenas de suministro, cada vez más complejas, fragmentadas y diseminadas geográficamente impide llegar a realizar una trazabilidad completa del producto sin un gran despliegue de medios e inversión.

Es por ello, que cuando el consumidor deja de confiar ciegamente en el ciclo que siguen los alimentos que compra, la tecnología blockchain puede ayudar a devolver esa confianza y probar la procedencia de dicho producto.

La aplicación de la tecnología blockchain al sector alimentario, principalmente en las cadenas de suministro de alimentos perecederos, podría ayudar al consumidor y al distribuidor, pues sería posible obtener una trazabilidad completa, sirviendo como certificación de origen del producto y de la cadena de suministro, con ello se incrementaría la seguridad y se mejorarían los tiempos de respuesta para la retirada de productos en caso de intoxicaciones o lotes en mal estado.

Para comprender la utilidad de la tecnología blockchain para asegurar la trazabilidad, cabe analizar los sistemas utilizados actualmente a lo largo de la cadena de suministro para conseguir dicha trazabilidad [MCBE18]:

- *1-up/1-back propietario*: es el sistema más utilizado actualmente. Cada participante implicado en la cadena de suministro almacena los datos que considera necesarios para la trazabilidad en un formato propio. Almacena por ejemplo de dónde y cuándo llegó un producto a sus instalaciones y a dónde y cuándo abandonó las mismas.

- *1-up/1-back estandarizado:* igual que en el caso anterior, los datos son almacenados individualmente por cada empresa, sin embargo, el formato de los datos a lo largo de la cadena de suministro es común.

- *SaaS*[14] *centralizado:* Tecnología emergente que supone el mejor sistema actual para poder tener trazabilidad completa de un producto, pues engloba a todos los partícipes en la cadena en un servidor centralizado.

- *Blockchain descentralizado:* Sistema similar al anterior pero basado en la tecnología blockchain, donde no existe una centralización.

En teoría, la trazabilidad en una cadena de suministro con el sistema 1-up/1-back implantado no resulta complicada (aunque si farragosa). Si existiese un problema de contaminación en un producto o lote, puede obtenerse trazabilidad hasta la fuente de la contaminación en cualquier punto de la cadena, ya sea en origen o durante el procesado. A este proceso se le denomina trazabilidad hacia atrás o *backwards*.

[14] Software as a service (software como servicio). Modelo de distribución de software en el que una compañía especializada almacena la información del cliente a la que este accede vía internet

Una vez identificado el origen de la contaminación, la trazabilidad hacia delante o *downstream* permite identificar dónde se encuentran los productos o lotes que han pasado por la instalación contaminada.
El proceso descrito parece sencillo y preciso, sin embargo, existen dos desventajas de gran calado:

- En la práctica, se utilizan muchos registros en papel, por lo que el proceso descrito es extremadamente lento y conlleva alta probabilidad de error.

- Los registros (en papel o electrónicos) son almacenados por cada uno de los partícipes por lo que pueden ser falsificados con facilidad para evitar responsabilidades.

A continuación se ilustra el proceso 1-up/1-down ampliamente implementado en el sector alimentario con un ejemplo; la supuesta intoxicación de un consumidor y el camino que deben seguir las autoridades hasta identificar el origen de la contaminación (trazabilidad *upstream*) en una máquina de procesado y la subsiguiente investigación del paradero del resto de lote afectados (trazabilidad *downstream*).

El ejemplo de cadena de suministro alimentaria generalista de la Figura 15 resume el uso de los códigos estándar de la industria desarrollados por GS1 y detallado en el apartado 2.3 del presente documento. Puede observarse que los estándares de la industria se centran en el producto, cantidad, lotes y fecha. Estos datos se recogen y se recogen en una etiqueta estandarizada en cada producto, caja o lote (Figura 14)

Figura 14. Ejemplo de etiqueta estandarizada propuesta por GS1

Nótese que este sistema corresponde al modelo 1-up/1-down estandarizado, y que un modelo 1-up/1-down propietario sería similar pero incluyendo cada participante de la cadena los datos que considerase oportunos, sin ningún tipo de estandarización.

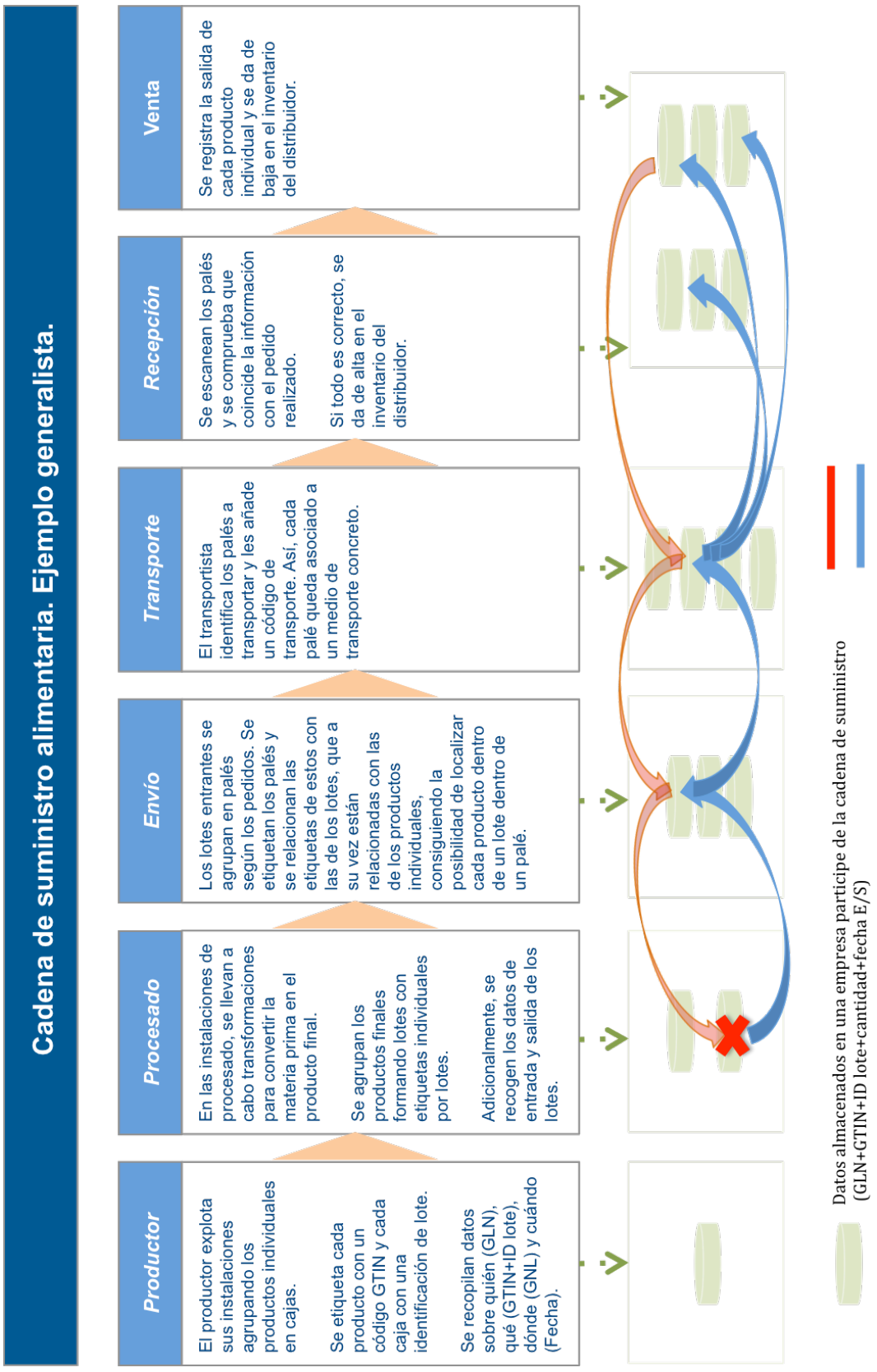


Figura 15. Ejemplo de cadena de suministro alimentaria generalista

Tal y como se ha descrito, y como puede observarse en la Figura 15, la trazabilidad con un modelo 1-up/1-back es engorrosa y presenta importantes desventajas. La solución existente que supone una solución mucho mejor es el uso de internet para adoptar una centralización en la nube (en adelante, SaaS).

Existen dos modelos de SaaS posibles. La arquitectura de ambos sistemas es similar, con los datos aglutinados en la nube, sin embargo existen algunas diferencias:

1. *SaaS propio:* aunque los datos se almacenan en la nube, no existe un modelo para compartir dichos datos entre los partícipes

2. *SaaS en red*[15]*:* Los datos almacenados en la nube son accesibles por todos los partícipes autorizados

Estos sistemas en red hace que la trazabilidad de los productos (tanto *upstream*, tanto *downstream*) reduzca los plazos temporales significativamente, de días o semanas a segundos.

En el caso de SaaS, aunque físicamente los sistemas se encuentren distribuidos, el control es centralizado, sin embargo, la implantación de un modelo basado en blockchain sería descentralizado. Este modelo permitiría la interacción entre todos los participantes de la cadena de suministro para la verificación y validación de datos.

Una digitalización del sistema de gestión de los datos de una cadena de suministro, además de mejorar la trazabilidad tiene importantes impactos en otras características importantes, como el control y la frescura de los productos.

Esta mejora de parámetros distintos de la trazabilidad y la transparencia, es posible porque la digitalización de la gestión de los datos permite la colecta y tratamiento de numerosos datos que con un sistema tradicional sería imposible sacar partido.

En la actualidad, existen algunos estudios teóricos que ofrecen propuestas para la recolección de estos datos. Una de las propuestas con mayor impacto en el mercado es la realizada por Zest Labs, e incluye [MCBE18]:

- Monitoreo constante de temperatura

[15] Traducción libre de las designaciones Enterprise SaaS y Networked SaaS.

- Calculo dinámico de la fecha de caducidad basado en la temperatura y condiciones a las que el producto ha sido expuesto

- Días de tránsito del producto, desde el proveedor al consumidor final

Todos estos datos serían gestionados por un algoritmo que en cada punto de la cadena de suministro podría tomar decisiones relevantes como a dónde mandar cada producto en función de los días de tránsito estimado al destino.

Todo lo expuesto hasta ahora podría realizarse con un sistema SaaS centralizado, sin necesidad de utilizar la tecnología blockchain. Entonces, ¿Qué aporta esta tecnología en la cadena de suministro del sector alimentario? La respuesta es confianza y mayor potencial.

La implementación de blockchain significaría mejorar la seguridad y la disponibilidad de los datos. Con la descentralización y el nivel de la encriptación que forma parte del núcleo de blockchain, un sistema basado en esta tecnología es mucho más difícil (sino imposible) de hackear y colapsar [PROV15]. Como contrapartida, existe un coste de procesado asociado, por la redundancia en almacenamiento descentralizado y la potencia necesaria para la encriptación de los datos.

La validez y confiabilidad de los datos recolectados también se verían mejoradas. La estructura propia de blockchain es la base para ello, y la inclusión de dispositivos de medición con algoritmos que sean capaces de detectar la toma de datos irregular (e.g. calentamiento o enfriamiento artificial del sensor) hace que los datos tomados y guardados puedan ser totalmente aceptados por todas las partes implicadas. Esa confianza en la colecta de datos es de vital importancia, pues unos datos erróneos o con posibilidad de ser falseados previamente a su registro, eliminaría las ventajas de la implantación de blockchain.

Otro de los grandes aportes sería la automatización de los procesos vía *smart contracts*. La implantación de un sistema basado en blockchain abriría la puerta a la ejecución automática y transparente de las distintas transiciones de la cadena mediante el uso de contratos inteligentes, cuyas condiciones de ejecución pueden (y deben) ser modificadas y aceptadas por todos los partícipes implicados en la transacción.

Posibilidad de auditoría, trazabilidad y transparencia. Aunque un sistema SaaS puede llegar a ser tan transparente para los partícipes como un sistema basado en blockchain, la inmutabilidad de los datos registrados y la facilidad de auditoría de los mismos, hacen preferente el sistema basado en blockchain.

Además de todas estas ventajas principales, existen algunas otras secundarias, como por ejemplo la posibilidad de eliminar intermediarios, tanto financieros en la realización de pagos, ejecutándolos mediante criptomonedas, como logísticos, existiendo la posibilidad de ajustar los desajustes de la oferta y la demanda (e.g. excedente en una explotación agrícola) con la creación de un mercado directo al consumidor.

4.2.1. Implantación de los sistemas

Actualmente, la practica totalidad de los proyectos de blockchain que han superado la fase piloto se han dado en el sector financiero. En el resto de sectores, incluyendo el alimentario y las aplicaciones en supply chain, se han realizado proyectos pilotos, con resultados esperanzadores, pero todavía no se ha definido una implementación específica para los sistemas de gestión descentralizados. Así, una empresa que decida innovar y apostar por estos sistemas, debe tener en cuenta las diferentes tecnologías existentes en este ámbito y las que podrían desarrollarse, porque es demasiado pronto y no se han establecido estándares entre el abanico de tecnologías, por lo que apostar la implantación a una sola en lugar de hacer una implementación progresiva, más general, que pudiese compatibilizarse con cualquier tecnología que acabe siendo estándar es demasiado arriesgado [KEMP18]. Sin embargo, independientemente de las distintas tecnologías, es importante señalar algunas de las características que por ahora parece que serán beneficiosas en la implantación.

El primer punto a tener en cuenta en la implantación de un sistema descentralizado es la elección entre una cadena de bloques pública o privada. Las diferencias entre ambas, analizadas en detalle en el apartado 3.3 de este documento, hacen que para la gestión de una cadena de suministro, una blockchain privada sea la elección acertada.

Esto es porque una blockchain privada cumple con varias características necesarias:

1. En una cadena pública, cualquiera puede ser partícipe, mientras que en una privada, solo los participantes autorizados tienen acceso. La forma de autorizar participantes puede variar, pero como en una cadena de suministro los participantes son limitados, es necesario que exista algún tipo de filtro o

veto a participantes no deseados. Asimismo, en una blockchain privada, la asignación de permisos de lectura y escritura puede limitarse con el fin de proteger datos que pueden ser sensibles.

2. En una blockchain pública, los registros son pseudoanónimos, mientras que en una blockchain privada, los participantes pueden ser identificados. En la cadena de suministro, resulta primordial la identificación de los partícipes, no es deseable en ningún caso ni por ninguna razón el anonimato.

3. El consenso para integrar nuevos registros en una blockchain pública viene determinado por la mayoría, sin embargo, en una blockchain privada, puede decidirse cómo realizarse, si por mayoría, eligiendo ciertos nodos como controladores de contenido (e.g. consorcio), etc.

Todas estas características, además de adaptarse a las necesidades de una cadena de suministro, hacen el sistema más eficiente en términos de requerimientos computacionales.

Una de las ventajas más importantes del uso de un sistema distribuido es la posibilidad de utilizar contratos inteligentes (*Smart Contracts*), automatizando las decisiones en los puntos clave de la cadena de suministro, donde las partes desean visibilidad y transparencia absoluta. Descritos con detalle en el apartado 3.4 de este documento, los contratos inteligentes son reglas lógicas programadas en la cadena de bloques que se ejecutan cuando suceden determinados eventos (e.g. pago automático cuando un lote pasa del proveedor al camión).

Sin embargo, los primeros pilotos existentes en supply chain solo utilizan estos contratos para transacciones generales, de alto nivel (e.g. agilización en el cruce de aduanas) y en pocos o ningún caso para transacciones muy especificas, ¿Por qué?. La respuesta se encuentra en el coste tanto computacional como económico que tiene la ejecución de estos contratos debido a que implican a toda la cadena de bloques. El coste puede ser varios órdenes de magnitud mayor en una blockchain pública que utilizando medios tradicionales (reduciéndose a unas diez veces mayor en el caso de una blockchain privada con permisos especiales entre las partes). La solución que en estos primeros pilotos se considera es una hibridación entre el sistema SaaS para decisiones específicas y blockchain para el resto.

Una de las grandes posibilidades del uso de contratos inteligentes sería la posibilidad de incluir verificaciones en materia de seguridad alimenticia antes de su ejecución,

esto es, verificar antes de la llegada al consumidor que los productos han sido sometidos a los controles y los procesos pertinentes de forma adecuada. La información de esos controles y procesos puede ser introducida en el sistema blockchain y utilizar un sistema SaaS como apoyo ya que facilita la búsqueda de lotes en caso de que se detecte una contaminación o problema en un producto [STEI17]. En caso de encontrarse con algún resultado no deseado, el contrato no se ejecutaría y el lote con productos en los que por ejemplo se ha roto la cadena de frío no sería aceptado por el distribuidor y por tanto no llegaría a los consumidores, evitando posibles intoxicaciones.

Tal y como se ha comentado anteriormente, un sistema híbrido que aúne SaaS y blockchain parece ser la tendencia en la gestión de la cadena de suministro, puesto que el sistema SaaS proporciona la capacidad algorítmica y de procesado mientras que blockchain proporciona la transparencia, validez y verificación de todas las transacciones. Por ejemplo, el sistema SaaS podría realizar las mediciones de los identificadores RFID de un producto y grabar la información en blockchain, lo que eliminaría la necesidad de que una persona introdujese esa información en la cadena de bloques, lo que desemboca en un incremento en la confiabilidad de los datos ya que reduce una gran fuente de error, la acción humana [JUST17].

La implantación de un sistema descentralizado solo es beneficiosa para las partes si todos los partícipes de la cadena de suministro lo implantan, así, uno de los parámetros clave es el coste de implantación y migración. Utilizando un sistema híbrido como el descrito, se consigue una combinación que resulta mucho más efectiva en términos económicos.

5. Caso práctico de aplicación al sector alimentario. El jamón ibérico.

En este apartado se va a realizar una propuesta teórica de implantación de un sistema de gestión de la cadena de suministro del jamón ibérico fundamentado en blockchain. Se va a realizar una descripción del sector porcino para luego proceder a realizar la propuesta.

5.1. Contexto y motivación

El jamón ibérico es probablemente el producto más reconocido de la gastronomía española. Potenciado durante décadas, no cabe duda de que se ha convertido en Marca España. Sin embargo, durante los últimos años ha caído sobre este producto la sombra del fraude.

En Mayo de 2017, el mayor periódico alemán, el *Süddeutsche Zeitung* públicaba un reportaje[16] titulado *Obscenidad en el ibérico* en el que denunciaba como España comete un fraude constante y masivo con los jamones, exportando jamones de cebo como si fuesen de bellota. Dicho artículo cifraba como fraudulentas un 90% de las piezas de ibérico que se venden en el extranjero.

Por este motivo, el caso de aplicación seleccionado es el sector del jamón ibérico. Es un sector importante, que genera 800 millones de euros anuales y emplea casi 100.000 personas de forma directa e indirecta. La cadena de suministro en este sector se enfrenta a dos retos:

- El jamón es un alimento y como tal debe cumplir unos estándares muy elevados de calidad, tiene unos tiempos, temperaturas y otros parámetros de procesado que deben ser controlados y verificados para evitar que jamones contaminados puedan llegar al consumidor

- La sombra del fraude que destapó el citado artículo supone un mayor control de las autoridades, por lo que las certificaciones, el etiquetado y la trazabilidad se vuelven esenciales

[16] http://www.sueddeutsche.de/wirtschaft/report-schweinerei-1.3512914

Es en este contexto, donde, por todo lo que aporta a la trazabilidad y la confiabilidad de los datos, la sustitución de la gestión de la cadena de suministros tradicional por una descentralizada basada en blockchain puede ser de gran utilidad para el sector del jamón.

5.2. AS-IS. El sistema actual

En este apartado del documento se va a realizar una presentación del sector porcino en España, cuyo objetivo es contextualizar para aportar posteriormente una visión general del estado actual (AS-IS) de la cadena de suministro del jamón ibérico.

5.2.1. El sector porcino ibérico

Antes de comenzar a definir la cadena de suministro actual del jamón ibérico, es necesario realizar una introducción al sector porcino. En particular, es necesario definir la cadena de valor del sector, las distintas categorías existentes en los animales y en los productos, así como las posibilidades de etiquetado y trazabilidad.

5.2.1.1. Cadena de valor del sector porcino

El actual ecosistema empresarial de cualquier sector esta formado por una red de empresas que interactúan y compiten entre ellas. En este contexto, adquiere gran relevancia la gestión de las actividades realizadas por las distintas empresas ya que se encuentran interrelacionadas y sus intereses deben estar alineados con el fin de llegar al consumidor y adquirir la mayor cuota de mercado posible.

El concepto de cadena de valor nace en 1985, de la mano de Porter, que define una herramienta para identificar las actividades generadoras de ventaja competitiva, de valor para una empresa. Este valor debe entenderse como el precio que los consumidores están dispuestos a pagar por el producto final, por lo que la empresa debe añadir suficiente valor a las materias primas como para que el precio de venta sea mayor que los costes de añadir dicho valor.

Las actividades que aportan valor son aquellas que desmarcan física, estratégica o tecnológicamente a una empresa en sus procesos de negocio. Las ventajas competitivas hacia las que se dirige una empresa son liderazgo en costes, o diferenciación, asegurando innovación y calidad.

En *Competitive strategy: Techniques for analyzing Industries and Competitors* (Porter, 1985) se describe la cadena de valor de una empresa dividida en:

- Actividades primarias: Logística, operaciones, ventas, etc.

- Actividades de soporte: Aprovisionamiento, RRHH, etc.

Es imprescindible que las dos tipologías de actividades se desarrollen de forma correcta en el momento preciso para que la transformación de materias primas en producto final sea satisfactoria y la empresa consiga un margen económico.

Figura 16. Cadena de valor (Porter, 1985)

Porter también hace referencia al ecosistema que rodea a la compañía, argumentando que la obtención de ventajas competitivas no depende únicamente de la empresa, sino de la comprensión del entorno y del encaje de la misma. Las empresas no se encuentran aisladas si no que se encuentran en el denominado Sistema de valor, que engloba, desde el proveedor al comprador, todo el ciclo de vida de un producto.

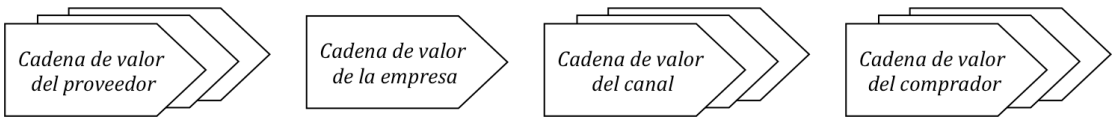


Figura 17. Sistema de valor de un sector

Los conceptos definidos por Porter hace más de treinta años han evolucionado, hasta definir valor en los complejos ecosistemas empresariales actuales, donde los flujos no son lineales y hay multitud de empresas implicadas en todos los procesos existentes. Estos análisis, que extienden el análisis de valor dentro de una empresa a actividades entre compañías de varios sectores no se incluyen porque no resultan de interés en este proyecto, ya que el sector porcino español es analizable desde un punto de vista unisectorial siguiendo el esquema de valor propuesto por Porter.

5.2.1.2. Calidad en el sector porcino

En el Real Decreto 4/2014 se aprueba la norma de calidad para el jamón ibérico, donde se definen todas las características, parámetros y componentes de la materia prima, los procesos y el producto final.

La norma de calidad establece las distintas categorías de producto (jamón) en función de la raza y la alimentación suministrada al animal. La alimentación durante la etapa de cebo será la que defina la calidad del producto final, así como la posibilidad de vender el producto en una categoría u otra.

En función de la raza, se definen:

1. *Ibérico puro*: La pieza se obtiene de animales con progenitores inscritos en el libro genealógico de la raza porcina ibérica, un registro oficial de la asociación de criadores.

2. *Ibérico*: La pieza se obtiene de un animal que es cruce de raza porcina ibérica y de raza porcina Duroc, con el cumplimiento de unos requisitos que escapan al ámbito de este proyecto. Dentro de ibérico se pueden diferenciar 75% y 50% ib

En función de la alimentación se definen:

1. *De bellota*: Productos elaborados a partir de animales que han sido alimentados exclusivamente con bellotas, hierba y demás recursos naturales de la dehesa sin alimentación suplementaria.

2. *De cebo de campo*: Productos elaborados a partir de animales con una alimentación basada en piensos, con un complemento de alimentación en dehesa de 60 días, durante la cual también reciben pienso

3. *De cebo*: Productos elaborados a partir de animales con una alimentación basada en piensos

Para cada categoría, se establecen una serie de requisitos y características que se deben cumplir tanto en la crianza como en el animal propiamente dicho, y que en el presente trabajo no se describen por escapar al ámbito del mismo.

5.2.2. La cadena de suministro del jamón ibérico.

La cadena de suministro del jamón ibérico no se encuentra definida por la regulación. La cadena que se muestra en la Figura 18 es el resultado agregar la información obtenida a través de entrevistas a profesionales y personas cercanas al sector.

En este apartado se muestra y se analizan los diferentes eslabones de la cadena, describiendo los procesos más significativos que además se encuentran regulados y controlados y que pueden resultar de interés en la recolección de datos para la correcta gestión de la cadena de suministro.

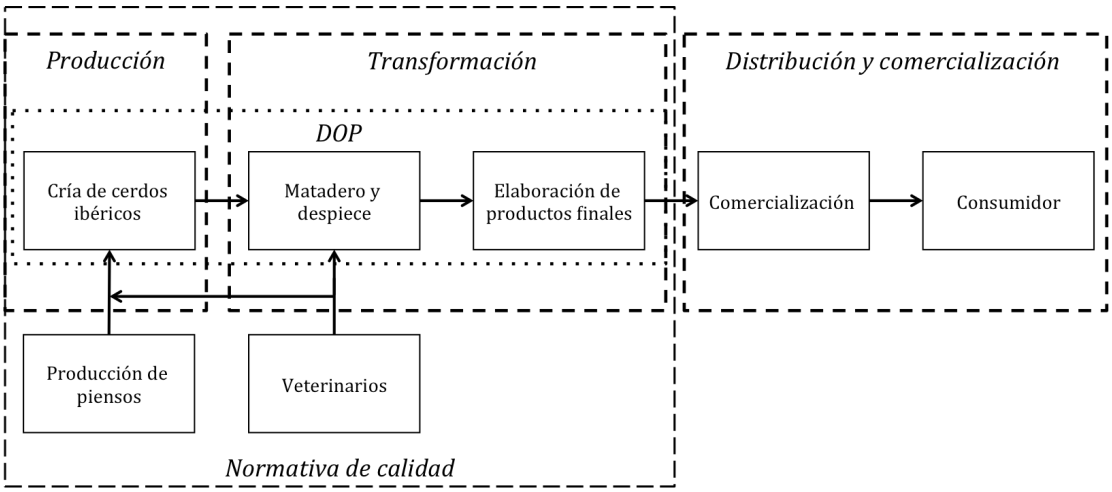


Figura 18. Cadena de suministro del jamón ibérico. Elaboración propia

La producción implica la cría y alimentación del cerdo, que se realiza en las dehesas. Existen numerosas asociaciones que ofrecen asesoramiento y distintos servicios a los ganaderos, como es el caso de AECERIBER (Asociación Española de Criadores de Ganado Porcino Selecto Ibérico Puro y Tronco Ibérico), que se encarga del libro genealógico en las explotaciones con ibérico puro. Para garantizar la máxima calidad, distintos partícipes realizan inspecciones y verificaciones en este eslabón de la cadena:

- *Veterinarios*: Realizan las inspecciones según se establece en la norma de calidad para establecer la alimentación recibida por los cerdos durante el engorde. Son los encargados de realizar informes para la trazabilidad de los cerdos.

- *Entidades inspectoras*: Realizan inspecciones en las dehesas, certificando su idoneidad para la alimentación de los animales. Además, realizan las inspecciones pertinentes recogidas en la norma de calidad, certificando raza,

edad y alimentación de los cerdos, que, junto con la identificacióservirá para evitar el fraude en su venta.

En el bloque de transformación se agrupan todos los procesos que sigue el jamón desde el sacrificio hasta el producto final. En el matadero se sacrifica al animal, cumpliendo las reglas sanitarias y de calidad. Para cumplir los requisitos de las DOPs (Denominaciones de Origen Protegidas) y disminuir el riesgo de fraude, no pueden coincidir en el matadero animales pertenecientes a la DOP con otros que no. Además, debe mantenerse la trazabilidad en las salas de despiece, esto se realiza mediante la aplicación de una marca indeleble en las piezas. Todos estos procesos son certificados por empresas externas registradas en la DOP. Cabe destacar que a día de hoy siguen existiendo contratos verbales entre las explotaciones y los mataderos, lo que supone una importante desventaja en cuanto a trazabilidad se refiere.

En la planta de elaboración, el proceso seguido por los jamones se puede observar en la Figura 19.

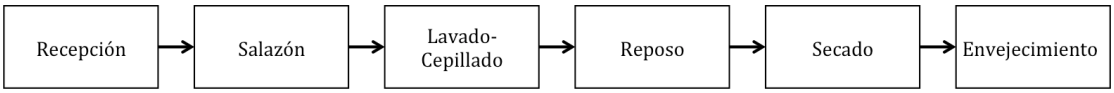


Figura 19. Procesos del jamón en la industria elaboradora

El detalle de los procesos se escapa al ámbito del proyecto, sin embargo, es importante destacar los parámetros aplicables a cada uno recogidos en la norma de calidad, pues serán la base de la recolección de datos a verificar por la organización pertinente.

	Recepción	***Salazón***	***Lav.-Cep.***	***Reposo***	***Secado***	***Envejecim.***
Humedad relativa (%)	70-80	75-95		70-95	55-85	60-90
Temp. (ºC)	5,5-10,5	0-4		0-6	6-26	12-22
Otros		0,62-2 días/kg		40-60 días	180 días	115 días

Tabla 4. Detalle parámetros a controlar en industria elaboradora

Cabe destacar que los parámetros recogidos en la tabla son generalistas y que se detallan los intervalos más amplios, pues en muchos procesos, la temperatura y la humedad relativa deben ir variando con el paso del tiempo.

Una vez los jamones abandonan la industria, lo hacen con el etiquetado de producto según corresponda.

En el bloque de comercialización, se pueden distinguir los distintos canales de distribución de la industria; venta a mayoristas, a minoristas, exportaciones, venta directa por internet y la red Horeca (HOteles, REstaurantes y CAfés).

Una vez en el eslabón de comercialización, solo es cuestión de tiempo que llegue al consumidor final. El proceso seguido por el jamón es largo, implica a muchos partícipes y aunque se han reforzado las medidas de trazabilidad y transparencia, existe margen para conseguir una mejora.

5.2.3. Certificaciones, etiquetado y trazabilidad.

En el sector agroalimentario español existen una gran variedad de sistemas de certificación, para el caso concreto del jamón ibérico, el sistema más representativo es la DOP (Denominación de Origen Protegida). Se aplica en productos cuya producción, transformación y elaboración se realicen en el entorno geográfico al que esta vinculada, con unos conocimientos reconocidos y comprobados. En España, existen varias DOP para el jamón ibérico:

- Los Pedroches
- Jabugo
- Dehesa de Extremadura
- Guijuelo

Con este sistema, se añade valor por el reconocimiento de marca a los productos de alta calidad procedentes de un área geográfica determinada.

En cuanto al etiquetado, la normativa establece que además de cumplir con los requisitos propios de un producto cárnico, existen requisitos exclusivos para el jamón ibérico.

El etiquetado de los jamones se compone de varios tipos de etiquetado, algunos son obligados por la norma y otros suponen una certificación de la calidad del producto. A continuación se describen los más relevantes.

- *Etiqueta o vitola*. Incluye la denominación de venta. Se compone de tres designaciones obligatorias y designa la procedencia y calidad del producto. Para una correcta denominación de venta debe figurar:

    - Designación de tipo de producto (jamón, paleta, lomo, etc.)

- Designación racial (ibérico 100% o ibérico X% según las características ya descritas)
- Designación de tipo de alimentación (bellota, cebo de campo, cebo)

En la denominación de venta, debe ir incluido el organismo de control y certificación. Además, la norma establece que la expresión "pata negra" queda reservada a los productos de bellota 100% ibérico)

Figura 20. Ejemplo de etiquetado con denominación de venta

- *Precintos*. Es una brida de plástico que va sujeto a la caña del jamón. Si el jamón se encuentra bajo la normativa, debe aparecer el logotipo de ASICI (Asociación Interprofesional del Cerdo Ibérico). Se distinguen cuatro colores (Figura 21):

  - Negro: Jamón de bellota 100% ibérico
  - Rojo: Jamón de bellota ibérico
  - Verde: Jamón de cebo de campo ibérico
  - Blanco: Jamón de cebo ibérico

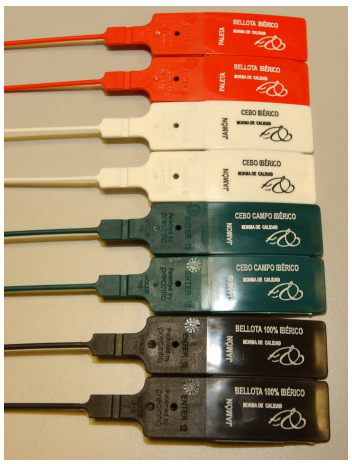


Figura 21. Ejemplo de precintos

Adicionalmente, si el jamón corresponde a una DOP, deberá aparecer el logo de la misma. Actualmente, existen precintos propios de cada DOP (solo en colores negro, rojo y verde), que pueden presentarse en lugar de los precintos de la norma (Figura 22)

Figura 22. Precintos propios de cada DOP

Además de estas dos formas de etiquetado, existen el sello MAPA y el sello SIV, impresas en la pieza tal y como puede observarse en la Figura 23.

El sello MAPA está compuesto por cuatro números. Los dos primeros indican la semana y los segundos el año de inicio de la curación del jamón. 1213 correspondería a un jamón que ha iniciado su curación la semana 12 del año 2013. Cabe destacar que este sello no es obligatorio, por lo que puede o no aparecer en los jamones.

El sello SIV (Servicio de Inspección Veterinaria) es un sello en forma de óvalo que se pone a la pieza y que indica el país se sacrificio, el numero de registro sanitario del matadero, la provincia en la que se ha sacrificado y las siglas de la Comunidad Europea.

Figura 23. Detalle sellos SIV (superior) y MAPA (inferior)

Durante toda la producción se llevan a cabo controles de calidad, definidos en la norma según el número se animales sacrificados anualmente. Además, cada pieza queda identificada mediante todo el etiquetado descrito, la trazabilidad existente en el jamón ibérico es el resultado de la exigencia del mercado, que demanda la certificación de la procedencia del producto.

La trazabilidad es el resultado de una serie de controles, inspecciones e identificaciones que se llevan a cabo a lo largo de toda la cadena de valor de la producción de jamón.

- *Producción*: Se realizan inspecciones en la explotación porcina para el control de calidad, se verifican las parcelas y dehesas, se verifica la identificación de los animales mediante un código único, informando de la raza, edad y alimentación de los cerdos antes de su sacrificio.

- *Matadero*: Se comprueba el peso mínimo y la correcta identificación de cada animal. Durante el despiece, se mantiene una trazabilidad entre cada pieza y el animal de procedencia.

- *Elaboración*: En la industria elaboradora, se mantiene, mediante la identificación de los productos, la trazabilidad con su procedencia, quedando ligado cada producto final a una pieza que a su vez está ligada al animal.

- *Distribución y venta*: Se mantiene la información dada por la industria elaboradora. Idealmente, se añade información sobre el transporte, almacenaje y venta.

Desde la aplicación de la norma de calidad, la transparencia del sector porcino se ha incrementado. Sin embargo, la debilidad de esta norma en cuanto a trazabilidad viene dada por la dependencia en entidades inspectoras y certificadoras que se encargan mayoritariamente de la inspección en producción y elaboración, dejando de lado el etiquetado para la venta, que es uno de los mayores problemas y que favorece la aparición del fraude.

Asimismo, la existencia de diversas asociaciones, con intereses propios e influencia política, hace que los etiquetados no sean excesivamente claros, manteniéndose las designaciones ibérico 100% e ibérico x%, cuando existe una demanda por parte de los

productores del sur de España de cambiar la designación a ibérico y cruce de ibérico respectivamente.

5.2.4. Influencia del etiquetado en el consumidor

Las crisis y escándalos alimenticios padecidos durante los últimos años han cambiado los hábitos del consumidor, desplazando a este a buscar alimentos de mayor calidad y seguridad alimentaria [ZAPA13]. Según diversos estudios [VERB05] los consumidores desean información para lograr una dieta equilibrada, evitar alérgenos, conocer la procedencia de los alimentos, etc. La seguridad alimentaria de ha convertido en parte integral de la calidad y es de gran importancia en la decisión de compra del consumidor.

El objetivo del etiquetado debe ser reducir la asimetría de información en la cadena de valor, por la cual el productor tiene más información que el comprador sobre el origen, procesado o contenido nutricional de un producto. Sin embargo, aunque la información esté disponible y sea gratuita, los consumidores no acceden a ella por regla general, ya que el coste de adquisición y procesado de toda la información de todos los productos que una persona consume no es mayor al beneficio esperado. [VERB05] Así, aunque el etiquetado es el canal de referencia en cuanto a calidad y seguridad alimentaria, los medios de comunicación juegan un papel muy relevante en la percepción de los productos.

Cabe destacar que los consumidores suelen tener dificultades para comprender la información presentada en el etiquetado y para suplir eso, los consumidores prefieren comprar marcas de calidad reconocida antes incluso que marcas ecológicas.

Así pues, para los consumidores es importante la información y la posibilidad de acceso a ella, pero no están dispuestos a pagar un precio más alto por presentar más información que no les resulta relevante.

En concreto, en el caso del jamón ibérico, el estudio *The role of protected designation of origin in consumer preference for iberian dry-cured-cured ham in Spain* de 2010 encabezado por Francisco J. Mesías asegura que el mercado del jamón se compone de consumidores que pertenecen a un nicho elitista y exigente. Tan solo un 6% de los jamones comercializados están acogidos a una de las DOPs existentes, que elevan la percepción de calidad. Además, la raza ibérica y la designación de bellota son, para el consumidor, garantías en si mismas de una mayor calidad del jamón.

5.3. TO-BE. Gestión mediante blockchain

En este apartado se va a proponer un sistema de gestión de la cadena de suministro del jamón haciendo uso de la tecnología blockchain.

5.3.1. Gestión mediante blockchain

Tal y como se ha descrito en el capítulo 3 de este documento, la tecnología blockchain no es más que una base de datos encriptada y distribuida que permite la confianza entre las partes sin necesidad de un tercero. Además, por las características ya descritas en el apartado mencionado, esta tecnología se vuelve ideal para aplicaciones relacionadas con la trazabilidad. En la Figura 24 se ilustra a modo resumen el proceso seguido en cada transacción .

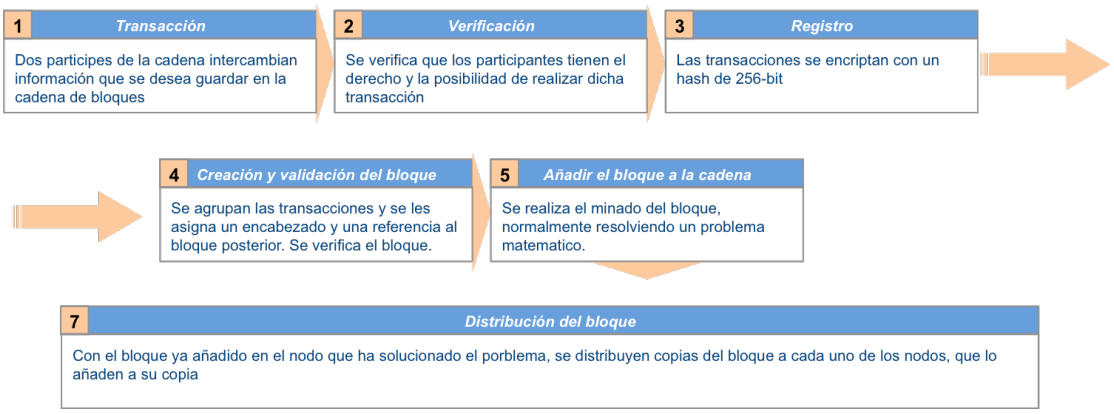


Figura 24. Esquema de registro de una transacción

En cada una de las transacciones entre partícipes, el producto, en este caso jamón puede sufrir algún tipo de alteración o cambio que lo haga fraudulento. Para evitar esto, el sistema de trazabilidad basado en blockchain podría crear un token en el primer eslabón de la cadena, de forma que al llegar al cliente este pueda verificar el token, asegurando la veracidad del producto. Esta tecnología se aplica ya en el mundo de los diamantes mediante el proyecto Everledger, en colaboración con el banco Barclays, sin embargo, la aplicación de un sistema similar en el sector del jamón resulta novedosa.

La implementación de blockchain significaría la asignación a cada jamón de un pasaporte virtual, creando un registro auditable de cada uno de los pasos seguidos por ese producto hasta que llega al consumidor, evitando el fraude y previniendo las posibilidades de contaminación masiva.

En el caso especifico del jamón, en la cadena de suministro intervienen varios participantes, que deben trabajar alineados para conseguir que todo quede registrado en la blockchain y su implementación constituya un éxito. Estos participantes son:

1. *Productores*. En referencia a los dueños de las explotaciones porcinas
2. *Industria elaboradora*. Distinguiendo entre matadero y elaboración
3. *Comercialización*. Incluyendo todos los canales de distribución
4. *Certificadores y auditores*
5. *Consumidores*
6. *Asociaciones* (debido al elevado numero de las mismas, su inclusión en la blockchain no se considera en el modelo propuesto)

Cada uno de estos participantes debe gestionar todos los datos referentes a su proceso e incluir lo que sea de interés en el registro de la cadena de bloques.[PROV15] Además, como cualquier cadena de bloques dedicada a gestionar una cadena de suministro, debe contar con la siguiente arquitectura modular:

- *Registro*: En este módulo los distintos participantes quedan registrados. Introducen todos los datos requeridos para la correcta identificación de cada uno posteriormente. Es el módulo que asegura un link entre la identidad digital y la física de los participantes. Si por alguna razón algún participante desea permanecer en el anonimato, se puede llevar a cabo, pero a costa de la transparencia de la cadena de suministro.

- *Producción*: Este es el módulo dedicado a los registros de la producción. Registra tanto datos y características de los productores como de los productos (e.g. hectáreas dedicadas a la producción, número de cerdos, descripción del animal y del jamón). Este módulo es la base sobre la que se sustenta el resto, ya que cuando un cliente quiera conocer el origen del producto, la cadena de suministro le mostrará información recogida en este módulo y por ello, algún certificador externo debería ser el encargado de gestionarlo.

- *Elaboración*. Se distingue entre los mataderos y la industria que elabora el producto final. En este módulo se registran todos los datos relativos tanto a los controles sanitarios y de cualquier otra índole que la regulación exija como las etapas por las que pasa el producto, con los parámetros más importantes de las mismas (e.g. temperaturas, humedad relativa, tiempos, etc.)

- *Distribuidor*. Se incluye en este módulo todo el registro relativo a la logística y la comercialización. Debe quedar registrado el canal de venta, las etapas por las que pasa el producto, el tiempo en cada una de ellas, etc.

Esta es la estructura que el sistema de gestión debe tener, con información relativa a todas las etapas de la cadena de suministro, accesible en gran medida por el consumidor y por las autoridades en caso requerido. Sin embargo, los registros digitales por si solos no garantizan la veracidad de los datos registrados, es necesario establecer un sistema que conecte el mundo digital con el físico, este sistema es el etiquetado del producto.

Un sistema de etiquetado que identifique unívocamente a un producto es vital para el correcto funcionamiento del sistema de trazabilidad. Por ello, se propone como tecnología de etiquetado, la aplicación de tecnología RFID.

Descrita con detalle en el apartado 2.2, esta tecnología posee tres características perfectas para el uso deseado:

1. Sirve de identificación única mediante codificación. Utilizando dicho código encriptado mediante una función hash, este código puede actuar como un puntero para recoger toda la información existente en los diferentes registros guardaos a lo largo de la cadena de suministro. Para el consumidor, esto es lo que le permitiría conocer toda la información relativa al producto concreto que está adquiriendo.

2. La tecnología RFID permite almacenar datos, pero no sólo eso, también ir añadiendo y actualizando los datos guardados a lo largo de la cadena. Así, con esta tecnología se pueden recoger datos de temperatura y humedad, críticos en distintas etapas de la cadena de suministro y comprobar que en ningún momento se han salido de los límites establecidos.

3. La captura de los datos con esta tecnología es automática, tal y como recomienda GS1 para un sistema de trazabilidad.

Finalmente, es necesario un sistema mediante el cual el cliente tenga acceso a la información almacenada en la cadena de bloques. Es necesario un sistema que no suponga un gran esfuerzo o sea tedioso para el consumidor. Se propone una aplicación para *smartphone* que mediante la lectura de un código QR o similar en el

etiquetado, muestre toda la información del producto (aquella que resulte de interés para el cliente, no toda la disponible).

Cabe destacar que el éxito de este sistema de trazabilidad depende en gran medida del registro inicial de todos los partícipes, pues sin ese correcto registro no es posible realizar un correcto *tracking* del producto. Asimismo, el sistema carece de sentido sin el registro de las transacciones por parte de los distintos partícipes.

De las conversaciones mantenidas con trabajadores de empresas del sector cabe mencionar la opacidad del sector, donde algunos partícipes de la cadena podrían ser recelosos de compartir toda la información con el consumidor por el acceso que la competencia ganaría. Para subsanar este problema, además de compartir con el cliente solo la información necesaria para certificar el origen y el camino seguido por el producto, sería posible no identificar a ciertas empresas de cara al cliente, mientras que este podría seguir confiando en la información almacenada en al cadena. Siendo toda la información accesible solo a certificadores, auditores y autoridades que lo requieran.

5.3.2. Modelo de implantación

En el apartado anterior se ha descrito el funcionamiento del sistema a implantar. Sin embargo, existen diferentes modelos de soluciones que cumplirían los requerimientos descritos.

En la elección de un sistema de trazabilidad basado en blockchain en el sector alimentario debe tenerse en cuenta principalmente que el un coste por sea bajo. Cabe mencionar que el nivel de seguridad requerido es menor que en el caso de sistemas basados en blockchain para el sistema financiero. Esto es debido a que los activos como Bitcoin basados en blockchain tienen un valor intrínseco asignado por el mercado, sin embargo, si alguien consiguiese ilegítimamente la identidad virtual de un producto alimentario, seguiría sin poseer ese producto físicamente. Esta demanda más relajada de seguridad abarata mucho los costes de transacción.

Para la implementación del sistema de trazabilidad, se ha realizado una búsqueda de plataformas disponibles dedicadas a la gestión de cadenas de suministro agroalimentarias mediante blockchain. Cabe destacar Hyperledger. Pensada inicialmente para grandes compañías (los primeros pilotos se lanzaron con los almacenes estadounidenses Wal Mart), actualmente esta abierta para cualquier empresa, con unas tarifas verdaderamente asequibles. Es la que mayores facilidades

tiene para la integración con sistemas actuales e incorpora estándares GS1. Existen otras compañías más pequeñas, entre las que destaca Ripe, dedicada a la gestión de la cadena de suministro con mucho detalle, especialmente útil cuando los parámetros de la cadena de suministro son vitales para el consumidor y el vendedor (e.g. cadenas de frio en marisco). En el caso de aplicación propuesto se recomienda la utilización de Hyperledger, por ser la pionera y más reconocida, fácilmente accesible y contar con el soporte de grandes multinacionales.

Cualquiera de las empresas proveedoras de soluciones basadas en blockchain funcionan de modo similar, constando de:

1. *Interfaz de usuario.* Distingue entre los distintos tipos de usuario existentes a lo largo de la cadena de suministro:

    - *Consumidores*. Interfaz basada en aplicación para Smartphone con permiso de lectura (el consumidor no debe ser capaz de introducir registros en la cadena de bloques). La lectura se puede realizar mediante un código QR y la información mostrada depende de los partícipes de la cadena.

    - *Partícipes en la cadena*. Cada uno de los partícipes de la cadena, desde el productor hasta el distribuidor tendrá una interfaz de usuario propia, con acceso propio o integrado en el sistema ERP. Cada uno de los partícipes podrá acceder a la información que hayan introducido el resto en etapas pasadas de la cadena de suministro.

2. *Servidores propios.* No todos los partícipes querrán compartir toda la información con todos los partícipes de la cadena (e.g. La industria elaboradora puede recibir productos procedentes de varios proveedores y estos deben ser solo capaces de acceder a la información de sus productos, no del resto de competidores). Así, es bueno y en muchos casos necesarios que existan sistemas de almacenamiento de datos propios de cada empresa, para poder decidir qué datos y cómo se comparten con el resto de participantes a través de la blockchain. Así, cada empresa seguiría teniendo el control total de sus datos, pudiendo gestionar los permisos de acceso a los mismos según considere.

3. *La cadena de bloques (blockchain).* La base de datos distribuida donde se van a almacenar los registros de todos los participantes (que actuarán como nodos). Como se ha comentado en apartados anteriores, es recomendable el uso de una blockchain privada, para poder gestionar los permisos de los nodos, de forma que solo los nodos registrados y verificados puedan validar transacciones y bloques. Además, el coste por transacción en una cadena de bloques privada es mucho menor que en una pública como Bitcoin o Ethereum. Como ya se ha mencionado, por antigüedad, facilidad de uso y por ser la más extendida, se recomienda el uso de Hyperledger como sistema de gestión de la blockchain privada.

4. *Registro.* El registro de los diferentes partícipes debe ser seguro y verificable. Desarrollar un sistema que lo permita sería una tarea con un coste enorme que no sería rentable para ninguna empresa del sector. Sin embargo, las empresas que ofrecen soluciones para la integración, suelen ofrecer los sistemas necesarios para hacer que los registros de los diferentes actores sean veraces y seguros. Además, las asociaciones que sean necesarias en la cadena de suministro también pueden registrarse para auditar y verificar que se cumplen las condiciones del producto para que lleve su certificación.

En cuanto al funcionamiento de estos sistemas, conceptualmente, se pueden distinguir dos funciones:

- *Certificación de origen.* A día de hoy, las certificaciones de origen las realizan organizaciones como las DOPs. El sistema es tedioso y las inspecciones frecuentes, además, las instalaciones que no pertenecen a una DOP, pueden carecer de certificación de origen. Con la implementación de blockchain, pequeñas explotaciones independientes podrían certificar la procedencia de sus productos de forma más sencilla. Podrían registrar en la cadena de bloques el estado de las instalaciones y todos los datos que consideren necesarios. Posteriormente, cualquier certificador independiente (e.g. notario), podría comprobar que los registros de la cadena de bloques corresponden a la explotación.

- *Trazabilidad en la cadena de suministro.* Es donde se concentra el mayor potencial de esta tecnología, pues es posible localizar y *trackear* cualquier producto al que se le haya asignado una identificación. Además, con la tecnología RFID es posible automatizar estos registros, eliminando el factor

humano, que supone una gran fuente de error y encarece el proceso. Por ser un estándar se propone que las identificaciones de los productos se realicen de acuerdo a las normas establecidas por GS1, como ya sucede en gran parte de otros sectores alimentarios. Además, en caso de que se requiera, es posible conocer la identidad de cada partícipe detrás de cada transacción. Cada participante en la cadena conocerá el código de los participantes de etapas anteriores o no, según considere cada participante, ya que es posible registrar dichos códigos encriptados.

Con esta solución, el control sobre los jamones sería prácticamente total. El riesgo de fraude muy pequeño ya que se eliminaría el riesgo en todo el proceso, la única ventana existente sería en la producción (alimentación de un cerdo con pienso y que el productor lo registre como bellota) sin embargo, además de ser una posibilidad con los sistemas actuales, es combatible mediante inspecciones y controles independientes.

En detrimento de este sistema de encontraría el coste económico, que para un sector que sale de una crisis puede suponer un gran impacto. Podría mitigarse este coste mediante regulación o con un incremento del precio si el cliente está dispuesto a pagar más por un jamón que cuente con este sistema.

5.3.3. Ejemplo de funcionamiento de la solución elegida

A continuación se describen paso por paso las acciones necesarias para que el sistema tenga éxito:

1. Registro de los animales y certificación de origen

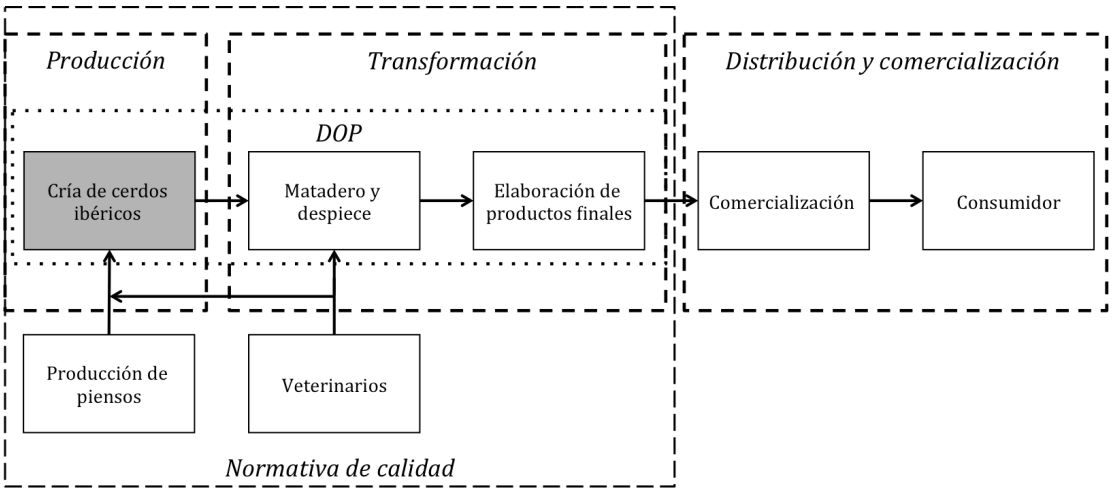


Figura 25. Funcionamiento solución I

Estado anterior	*Descripción*	*Estado posterior*
No aplica	Se realiza la identificación de los animales con chips RFID en la oreja. Además, se realiza la certificación del origen de los animales.	Los animales quedan unívocamente identificados y registrados y la explotación de origen certificada. La certificación de origen es registrada en la blockchain.

Tabla 5. Funcionamiento solución I

2. Registro transporte animales vivos

3. Registro de dos etiquetas RFID y link con animal

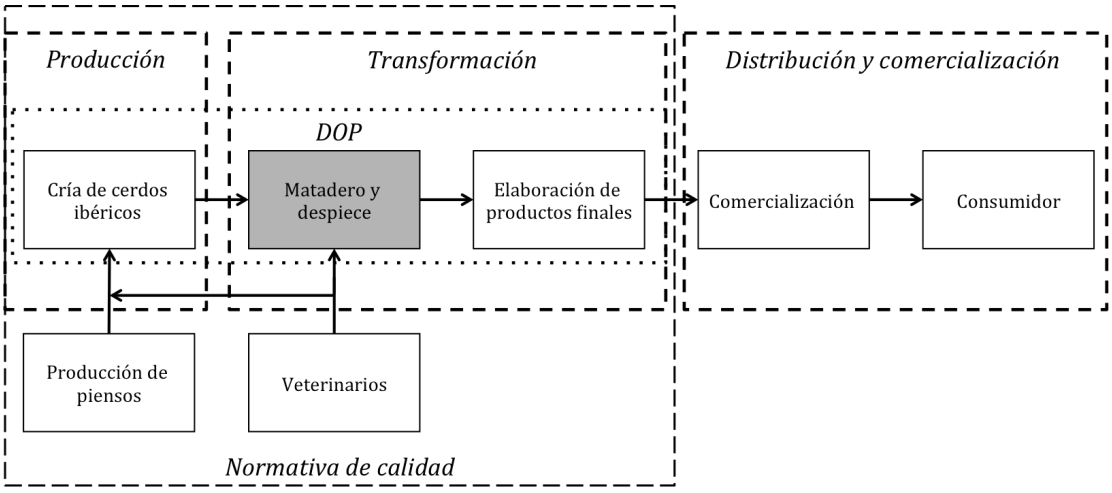


Figura 26. Funcionamiento solución II

Estado anterior	*Descripción*	*Estado posterior*
El animal está identificado	Se registran dos etiquetas RFID con sensores de temperatura y humedad. Se etiquetan los jamones con dichas etiquetas. Se registra el código del animal y se relaciona con las dos etiquetas RFID.	Las etiquetas RFID que se asignan a los jamones se encuentran relacionadas con un animal en concreto.

Tabla 6. Funcionamiento solución II

4. Registro transporte de los jamones

5. Elaboración de productos finales

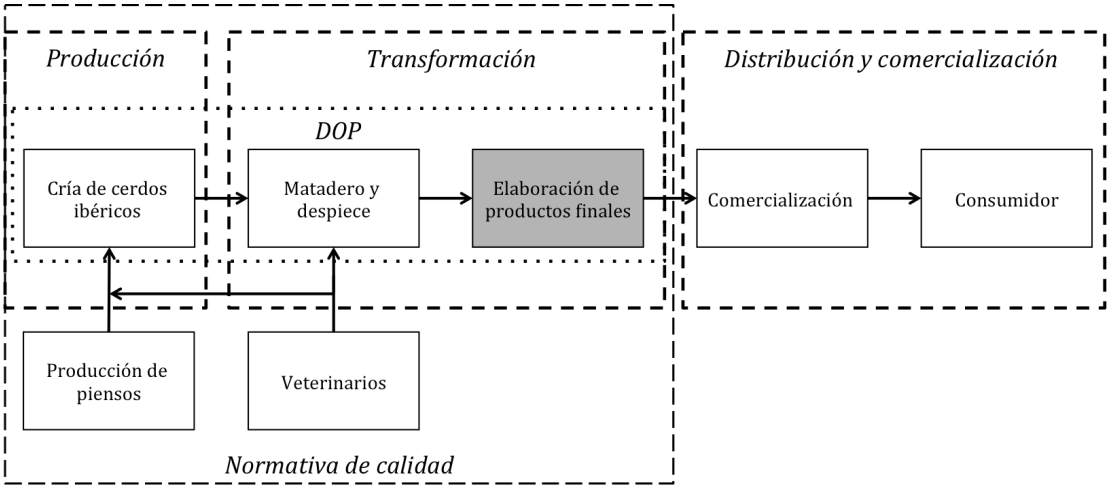


Figura 27. Funcionamiento solución III (a)

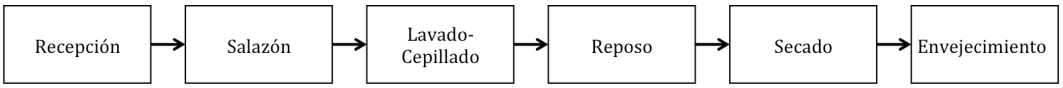


Figura 28. Funcionamiento solución III (b)

Estado anterior	*Descripción*	*Estado posterior*
Los jamones se encuentran registrados.	Se realiza la toma de datos continua temperatura y humedad relativa mediante los sensores RFID. En las diferentes etapas se mide el tiempo transcurrido.	Las diferentes etapas y sus principales parámetros quedan registrados. El producto final abandona la industria.

Tabla 7. Funcionamiento solución III

6. Registro transporte de producto final
7. Distribuidor

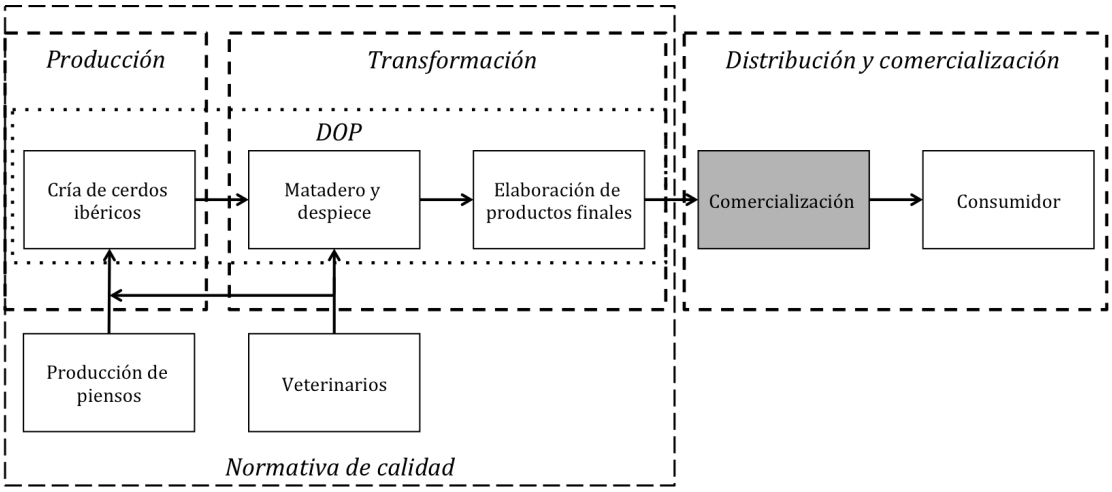


Figura 29. Funcionamiento solución IV

Estado anterior	*Descripción*	*Estado posterior*
El producto final se encuentra registrado	Se realiza la lectura de los RFID de los jamones recibidos, el control de calidad pertinente y se da de alta en inventario. Generación etiqueta QR con la información accesible al consumidor.	El jamón se encuentra dado de alta en el inventario de la tienda y registrado. El jamón se encuentra etiquetado con un código QR que posibilita al lector el acceso a la información del producto.

Tabla 8. Funcionamiento solución IV

8. Consumidor

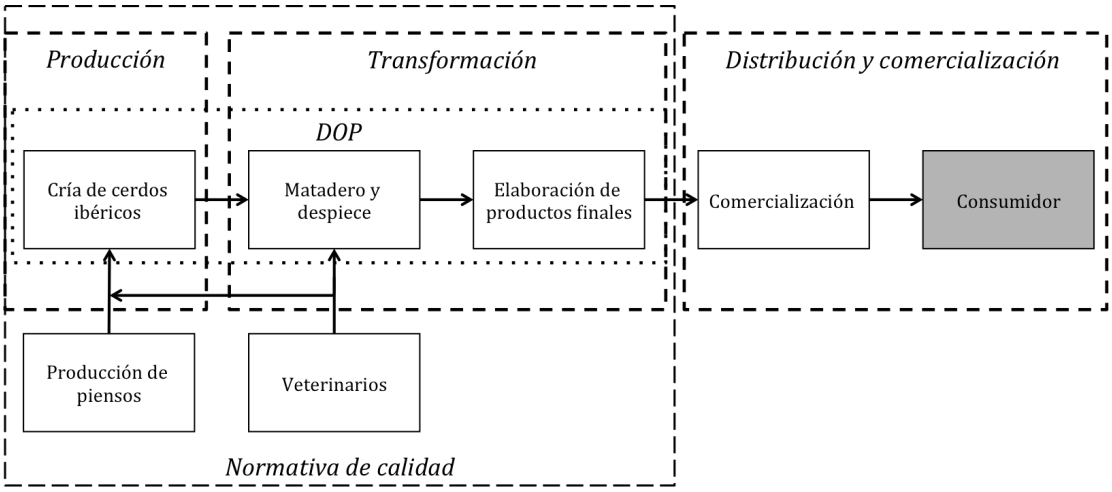


Figura 30. Funcionamiento de la solución V

El consumidor adquiere el producto, pudiendo visualizar la información de la cadena de suministro que los partícipes habiliten.

En las etapas 2, 4 y 6, que constituyen los transportes entre los diferentes agentes de la cadena, se registra el medio de transporte donde viaja el producto (animal o jamón), el origen, el destino y tiempos de salida y llegada.

Cabe también mencionar que en cada una de las etapas se debe registrar la entrada y la salida del producto.

5.4. Evaluación de la solución

5.4.1. Análisis económico de la solución propuesta

En este apartado se va a realizar un análisis económico de la solución propuesta. Al tratarse de un proyecto teórico, el análisis económico se basa en hipótesis que se irán detallando a lo largo del apartado.

En el apartado se estudian por un lado los costes asociados a la inversión, que son considerados como *one-off* y los costes recurrentes que se generan con el nuevo sistema de gestión. Además, con el fin de establecer un *payback* razonable para la inversión se realizan hipótesis que dan lugar a distintos escenarios.

El cálculo de la inversión inicial se realiza bajo el supuesto de que es una sola empresa la que controla toda la cadena de suministro. Realmente, existen muchas empresas implicadas, por lo que la inversión inicial por empresa sería menor.

La inversión inicial se reparte entre las siguientes partidas:

- *Etiquetas RFID*: Solo se consideran las etiquetas correspondientes al primer año, en años sucesivos se considerarán gastos corrientes. Para calcular el número de etiquetas que harían falta, se toma como referencia el número de jamones comercializados por cada explotación porcina.

  Según los datos proporcionados directamente por la DO Guijuelo, en 2017 se comercializaron un total de 177.010 jamones y paletas, procedentes de 371 explotaciones registradas, lo que arroja un resultado medio de 477 jamones comercializados por explotación. Se supone entonces una comercialización de 477 jamones (Información proporcionada por la dirección de certificación de la DO Guijuelo).

  El sistema RFID descrito debe llevar integrados los sensores de temperatura y humedad relativa. Realizando una búsqueda de los modelos disponibles en el mercado, se selecciona el sensor Farsens Hydro-H1401-DKSWB[17], cuyo rango de funcionamiento se ajusta a lo necesario. El precio unitario de venta al público es de 20€ (nótese que no se tienen en cuenta posibles descuentos por compra de volumen) esto supone un gasto total para la explotación de 477*20=9.540€ en sensores RFID.

[17] www.farsens.com/wp-content/uploads/2016/10/DS-HYDRO-H401-V02.pdf

- *Lectores RFID.* Además de los sensores, es necesario contar con lectores de RFID que además puedan registrar nueva información en la etiqueta. Se deben incluir como mínimo, sensores en cada entrada y salida de las etapas del proceso. Descomponiendo las etapas de la industria elaboradora, la cadena de suministro cuenta con un total de diez etapas sin contar con los transportes de una a otra que se suponen realizados por una empresa especializada con sus propios lectores.

  Así, se necesitarían un total de 20 lectores (entrada y salida de cada etapa). Se selecciona como producto a utilizar el lector fijo FX7500[18] de Zebra, cuyo precio de venta al público es cercano a los 1.000€. Así pues, el gasto necesario en lectores a lo largo de toda la cadena sería de 20.000€.

- *Software*. En la solución propuesta se propone Hyperledger como software de cadena de bloques para el registro de todos los datos. La inscripción en el programa cuesta entre 10.000 y 20.000€ según el tamaño de la empresa, entre 50 y 500 empleados. Con el objetivo de tomar un cálculo conservador, al alza, y teniendo en cuenta que en este análisis se incluye a toda la cadena de suministro, se supone una empresa de 500 empleados y un coste asociado de 20.000€.

- *Mano de obra.* En este concepto se incluyen tanto el montaje de hardware como el desarrollo de la implantación a nivel software. Se toma como referencia un equipo de consultores especializados compuesto por Project manager, consultor junior y becario.

  Se supone también un tiempo de implantación de los sistemas de una semana de dedicación plena (8 horas/día) por etapa (explotación, matadero, industria, distribución) para la implantación y un tiempo de 10 días (2 semanas) de dedicación plena (40 horas/semana) de consultor y becario y media (20 horas/semana) del Project manager para la verificación de los sistemas y la corrección de errores.

  Tomando como referencia estas hipótesis, el coste total es de 14.240€ y su desglose puede observarse en la Tabla 9.

[18] www.zebra.com/es/es/products/rfid/rfid-readers/fx7500.html

Persona	€/Hora	Horas dedicadas	Total persona (€)
Project Manager	40	200	8.000 €
Consultor Junior	20	240	4.800 €
Becario	6	240	1.440 €
Total			14.240 €

Tabla 9. Desglose coste mano de obra[19]

Así, se tiene un coste total de inversión de 63.780€. Cabe recordar que este coste sería aplicable a toda la cadena, por lo que no es un coste que en el caso real, asumiría una sola empresa, sino que el coste asumido por cada empresa partícipe sería menor (de igual forma, los ingresos extra también se repartirían entre los partícipes).

Con el fin de tener en cuenta otros posibles costes (renovación de equipos, alquiler de servidores, cambio de líneas, etc.) se va a implementar un factor de corrección del 20% del coste, obteniendo un total de 76.536€.

Concepto	Total (€)
Etiquetas RFID	9.540 €
Lectores	20.000 €
Software	20.000 €
Mano de obra	14.240 €
Total Inversión	63.780 €
Total con margen (20%)	76.536 €

Tabla 10. Desglose inversión inicial

Cabe destacar que sería posible aplicar una amortización a 10 años, sin embargo, se considera amortización en el análisis.

A este coste de inversión inicial, le siguen otros costes recurrentes anuales, que se pueden observar en la Tabla 11. El concepto otros incluye imprevistos que pudiesen surgir o costes no contemplados que apareciesen.

Concepto	€/Hora	Horas dedicadas	Total (€)
Mantenimiento	20	96	1.920 €
Etiquetas RFID	-	-	9.540 €
Membresía	-	-	20.000 €
Otros	-	-	2.000 €
Total			33.460 €

Tabla 11. Desglose costes recurrentes anuales[20]

[19] (i) Cálculo de €/hora basado en 2.000 horas al año trabajadas con sueldos de 80.000, 40.000 y 12.000 euros anuales para cada posición. (ii) Horas dedicadas incluye las horas de implantación (1 semana por etapa, 4 etapas) y las de supervisión posterior (2 semanas). (iii) Dedicación completa 40 horas semanales y dedicación media 20 horas semanales.

[20] Mantenimiento realizado por un consultor junior con dedicación de una jornada mensual.

Sin embargo, como toda inversión empresarial, carece de sentido si no se espera un retorno económico positivo. Para analizar las posibles vías en las que este sistema produce un retorno positivo, se proponen distintos escenarios.

5.4.1.1. Escenario optimista

En este escenario, la implantación del sistema de gestión supone un aumento de los ingresos y una reducción de los costes:

- Aumento de los ingresos por medio de:
    - Incremento de cuota de mercado. Aumento de las ventas por la innovación y la demanda de los clientes por conocer el origen de lo que consumen.
    - Incremento del precio medio de venta. Aumento del precio medio de venta debido a la diferenciación que aporta este sistema y la posibilidad que se ofrece al cliente de acceder a toda la información relativa al producto, por lo que está dispuesto a pagar un extra.
    - Incremento de las compras directas por el consumidor (B2C). La certificación y la implementación de certificaciones de origen hace que el cliente deje de delegar esta tarea en la confianza que deposita en el distribuidor y que adquiera jamones directamente del productor.
- Reducción de los costes por medio de:
    - Reducción de intermediarios. El sector del jamón tradicional cuenta con una gran cantidad de intermediarios, que por ejemplo, agrupan la producción de pequeñas explotaciones. Con la implantación de este sistema, muchos podrían ser eliminados, reduciendo los costes totales del proceso al eliminar el margen de estas figuras.
    - Incremento de la eficiencia de los procesos. La implementación de este sistema elimina trabas e ineficiencias administrativas que agilizan los procesos y reducen los costes de los mismos.

5.4.1.2. Escenario neutro

En este escenario, la implementación del sistema no consigue reducir los costes, pues la principal reducción de costes planteada, procedente de la eliminación de intermediarios es compleja por la tradición y el arraigo del sector. Los ingresos consiguen aumentarse mediante las vías planteadas con anterioridad.

5.4.1.3. Escenario pesimista

En este escenario, no se produce ni un aumento de los ingresos ni una reducción de los costes. El sistema implantado conlleva la inversión y los gastos mencionados, pero no produce retorno económico positivo ni se recupera la inversión en ningún momento.

5.4.1.4. Análisis cuantitativo del escenario neutro

El aumento de las ventas y la cuota de mercado es complejo de cuantificar puesto de conlleva la cría de más animales para incrementar la producción, y es una variable limitada por diversos factores, entre los que destaca la extensión de tierra, ya que la regla de calidad establece un máximo número de animales por hectárea de dehesa disponible en la explotación. Es por ello que el análisis de ingresos se va a realizar teniendo en cuenta solo el incremento de los precios y el aumento de las ventas directas B2C.

Según un informe de la consultora Boston Consulting Group [SMIT14], los consumidores están dispuestos a pagar entre un 15% y un 25% más por un producto ecológico, con origen certificado o que provenga de una empresa con una política de responsabilidad social corporativa muy activa. Tomando estas cifras como referencia, se supone para el caso de estudio un aumento del precio medio del jamón del 25%., desde el precio de venta del canal B2C.

Extrapolando los datos del informe [MART10] accesible a través de MAPAMA, aproximadamente el 55% de los jamones que se consumen en hogares se adquieren a través de supermercados e hipermercados, y tan solo un 15% mediante venta directa por canales especializados. Con el nuevo sistema de trazabilidad, se intentarán potenciar los canales especializados, intentando conseguir que una cuarta parte de las ventas (25%) se realicen a través de dicho canal.

Además, se ha realizado un pequeño *benchmark* del precio de un jamón 100% ibérico en dos canales de venta, con un resultado de 95€/kg de precio medio en grandes

superficies y de 75€/kg en venta directa. Obsérvese que tal y como se ha comentado anteriormente, el precio de venta directa posterior será un 25% mayor a 75€, lo que supone 94€, aproximadamente igual al precio de venta actual en grandes superficies.

Con todo esto, se han realizado unas proyecciones financieras aproximadas, a diez años vista e ilustradas en la Tabla 13.

Precio actual venta directa (€/kg)	75
Precio actual venta distribuidor (€/kg)	95
Precio posterior venta directa (€/kg) (+25%)	94
Tamaño explotación (jamones)	477
Jamones vendidos venta directa actual (15%)	72
Jamones vendidos venta directa posterior (25%)	119
kg/jamón	8
Ganancias actuales venta directa[21]	42.930 €
Ganancias posteriores venta directa	89.438 €
Incremento de ingresos por explotación	46.508 €

Tabla 12. Detalle incremento ingresos

[21] Las ganancias se calculan como jamones vendidos * kg/jamón * precio venta

	Año 0	*Año 1*	*Año 2*	*Año 3*	*Año 4*	*Año 5*	*Año 6*	*Año 7*	*Año 8*	*Año 9*	*Año 10*
Coste inversión	76.536€	-	-	-	-	-	-	-	-	-	-
Costes recurrentes	-	33.460€	33.460€	33.460€	33.460€	33.460€	33.460€	33.460€	33.460€	33.460€	33.460€
Incremento ingresos	-	46.508€	46.508€	46.508€	46.508€	46.508€	46.508€	46.508€	46.508€	46.508€	46.508€
Beneficio anual	-76.536€	13.048€	13.048€	13.048€	13.048€	13.048€	13.048€	13.048€	13.048€	13.048€	13.048€
Beneficio acumulado	-76.536€	-63.489€	-50.441€	-37.394€	-24.346€	-11.299€	1.749€	14.797€	27.844€	40.892€	53.939€

VAN	3.635€
Tasa de descuento	10%
TIR	11%
Payback (años)	5,87

Tabla 13. Proyecciones financieras

Con estas cifras, se ha realizado el cálculo del VAN (Valor Actual Neto), con el fin de discernir si el proyecto es o no viable. El VAN, calculado como:

$$\sum_{t=1}^{t} \frac{V_t}{(1+r)^t} - I_0$$

donde V_t corresponde a los flujos de caja de cada periodo, I_0 es la inversión inicial y r es la tasa de descuento, en este caso, establecida en 10%.

Con el fin de tomar la decisión de realizar un proyecto, se tiene en cuenta el siguiente criterio de VAN:

1. VAN>0. El proyecto aporta valor, generando ganancias.
2. VAN<0. El proyecto destruye valor, generando pérdidas.
3. VAN=0. El proyecto no genera ni pérdidas ni ganancias, es necesario considerar otros criterios para tomar la decisión de inversión.

En el caso analizado, el cálculo del VAN arroja un valor de 3.635 €, por lo que el proyecto se determina como viable, con un periodo de *payback* o recuperación de la inversión de 6 años aproximadamente, un horizonte temporal medio, acorde con un proyecto de las características e impacto propuestos.

5.4.2. Indicadores de impacto

Además del análisis económico descrito en el apartado anterior, cabe definir una serie de indicadores o KPIs (*Key Performance Indicator*) para comprobar el impacto de la implantación del sistema de gestión descentralizado en otros aspectos que no sean el económico. Se proponen de forma general KPIs que deberán ampliarse, detallarse, monitorizarse y analizarse en caso de implementación de un proyecto piloto.

- *Indicadores en tiempos:* Reducción de tiempos a lo largo de la cadena, principalmente en la logística y los trámites administrativos de entrada y salida de los distintos proveedores.

- *Indicadores de optimización:* Reducción de intermediarios, reducción de contratos y acuerdos verbales en la cadena, aumento de la digitalización, aumento de las ventas directas.

- *Indicadores de funcionamiento:* Registro de caídas del sistema, pérdidas de datos, consultas de clientes. Estos indicadores son muy importantes durante la etapa de transición de un sistema centralizado a descentralizado para mostrar la estabilidad y correcto funcionamiento del nuevo sistema.

- *Indicadores de calidad:* número de piezas que por los datos registrados mediante la etiqueta RFID sobrepasan los límites establecidos.

- *Indicadores de emergencia*: En caso de necesidad de retirada de productos, tiempo de retirada, identificación de otros productos del lote, etc.

6. Planificación

6.1. EDP (estructura de descomposición del proyecto)

En este punto se detalla la estructura de descomposición del proyecto que se ha seguido. Tiene estructura jerárquica y ordenada de arriba abajo y de izquierda a derecha.

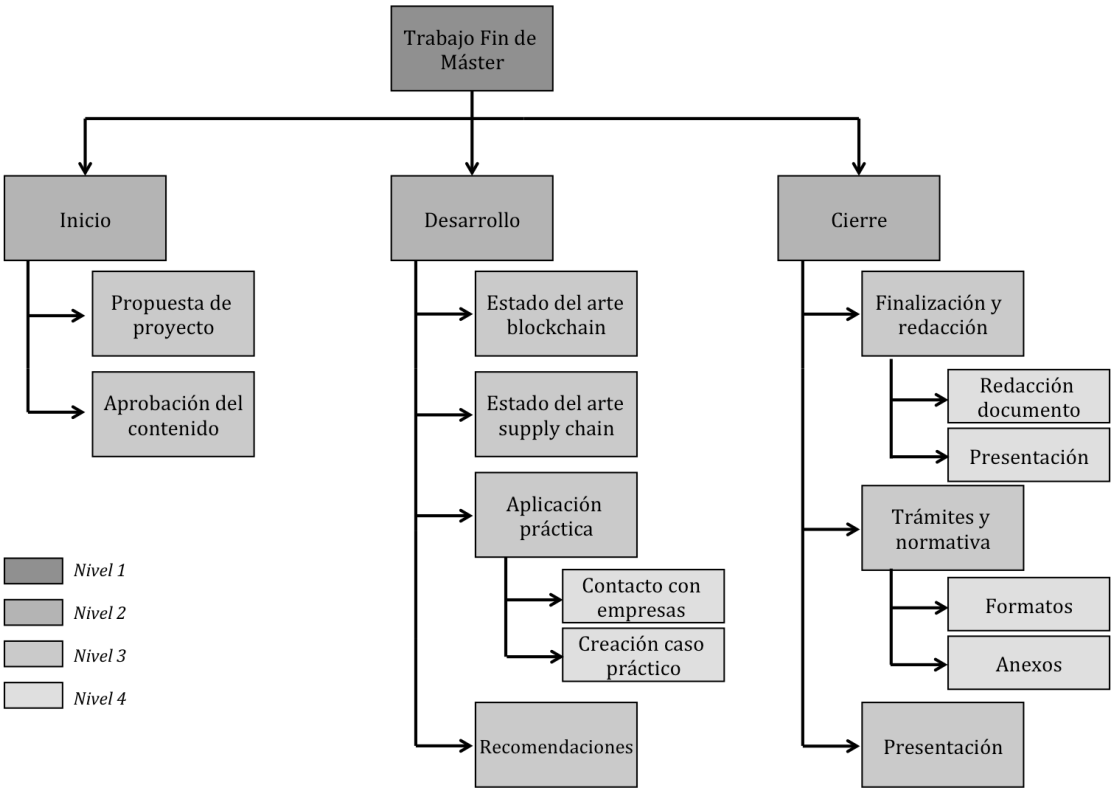


Figura 31. Estructura de descomposición del proyecto

6.2. Diagrama de Gantt

En el diagrama de Gantt que se exhibe a continuación (Figura 32 y Figura 33) se muestran las tareas principales y la duración de las mismas. Cabe destacar que:

- Las fechas y duraciones mostradas son aproximadas
- No se han incluido detalles de reuniones, llamadas, conferencias, etc. por no considerarlas actividades críticas, sino englobadas dentro de la búsqueda de información e investigación inherente al TFM

	Nombre de tarea	Duración	Comienzo	Fin
1	**Inicio del TFM**	**38 días**	**mar 26/09/17**	**jue 16/11/17**
2	Propuesta del proyecto (Anexo A)	8 días	mar 26/09/17	jue 05/10/17
3	Aprobación del contenido (Anexo B)	30 días	vie 06/10/17	jue 16/11/17
4	**Desarrollo del TFM**	**142 días**	**lun 20/11/17**	**mar 05/06/18**
5	Búsqueda de información blockchain	71 días	lun 20/11/17	lun 26/02/18
6	Búsqueda de información supply chain	20 días	lun 05/03/18	vie 30/03/18
7	Redacción estado del arte blockchain y supply chain	21 días	lun 02/04/18	lun 30/04/18
8	Generación del caso práctico	26 días	mar 01/05/18	mar 05/06/18
9	**Finalización del TFM**	**31 días**	**mié 06/06/18**	**mié 18/07/18**
10	Redacción final del documento	19 días	mar 05/06/18	vie 29/06/18
11	Trámites y normativas	5 días	lun 02/07/18	vie 06/07/18
12	Entrega documento	1 día	mar 10/07/18	mar 10/07/18
13	Presentación TFM	1 día	mar 17/07/18	mar 17/07/18

Figura 32. Lista de tareas realizadas en el transcurso del TFM

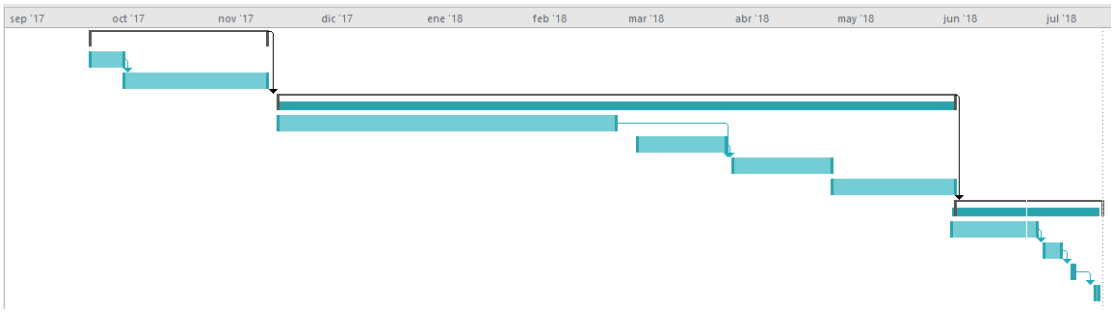


Figura 33. Diagrama de Gantt del TFM (Sept '17 - Jul '18)

7. Conclusiones, recomendaciones, impactos y futuros desarrollos

7.1. Conclusiones y recomendaciones

Con la llegada de blockchain, parece que sus aplicaciones son infinitas y todo el mundo, en todos los sectores intenta aplicarlo. Han surgido infinidad de startups que anunciaban disrupción en determinado sector por la utilización de blockchain y no lo han conseguido, así que cabe preguntarse tras realizar un análisis del estado actual y del posible estado futuro si merece la pena la implantación de blockchain en la cadena de suministro del jamón.

El objetivo principal de este trabajo era realizar una aplicación teórica de blockchain como sistema de gestión de la cadena de suministro en el sector alimentario. Tras llevarlo a cabo se pueden extraer las siguientes conclusiones:

1. Actualmente el sector porcino en España es un sector opaco, altamente tradicional, en el que el consumidor sigue confiando a pesar de los fraudes destapados en los últimos años. Aún así, el sector debe evolucionar, y una de las mayores demandas generales de los consumidores en cualquier tipo de producto es conocer su procedencia, trato animal, etc.

2. Blockchain aportaría la seguridad y confianza extra al consumidor de que el producto que adquiere es el que el etiquetado dice ser, además, lo hace a un coste no excesivamente alto, por lo que se genera la posibilidad de utilización de los sistemas por las explotaciones más pequeñas.

3. Incluso con la implantación de blockchain, quedan remanentes pequeños riesgos de fraude, principalmente ligados a las acciones humanas, pues una automatización total no es posible en el sector.

4. Las ventajas de implantar un sistema de gestión basado en blockchain en el sector alimentario son numerosas, sin embargo, el gran número de partícipes de estas cadenas y la diseminación en ellas hace que las soluciones basadas en blockchain tengan una implementación compleja que requiere un horizonte temporal significativo.

En definitiva, son muchas las incógnitas que no se pueden despejar hasta llevar a cabo la implantación real en proyectos piloto en el sector, no obstante, se sugieren una serie de recomendaciones (resumidas en la Tabla 14) sobre las que podría proponerse en un futuro un estándar para la trazabilidad de jamones. Se trata de unas recomendaciones sencillas, con el objetivo de llevar a cabo una transición de un modelo de trazabilidad muy poco desarrollado y con etapas aisladas a una trazabilidad completa e integral.

Ítem	*Detalles*
Blockchain privada	Inscripción en el proyecto hyperledger
Etiquetas RFID con sensor de humedad y temperatura integrado	
Registros en blockchain	Entrada y salida de cada etapa y parámetros de control oportunos
Control continuo de temperatura y humedad relativa durante elaboración	Junto al tiempo de procesado (obtenido por los registros de entrada y salida) son parámetros críticos para asegurar la calidad
Control de origen y destino en transporte	
Acceso del consumidor	Una vez el distribuidor da de alta el jamón en su sistema, genera un código QR que contiene toda la información

Tabla 14. Recomendaciones para el sector porcino

7.2. Impactos

La implantación de un sistema de gestión por blockchain, conlleva impactos en términos económicos, sociales y medioambientales.

En el plano económico, el impacto al principio, tal y como se ha desarrollado en el análisis económico de la solución propuesta, es una inversión y un aumento de los costes. Sin embargo, este impacto una vez amortizada la inversión no es significativo.

El mayor impacto económico se da en caso de que exista un problema y se necesite recurrir al sistema de trazabilidad para identificar y localizar los jamones. La eficacia y eficiencia del sistema de trazabilidad disminuirían notablemente los costes para llevar a cabo una trazabilidad completa. Además, supondría un impacto más reducido en la imagen de marca.

En el aspecto social, la digitalización de sistemas conlleva la necesidad de contratar trabajadores, bien directamente o bien mediante empresas especializadas, en cualquier caso, supone un aumento de los puestos de trabajo que el sector ofrece.

Además, los propios trabajadores del sector también resultarían beneficiados, pues verían mejorada su productividad y eficiencia gracias a la automatización de procesos (e.g. lectura automática de las etiquetas RFID).

Además, mejorando los procesos internos de las empresas del sector, se mejora la calidad de los mismos y como resultado directo, la calidad del producto final, lo que conlleva un impacto en la sociedad, pues mejora la calidad de los productos que consume (en este caso, de los jamones).

En el plano medioambiental, el impacto es potencial, pero de conseguir una cadena de suministro totalmente trazable y transparente en el sector, se conseguiría:

- Eliminar los fraudes, reduciendo o eliminando las explotaciones que se dedican a prácticas ilegitimas y cuyo trato a los animales y los productos suele ser interesado y deficiente

- Certificar las condiciones de origen de todas las explotaciones, no solo las pertenecientes a DOPs, lo que supondría un incentivo para mejorar el mantenimiento de las dehesas y fincas de explotación independientes

7.3. Futuros desarrollos

La tecnología blockchain es una tecnología con una aplicación a nivel industrial que resulta novedosa y realmente reciente. En el ámbito de la cadena de suministro existen pilotos de diversas empresas, pero no una implantación total.

Así, el futuro de este sector con respecto a la tecnología de cadena de bloques se basa en conseguir realizar una implantación integral del sistema de gestión descentralizado de la cadena de suministro.

En el sector porcino español en concreto, caso de aplicación de este proyecto, las líneas futuras deberían dirigirse hacia:

- El establecimiento de proyectos piloto. Preferentemente en empresas o cooperativas que gestionen de forma integral todos los procesos de la cadena de suministro.

- La incorporación de *smart contracts,* sobretodo en las exportaciones de jamón, para prevenir fraudes y agilizar los trámites de aduanas y comercio internacional. Otra posible aplicación de estos contratos sería la posibilidad de rechazo de los jamones en caso de que los parámetros medidos mediante los sensores se escapen de las tolerancias de los límites de control de los mismos. (e.g. Un distribuidor lee la información contenida en el RFID y comprueba que durante tres días la cámara en la que se envejecía el jamón estuvo a una temperatura mucho más elevada de la recomendable. Esto podría interferir en los estándares de calidad, por lo que el smart contract no se ejecuta y no permite la compra de ese jamón)

El resultado de los proyectos piloto propuestos indicarán de forma práctica y más allá de las hipótesis teóricas realizadas en este documento si la implementación de blockchain en supply chain supone la revolución que el sector estaba esperando o si simplemente es una tecnología con mucha expectación.

8. Bibliografía

[PREU17] - Preukschat, A. Et al. “Blockchain, la revolución industrial de internet”, Gestión 2000, 2017.

[KEMP18] – Kempe, M., Sachs, M., Skoog, H. “Blockchain use cases for food traceability and control”, Kairos Future, 2018.

[LING12] – Ling, L. “Technology designed to combat fakes in the global supply chain”, Business Horizons (2013) 56, 167-177.

[DABB13] – Dabbene, F. Et al, “Traceability issues in food supply chain management: A review” Biosystems Engineering (2013)

[STEI17] – Stein, T. “Supply chain with blockchain showcase RFID” R&D faizod, 2017.

[VORS09] – Van der Vost, J. Et al, “ Agro-Industrial supply chain management: concepts and applications”, Food and agriculture of the United Nations, 2007.

[PROV15] – Provenance Ltd. “Blockchain: the solution for transparency in product supply chains” Provenance, 2015

[ZAPA13] – Zapatero, A. “Problemática estructural y de funcionamiento de la cadena de valor del jamón ibérico de bellota: El caso de Guijuelo en España” Tesis doctoral, Universidad Politécnica de Madrid, 2013.

[JUST17] – Just, K. “Blockchain in supply chain”, 2017

[MCBE18] – McBeath, B. “Blockchain's Role in the Produce Supply Chain” Chainlink research, 2018.

[NAKA08] – Nakamoto, S. “Bitcoin, a peer-to-peer electronic cash system”, 2008

[PERE14] – Pérez-Solà, C. Et al. “Bitcoin y el problema de los generales bizantinos” RECSI 2014.

[BACK02] – Back, A. "Hashcash - a denial of service counter measure", 2002.

[KIMH16] – Kim, H. and Laskowski, M., "Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance" 2016.

[GS116] – Various contributors, "GS1 Global Traceability Compliance Criteria for Food Application Standard", 2016.

[UPS05] – UPS White paper "Demystifying RFID in the Supply Chain", 2005

[SMIT14] – Smits, M. Et al, "An Imperative for Consumer Companies to Go Green When Social Responsibility Leads to Growth" Boston Consulting Group report, 2014.

[SACH18] – Goldman Sachs White paper, " Blockchain, the new technology of trust", 2018.

[BOSO13] – Bosona, T. and Gebresenbet, G. "Food traceability as an integral part of logistics management in food and agricultural supply chain" Food Control, 33,32-48. 2013.

[RESE10] – Resende-Filho, Moises A and Buhr, Brian L., "Economics of Traceability for Mitigation of Food Recall Costs" 2010.

[CHEU01] – Cheung, H. and Choi, S. "Implementation issues in RFID- based anti-counterfeiting systems" Computers in Industry, 62, 708-718. 2001.

[AURO12] – Aurora, Mohit. "How secure is AES against brute force attacks?" públicado en eetimes.com, 2012.

[LEVY93] – Levy, S. "Crypto rebels" públicado en wired.com, 1993.

[BCB17] – Banco Central de Bolivia. Comunicado uso criptomonedas Abril 2017. bcb.gob.bo/webdocs/11_comunicados/04_2017_COMUNICADO_Uso_monedas.pdf

[MARK17] – Marks, H. "There they go… again". Carta a inversores Oaktree Capital.

[MACK17] – Mckinsey and Company. "Blockchain Technology in the insurance sector", 2017.

[CANT17] – Cant, B. Et al. "Smart Contracts in Financial Services: Getting from Hype to Reality" Capgemini consulting, 2017.

[LINK17] – Linklaters White paper "Smart Contracts and Distributed Ledger – A Legal Perspective", 2017

[HEAR16] – Hearn, M. "The resolution of the Bitcoin experiment" 2016.

[STIN17] – Stinchcombe, K. "Ten years in, nobody has come up with a use for blockchain" 2017.

[VERB05] – Verbeke, W. "Consumer acceptance of functional foods: Socio-demographic, cognitive and attitudinal determinants" 2005

[MART10] – Martín Cerdeño, V. J. "Consumo de jamón en España", Ditribución y consumo Noviembre-Diciembre 110-115. 2010.

ANEXOS

Anexo I. Hyperledger

Hyperledger (hyperledger.org) es el proveedor de la solución de blockchain propuesta en el documento, por ello se va a describir brevemente su origen, y funcionamiento.

Hyperledger es un proyecto que surge en 2015 y es albergado por la Linux Foundation, con la intención de crear un ecosistema de desarrollo de blockchains privadas para corporaciones. Actualmente, centran sus esfuerzos en el desarrollo de protocolos y estándares para esta tecnología, queriendo emular a los conocidos protocolos TCP/IP de internet.

Dentro de hyperledger, existen nueve proyectos pudiendo diferenciar plataformas blockchain (Burrow, Fabric, Indy, Iroha, Sawtooth) y software para la interacción entre estas (Composer, Explorer, Cello, Quilt). Cada proyecto esta potenciado por empresas y responde a necesidades distintas, diferenciándose en aspectos técnicos que no se detallan en este anexo.

En el contexto actual, no existe una plataforma única, desarrollada sino que las opciones son múltiples y la decisión dependerá del uso que se le desee dar.

Una de las claves para la elección de esta plataforma para el sistema de gestión es que es accesible para cualquier empresa. Actualmente cuenta con más de 170 miembros. Las empresas que deseen formar parte deben formar también parte de la Linux Foundation y existen diferentes tipos de membresías que incluyen diferentes tipos de beneficios:

- *Premier members*. Es necesaria una aportación anual de 250.000 dólares. (e.g. Airbus, American Express, Cisco, etc.).

- *General members*. Pagan una tarifa en función del tamaño de la empresa, entre 5.000 y 50.000 dólares para empresas entre 50 y 5000 empleados respectivamente (si se incluye la membresía de la Linux Foundation, la tarifa se sitúa entre 10.000 y 70.000 dólares). (e.g. BBVA, Deloitte, Samsung, etc.).

- *Associate members*. No realizan ningún pago, deben ser aprobados y son proyectos gubernamentales o de ONGs. (e.g. Bank of England, University of Cambridge, etc.).