



UNIVERSIDAD
DE LA REPÚBLICA
URUGUAY



Universidad de la República

Facultad de Ingeniería

Proyecto de Grado - Ingeniería de Producción

MEJORA DE LA CADENA DE SUMINISTRO POR APLICACIÓN DE BLOCKCHAIN

Juan Fermín Remedi

5.415.182-3

Francisco Stanham

4.737.671-5

Tutor: Ing. Guillermo Rela

2021

Agradecimientos

El proyecto de grado representa un gran desafío y esfuerzo para todos los estudiantes de nuestra Facultad, pero también una gran oportunidad. Una oportunidad de aprendizaje y desarrollo tanto en lo personal, como en lo académico y profesional. A lo largo de este proceso, fuimos guiados por personas que dejaron una huella en cada uno de estos aspectos y por este motivo consideramos de gran importancia su presencia en esta sección.

En primer lugar, agradecer a nuestro tutor Guillermo Rela por su apoyo y asesoramiento a lo largo del proyecto como también en la carrera como director de la misma y docente de diversas asignaturas. Su visión de futuro, entusiasmo y sugerencias innovadoras fueron un gran aporte al proyecto.

También a Marcelo Secco, director de Marfrig, Fernando Thul, Gerente de Tecnologías de Información en Jaume & Seré, y Alexander Wolff, Gerente de Desarrollo en Concepto, quienes nos brindaron con mucho entusiasmo sus conocimientos para poder llevar a cabo el proyecto, además de dedicar su tiempo en un prolongado asesoramiento a lo largo del proyecto. Compartieron de forma auténtica sus ideas y estudios previos, y fueron sin duda una constante fuente de motivación.

Por otro lado, Cecilia Acosta, Gerente de Calidad de Marfrig, Antonio Chiesa, Asistente de Producción de Marfrig, José Ignacio Gamio, CEO de Athena Foods, Martín Gastañaga encargado del Departamento de Control de Comercio Internacional del Ministerio de Ganadería, Agricultura y Pesca, y Agustín Inthamoussu, exgerente general de Carbosur e integrante de la *United Nations Framework Convention on Climate Change*, también dedicaron su tiempo y experiencia para guiarnos en distintos puntos del proyecto y también tienen nuestra gratitud.

Resumen ejecutivo

El informe presenta la descripción, metodología y resultados obtenidos correspondientes a la investigación acerca de la mejora de la cadena de suministro por aplicación de *blockchain* elegida como consigna del Proyecto de Grado de la carrera Ingeniería de Producción.

Para llevar adelante dicha investigación, en primera instancia se llevó a cabo una revisión bibliográfica de los temas principales abordados en el proyecto. Principalmente se profundizó la investigación en la tecnología de cadena de bloques denominada *blockchain*, en conceptos acerca de las cadenas de suministro, y en la realidad de la industria cárnica en el mundo y en Uruguay. Se constató que esta industria cuenta con ventajas competitivas importantes que la destacan por sobre sus competidores regionales. De todas formas, se presentan una serie de desafíos de cara al futuro como el poder adaptarse a las nuevas necesidades de los consumidores y consolidar otros tipos de producción para acceder a nuevas cuotas de exportación y capturar nuevos mercados.

En este contexto, la mencionada tecnología de cadena de bloques podrá brindar nuevas funcionalidades en muchas de las actividades que se dan al producir cortes cárnicos, incluyendo la producción industrial y las distintas etapas de transporte de mercadería en distintos grados de procesamiento. Estas nuevas funcionalidades son un medio confiable para hacerle frente a los desafíos presentados y así poder desarrollar aún más la industria.

Específicamente, se modeló un sistema basado en *blockchain* capaz de recabar información y datos claves generados por distintos actores de la cadena de suministro cárnica y almacenarlos de manera confiable, inmutable y segura. Esto permitirá que cualquier actor de la cadena acceda a una gran cantidad de información que actualmente no está del todo disponible, y lograr resultados como el aumento de la fidelidad de los consumidores finales a través de un aumento en la transparencia, evaluación de proveedores más confiable o el agregado de valor en general para la industria. Posteriormente se procedió a crear una red funcional de prueba como punto de partida en la concreción real del proyecto.

Luego de analizar el sistema diseñado a través de la presentación del mismo a distintos profesionales del rubro, se llega a la conclusión de que un sistema de tales características es definitivamente capaz de potenciar mejoras como las mencionadas y muchas otras no previstas inicialmente. Si bien su implementación completa resulta, en principio, poco factible, una implementación escalonada en la cual se consideren solamente algunos actores claves en una primera instancia, para luego incluir a los restantes, no está tan alejada de la realidad. De hecho, algunos de los profesionales contactados manifestaron intenciones de llevar a la práctica la implementación de un sistema similar al propuesto. En ese sentido, el mayor desafío es integrar a todas las entidades públicas y privadas en un único sistema descentralizado, pero esto no debe desmotivar a los involucrados a comenzar con innovaciones de este estilo en el mediano plazo para obtener ventajas por sobre los competidores de la región.

Palabras claves: *blockchain*, *Smart Contract*, criptografía, mecanismos de consenso, sistemas descentralizados, *Hyperledger Fabric*, cadena de suministro, Industria Cárnica, agregado de valor.

Índice

Agradecimientos	3
Resumen ejecutivo	5
Índice	7
Introducción	9
Objetivos	10
Marco teórico	13
Fundamentos Cadena de Suministro	13
Sistemas Centralizados y Descentralizados	15
Sistemas <i>peer-to-peer</i>	16
<i>Blockchain</i>	16
Transacciones	18
<i>Hashing Data</i>	18
Criptografía	19
Cadena de bloques	19
Capas	19
Mecanismos de Consenso	20
Casos de Uso	23
Gestión compartida de energía solar	25
Análisis contextual de la industria cárnica	29
El complejo cárnico - motivación	29
Casos de uso en el negocio cárnico	31
Análisis tecnológico	33
Elección de <i>blockchain</i>	35
<i>Ethereum</i>	36
<i>Hyperledger Fabric</i>	36
<i>R3 Corda</i>	37
Prueba de concepto en <i>Hyperledger Fabric</i>	39
Prerrequisitos	40
<i>Instalar Samples, Binarios y Docker Images de Hyperledger Fabric</i>	41
Levantamiento de la red y sus componentes	41
<i>Creación de la red</i>	41
<i>Creación del canal</i>	45
	7

<i>Configuración del chaincode en el canal</i>	47
Prueba de operación en el sistema	48
<i>Inicialización de activos</i>	51
<i>Ejecución de transacciones</i>	53
Diseño del sistema	57
1. Identificación de los principales actores del proceso.	57
2. Determinación de documentos e información (datos relevantes) requerida en la cadena	60
3. Desarrollo práctico de aplicación en cadena de suministro	63
4. Relación lógica entre documentos	71
5. Definición de canales de comunicación	71
6. Establecimiento de la gobernanza	73
Agregado de valor a la cadena de suministro	77
Producción de cortes orgánicos	77
Carne producida a bajo carbono	79
Producción de carne <i>Kosher</i>	83
Certificaciones de bienestar animal	84
Registro de hitos relevantes durante la producción de carne	87
Sinergia entre IoT y la trazabilidad con <i>blockchain</i>	89
Trazabilidad hacia atrás y logística de retiro de productos	89
Análisis de implementación	91
Retroalimentación Plantas de Faena	92
Retroalimentación Jaume & Seré y Concepto	93
Conclusiones	95
Bibliografía	99
Anexo I – flujo de procesos desde ingreso de ganado a planta hasta envasado de cortes cárnicos	105
Anexo II – flujo de procesos correspondientes a la negociación entre planta de faena y cliente	107
Anexo III – funcionamiento del <i>smart contract</i> como sustituto de la carta de crédito	109
Anexo IV – la ganadería uruguaya y el cuidado del medio ambiente	111
Anexo V – Proceso de prueba de concepto en Hyperledger Fabric	115
Anexo VI – Ejecución de instalación de Prerrequisitos Hyperledger Fabric	117
Anexo VII- Creación de la red Hyperledger Fabric	121

Introducción

En el mundo productivo, todas las actividades que se realizan por distintas organizaciones, instituciones, empresas y personas que llevan a que una materia prima -en su estado más primitivo- logre llegar a un consumidor final en forma de producto manufacturado -al que se le agregó valor a partir de la materia prima- forman lo que se denomina cadena de suministro.

Para que los consumidores finales puedan obtener ese producto manufacturado, la transferencia de información entre estos actores -llamados nodos de manera genérica- pasa a tener un rol fundamental. Desde el proveedor inicial de insumos hasta el consumidor final ocurren muchos procesos internos en cada nodo, como también entre ellos. Naturalmente, los distintos trámites, transportes de mercadería, negociaciones y comunicaciones involucradas en que el producto terminado llegue al cliente a partir de la materia prima, agregan costo y complejidad al flujo de actividades entre nodos.

Por estos motivos, la colaboración entre nodos es de vital importancia para reducir los costos totales. Si cada nodo busca facilitar las tareas del nodo siguiente -cumpliendo plazos de entregas, completando pagos a tiempo, comunicando de manera rápida los imprevistos o cambios en demanda, entre otros- los costos de la cadena se reducen y la misma se vuelve más eficiente. Para esto, surgieron y seguirán surgiendo distintas tecnologías para efectuar comunicaciones entre nodos, que evolucionan en el tiempo para lograr sistemas más efectivos y eficientes.

En ese contexto, este trabajo busca investigar los distintos conceptos que hacen una cadena de suministro, así como las tecnologías actuales en las cuales se apoyan dichos sistemas. Si se analiza la introducción del Internet en el mundo de la década del 90, se puede afirmar que dicha tecnología fue creada para el transporte de información, sin contemplar el intercambio de propiedad de valor. Para estos motivos, la sociedad ha dependido históricamente de intermediarios para garantizar la confianza necesaria entre partes.

Particularmente, la tecnología de cadena de bloques o *blockchain* se presenta como una buena solución para el intercambio de propiedad de valor, por lo que en este caso puede apoyar la gestión de una cadena de suministro. Esta tecnología ha estado en el foco de las noticias, principalmente por ser la base de las criptomonedas, que tuvieron un gran crecimiento en el mercado. Tal es el caso de *Bitcoin*, una criptomoneda descentralizada, *peer to peer*, construida a partir del almacenamiento encadenado de información llamado *blockchain*. Por esto, carece de un emisor central u organismo controlador logrando que todas las transacciones se realicen directamente entre las personas, sin intermediarios, con gran rapidez en todo el mundo. Aun así, el sistema fue creado con una estructura capaz de brindarle seguridad a las transacciones, respetando por completo la identidad de los participantes y basando la confianza en el protocolo de funcionamiento de *blockchain*, no en la reputación de las partes. El exitoso caso de *Bitcoin* demuestra el potencial de esta tecnología disruptiva, e invita a las personalidades innovadoras a aventurarse en la infinidad de posibilidades que la misma brinda. Como se detalla posteriormente en este documento, su aplicabilidad en otros rubros ya es una realidad, al irrumpir en áreas como la logística, medicina y la industria alimenticia, pero aun así, queda mucho terreno por abarcar.

Utilizando a la igualdad, transparencia, seguridad e inmutabilidad como bandera, *blockchain* se presenta como una de las principales alternativas para combatir, desde un tema tan crítico a nivel global como el fraude, hasta la mejora de la eficiencia en el manejo y comunicación de datos a escala local.

Para comprender completamente el motivo por el cual la tecnología *blockchain* puede garantizar los mencionados beneficios y características, es necesario consolidar conceptos fundamentales de ingeniería de software, definir la terminología relevante y desarrollar el conocimiento a partir de los distintos pilares que constituyen los cimientos de la tecnología.

Objetivos

Los objetivos del proyecto son diversos, pero principalmente se busca el acercamiento por parte de los estudiantes a la aplicación de los distintos conceptos que se adquirieron en la carrera de Ingeniería de Producción. El propio trabajo investigativo y analítico brinda a los estudiantes la posibilidad de apoyarse en distintos conceptos, técnicas y metodologías que fueron presentadas en los programas de estudio de las distintas materias de la carrera. De esta forma, se logra utilizar un bagaje conceptual íntegro y diverso que atraviesa distintas áreas de conocimiento -en lugar de conceptos aislados como se utilizaron en las distintas materias de forma particular- lo que permite tomar cuenta del alcance de los conocimientos adquiridos por los estudiantes, para concluir esta carrera ingenieril.

Como fue mencionado anteriormente, el tema elegido para llevar adelante dicha investigación es la mejora de la cadena de suministro por aplicación de *blockchain*.

Para eso, en primera instancia se buscará investigar acerca de la temática y retomar conceptos adquiridos a lo largo de la carrera para llegar a presentar un estado del arte de la tecnología involucrada, así como de la realidad y desafíos de las cadenas de suministro en el mundo actual. En el estado del arte se definen todos los conceptos a utilizar, y sirve como punto de partida desde el cual los estudiantes deberán estudiar sistemas ya existentes, así como diseñar nuevos sistemas.

Posteriormente, se presentarán varios casos de uso del mundo real, para luego centrarse en un caso de uso particular.

La construcción de este caso particular es el objetivo práctico principal del proyecto, por lo que los estudiantes presentarán su diseño y posible extensión con detenimiento. El mismo debe ser aplicable a alguna industria, por lo que deberá ser validado por una contraparte del mundo profesional. Con respecto al desarrollo práctico de la tecnología en sí, se pondrá en práctica el proceso simplificado de creación y ejecución de una *blockchain* específica, en una prueba de concepto.

Habiendo cumplido estas etapas de acercamiento incremental hacia el objetivo práctico final - investigación inicial, aplicación teórica, aplicación práctica, validación de la aplicación práctica- se dará por concluido el proyecto.

Naturalmente, el tema elegido obliga a los estudiantes a acercarse al entorno industrial y al mundo laboral, teniendo que discutir e intercambiar de par en par con profesionales, así como presentar conclusiones de la investigación. Además, esta oportunidad permite que los estudiantes se sigan desarrollando como futuros profesionales egresados y comiencen a entablar contactos y relaciones de interés en el mundo empresarial.

Marco teórico

Fundamentos Cadena de Suministro

Según el *Council of Supply Chain Management Professionals* el concepto de logística -citado por las notas del curso de Elementos de Gestión Logística - Fing- puede definirse como “aquella parte del proceso de la cadena de abastecimiento que planea implementa y controla el eficiente y efectivo flujo hacia delante y reverso y almacenamiento de bienes, servicios e información vinculada desde el punto de origen hasta el punto de consumo, para satisfacer los requerimientos de los clientes.” [1]

Resulta interesante detenerse en el concepto de cadena de abastecimiento, que se puede definir como las relaciones entre proveedores, manufacturers, distribuidores y consumidores que aseguran que ciertos bienes, confeccionados a partir de distintas materias primas, puedan ser comercializables [2]. Una cadena de abastecimientos está compuesta por distintos nodos u organizaciones. Al observar la **¡Error! No se encuentra el origen de la referencia.** [2], el nodo Z representa una industria, y el resto de los nodos representan los distintos niveles de proveedores y distribuidores. La cadena de suministro determina los flujos de información y materiales que se dan hacia el proveedor y hacia el consumidor.

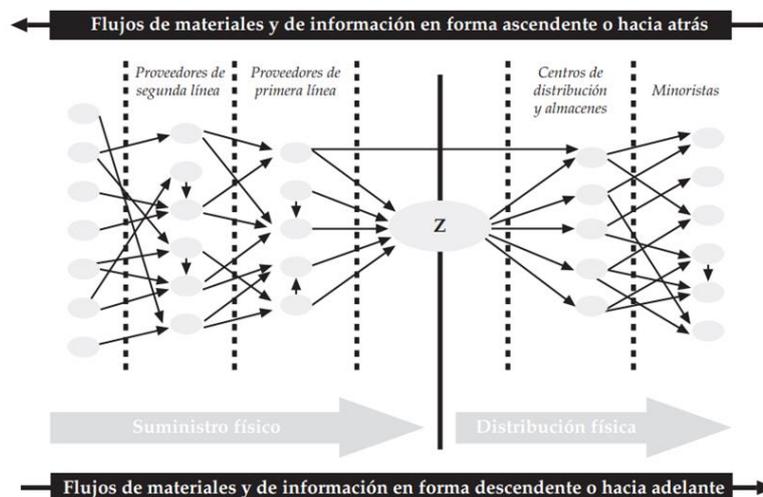


Figura 1 - Modelo teórico de una cadena de suministro

La administración de esta cadena de abastecimiento tiene como objetivo gestionar los procesos involucrados de tal forma que se satisfagan las necesidades de los clientes. Estos procesos deben de estar administrados de manera diligente y deben tener un alto grado de cohesión para que la información pueda fluir y ser utilizada a lo largo de la cadena.

La expansión del comercio internacional y los grandes avances en la logística internacional han sido impulsados por innovaciones capaces de reducir los costos implícitos en estas actividades. A grandes rasgos, se han logrado importantes avances relacionados con la reducción de los costos de transporte, a través de la creación del container estandarizado, y lo mismo con los costos regulatorios, a través

de los órganos de coordinación del comercio mundial, pero aún queda mucho por hacer con relación a los costos de información. Estos son los costos de proveer y distribuir información de confianza acerca de los productos a los clientes, productores y entidades regulatorias. A medida que un producto avanza a lo largo de la cadena de suministro, documentos sobre origen, calidad y propiedad deben fluir consigo a través de los distintos actores involucrados.

Históricamente las cadenas de suministro se administraron de manera de que cada nodo busque maximizar su beneficio de manera individual. Esto resultó en cadenas cuyos altos precios se transfirieron al cliente. Esta lógica se fue dejando de lado hasta llegar al concepto de *cadena integrada* [3], en el que se busca maximizar la ganancia de la cadena entera no sólo centrándose en los resultados individuales.

Una integración hacia adelante y hacia atrás en la cadena de suministro permite que cada nodo se coordine con el anterior y el siguiente para reducir costos, inventarios y tiempos de espera, y así lograr una reducción de costos significativa. Un aumento en la incertidumbre en un nodo, a la hora de tomar decisiones, se traslada al siguiente nodo, y se suma a su incertidumbre propia, generando un efecto acumulativo. Esto genera una cadena con una gran incertidumbre como conjunto, que de alguna forma pone en riesgo el cumplimiento de las expectativas de los clientes. Al administrar la cadena con un enfoque sistémico, considerando el impacto de las decisiones de un nodo sobre los otros, y con un compromiso a beneficiar a la cadena entera, se logra reducir la incertidumbre total de la misma. Es por esto que al considerar cualquier cadena de abastecimiento se deben conocer cada uno de los nodos participantes, cuál es su rol en la cadena, y de qué manera sus decisiones afectan al resto.

La revolución de las comunicaciones y el acceso a internet fueron factores preponderantes para que las cadenas de suministro se conviertan en sistemas interconectados, permitiendo una mayor eficacia y velocidad en el intercambio de información. Esto da como resultado una coordinación mayor entre compañías, resultando en un mejor servicio al cliente. Otro factor que aumenta el servicio al cliente es la disponibilidad de información -como ser las existencias de un artículo en el inventario, su ubicación, y el tiempo esperado de entrega en caso de que sea ordenado- al momento de ofrecer un producto. Tener acceso a esta información, y que la misma sea fidedigna se puede transformar en una ventaja competitiva [4].

En el curso *Teoría, algoritmos y aplicaciones de gestión logística - Fing* se introduce la logística en Uruguay con un enfoque en la cadena de suministro *cárnica*. Se comenta que la carne uruguaya adquiere un valor muy importante en los mercados mundiales por la calidad de su producción, pero también por su robusto sistema de trazabilidad. Según el Comité de Seguridad Alimentaria de la Asociación de Fabricantes y Distribuidores (AECOC), la trazabilidad es el conjunto de procedimientos destinados a registrar la ubicación, trayectoria y demás información de un producto o lote de productos en un momento dado a lo largo de la cadena de suministro [5].

En Uruguay la trazabilidad pública del movimiento de bovinos surgió a partir de exigencias de los mercados de exportación para obtener garantías sanitarias. Los sistemas de trazabilidad pueden abordarse desde iniciativas privadas o públicas. Según datos del Instituto Nacional de Carnes (INAC), Uruguay es uno de los pocos países en el mundo donde es obligatorio identificar a los bovinos de

forma individual y universal, previo al cumplimiento de los 6 meses de edad. Se implementa utilizando dispositivos electrónicos (caravanas con tecnología de identificación por radiofrecuencia o RFID), y se regula mediante la Ley 17.997.

Esta Ley define un animal trazado como *“aquel animal debidamente identificado y cuyos movimientos, cambios de propiedad, transacciones y todos aquellos eventos que la autoridad competente determine relevantes, hayan sido debidamente registrados sin interrupciones o inconsistencias desde el momento de su ingreso al Registro en las condiciones establecidas en los artículos 4º y 5º de la presente ley.”* [6]

Algunos especialistas afirman que las condiciones que se mantienen a lo largo de la cadena de suministro son tan importantes como la producción en sí, al momento de asegurar la calidad de la carne. Mantener el sistema de trazabilidad funcionando implica un esfuerzo importante debido a la necesidad de controlar activamente las caravanas de los animales, realizar un seguimiento de los cortes en la planta de faena, trazar los contenedores en el puerto y durante su viaje a otro destino, conocer las condiciones de conservación del producto, entre otros aspectos. Sin embargo, esto tiene una gran importancia a la hora de construir un producto de calidad.

En el mundo actual, toda trazabilidad se apoya en uno o varios sistemas informáticos que permiten gestionar la información de manera correcta, para poder operar con eficacia. Estos sistemas de información deben cumplir con ciertas características que ayuden a las cadenas de suministro a satisfacer los requerimientos de mercados cada vez más exigentes. Para empezar, deben ser sistemas amplios, que permitan registrar una gran cantidad de información. Además, deben ser sistemas con un profundo alcance hacia adelante y hacia atrás en la cadena de suministro. Idealmente, un único sistema gestiona la cadena completa desde el productor hasta el consumidor final, pero en la práctica esto resulta difícil por la gran cantidad de organizaciones que están involucradas. Por otro lado, resulta importante que el sistema sea preciso y que dé un alto grado de seguridad acerca de las características y movimientos de cada producto. Por último, el grado de accesibilidad debe ser adecuado, y se mide como la velocidad con la que se obtiene información y se comunica al resto de los miembros de la cadena de suministro [7].

Sistemas Centralizados y Descentralizados

En las cadenas de suministro, se puede categorizar como intermediarios a los que históricamente han sido utilizados para proporcionar información relevante acerca de la oferta y demanda y la comunicación de precios y requisitos, entre productores y clientes. Muchas veces brindan tareas de distribución de productos, cobranza, consultoría o servicios fiduciarios, y fueron adquiriendo gran importancia. Pueden ser el nexo de conexión entre clientes y productores, capaces de brindar confianza y reducción de riesgos a negocios entre desconocidos. Muchas de estas especializaciones de los intermediarios jamás podrán ser sustituidas por la tecnología, principalmente por la incapacidad de transferir la experiencia en el mercado. De todos modos, una desintermediación podría llevarse a cabo. Como se mencionaba, una de las responsabilidades asignadas a los intermediarios es el manejo de la información. En general, la información en las cadenas de suministro está distribuida irregularmente entre actores e intermediarios, al estar compartida entre pocos, o totalmente centralizada en un intermediario responsable de almacenarla y compartirla. En ambos casos, se

generan consecuencias negativas que afectan el funcionamiento de la cadena de suministro. Por un lado, la falta de comunicación puede generar inseguridad, fricción, incongruencias y desperdicios y por otro, la centralización de la información puede crear dependencia, manipulación y una posición de poder también indeseada.

Los sistemas informáticos se pueden categorizar como sistemas centralizados o descentralizados desde las perspectivas de la arquitectura, el enfoque político o la lógica. Desde la arquitectura se estudian los nodos, su distribución, cantidad e interacciones en el sistema. La perspectiva política analiza el control que puede tener cada individuo, grupo u organización en el sistema. El estudio de la lógica determina el grado de centralización en base a la capacidad del sistema de funcionar en unidades independientes al dividir al mismo en subsistemas [8].

Desde todo punto de vista, el sistema centralizado tiene un nodo preferencial con el control y con la administración total del sistema. Lo contrario ocurre en un sistema descentralizado, ya que cada nodo posee la misma autoridad e importancia con respecto a los demás. En la práctica, es posible identificar un sistema centralizado, si existe la posibilidad de cerrarlo por completo a través de la voluntad de un solo componente. Muchas veces, una interacción entre dos participantes de un sistema requiere necesariamente de la acción de un nexo para llevar a cabo el intercambio de información buscado. La influencia de dicho intermediario resulta tan determinante que le otorga poder ante los demás usuarios, lo que puede resultar indeseado en términos de tiempos y costos. Por esto, la eliminación de este nexo intermediario es uno de los principales objetivos alcanzados a través de la utilización de los sistemas descentralizados. Un claro ejemplo de la situación presentada anteriormente es visible en el negocio bancario. Con la creciente tendencia de bancarización de las personas, uno de los principales propósitos de los bancos ha derivado en actuar de intermediario entre productores y consumidores. Una simple transacción de dinero necesita inexorablemente la voluntad del banco de realizar dicha acción.

Sistemas *peer-to-peer*

Los sistemas *peer-to-peer*, es decir, usuario a usuario, son sistemas descentralizados constituidos por usuarios (nodos) que ofrecen sus recursos computacionales a la red, a la vez que disponen de igual manera de los recursos brindados por los demás [9]. Por ejemplo, cada vez que un usuario desea descargar un archivo en estos sistemas, lo obtiene de cualquier otro usuario que lo tenga disponible. A su vez, ese mismo usuario, en paralelo, tiene a disposición información para compartir con los demás nodos.

Blockchain

Inicialmente, esta tecnología se puede definir como un sistema distribuido entre usuarios (*peer-to-peer*) con una estructura de datos apoyada en criptografía y algoritmos, para el almacenamiento de transacciones de forma segura, en lo que se denomina cadena de bloques. El propósito de la misma es garantizar al usuario y al sistema, el siguiente conjunto de propiedades fundamentales [10]:

- Incorruptibilidad
- Inmutabilidad
- Integridad
- Funcionamiento democrático
- Confianza
- Consistencia
- Resiliencia
- Auditabilidad
- Transparencia

Una de estas propiedades, la confianza, puede definirse como la expectativa de que un actor externo actúe con integridad [10]. Por su parte, la integridad puede determinarse por cuatro valores fundamentales: honestidad, consideración, responsabilidad y transparencia.

- La honestidad consiste de una auténtica comunicación, en la cual se comunica con veracidad, precisión y completitud.
- La consideración implica un genuino respeto por los intereses de la contraparte, para poder actuar con buena fe.
- La responsabilidad deriva en la capacidad de asumir compromisos y cumplirlos.
- La transparencia, apunta a la disposición de cada actor de mostrar información relevante en la medida suficiente y necesaria, para satisfacer las inquietudes razonables de la contraparte.

Entonces, el grado de confianza que se tiene en una persona puede ser consecuencia de una imposición intuitiva o de la evaluación de resultados de anteriores interacciones con dicha persona, y por ende puede aumentar o disminuir con el tiempo. Dado que los sistemas *peer-to-peer* se basan en la obtención de resultados esperados en las interacciones entre usuarios, el éxito de dichos sistemas depende totalmente del grado de confianza que se pueda alcanzar entre sus usuarios. El principal propósito de la tecnología *blockchain* es garantizar la integridad en la información en estos sistemas *peer to peer*, asegurando un grado total de confianza en las transacciones entre pares.

En primer lugar, al ser un sistema descentralizado, cada usuario o nodo almacena un registro con todas las transacciones realizadas en el sistema. Para llevar a cabo una transacción es necesario definir el objeto a intercambiar, identificar los usuarios participantes y probar la posesión del objeto por el usuario propietario. En este proceso, la criptografía se encarga de garantizar la identificación y autenticación de los usuarios como dueños de ciertos objetos, para poder autorizar una operación. La posesión del objeto se verifica a través del historial de transacciones del mismo, por lo que se debe tener fácil acceso a todos los intercambios en los que estuvo presente el objeto, y así saber quién fue el último usuario en recibirlo. A través de un algoritmo, todos los nodos corroboran la validez y coincidencia de su versión colectivamente, llegando a un consenso acerca del registro aceptado. A continuación, se entra en detalle acerca de cada paso mencionado anteriormente.

Transacciones

Las transacciones describen la acción de transferir la posesión de cierto objeto entre usuarios [11]. El historial de transacciones es lo que determina a los usuarios la posesión de cierto objeto, asumiendo como propietario al último receptor en el registro de transacciones del objeto. Para poder ejecutar las transacciones de forma completa y agregarlas al historial de transacciones, la siguiente información es necesaria:

- Identificación del usuario que entrega la posesión (origen)
- Identificación del usuario receptor
- Cantidad de cierto objeto a transferir
- Fecha y hora en la que se lleva a cabo la transacción
- Comisión o recompensa por ejecutar la transacción (si aplica)
- Prueba de que la transacción haya sido aceptada por el usuario que entrega la posesión

Dada su importancia, el historial de transacciones es almacenado en la estructura de datos *blockchain*, de acuerdo con el orden cronológico de los sucesos. Al hacerlo, se garantiza la validez de una transacción en relación con tres aspectos: la formalidad, la semántica y la autorización. El aspecto formal de una transacción refiere a la completitud de la descripción de la transacción. Es decir, que se hayan detallado todos los campos necesarios en el formato correcto. La semántica se enfoca en el propósito y la lógica de la transacción a realizar, y se evalúa la transferencia en base al cumplimiento de una serie de reglas del negocio, detalladas a continuación:

- La cuenta origen no puede transferir más de lo que posee
- La cuenta origen no puede intentar transferir el mismo objeto a dos cuentas receptoras distintas (*double spending*)
- Se puede limitar la cantidad máxima a transferir por transferencia
- Se puede limitar la cantidad máxima de transferencias por cuenta
- Se puede limitar la cantidad máxima a transferir por período de tiempo
- Tras recibir una transferencia, se puede imponer un tiempo mínimo antes de poder transferir el objeto
- El orden de las transacciones debe ser mantenido

La autorización determina que solamente el dueño de la cuenta origen sea capaz de ejecutar una transacción en su nombre, por ende, cada transacción debe tener pruebas del consentimiento de dicha cuenta.

Hashing Data

Se ha mencionado que la tecnología *blockchain* es capaz de brindar una serie de beneficios relacionados a la integridad e inmutabilidad de los datos almacenados [12]. Muchos de éstos son adquiridos a través de la aplicación del concepto criptográfico llamado *Hashing*. Las funciones criptográficas *hash*, como *Secure Hash Algorithm* o *SHA-256*, toman como entrada cualquier tipo de información y la transforman en un único número pseudo-aleatorio de longitud fija. De esta forma,

para tener un mismo número *hash* es necesario tener exactamente la misma información de entrada. Además, por ser pseudoaleatoria la asignación del valor *hash*, es imposible predecirlo a través de los datos de entrada. Por este mismo motivo, tampoco es posible deducir la información de entrada a partir del valor *hash*. La capacidad de anidar o combinar valores *hash* resulta muy útil para corroborar varias entradas de información encadenadas solamente a través del último valor *hash* obtenido, y es un concepto muy importante en el uso de *blockchain*.

Criptografía

La base para identificar a las personas y proteger sus pertenencias se encuentra en la criptografía. El desafío está en permitir la capacidad de acceder y transferir las propiedades que se encuentran en la *blockchain* solamente a los propietarios de las mismas. Para esto se utiliza la criptografía simétrica o la asimétrica. La idea en común es que se busca encriptar cierta información, utilizando lo que se conoce como “llave”, enviarla al receptor y luego desencriptarla para que el mismo pueda acceder a ella.

La criptografía simétrica utiliza la misma llave para encriptar y desencriptar la información, mientras que la asimétrica utiliza dos llaves complementarias, la pública y la privada. La llave pública de un usuario es la dirección donde recibe las propiedades transferidas por terceros. La información es encriptada por la llave pública y enviada al remitente. Éste desencripta la información con su llave privada.

En *blockchain*, la criptografía asimétrica se utiliza con dos propósitos, la identificación de cuentas y la autorización de transacciones [13].

Cadena de bloques

Con la meta de almacenar grandes cantidades de información, *blockchain* utiliza una estructura de cadena de bloques. Un bloque es un activo informático que empaqueta transacciones, se identifica de manera individual con un *hash* y se asocia a otros bloques para formar el estado de información del sistema. Además, en un bloque se registra el momento de su creación, y el *hash* del bloque anterior, junto con el suyo propio, entre otras cosas. De esta forma, el *hash* del bloque anterior forma parte de los datos de entrada necesarios para generar el *hash* del bloque actual. Por ende, al concatenar *hashes*, cualquier modificación en un bloque ya establecido en la cadena, desencadenaría una alteración en el *hash* de todos los bloques posteriores. Esto permite detectar una eventual corrupción de datos de forma rápida y eficiente.

Capas

Según los conceptos de arquitectura de software del curso *Fundamentos de ingeniería de software - Fing*, el desarrollo de un software por capas se basa en la agrupación de funcionalidades para crear un sistema ordenado y sencillo [14]. Cada capa le brinda servicios a las capas superiores y demanda servicios de capas inferiores. El sistema se vuelve mantenible puesto que, al detectar una solicitud de

mantenimiento de una funcionalidad de una capa específica, se puede trabajar sobre esa capa únicamente sin tener que modificar el resto del sistema. La cantidad de capas debe ser escogida tomando en cuenta la complejidad, la robustez y la adaptabilidad necesaria para el sistema, entre otros.

Las capas existentes en una estructura de *blockchain* teórica se detallan a continuación [15].

Capa de aplicación

La capa de aplicación es aquella capa en la que se codifican las funcionalidades y la aplicación para los usuarios finales.

Capa de ejecución

En esta capa se ejecutan las instrucciones accionadas en la capa de aplicación en cada nodo de la cadena. Estas instrucciones pueden estar asociadas en forma de contratos inteligentes o *smart contracts*.

Capa semántica

En la capa semántica ocurren las validaciones de las distintas instrucciones que provienen de la capa de ejecución. En esta capa se definen las distintas reglas que gobiernan el sistema, como son modelos de datos y estructuras. Se define, por ejemplo, cómo están asociados los distintos bloques. Además, esta capa se encarga de autorizar las distintas transacciones. Si bien el sistema como un todo funciona gracias a la interacción de todas las capas, las relaciones entre bloques se definen en la capa semántica.

Capa de propagación

Esta capa permite la conexión y sincronización entre los distintos nodos para establecer el estado de la cadena. Todas las comunicaciones entre nodos como ser la propagación de una nueva transacción o la propagación de un nuevo bloque, se ejecutan en esta capa, asegurando la estabilidad de la cadena entera.

Capa de consenso

La principal función de esta capa es lograr el consentimiento de todos los bloques sobre el estado del registro, aunque en ésta también se asegura la seguridad de la cadena. En las cadenas públicas es necesario que exista un mecanismo de incentivo para fomentar la búsqueda de este consenso y para mantener la red viva. De esta forma aparecen conceptos como el *mining* o el *Proof of Work*, en los cuales se ahondará en la siguiente sección.

Mecanismos de Consenso

En la *blockchain*, los nodos comparten en tiempo real su versión de la cadena de bloques. En general, los nodos del sistema se encuentran realizando permanentemente dos posibles actividades: evaluando la validez de un bloque recientemente agregado o intentando agregar un nuevo bloque a la cadena. En la práctica, la seguridad del sistema es garantizada en el momento de creación de nuevos

bloques, a través de los mecanismos de consenso, que garantizan la utilización de una única versión de la cadena en todos los nodos. Los mismos determinan el procedimiento para verificar la validez de la información a agregar en los bloques y previenen los ataques a la integridad del sistema. Las más conocidas amenazas son las siguientes:

- **Doble gasto:** Es un potencial defecto que permitiría la utilización de la misma moneda para efectuar dos pagos distintos, si se realizan al mismo tiempo. Ambos pagos son comunicados, pero solo una de las transacciones podrá ser aceptada y validada en un bloque, dejando a uno de los vendedores con su transacción denegada y por ende, sin cobrar.
- **Ataque del 51%:** Ocurre cuando un hacker posee el control del 51% de los nodos del sistema. Puede alterar la cadena a la versión que mejor le convenga, ya que tendría consenso acerca de la validez de la misma.
- **Sybil Attack:** Se intenta corromper la red agregando nodos falsos que intentan validar transacciones desautorizadas y alterar transacciones válidas. El objetivo es denegar bloques legítimos y superar el poder de decisión de los nodos independientes.

Para combatir en gran medida dichas amenazas, existe una variedad de métodos de consenso que, en base a sus protocolos y naturaleza, requieren de distinta capacidad computacional, impactando en distintos costos y rendimientos energéticos. Los más utilizados son *Proof of Work* y *Proof of Stake*, que serán introducidos a continuación:

Proof of Work (PoW): Este método se basa en la resolución de una ecuación matemática por parte de los mineros, para poder autorizar y grabar un nuevo bloque en la cadena. La solución de dicho problema requiere de gran esfuerzo computacional, ya que es obtenido a través de ensayo y error, pero su verificación es muy sencilla. El objetivo consiste en encontrar un número (llamado *nonce*) e incluirlo en el bloque, de forma que a través de la función *hash*, se genere un resultado menor al *hash* objetivo.

Su principal desventaja es el alto consumo eléctrico y el tiempo comparativamente mayor de minado. El proceso en el que el sistema *blockchain* maneja la constante actualización de información con PoW es el siguiente:

1. Nuevas transacciones son enviadas a todos los nodos.
2. Cada nodo elige estas transacciones para intentar procesarlas y almacenarlas en un bloque.
3. Se verifica la correctitud semántica, formal y autorización de las transacciones seleccionadas.
4. Se intenta resolver el problema *hash* para este conjunto de información seleccionada.
5. Al resolverlo, se envía el bloque a todos los demás nodos.
6. Cada nodo verifica la resolución del problema *hash* del bloque agregado, así como la validez de las transacciones que contiene.
7. Cada nodo agrega entonces el bloque validado a su versión de la *blockchain*.
8. El nodo que propuso el bloque recibe la recompensa por haberlo logrado.

Proof of Stake (PoS): En este caso, la creación de un nuevo bloque por parte de un nodo es determinada en base a un factor denominado participación. La participación de un nodo es medida en función de la cantidad de tokens o monedas que posee. Al tener una mayor cantidad de monedas,

mayor es la probabilidad de ser asignado con la tarea de creación del bloque. Esto reduce el consumo de energía necesario y asigna la responsabilidad de validación a quienes tienen interés y participación monetaria en la *blockchain*. La recompensa se realiza en función a comisiones por transacción validada y no por minado de bloque [16].

Casos de Uso

Si bien hoy en día la tecnología *blockchain* se conoce principalmente por su utilización en criptomonedas, se considera que, en muchas otras áreas, la misma podría ser tan disruptiva como lo fue el internet a fines del siglo XX. A modo de ejemplo, se presenta un resumen acerca de la utilidad de *blockchain* en distintas industrias y servicios [17].

Salud:

- Pfizer: La corporación farmacéutica estadounidense utiliza *blockchain* junto con Biogen para la gestión digital del inventario de productos.
- *The United States Food and Drug Administration* (FDA): esta organización del Gobierno de Estados Unidos incorporó *Hyperledger* para potenciar una plataforma de almacenamiento seguro de datos. Esto permite que los clientes registren de manera confidencial y segura su información clínica como estudios, información genómica y otros registros médicos.
- DHL: esta empresa está trabajando en un sistema de trazabilidad de farmacéuticos del punto de origen al punto de consumo, apoyándose en *blockchain*. Esto busca controlar la problemática diaria de alteración y falsificación en sus productos.

Seguros:

- AEGON: utilizando la plataforma *R3Corda*, esta empresa del Reino Unido respalda su plataforma de seguros.
- *Prudential Financial*: la aseguradora americana planea utilizar *blockchain* para garantizar la ausencia de fraudes en los negocios aseguradores, y que sus clientes puedan probar la propiedad de su documentación de manera transparente, mejorando el servicio brindado.
- AIG: este grupo trabaja en el desarrollo de la “plataforma de seguros inteligente” mediante *blockchain*, de manera de poder abarcar en su gestión digital todas las casuísticas de la prestación de seguros internacional.

Cadenas de suministro:

- Walmart: la cadena de supermercados es una de las instituciones pioneras en la utilización de *blockchain*. Junto con IBM -utilizando *Hyperledger Fabric*- se buscan respaldar los procesos de la cadena de suministro trazando los alimentos vendidos desde el origen hasta el consumidor final. El objetivo es que los clientes en el supermercado tengan acceso a la información de producción de cada alimento, para poder seleccionarlos considerando su procedencia.
- Ford: nuevamente IBM trabaja junto con la ensambladora de autos en una solución que permita rastrear el proceso de extracción y traslado de algunas materias primas críticas como el cobalto. En este caso, se pretende crear registros en el momento mismo del minado de esta materia prima, y agregar información relevante desde ese momento hasta su entrega a las industrias. Esto radica en la necesidad de garantizar la autenticidad de estas materias primas; un esfuerzo más en la búsqueda de la calidad en sus productos.
- Unilever: esta multinacional del Reino Unido utiliza *blockchain* para mantener registro de todas las transacciones que se dan en la cadena de suministro de productos particulares como el té.

Generación de energía:

- Shell: esta multinacional angloholandesa se encuentra en la investigación activa para lograr usos particulares en plataformas de *blockchain* como el comercio del petróleo, el aseguramiento de la transparencia y la prevención del fraude.
- *Abu Dhabi National Oil Company* (ADNOC): de similar forma, este grupo de compañías garantiza la transparencia entre las empresas participantes a través de *blockchain*, y también pretende extender los usos hasta la administración de la cadena de suministro.
- Comisión Nacional de Energía de Chile: el sector de producción de energía sufre de discrepancias en el manejo de la información, por lo que esta comisión decidió utilizar una plataforma de *Ethereum* para almacenar la información en registros inalterables.

Transporte internacional:

- British Airways: trabajan con una *startup* de desarrollo de software para acelerar sus procesos de chequeos de seguridad, para evitar generar demoras en los vuelos.
- Lufthansa: comenzaron la iniciativa “*blockchain for Aviation (BC4A)* para integrar a los principales actores de la industria: fabricantes, proveedores logísticos, proveedores de servicios de mantenimiento y desarrolladores de software, entre otros.
- Singapore Airlines: utiliza la tecnología para ofrecerle promociones a sus clientes frecuentes, a través de una aplicación celular.

Gobiernos:

- *Government of Dubai*: apunta a transformar la ciudad en la primera ciudad inteligente, a través de, entre otras cosas, *blockchain*. Se busca volcar en *blockchain* toda la información relativa a la vida cotidiana de un ciudadano, como los consumos del hogar y pago de servicios.
- *Seoul Metropolitan Government*: su sistema administrativo será basado en *blockchain* y se establecerá una criptomoneda nacional para el pago de servicios públicos.
- Lantmäteriet: es el nombre de la autoridad de registro de tierras suiza y aplicaría *blockchain* para la reducción de tiempo y papeleo involucrado en el proceso de compra de una propiedad. Se iniciaría un almacenamiento de documentos de forma digital para eliminar de esta forma el consumo de papel.
- *Monetary Authority of Singapore*: este proyecto planea ofrecer pagos en distintas criptomonedas a través del mismo sistema e incentivar el uso de la tecnología en la industria.

Internet of Things (IoT):

La tecnología *Internet of Things (IoT)* es definida en el libro *Internet of Things from Hype To Reality*, como la intersección entre objetos, Internet y datos. Refiere a una conexión digital, capaz de compartir datos, entre objetos cotidianos y la Internet. Para esto se necesita indispensablemente la equipación de sensores en los objetos capaces de recolectar información disponible y así crear los datos a ser comunicados a través de un puerto IP.

Al generar una gran cantidad de datos, las principales preocupaciones relacionadas a IoT se centran en la privacidad, seguridad y el control de esta información valiosa y representativa. Es importante recordar que los mencionados objetos están continuamente presentes en la vida cotidiana de las personas, por lo que pueden ser una fuente de información sensible y personal. Las plataformas de

blockchain con mecanismos de consenso como *Proof of Stake (PoS)* o *Proof of Elapsed Time (PoET)* se pueden perfectamente utilizar junto con IoT para desarrollar casos de usos innovadores. Además, la arquitectura descentralizada propia de *blockchain* puede potenciar aplicaciones de IoT a gran escala, permitiendo interacciones M2M (máquina a máquina) -interacciones que son esenciales para alcanzar el máximo potencial de IoT-, y también asegura privacidad de los datos y protocolos de seguridad confiables. Es por este motivo que se evidencia una importante sinergia entre dicha tecnología y *blockchain*, que permite compensar sus mencionadas limitaciones o riesgos y apalancar sus beneficios de manera auspiciante.

Un ejemplo de la implementación integrada de ambas tecnologías es la utilización de contadores inteligentes conectados por IoT para el monitoreo en vivo de los consumos energéticos en hogares, que permita que los proveedores de energía puedan establecer patrones de consumo para ajustar el pronóstico de generación de energía. El uso de *smart contracts* en una *blockchain* también habilitaría la transferencia de energía entre hogares de manera automática, ya sea por contar con excedentes de energía según la previsión desde el proveedor, y además se podría transferir la energía generada en paneles solares o molinos de viento, como se desarrolla en el caso de uso de *Gestión compartida de energía solar*. También se destaca el caso de uso de la compañía naviera danesa Maersk; el desarrollo de una *blockchain* respaldada en IoT para optimizar el flujo de su cadena suministro y aumentar la trazabilidad de sus navieras. Por otro lado, la organización no gubernamental *Smart Electric Power Alliance* busca brindar energía renovable a distintos pilares claves de la sociedad como la educación e investigación a través de IoT, respaldada con la seguridad de *blockchain*.

Se eligió un caso de uso específico para profundizar en la utilización de blockchain desde un punto de vista técnico.

Gestión compartida de energía solar

La necesidad de efectivizar el consumo de energía eléctrica por parte de un grupo de hogares conectados a una central fotovoltaica motivó el desarrollo de este caso de uso [18]. Se ideó un sistema en el cual una cierta cantidad de participantes (hogares) puede solicitar cantidades fijas mensuales de energía eléctrica a la planta, pudiendo además colocar excedentes a otros usuarios que necesiten una cantidad mayor a la que la planta le puede entregar. De esta forma, se planteó el montaje de una plataforma que permita gestionar la transferencia de energía eléctrica entre los participantes y la planta, permitiendo contabilizar las cantidades consumidas y transferidas por cada usuario para su posterior facturación.

El sistema funciona en base a cuotas preasignadas de energía eléctrica que recibe cada hogar desde la central. Esta información se envía al proveedor que crea facturas individuales. Independientemente a la cuota recibida por la central, los usuarios pueden transferir energía entre ellos, lo que se modela sobre una estructura de *blockchain*.

Cada participante cuenta con un dispositivo de hardware (nodo) que ejecuta el software de *blockchain* además de una aplicación móvil que permite enviar datos al nodo, acerca de las porciones enviadas y recibidas de energía solar. Estos nodos se conectan por internet, en una red privada (VPN).

La aplicación móvil se conecta al nodo del cliente para enviar y recibir información acerca de nuevas transacciones a la red, y además se conecta al sistema de facturación. De esta forma, la aplicación de un cliente particular lee la cadena más larga, y filtra las transacciones particulares de su cliente, para desplegar los consumos y transferencias de energía en cada instante temporal.

Al momento de realizar la facturación por la energía consumida, el sistema de facturación utiliza una interfaz de programación de aplicaciones (API) en cada nodo para solicitar la información de todas las porciones consumidas por cada cliente, y mapear los balances finales. El resultado de este proceso se despliega en la aplicación móvil del usuario para que lleve adelante el cobro y pago correspondiente.

Las comunicaciones entre nodos, con la aplicación y el servicio de facturación se ejecutan en la capa de aplicación. Todos los mensajes son firmados por los emisores, y puesto que cada participante conoce las claves públicas del resto de los participantes, aquellos mensajes con firmas inválidas son descartados. Todos estos componentes del sistema se comunican sobre una red privada (VPN).

A pesar de las ventajas mencionadas (descentralización, confiabilidad e inmutabilidad), las principales desventajas de un sistema de *blockchain* son su limitada escalabilidad y su alto consumo de recursos computacionales.

La escalabilidad se define como el tiempo necesario para la propagación, procesamiento y validación de las transacciones. Cuanto mayor cantidad de nodos, se precisa un mayor ancho de banda, mayor espacio de almacenamiento y mayor consumo de energía. A modo de ejemplo, el consumo de energía a mayo de 2018 de la red de *Bitcoin* fue aproximadamente de 70 TWh por año.

Para aplicar en este caso particular, se exploraron 4 distintos tipos de *blockchain* y se analizó hasta qué punto son competentes para este caso. Los 3 tipos de *blockchain* analizados son:

1. *Ethereum*: La utilización de *smart contracts* permite representar transacciones complejas, que permiten gestionar y actualizar los estados de cada nodo. De todas formas, se considera que la implementación en *Ethereum* es compleja y por ende excede los requerimientos del caso. Además, el almacenamiento de datos a través de un *smart contract* puede implicar altos tiempos de procesamiento que se transforman en una ejecución lenta. En este caso desde la perspectiva del usuario será necesario disminuir al máximo los tiempos de ejecución, por lo que no resulta beneficioso utilizar *Ethereum*.
2. *MultiChain*: Esta red se focaliza en transacciones financieras, y como el caso de uso no las precisa, sería necesario modificar el mecanismo de consenso. Además, las plataformas que soportan esta *blockchain* presentan limitaciones para adaptarse a este caso, por lo que se decide desestimar esta opción.

3. *OpenChain*: Es una red privada diseñada específicamente para ser eficiente en términos de consumo energético. El mecanismo de consenso es *proof of authority* en lugar de *proof of work*, por lo que se aplica para casos en que se busque una red centralizada. Sin embargo, en este caso se busca una red descentralizada por lo que esta plataforma no aplica.

Finalmente, se decidió construir una *blockchain* específica para este caso, puesto que ninguna de las *blockchain* analizadas cumplía los requisitos necesarios.

Por otro lado, en lo que respecta a la implementación en sí, se obtuvieron algunas conclusiones técnicas que son valiosas para considerar en el proyecto actual. Por ejemplo, se verificó que, para sistemas con poca cantidad de usuarios, el *Proof of Work* no es la opción más conveniente por cuestiones de escala de aplicación relacionadas al consumo energético que requiere. De esta forma, se menciona que para aquellos sistemas con menos de 1000 usuarios es más conveniente utilizar algoritmos de consenso del tipo *Byzantine Fault Tolerance (BFT)*. Por otro lado, se observó que para aquellas comunicaciones y transacciones que incluían conexiones encriptadas, el tiempo de transferencia de la información fue mucho mayor que para las transacciones no encriptadas, más allá de la cantidad de datos que se transfirió. Por esta razón, será conveniente mantener las comunicaciones encriptadas sólo para casos que sean realmente indispensables.

La principal conclusión del artículo se centra en que si bien implementar *blockchain* para casos de uso de este estilo (cantidad reducida de nodos, red privada, utilización de aplicaciones móviles, conexión con sistema externo) es complejo, sigue siendo viable. A medida que la cantidad de usuarios aumenta, se ve un aumento exponencial de los beneficios de utilizar esta tecnología.

La arquitectura del sistema del caso se esquematiza a continuación en la Figura 2.

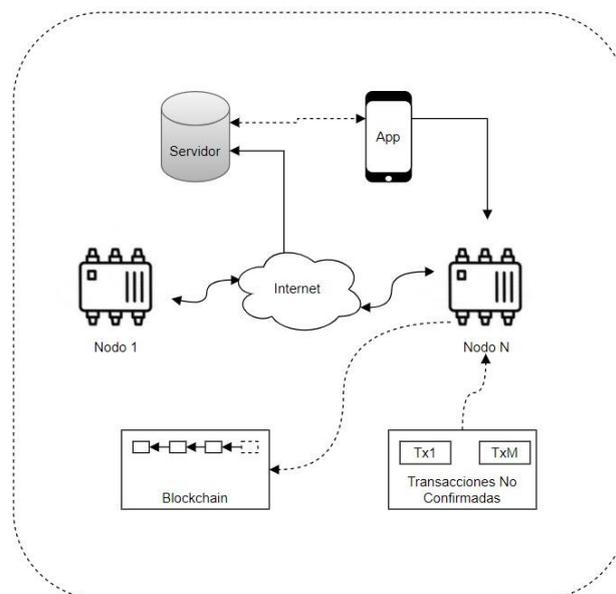


Figura 2 - Arquitectura del sistema del caso

Análisis contextual de la industria cárnica

El complejo cárnico - motivación

La Organización Mundial de la Salud (OMS) asegura que en la actualidad la contaminación alimenticia provoca enfermedades en el 10% de la población y se registran 420.000 muertes al año por esta causa, un tercio de ellas en niños menores de cinco años [19]. Por fortuna o desgracia, todas esas muertes son prevenibles, pero son necesarios recursos y herramientas que aún no han sido utilizados. Si se quisiera localizar la fuente de contaminación de un producto, actualmente este proceso llevaría semanas, en las que se desperdicia tiempo clave de toma de acciones de contingencia. Esto depende del grado de integración de los sistemas de trazabilidad, que en general no logran involucrar a todos los actores relevantes. Además, se basan en información incompleta, que precede de diversas fuentes con distintos formatos no compatibles entre sí. Al mismo tiempo, la transferencia de información no siempre ocurre de manera transparente, inmutable y fiable.

Por otro lado, las nuevas tendencias de los consumidores exigen mayor información acerca de la procedencia de los alimentos consumidos. En la industria cárnica, interesa informar si se cumplieron las buenas prácticas de trato animal o si se utilizaron antibióticos, y disponibilizar información acerca de la huella ecológica o de qué manera fue criado el ganado, entre otros. Por ejemplo, es sabido que la carne proveniente de pastoreo extensivo y la carne producida en *feedlot* se valoran de forma distinta e incluso se comercializan con precios distintos. Esta información no sólo es relevante para el consumidor, sino que también debe estar disponible para evitar fraudes y para garantizar al productor el reconocimiento por cumplir las buenas prácticas y así asegurar la prima adicional por el diferencial de su producto, cualquiera sea. De hecho, un reporte de la *IP Commission* de Estados Unidos que trata sobre la propiedad intelectual de dicho país, evidencia que la producción no original de bienes -entre otros, productos cárnicos indicados con una certificación no fidedigna- genera un costo de entre 225 y 600 mil millones de dólares anuales a la economía estadounidense. Es por esto que se considera oportuno investigar hasta encontrar un sistema que logre certificar esta información para mayor satisfacción del consumidor y como incentivo al productor.

El sector Cárnico en Uruguay

El campo siempre fue parte de la identidad del pueblo uruguayo. Aún sin tener la capacidad de proveer inmensos volúmenes al mundo, el país es reconocido mundialmente por la calidad y confiabilidad de los productos ganaderos y agropecuarios exportados. Como ejemplo de esto y del rumbo hacia donde apunta Uruguay, es que desde el 2006 los productores ganaderos registran el 100% de sus bovinos, en un sistema de trazabilidad total, ejemplar en el mundo. Además, como fue mencionado al principio de esta sección, y debido a las deficientes condiciones higiénicas y sanitarias en distintos países del mundo, la tendencia mundial empieza a quitar el foco en la eficiencia de producción del producto, para dar mayor importancia a la ética en los procesos. Esto deriva en un aumento en la regulación de

los mercados y en el interés por la bioseguridad en los alimentos, por lo que comienza a adquirir gran valor la información legítima acerca la producción de los mismos.

Luego de una extensa investigación que incluyó contacto con distintos actores de la cadena cárnica (productores, directores de plantas de faena, despachantes de aduana, técnicos del INAC y del MGAP), así como acceso a publicaciones y seminarios [20] se llega a la conclusión de por qué Uruguay está en un punto de inflexión en el que puede potenciar su productividad y aumentar sus exportaciones en base a productos ganaderos con la incorporación de nuevas tecnologías, como puede ser *blockchain*. Son varios los expertos (asesores de las cadenas BPU y Marfrig, periodistas, desarrolladores de software asociados al rubro, autoridades del INAC) que coinciden en el análisis de la situación en que se encuentra Uruguay, en sus desafíos y oportunidades de mejora. Habiendo recabado todas estas opiniones, se describe a continuación la situación actual de la industria cárnica en Uruguay.

Para empezar, se destaca que Uruguay tiene un complejo cárnico muy reconocido internacionalmente, con un saldo exportable del 70% para el rubro. Esta industria goza de una privilegiada gobernanza con una institucionalidad muy sólida -puesto que en las mesas de discusión se representa a públicos y privados- lo que llevó al desarrollo de sistemas de información que, a diferencia de otros países de la región, funcionan como bienes públicos de aplicación universal, en lugar de tratarse de bienes de club. De esta forma, todos los productores tienen la posibilidad de ingresar a los circuitos de mercados a los que accede Uruguay. En los últimos años, los sistemas de información uruguayos permitieron una gran ventaja sobre países competidores en acceso a mercados. Sin embargo, esa ventaja no es ilimitada, por lo que el Uruguay se encuentra en un punto crítico en el que debe buscar el mantenimiento y desarrollo de su ventaja competitiva, para evitar ser paulatinamente equiparado por otros países exportadores.

Esto se da en el contexto de un cambio en las demandas del cliente; los mismos desean estar muy informados acerca de los procesos de producción de los productos consumidos, son analíticos y críticos, están más atentos a la salud física y mental, consideran especialmente la relación de confianza con la marca, y presentan una especial atención a la producción sostenible. En abril de 2021, Uruguay participó por primera vez de la feria de alimentos más grande del sur de China, lo que resultó una gran oportunidad para la industria cárnica uruguaya. A partir de su experiencia en la primera línea de la búsqueda de nuevos mercados, y acerca de dicha feria, el actual Gerente de Marketing del INAC, Lautaro Pérez, fue entrevistado por el diario El Observador, donde puntualizó, *"Lo que ha cambiado en el público chino y en las cadenas es que hay un foco mucho más fuerte hacia la seguridad y la transparencia de la integridad de los datos a lo largo de toda la cadena"*. Además, en el artículo comenta que *"el tema de trazabilidad de la carne ha pasado a ser "más fuerte". Hoy los consumidores están interesados en saber, por ejemplo, de qué planta frigorífica proviene la carne, cuándo salió embarcada de Uruguay, cuándo llegó al puerto en China y qué sucedió desde que desembarcó hasta que llegó al puesto de comercialización. Con certificados logísticos, códigos QR que están en las góndolas, se puede leer esa información."* [21]

Hasta ahora, los programas de trazabilidad, Sanidad en Campo e Inocuidad en Planta fueron suficientes para garantizar la confianza al consumidor acerca de las formas de producción. Según un trabajo del Centro de Investigaciones Económicas (Cinve) citado por el INAC, en 2017 el costo de los

bienes públicos para la Sanidad en Campo se elevó hasta US\$22 por cabeza de ganado, US\$9 por cabeza de ganado para la Sanidad en Planta, y la Inocuidad en Planta costó unos US\$9 por cabeza de ganado. Esto termina por establecer un costo de US\$40 por cabeza de ganado para mantener el estatus sanitario, inversión que realiza la sociedad para hacerse de los beneficios de este sistema.

Esto es, en parte, lo que motiva a buscar nuevas alternativas para el sistema -como una alternativa tecnológica- que permitan hacer un sistema más moderno, menos costoso y más eficiente. El sistema de trazabilidad actual es un sistema que, si bien se sigue apoyando en documentos a papel, tiene una trayectoria muy seria y reconocida. Actualmente la trazabilidad en campo es complementada por la trazabilidad en la industria. Sin embargo, la información asociada a esta trazabilidad se gestiona por distintas organizaciones independientes, dificultando por momentos su rápido y global acceso.

Otro desafío al que se enfrenta dicho sistema es el flujo transparente y eficaz de la información hacia adelante, y, sobre todo, hacia atrás en la cadena de suministro. La inclusión de tecnologías que mitiguen esta desventaja permitiría formar una cadena de suministro con mayor colaboración y en la cual se puedan generar sinergias positivas. Por estos motivos, el sistema se debería rediseñar para que sea más liviano, menos invasivo, más efectivo, y que dé lugar al aseguramiento de otros aspectos cualitativos del producto, según lo manifestaron las fuentes consultadas.

Por otro lado, se presenta un desafío para el mercado en lo que respecta al acceso a créditos. Históricamente, los robustos sistemas de información brindaron beneficios como garantizar buenas condiciones sanitarias, obtener certificaciones y, justamente, mejorar el acceso al sistema financiero. Por lo tanto, la necesidad de actualizar y escalar el alcance de las tecnologías existentes también puede catapultar al mercado mediante un mejor acceso al sistema financiero, y obtención de seguros que generen mayor confianza. El agregado de valor que trae consigo este rumbo, debe ser distribuido a lo largo de la cadena de valor, para potenciar el sistema en su conjunto y generar sinergia entre actores de la misma cadena, más que competencia.

A partir de estas necesidades, se analizaron distintas soluciones desarrolladas en distintos países, y algunas de ellas se presentan a continuación.

Casos de uso en el negocio cárnico

IBM Food Trust – China

Este proyecto comenzó con el objetivo de lograr la trazabilidad y transparencia alimentaria en la carne de cerdo en China [22]. Es una plataforma que logra conectar a productores, procesadores, distribuidores y minoristas a través de un registro permanente, compartido y con permisos de todos los datos del sistema alimentario permitiendo rastrear alimentos en 2,2 segundos.

Funciona como un sistema de 4 módulos (*Trace, Certification, Fresh Insights y Third-Party APIS*) que permiten acceder a una base de datos segura que contiene el historial de todos los actores que han participado en la cadena alimentaria.

Carnes Validadas – Argentina

El objetivo de la plataforma Carnes Validadas es el de proveer al consumidor, del historial de procesamiento del producto para validar información relacionada a quién, dónde, cómo y de qué modo fue producido el producto final [23]. Brinda una trazabilidad específica de las reses y terneros identificados electrónicamente para levantar datos sobre su desarrollo y entrega un registro en tiempo real sobre los movimientos de la res, el cual incluye plan sanitario del animal, pesaje, sistema de producción y alimentación, comercialización y/o transporte.

Gracias a la seguridad y fiabilidad del registro de datos que facilita la *blockchain*, tanto distribuidores como consumidores pueden obtener los detalles que hacen a la calidad y modo en que fue producida la carne.

Carnes Validadas logra que el producto final, además de sus cualidades físicas (sabor, olor, frescura, etc.), tenga toda la información sobre las prácticas en las que se incurrió en las distintas etapas de producción de este alimento. De esta forma los agentes de la cadena pueden conseguir un premio por sus buenas prácticas, o por su buena reputación.

Beef Ledger – Australia

Beef Ledger ofrece una plataforma *blockchain* en la que los consumidores pueden validar las credenciales del producto que adquieren, con la certeza de acceder a información fidedigna [24]. Los distintos actores de la cadena de suministro registran información relevante creando un historial de cada producto, que es accesible por el consumidor. La aplicación disponible para los clientes permite leer códigos QR, para que, a partir de esa lectura, se despliegue este historial.

Los seis grandes objetivos de esta plataforma son los siguientes.

1. Aumentar confianza acerca del origen de los productos cárnicos
2. Potenciamiento de la marca y aumento de la rentabilidad de la cadena de suministro
3. Aumento de la seguridad para realizar transacciones monetarias asociadas al proceso productivo
4. Mitigación del riesgo de fraude alimentario
5. Posibilidad de brindar mayor *feedback* a los productores para fomentar la mejora continua del proceso
6. Aumento de la transparencia en las distintas implicancias ecológicas, sociales y económicas

Análisis tecnológico

Tomando en cuenta los desafíos del rubro, resulta menester contar con un sistema más integral de trazabilidad a lo largo de la cadena entera, como lo puede brindar *blockchain*. En este contexto, las organizaciones que no puedan brindar transparencia, seguridad alimentaria, o garantías sobre el respeto al medio ambiente y sobre la sostenibilidad del proceso de producción, no se podrán mantener en el mercado. Para confirmar que se esté apuntando hacia la dirección correcta en cuanto a la tecnología propuesta, se analizó el siguiente algoritmo que se enfoca precisamente en detectar, en base a las características del negocio, la aplicabilidad y concordancia de la integración de un sistema *blockchain* [25].

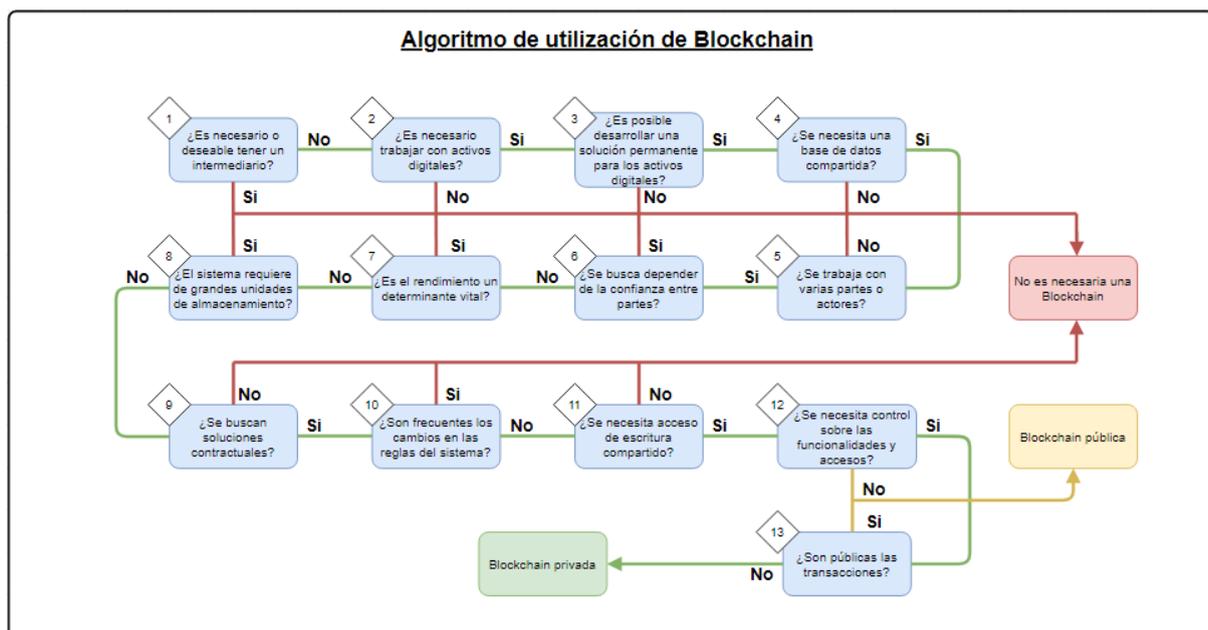


Figura 3 - Algoritmo de evaluación sobre la necesidad de utilizar blockchain

1. En función del primer cuestionamiento, se entiende que la posibilidad de evitar intermediarios brindaría a la cadena de suministro una reducción en el *lead time* y ahorro de los costos asociados a su participación y servicio. En este punto, también se consideran las ventajas de contar con un sistema sin intermediarios (descentralizado) que fueron detallados en la sección *Sistemas Centralizados y Descentralizados*.
2. Uno de los propósitos de la aplicación de esta nueva tecnología es evolucionar hacia un modelo de negocio libre papel, con una transición hacia la digitalización, para aprovechar los beneficios que esta condición proporciona, entre ellas, la fácil accesibilidad a documentos y su inmediato intercambio entre partes. Los activos considerados son principalmente documentación e información.
3. Al analizar la posibilidad de desarrollar una solución permanente para la gestión de estos activos digitales, queda claro que en ese caso serán necesarias definiciones estructurales como la definición de los canales de comunicación con reglas de gobernanza establecidas

desde un principio y no frecuentemente modificables. De esta forma, una solución permanente es aplicable para el caso de estudio.

4. Resulta evidente la necesidad de trabajar con una base de datos compartida puesto que el complejo se compone por varios participantes distintos (productores, despachantes de aduana, plantas de faena, INAC, MGAP, Aduana, etc) que intercambian información, y en ocasiones se completan registros o documentos únicos a partir de información que está repartida por los distintos nodos.
5. Por lo descrito en el punto anterior, queda claro también que el sistema trabajará con varios actores distintos.
6. En la cadena de suministro se intentan crear vínculos de confianza entre proveedores y clientes para poder garantizar cumplimientos de entrega de mercadería, información y pagos. Si fuera posible mantener y dar por sentado esto, aún sin el vínculo de confianza, se podría cambiar de proveedor y cliente de forma más dinámica para maximizar otros aspectos como los costos o la calidad. De esta forma, se busca no depender de la confianza de los actores.
7. Si bien la utilización de *blockchain* presenta grandes ventajas, una de las principales desventajas radica en el rendimiento. Aunque resulte sorprendente, la respuesta a esta pregunta es negativa. Obviamente esto no significa que no se desee que el sistema funcione con un alto rendimiento. Pero el costo de oportunidad de utilizar *blockchain* -y por ende sacrificar la calidad de rendimiento- es poco comparado con la utilización de una base de datos tradicional, por más que ésta pueda tener un mejor rendimiento. Por otro lado, los procesos involucrados en las cadenas de suministro en general manejan tiempos de respuesta mucho mayores a los ofrecidos por las distintas tecnologías.
8. Las cadenas de suministro, al involucrar un número limitado de actores, no requieren de grandes unidades de almacenamiento, como tal vez un sistema público y mundial de registro de transacciones si requiriera.
9. Una cadena de suministro es una consecución de relaciones contractuales, por lo que la posibilidad de utilizar *smart contract*, por ejemplo, para garantizar el cumplimiento de las partes es evidentemente un beneficio muy valorado.
10. Las reglas de gobernanza no deberían variar demasiado en cortos períodos de tiempo, pero, de todos modos, para acompañar el sistema con los avances tecnológicos y la evolución del negocio, se determinarán los procedimientos para alterar el sistema como se ve en la sección *Establecimiento de la gobernanza*.
11. En el caso de estudio, todos los usuarios deberían ingresar la información que les corresponda, y, si todos ellos están de acuerdo, la información podría estar disponible para todos. Por esta razón, se necesita un acceso de escritura compartida.
12. En este sistema será necesario tener control sobre las funcionalidades, principalmente por tratarse de un sistema cerrado, en el que se fijan reglas de gobernanza desde un comienzo y, eventualmente, los participantes podrán ponerse de acuerdo para actualizarlas o cambiarlas.
13. Ciertas cuestiones empresariales suelen ser sensibles y por ende no todas las transacciones deben ser públicas.

De esta forma, una *blockchain privada* se adapta a las necesidades del caso de estudio. A partir de esto, se diseñará un sistema particular para optimizar la cadena de suministro del complejo cárnico. La implementación del mismo implica una modernización tecnológica que abarca las necesidades

actuales de reducción de costos, optimización de transacciones, y reducción de burocracia y papeleo, entre otros beneficios que se mencionan. Además, permite brindar una plataforma en la cual los distintos actores podrán gestionar y acceder a información clave, y los clientes podrán obtener las demandas mencionadas.

Algunos ejemplos de tipo de información que se podrá transferir fácilmente a través de estos sistemas son:

- información desde balanzas para evitar fraudes
- información de cada animal particular vinculada a su número de caravana
- información acerca de la cuota de captura de carbono por uso de pasturas tanto durante la vida del animal como al momento del traslado de la mercadería
- información acerca del uso de antibióticos u hormonas
- certificaciones como la de productos orgánicos

Blockchain es capaz de brindar una mejor distribución de la información que se desea compartir, sin depender de ningún intermediario. Cada usuario es responsable de mantener, calcular y actualizar cada entrada y todos los nodos trabajan en conjunto para obtener una única versión verdadera del estado del sistema.

Por otro lado, la aplicación de *blockchain* contribuye con la búsqueda de la integración de la cadena de suministro al unificar la fuente de información en un mismo sitio confiable. De todos modos, dado que la información es poder en el mundo de los negocios, las empresas tienen gran cautela a la hora de entregar la información, y en este aspecto reside la diferencia entre la utilización de *blockchain* y cualquier base de datos encriptada. Al tener una base de datos centralizada, se le otorga la capacidad de obtener, controlar o manipular la información almacenada a quien esté a cargo de la misma, significando una ventaja estratégica con respecto a los demás participantes del sistema. Con *blockchain*, aun cuando la información no sea de visualización pública, la misma se encuentra almacenada por todos los integrantes de la cadena de suministro, para no permitir la alteración unilateral de la información. De esta forma, con la inmutabilidad de la información, se logra una igualdad de poder, una vez determinado el rol de cada actor de la cadena.

Elección de *blockchain*

En la actualidad existen decenas de distintos tipos de *blockchain*, que difieren en la tecnología implementada, en el grado de madurez alcanzado, en el propósito para el cual fueron creadas, en el método de consenso y en la privacidad intrínseca, entre otras. Dada la gran variabilidad de opciones, es necesario desarrollar un análisis para encontrar la *blockchain* que mejor se adapte a las necesidades del caso de estudio. Para esto, en primer lugar, se presentan algunas de las *blockchain* de mayor reconocimiento mundial, con sus características particulares, para luego evaluar la pertinencia de esas cualidades en el caso de aplicación. Para facilitar este proceso, se utiliza como fuente los artículos “*A blockchain platforms comparison*” [26] y “*Unhyped comparison of blockchain platforms*” donde se estudian las especificaciones de cada tipo de *blockchain* [27]. Evaluando dichos documentos se llega

a la conclusión que la *blockchain* que conviene utilizar es *Hyperledger Fabric*, pero aun así vale mencionar de forma sintética a las demás consideradas.

Ethereum

Es una *blockchain* pública que utiliza *Proof of Work* como mecanismo de consenso para acordar la cadena común entre todos los nodos [28]. Utiliza la criptomoneda *Ether* como recompensa a los nodos participantes que consoliden los bloques, a través de comisiones de transacción (*fees*). Al ser una plataforma de *blockchain* genérica, brinda la posibilidad de aplicarla en la industria a través de la utilización de *smart contracts*, aunque con la característica de ser totalmente transparente en cuanto a las transacciones realizadas, sin brindar privacidad. El lenguaje de programación de los *smart contracts* es "Solidity". La ejecución de los *smart contracts* en *Ethereum* es llevada a cabo por *Ethereum Virtual Machine*, garantizando que cada transacción respete las reglas declaradas en su contrato. Además de las transacciones, cada nodo incluye también la información acerca de cuánto *Ether* tiene cada cuenta, el código de los *smart contracts* y el estado de cada *smart contract*.

Hyperledger Fabric

Es una *blockchain* privada, que solamente buscará consensos dentro de los nodos participantes y no utiliza criptomoneda [29]. Su diseño y arquitectura está enfocada en el desarrollo de proyectos *blockchain* en el mundo empresarial. Tiene la capacidad de establecer canales de información entre distintos nodos, ofreciendo privacidad a las transacciones. Al ser una red permissionada, todos los miembros participantes tienen que obtener una certificación emitida por su organización para formar parte. Además, existen distintos tipos de nodos dentro de cada organización que se diferencian por sus roles y funcionalidades:

- *Orderers*: Se encargan de la comunicación entre nodos, y de que la información compartida sea consistente entre todos. Son los que reciben las transacciones, forman los bloques y envían los mismos a cada uno de los *leader peers* de cada organización.
- *Peers*: Mantienen su propia copia de las dos partes de la *ledger* que se almacena. Estas dos partes son, la *blockchain*, que almacena todo el historial de transacciones y el *world state*, que almacena el estado actual de cada *asset* (el concepto de *ledger* se profundiza en la sección [Prueba de concepto en Hyperledger Fabric](#)). Inclusive, los *peers* pueden tener varios roles dentro de las organizaciones, pudiendo tener más de uno a la vez:
 1. *Anchor peers*: son los únicos conocidos por participantes fuera de la organización, es decir que podrán ser visibles por otras organizaciones.
 2. *Leader peers*: son los encargados de recibir los bloques del *orderer*. Pueden ser elegidos de forma dinámica o estática, para cada canal. Tras recibir el bloque lo comparte a los demás *peers* de la organización.
 3. *Regular Peers*: se sincronizan y mantienen actualizada la información que se les comparte.
 4. *Endorsing Peers*: reciben las transacciones y las ejecutan sin actualizar ni dejar registro en el *ledger*. Si las transacciones se efectúan correctamente, se le envía una respuesta positiva al nodo que propone la transacción.

- *Client nodes*: usuarios que desean llevar a cabo las transacciones y envían las solicitudes a los *endorsing peers*. Luego de recibir la respuesta de suficientes *endorsing peers*, se comunica la transacción a los *orderers* para que la incluyan en un bloque y se comparta a la red.

Los *smart contracts* son empaquetados en archivos denominados *chaincode* y su idioma de programación puede ser *Go* o *Java*. Brindan una gran versatilidad y capacidad de adaptación a los distintos entornos de negocios que puedan existir. Cabe destacar que el consenso no se lleva a cabo sobre la cadena de bloques completa sino a nivel de transacciones [30].

En la sección *Prueba de concepto en Hyperledger Fabric* se profundiza aún más sobre el funcionamiento de *Hyperledger Fabric*.

R3 Corda

Es una *blockchain* privada que tampoco tiene criptomonedas y posee contratos inteligentes, pero se diferencia en la forma de lograr el consenso. Su lenguaje de programación es *Kotlin* y no es una *blockchain* de código abierto. Existen tres aspectos claves y distintivos de esta *blockchain* que se definirán a continuación:

1. *State object*: es el acuerdo o contrato en el que se basa la cadena. El consenso se lleva a cabo sobre cada *state object*, y no sobre el estado de toda la cadena de información entera. Además, es llevado a cabo entre los nodos participantes del contrato y un tercero, llamado *notary*. Si todas estas partes están de acuerdo se valida la operación inmediatamente, no dependiendo del añadido de un nuevo bloque.
2. *Flow*: son sub-protocolos usados para compartir la información de los *state objects* a las partes involucradas en ese *state object*.
3. *Notary*: un tercero presente en el consenso de los *state objects* que comprueba que las condiciones de la transacción sean válidas y las ordena en el orden temporal que le corresponda. Por ende, los notarios saben el estado de los nodos de su *flow* y su capacidad de realizar transacciones.

Lo que busca alcanzar *Corda* es crear un modelo y arquitectura que tenga la capacidad de emular las transacciones empresariales del mundo real, con posibles aplicaciones o reconocimientos legales. Por este motivo, los *smart contracts* contienen también prosa legal [31]. A diferencia de *Hyperledger*, que comunica la *ledger* completa a todos los nodos dentro de un canal de comunicación, *Corda* brinda la posibilidad de brindar aún más privacidad al compartir una transacción de forma directa solamente al *flow*. Sería lo equivalente a crear canales de comunicación en *Hyperledger* para cada transacción. En *Corda*, ninguna entidad tiene porqué tener el historial de todas las transacciones de la red. Dicha diferenciación puede ser vista en la Figura 4.

A modo de síntesis, se entiende que la elección de *Hyperledger Fabric* se fundamenta por la capacidad de brindar la privacidad necesaria en el intercambio de información entre partes, sin necesidad de la aplicación de prosa legal, que podría entorpecer o desmotivar el uso del sistema por precaución de las partes involucradas. Además, brinda una infinidad de alternativas a través de los *smart contracts* y su carácter de código abierto (*open source*), que permite siempre obtener lo mejor de los avances de

una comunidad en constante desarrollo. Comparte con *Corda* la instantaneidad del intercambio de información, que es crucial en un modelo que busca la eficiencia en el aprovechamiento del tiempo. Se entiende como una ventaja la ausencia de criptomoneda, contrario a *Ethereum*, dado que el fin del proyecto es aprovechar la funcionalidad práctica del sistema para generar ingresos por fuera de la cadena, y por ende se contrapone al concepto de generación de costos/beneficios monetarios dentro de la cadena en sí. Utilizar una *blockchain* con criptomoneda introduce un riesgo en la rentabilidad del proyecto que no es posible evaluar en el corto plazo, ya que es necesario considerar el rendimiento del mercado de criptomonedas, el impacto de la *transaction fee* involucrada y la capacidad de generación de ingresos por minado de nodos.

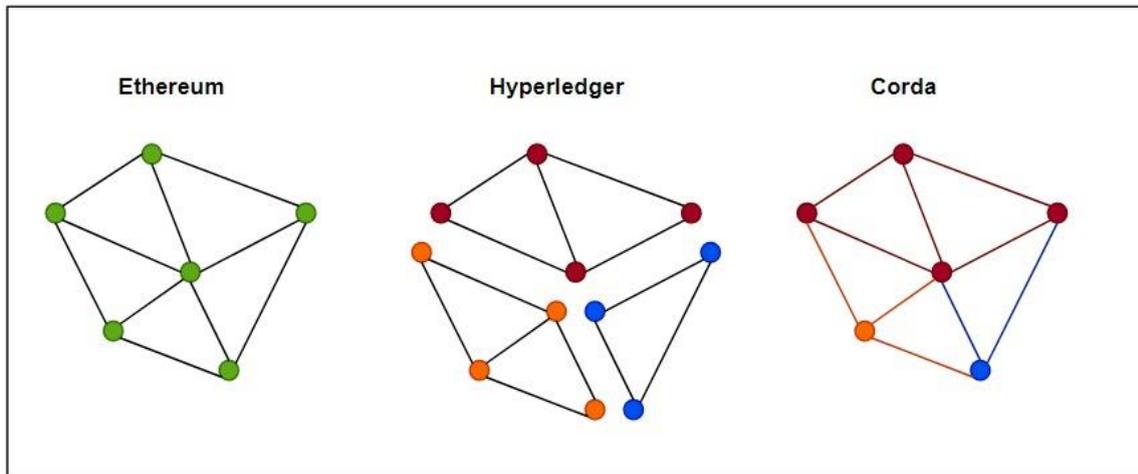


Figura 4 - Comunicación entre nodos de distintos tipos de blockchain [31]

Lo discutido anteriormente puede ser sintetizado con la tabla de la Figura 5 [26].

Plataforma	Ethereum	Hyperledger Fabric	R3 Corda
Descripción	Plataforma blockchain generica	Plataforma blockchain modular	Plataforma blockchain especializada para la industria financiera
Lenguaje de programación	Solidity	Go, Java	Kotlin
Gobernanza	Desarrolladores de la plataforma	Fundación Linux	R3
Open Source	Si	Si	No
Consenso	Proof of Work	Múltiple a nivel de transacciones	Múltiple a nivel de transacciones
Smart Contracts	Smart contracts	Chaincode	Smart contracts y legal prose
Criptomoneda	Ether	No tiene	No tiene
Permisos	No tiene	Permisos detallados	Permisos robustis
Tiempo de confirmación de transacciones	12 segundos	Instantáneo	Instantáneo
Costo de transacción	Se debe pagar una tarifa	No tiene	No tiene
Privada	No	Si	Si

Figura 5 - Comparación de plataformas de blockchain

Prueba de concepto en *Hyperledger Fabric*

Con el objetivo de adentrarse aún más en el funcionamiento de la tecnología, y así evaluar su aplicabilidad en el caso de estudio, se realizó una prueba de concepto en la que se construyó una red de prueba en la plataforma *Hyperledger Fabric*, con el apoyo del tutorial “Using the Fabric test network” [30].

Dados los requisitos, la red se construyó en una computadora con ambiente Ubuntu 20.04.2 LTS, con procesador Intel Core i7-8550U @1.80GHz y 16 GB de memoria RAM. A continuación, se desarrolla la ejecución de cada paso en la construcción de la red, analizando los códigos ejecutados en la terminal y los resultados obtenidos. El proceso completo, en base a la ejecución en la terminal de los códigos disponibles en los *Anexos VI, VII y VIII*, se mapea en la **Figura 6** y conta de 3 fases que serán desglosadas posteriormente.

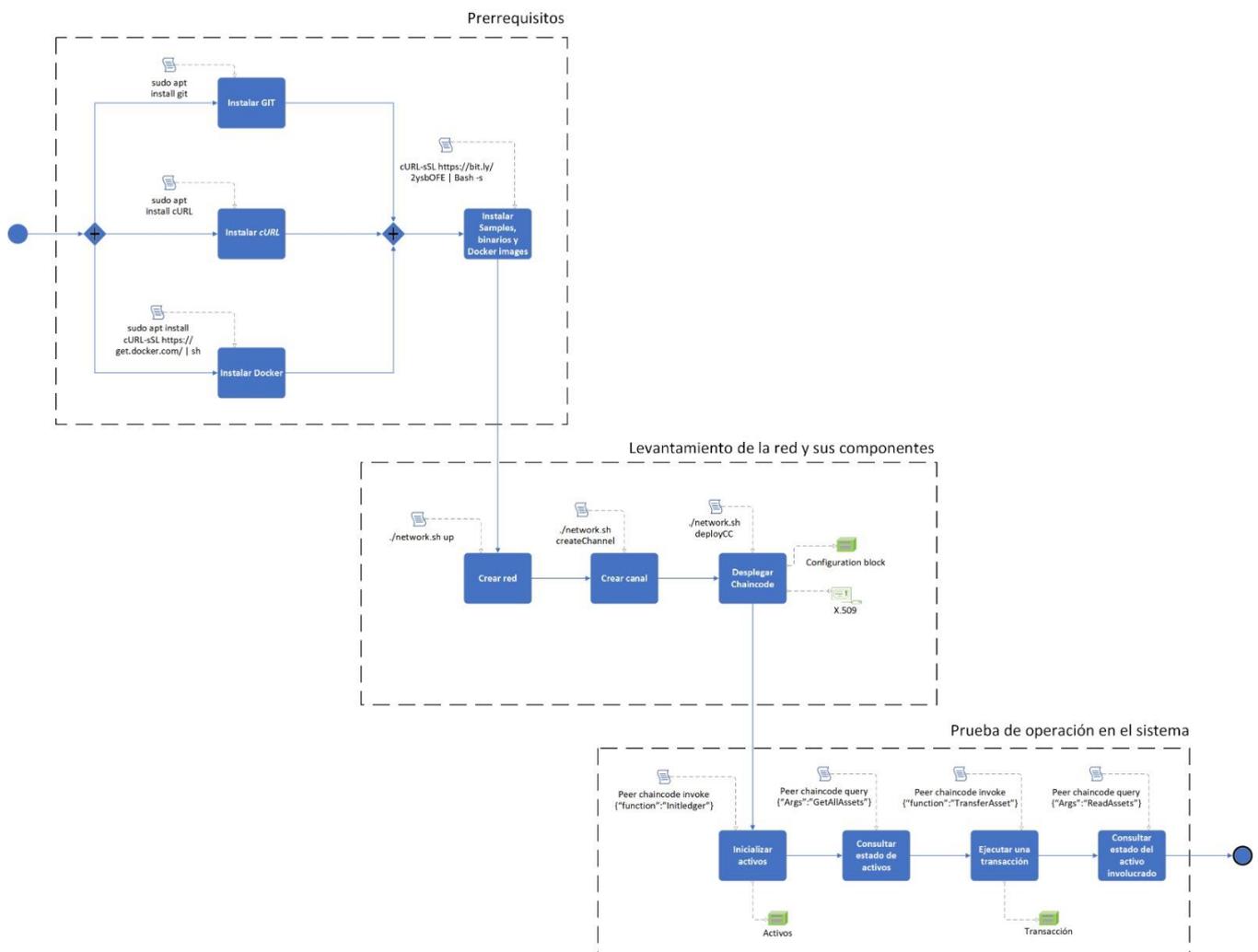


Figura 6 - Proceso completo de la prueba de concepto ejecutada

A continuación, se detallan los comandos ejecutados y resultados obtenidos en cada una de las fases.

Prerrequisitos

Para poder comenzar con la creación de la red, es necesario cumplir con ciertos requisitos -que se presentan en la Figura 7- y permitirán su correcto funcionamiento:

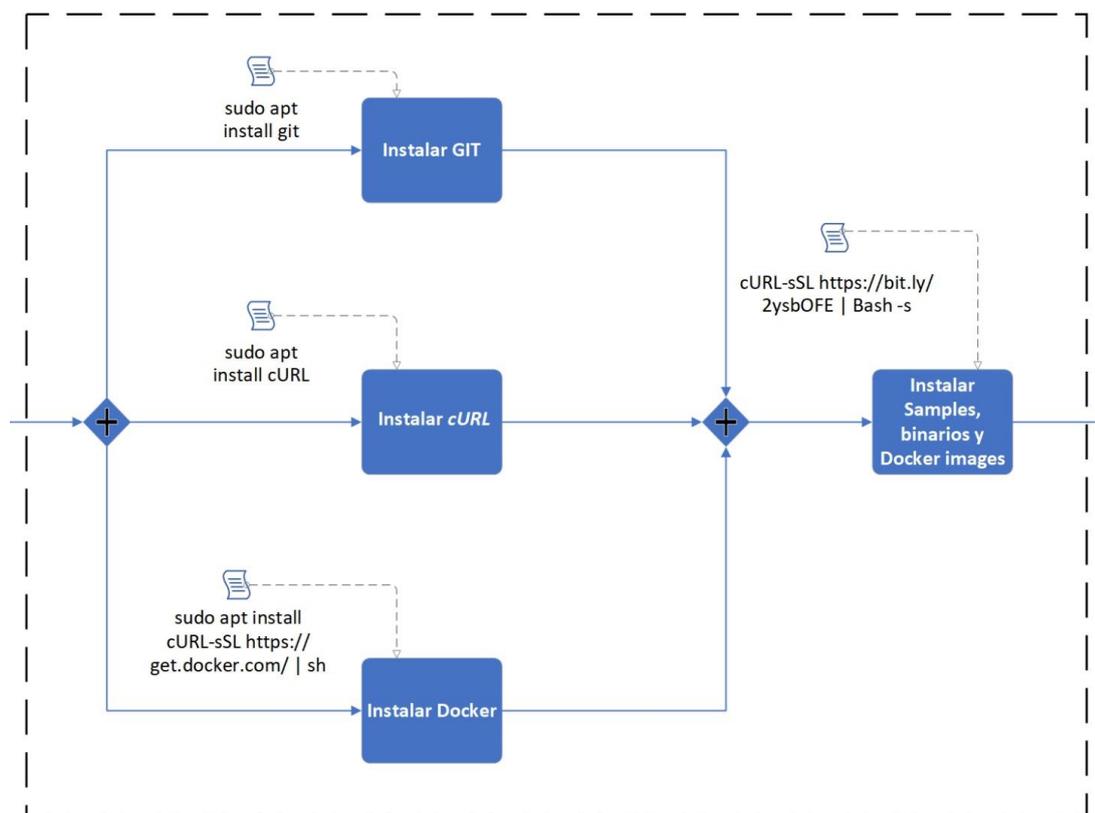


Figura 7 - Prerrequisitos para ejecutar prueba de concepto

Instalar Git

Es necesario descargar este software de administración y almacenamiento de código para poder descargar de allí los binarios y *samples* de *HyperLedger Fabric*. Como se ve en la [Figura 46 del Anexo VI](#), a través de los comandos “*sudo apt install git*” se descarga e instala el software del repositorio del sistema, con los permisos de administrador.

Instalar cURL

De la misma forma que *Git*, se instala este software para transferir datos a partir del código URL de un sitio web. En la [Figura 47 del Anexo VI](#), se puede ver el comando “*sudo apt install curl*” para realizarlo.

Instalar Docker

En la **Figura 48** del *Anexo VI*, se puede ver como se instala *Docker* a partir del URL detallado y el comando “`sudo apt install curl -sL https://get.docker.com/ | sh`”. *Docker* es una plataforma de software que permite correr aplicaciones en simultáneo, pero con ambientes de ejecución aislados entre sí, a través de contenedores. Luego de instalarlo, se inicializa el mismo y se ingresa el usuario que está operando al *Docker group*, para otorgarle la posibilidad de correr todos los *dockers* como administrador sin necesidad de ejecutar *sudo*.

Instalar Samples, Binarios y Docker Images de Hyperledger Fabric

Se descargan del repositorio *Git* de *Hyperledger*, a través del URL y el comando “`cURL-sSL https://bit.ly/2ysb0FE | Bash -s`” presentado en la **Figura 49** del *Anexo VI*. Los *samples* cumplen la función de demostrar las capacidades y/o escenarios del programa. Los binarios son código compilado que permite instalar un programa sin necesidad de compilar el código fuente. Por otro lado, las *Docker Images* empaquetan en capas las instrucciones para ejecutar aplicaciones y contenedores.

Levantamiento de la red y sus componentes

La etapa principal en la creación de una red de *Hyperledger Fabric* es constituida por las actividades detalladas en la *Figura 8*, que serán explicadas a continuación.

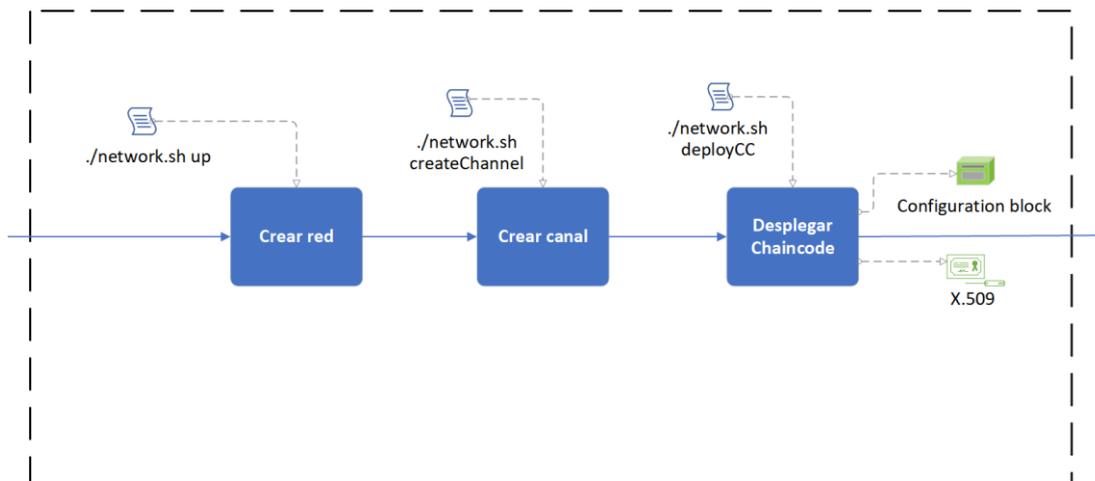


Figura 8 - Proceso de levantamiento de la red en la prueba de concepto

Creación de la red

La creación de la red es acordada por organizaciones interesadas que, como primera medida, acuerdan la configuración común que tendrá la misma. Puesto que las organizaciones transaccionan a través de un canal, lo que se define inicialmente es la configuración del canal del sistema, llamada *system channel configuration*, y que es consensuada por todos. Esta configuración se determina en un bloque inicial llamado *configuration block*, que define las políticas que gobernarán el canal, y

algunos detalles como el rol de cada organización en el mismo. En este caso, la configuración del canal es común a 3 entidades: 2 organizaciones activas en la red y un servicio de gestión de la red llamado *ordering service*.

Para crear la red en *Hyperledger Fabric*, incluyendo el *configuration block* con su configuración, se ejecuta el comando “*network.sh up*” como se muestra en la **Figura 50** del *Anexo VII*.

Para determinar los accesos y permisos de cada actor, al levantar la red, cada uno obtiene su identidad en el sistema a través de certificados digitales X.509, que almacenan información detallada de su poseedor, como su llave pública. En criptografía, X.509 es un estándar para infraestructuras de llaves públicas, donde se determinan, por ejemplo, los formatos de sus certificados, y el algoritmo de validación de certificación. Cada usuario, puede probar su identidad al mostrar su certificado, siempre y cuando los demás usuarios confíen en el emisor del mismo. Los emisores de certificados son llamados *Certificate Authority (CA)* y son los que crean y definen la identidad de cada actor. Los CAs pueden ser intermedios o principales, siendo los principales los de mayor jerarquía, que pueden emitir y firmar CAs intermedios. En esta red de prueba, los certificados son emitidos a través de la ejecución de la carpeta *cryptogen*. En la Figura 9 se puede ver el certificado generado para la organización *org1* de la *test network* con todos sus componentes.

ca.org1.example.com

Identity: ca.org1.example.com
Verified by: ca.org1.example.com
Expires: 15/05/31



Details

Subject Name

C (Country): US
ST (State): California
L (Locality): San Francisco
O (Organization): org1.example.com
CN (Common Name): ca.org1.example.com

Issuer Name

C (Country): US
ST (State): California
L (Locality): San Francisco
O (Organization): org1.example.com
CN (Common Name): ca.org1.example.com

Issued Certificate

Version: 3
Serial Number: 00 DE 79 F1 B1 B8 0F D0 CD 45 DC 96 BB 37 55 97 39
Not Valid Before: 2021-05-17
Not Valid After: 2031-05-15

Certificate Fingerprints

SHA1: 0A 65 C4 51 75 CF 08 70 12 B8 21 61 00 D2 F7 6F 62 67 E6 34
MD5: 72 E2 8F E4 A7 F6 3E C4 C6 E7 AB 77 63 3E CB F4

Public Key Info

Key Algorithm: Elliptic Curve
Key Parameters: 06 08 2A 86 48 CE 3D 03 01 07
Key Size: 256
Key SHA1 Fingerprint: 9F A7 2E E7 51 75 1D C0 19 AD 10 A2 27 E9 B9 30 D3 DD BC F9
Public Key: 04 B9 59 45 DE 6F B3 CB 13 43 91 DA D1 4F F5 CD 1A EF DB 0C
2E A1 30 70 41 03 62 E3 D2 FC E9 ED 23 14 12 E0 8B 53 73 6C
D5 83 FD 6D FA CE F9 90 FA E4 9D E0 F7 55 19 83 5C ED 57 C4
30 83 D8 FD C0

Key Usage

Usages: Digital signature ↕
Key agreement ↕
Revocation list signature
Critical: Yes

Extended Key Usage

Allowed Purposes: Client Authentication ↕
Server Authentication
Critical: No

Figura 9 - Certificado generado para la organización Org1

Además, es el mecanismo llamado *Membership Service Provider* (MSP) que reconoce y acepta dichos certificados como de confianza para que formen parte de la red. El MSP, le otorga a cada identidad los roles y permisos que le corresponden dentro de la red, y está determinado por las siguientes carpetas definidas en la configuración de la red:

- **config.yaml:** usada para clasificar cada identidad en los distintos roles posibles.
- **cacerts:** contiene la lista de certificados X.509 de los principales CA de confianza para esta red, como por ejemplo los certificados de las organizaciones involucradas.
- **intermediatecacerts:** contiene la lista de certificados X.509 de los CA intermedios de confianza para esta red.
- **keystore: (private key)** Esta carpeta es definida solamente para el MSP local de cada nodo y contiene su llave privada.
- **signcert:** Esta carpeta es definida solamente para el MSP local de cada nodo y contiene el certificado que le emitió un CA.

- **tlscacerts:** contiene los certificados de los CA principales confiados para establecer comunicaciones usando un estándar de transporte seguro o *Transport Layer Security (TLS)*
- **tlscintermediateacerts:** contiene los certificados de los CA principales confiados para establecer comunicaciones usando *TLS*.
- **Revoked Certificates:** Esta carpeta está definida solamente para el MSP de los canales, y en ella se almacena información de las identidades revocadas del sistema.

Una vez creada la red, es posible visualizar todos los comandos o “flags” existentes para interactuar con la misma (Figura 10).

```

juan@juan-VirtualBox:~/fabric-samples/test-network$ ./network.sh -h
Usage:
network.sh <Mode> [Flags]
Modes:
  up - Bring up Fabric orderer and peer nodes. No channel is created
  up createChannel - Bring up fabric network with one channel
  createChannel - Create and join a channel after the network is created
  deployCC - Deploy a chaincode to a channel (defaults to asset-transfer-ba
sic)
  down - Bring down the network

Flags:
Used with network.sh up, network.sh createChannel:
  -ca <use CAs> - Use Certificate Authorities to generate network crypto mat
erial
  -c <channel name> - Name of channel to create (defaults to "mychannel")
  -s <dbtype> - Peer state database to deploy: goleveldb (default) or couchdb
  -r <max retry> - CLI times out after certain number of attempts (defaults t
o 5)
  -d <delay> - CLI delays for a certain number of seconds (defaults to 3)
  -verbose - Verbose mode

Used with network.sh deployCC
  -c <channel name> - Name of channel to deploy chaincode to
  -ccn <name> - Chaincode name.
  -ccl <language> - Programming language of the chaincode to deploy: go, java
, javascript, typescript
  -ccv <version> - Chaincode version. 1.0 (default), v2, version3.x, etc

```

Figura 10 - Comandos para interactuar con la red o "flags"

El comando `docker ps -a`, que se ve en la Figura 11 permite obtener una lista de los contenedores de Docker que están corriendo en la máquina. Se pueden observar los 3 nodos creados: el `peer0` de la organización `org2`, el `peer0` de la organización `org1` y el `ordering node`.

```

juan@juan-VirtualBox:~/fabric-samples/test-network$ docker ps -a
CONTAINER ID   IMAGE                                COMMAND                                  NAMES      CRE
ATED          STATUS    PORTS
c1c4d109db05  hyperledger/fabric-ca:latest        "sh -c 'fabric-ca-se..."             ca_org2    8 d
ays ago      Dead     7054/tcp, 0.0.0.0:8054->8054/tcp
0fbbbc6cb568  hyperledger/fabric-ca:latest        "sh -c 'fabric-ca-se..."             ca_orderer 8 d
ays ago      Dead     7054/tcp, 0.0.0.0:9054->9054/tcp
1fb2280419f0  hyperledger/fabric-ca:latest        "sh -c 'fabric-ca-se..."             ca_org1    8 d
ays ago      Dead     0.0.0.0:7054->7054/tcp
227411b3df45  hyperledger/fabric-tools:latest     "/bin/bash"                             cli         8 d
ays ago      Dead
aa1f109fd064  hyperledger/fabric-peer:latest      "peer node start"                       peer0.org2 8 d
ays ago      Dead     7051/tcp, 0.0.0.0:9051->9051/tcp
49cb27ba11fd  hyperledger/fabric-peer:latest      "peer node start"                       peer0.org1 8 d
ays ago      Dead     0.0.0.0:7051->7051/tcp
487b372b2c89  hyperledger/fabric-orderer:latest   "orderer"                                orderer.ex 8 d
ays ago      Dead     0.0.0.0:7050->7050/tcp, 0.0.0.0:7053->7053/tcp

```

Figura 11 - Comando utilizado para visualizar la lista de contenedores de Docker que están Corriendo en la máquina

Creación del canal

Un canal es una capa privada de comunicación entre miembros de la red. Al crear un canal entre una cierta cantidad de nodos, el mismo será visible para las organizaciones involucradas, pero invisible para el resto de los actores. Se precisan como mínimo tres nodos para formar un canal, puesto que al menos dos de ellos deben ser nodos del tipo *peer*, que interactúan entre sí, a través de la asistencia de un *ordering node*. Cada *peer* debe pertenecer a una organización. El *ordering node* valida la identidad de cada nodo y se encarga de distribuir la información entre los nodos del canal, como se profundiza en [Habiendo desarrollado la](#) lógica de levantamiento de una red en *Hyperledger Fabric*, y luego de detallar sus prerequisites, se procede a explicar en profundidad el funcionamiento de una transacción en *Hyperledger*, para luego exponer acerca de la prueba de operación ejecutada como parte de la prueba de concepto.

Las aplicaciones desarrolladas por cada organización se conectan con los *peers* para acceder al *chaincode* y al *ledger*, con la posibilidad de realizar consultas (*query*) o actualizar su estado. Una transacción que busca actualizar el *ledger* de un canal se diferencia de una transacción de consulta, puesto que, si bien ambas pueden ser ejecutadas por un único usuario, la primera precisa del consentimiento de otros usuarios justamente por buscar actualizar el *ledger*, mientras que la segunda busca únicamente conocer el *world state* pero sin realizar ninguna modificación.

El flujo de creación y aprobación de este tipo de transacciones comienza cuando una aplicación de cliente desea crear una nueva transacción. Esta propuesta de transacción es enviada desde la aplicación a los nodos de las organizaciones que estén indicadas por la *Endorsement Policy*, para comenzar con el proceso de aprobación de la misma. Los nodos receptores de la propuesta invocan al contrato inteligente para producir una respuesta tentativa a esa transacción (propuesta de actualización de *ledger*), agregan su firma electrónica con su llave privada, y la devuelven a la aplicación. Esto permite trazar con exactitud que una respuesta R1 a la transacción T1 fue creada por el nodo P1 de la organización O1. Este paso es realizado en paralelo por los distintos nodos destinatarios, y todos envían su respuesta a dicha aplicación.

En la Figura 14 se puede observar como la Aplicación 1 envía 2 copias de la transacción propuesta PT1 a los nodos *Peer node 1* y *Peer node 2*. El nodo *Peer node 1* procesa la transacción utilizando el *chaincode 1* para producir una respuesta de transacción RT1. Esta respuesta está firmada con la autorización A1 y se envía de vuelta a la Aplicación 1. Lo mismo ocurre en paralelo en el nodo *Peer node 2*. Todo esto ocurre en el Canal 1.

Al recibir propuestas de respuestas de todos los nodos involucrados, la aplicación las procesa para verificar que todas las respuestas sean consistentes. En caso de que exista alguna inconsistencia, la aplicación rechaza las transacciones y puede solicitar una nueva respuesta a los nodos. Si las respuestas son todas consistentes, la aplicación las envía al *ordering node*.

El MSP que se encuentra en el *ordering node*, es el mecanismo que permite que cada identidad sea reconocida y válida por el resto de la red. Al contener las llaves públicas de todos los nodos, verifica que las transacciones hayan sido firmadas de manera fidedigna, pero sin revelar ninguna llave privada. Este servicio también es quien asigna los roles y permisos para cada identidad, por ende verifica que la acción que cada actor quiere realizar esté dentro de sus capacidades autorizadas. Dentro de los permisos que concede, se encuentra el de participar en los distintos canales de la red.

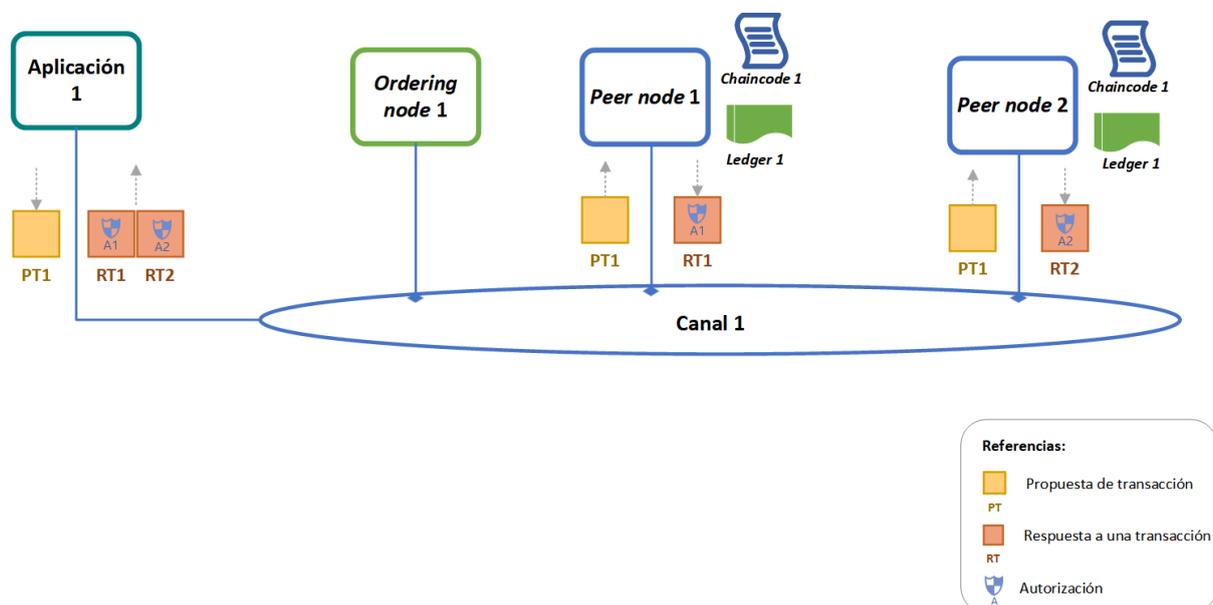


Figura 14 - Esquema de propuesta de transacción y respuesta

Luego de que el MSP valide las identidades y acciones solicitadas en cada transacción, el *ordering node* crea bloques de información para ejecutar transacciones acordadas, y los envía a todos los nodos del canal para una validación final. Cabe destacar que en este punto también se involucran los nodos del canal que no están en la *Endorsement policy* de la transacción.

Esta validación ocurre en 2 pasos. En primera instancia cada nodo verifica que se haya cumplido la *Endorsement Policy*, es decir que las transacciones estén firmadas por todos los nodos relevantes. Luego, se realiza una verificación de la consistencia del *ledger* para corroborar que las transacciones sigan siendo compatibles y evitar, por ejemplo, que hayan quedado invalidadas por la concreción de otra transacción previa durante el proceso de verificación de las transacciones actuales. Luego de validarlas, los nodos agregan el bloque a su *ledger*.

El procesamiento de los bloques es independiente en cada nodo, pero se realiza de igual forma en cada uno de ellos, para que, al aceptarlo en todos los nodos, el *ledger* final sea consistente. Si algunas de las transacciones de un bloque no son validadas, se identifican como inválidas dentro del mismo, para que no se apliquen al *ledger*. Esto permite que estas transacciones inválidas estén disponibles para auditar.

Esto mismo se puede observar en la Figura 15, donde el *ordering node* O1 envía el bloque B2 -que contiene varias transacciones- a los nodos P1 y P2. Al aprobarlas, cada nodo agrega el nuevo bloque B2 al *ledger* L1, confirmando las transacciones y actualizando el *ledger* del canal.

Con esta lógica, las redes de *blockchain* de *Hyperledger* aseguran la fiabilidad de la información gracias a que cada nodo dentro del canal cuenta con una copia de la información (*ledger*), y si un nodo modifica la información, ésta no coincidirá con la información en el resto de los nodos, invalidando dicho cambio.

A modo de resumen, se presenta la Figura 16 que describe la interacción completa entre la aplicación que solicita la transacción y los nodos del canal, demostrando cómo los nodos y los *ordering nodes* aseguran que el *ledger* siempre esté actualizado.

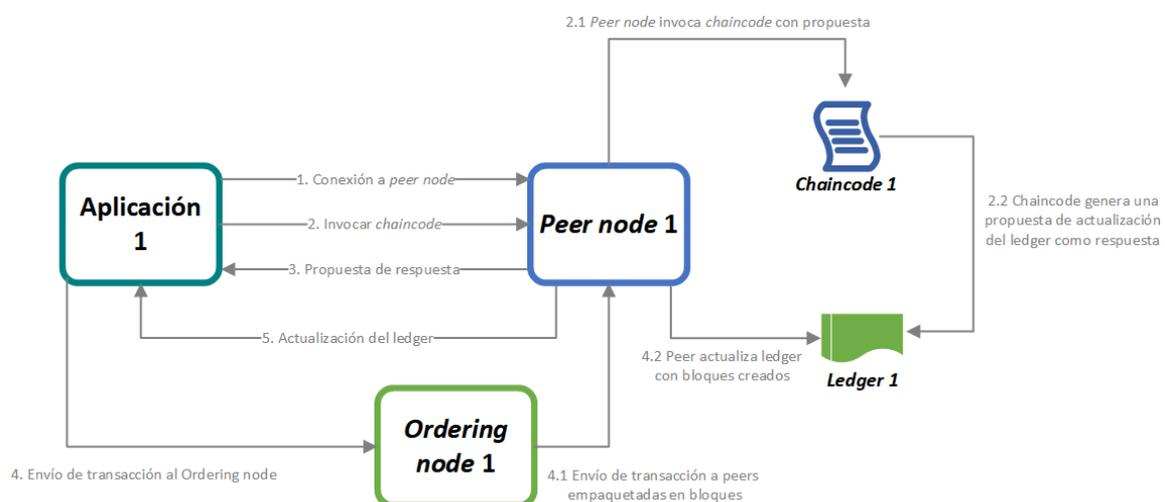


Figura 16 - Esquema de proceso completo de propuesta e inclusión al ledger de una transacción

Luego de profundizar acerca de la lógica de ejecución de transacciones en *Hyperledger Fabric*, se procedió a realizar una prueba de operación más acotada, siguiendo los pasos que se presentan en la **figura 17**.

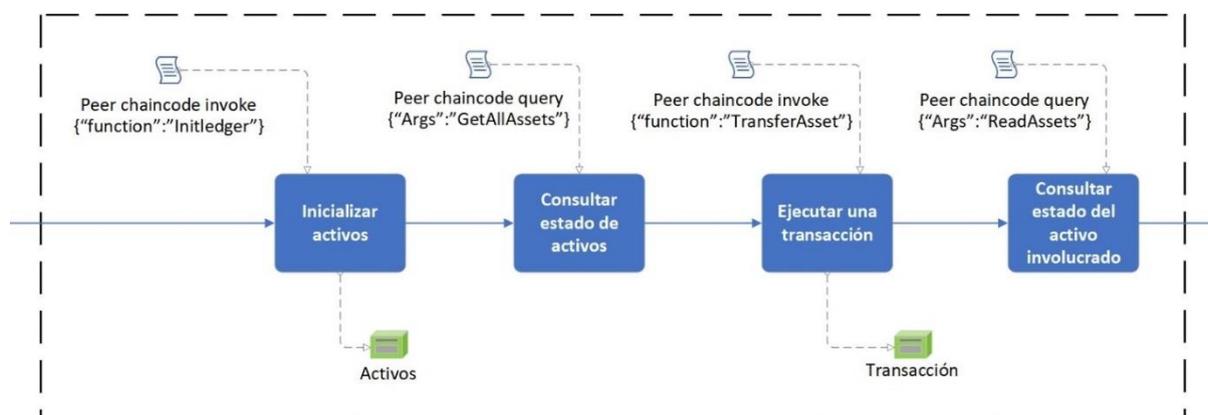


Figura 17 - Proceso de prueba de operación en el sistema como parte de la prueba de concepto

Todas las operaciones fueron llevadas a cabo desde *el peer 0* de la organización 1, con *localhost* número 7051. La serie de comandos para determinar el nodo en el que se iba a trabajar puede ser visto en la **Figura 56** del *Anexo VIII*.

Inicialización de activos

Para que los nodos puedan interactuar en el sistema, es importante contar con activos que puedan ser registrados, transferidos y consultados. En rasgos generales, toda transacción involucra una alteración en cierto activo del sistema. En el caso de la *test network* en cuestión, se ejecutó el comando *“peer chaincode invoke”* que invoca a la función *InitLedger* del *chaincode*, tal como se ve en la **Figura 57** del *Anexo VIII*, para determinar los estados iniciales de los activos.

Dichos activos pueden ser vistos en la **Figura 18**, que presenta el código de la función en el *chaincode*, donde se definen los 6 activos (*asset1* a *asset6*) y se asigna el color, tamaño, dueño y valor (*Color*, *Size*, *Owner*, *AppraisedValue*) de cada uno. Se nota también que no hay argumentos de

entrada para la función.

```
// InitLedger adds a base set of assets to the ledger
func (s *SmartContract) InitLedger(ctx contractapi.TransactionContextInterface) error {
    assets := []Asset{
        {ID: "asset1", Color: "blue", Size: 5, Owner: "Tomoko", AppraisedValue: 300},
        {ID: "asset2", Color: "red", Size: 5, Owner: "Brad", AppraisedValue: 400},
        {ID: "asset3", Color: "green", Size: 10, Owner: "Jin Soo", AppraisedValue: 500},
        {ID: "asset4", Color: "yellow", Size: 10, Owner: "Max", AppraisedValue: 600},
        {ID: "asset5", Color: "black", Size: 15, Owner: "Adriana", AppraisedValue: 700},
        {ID: "asset6", Color: "white", Size: 15, Owner: "Michel", AppraisedValue: 800},
    }

    for _, asset := range assets {
        assetJSON, err := json.Marshal(asset)
        if err != nil {
            return err
        }

        err = ctx.GetStub().PutState(asset.ID, assetJSON)
        if err != nil {
            return fmt.Errorf("failed to put to world state. %v", err)
        }
    }

    return nil
}
```

Figura 18 - Función InitLedger

Luego de inicializar los 6 activos, se invocó a la función *GetAllAssets* perteneciente al *chaincode* a través del comando “*peer chaincode query*” para realizar una consulta acerca de los activos actuales, como se ve en la Figura 58 en el Anexo VIII. A través de esta consulta se busca confirmar que los valores de cada activo hayan sido inicializados correctamente y que coincidan con los especificados en el *chaincode*. A modo informativo, la función *GetAllAssets*, detallada en la Figura 19, itera y obtiene todas las entradas en el *array* llamado *assets*.

```

// GetAllAssets returns all assets found in world state
func (s *SmartContract) GetAllAssets(ctx contractapi.TransactionContextInterface) ([]*Asset, error) {
    // range query with empty string for startKey and endKey does an
    // open-ended query of all assets in the chaincode namespace.
    resultsIterator, err := ctx.GetStub().GetStateByRange("", "")
    if err != nil {
        return nil, err
    }
    defer resultsIterator.Close()

    var assets []*Asset
    for resultsIterator.HasNext() {
        queryResponse, err := resultsIterator.Next()
        if err != nil {
            return nil, err
        }

        var asset Asset
        err = json.Unmarshal(queryResponse.Value, &asset)
        if err != nil {
            return nil, err
        }
        assets = append(assets, &asset)
    }

    return assets, nil
}

```

Figura 19 - Función GetAllAssets

Ejecución de transacciones.

En este caso, se construye un canal que permite que el nodo de la organización 1 y el nodo de la organización 2 puedan realizar transacciones entre sí. El comando utilizado es “./network.sh createChannel”, y se puede observar en la **Figura 51** del *Anexo VII* que el resultado arrojado es la correcta asociación de los nodos al canal “mychannel”. Es posible renombrar dicho canal con el flag -c.

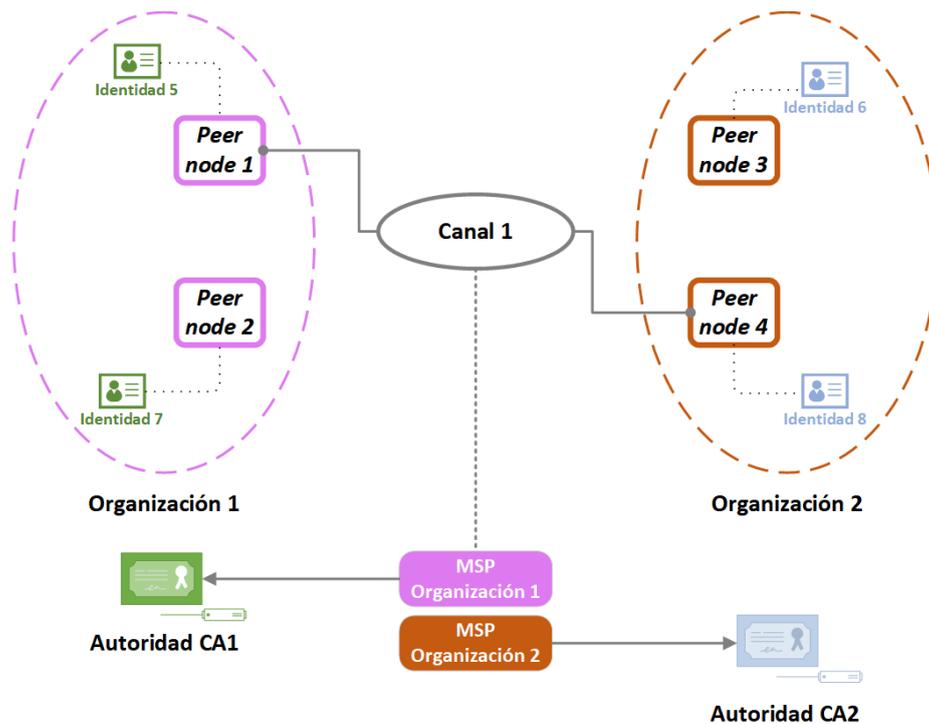


Figura 12 - Vista esquemática de la estructura de un canal

La Figura 12 [32] resume la estructura del canal. Los nodos *Peer node 1* y *Peer node 2* tienen las identidades 5 y 7 respectivamente, que fueron emitidas por la autoridad CA1. El canal 1 identifica que las identidades (certificados y llaves) de la autoridad CA1 se deben asociar a la organización 1, utilizando el servicio de verificación MSP de la Organización 1. Lo mismo ocurre con los nodos *Peer Node 3* y *Peer Node 4* de la organización 2.

En este punto resulta importante profundizar sobre el concepto de estado de información del canal o *ledger*. Este concepto se relaciona con la información que se encuentra en el canal en dos formas distintas. El primer componente del *ledger* de un canal es el estado global o *world state* y se refiere a el valor actual de los atributos de alguna entidad, como un único estado actual. Este estado cambia al ejecutar nuevas transacciones, pero cada vez que se consulte se obtendrá información acerca de un único valor para cada atributo, sin conocer el historial que llevó a que los atributos tengan esos valores. El *world state* se implementa como una base de datos, puesto que estas permiten almacenar y consultar de manera eficiente los estados. El otro componente del *ledger* es la cadena de bloques o *blockchain* tal cual se dio a conocer en este informe. Para terminar de materializar el concepto de *ledger*, mientras que el *world state* muestra el estado actual de los atributos de las entidades, la *blockchain* es el registro histórico de transacciones que demuestran cómo los objetos llegaron a ese estado actual. La *blockchain* registra cada versión de cada estado de información, y cómo se efectuaron los cambios entre estado y estado.

Tal como se observa en la Figura 13, la *blockchain* registra cada transacción desde el levantamiento de la red, y el resultado de la última transacción determina el *world state*, pero el *ledger* del canal incluye estos dos tipos de información.

Configuración del chaincode en el canal

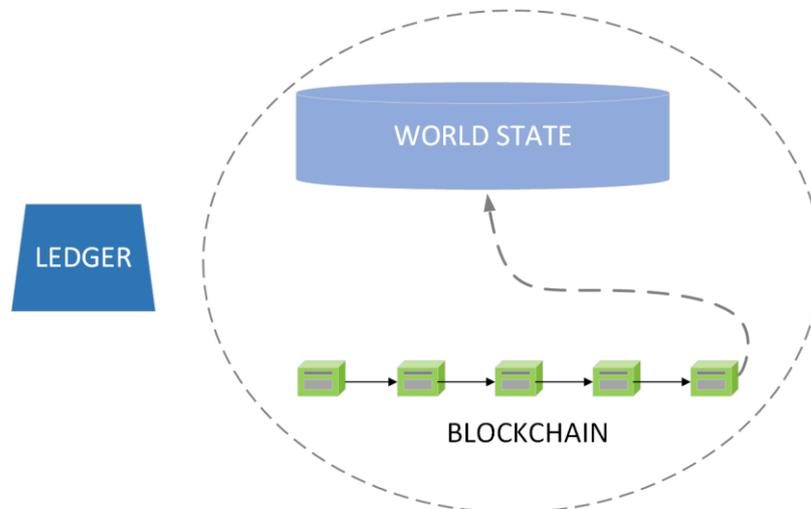


Figura 13 - Estructura del ledger

Las distintas aplicaciones de los miembros de la red podrán invocar *smart contracts* para crear, cambiar o transferir activos en el *ledger* del canal, como también para realizar consultas acerca de la información en el *ledger*, como se desarrolla en la subsección *Habiendo desarrollado la* lógica de levantamiento de una red en *Hyperledger Fabric*, y luego de detallar sus prerrequisitos, se procede a explicar en profundidad el funcionamiento de una transacción en *Hyperledger*, para luego exponer acerca de la prueba de operación ejecutada como parte de la prueba de concepto.

Las aplicaciones desarrolladas por cada organización se conectan con los *peers* para acceder al *chaincode* y al *ledger*, con la posibilidad de realizar consultas (*query*) o actualizar su estado. Una transacción que busca actualizar el *ledger* de un canal se diferencia de una transacción de consulta, puesto que, si bien ambas pueden ser ejecutadas por un único usuario, la primera precisa del consentimiento de otros usuarios justamente por buscar actualizar el *ledger*, mientras que la segunda busca únicamente conocer el *world state* pero sin realizar ninguna modificación.

El flujo de creación y aprobación de este tipo de transacciones comienza cuando una aplicación de cliente desea crear una nueva transacción. Esta propuesta de transacción es enviada desde la aplicación a los nodos de las organizaciones que estén indicadas por la *Endorsement Policy*, para comenzar con el proceso de aprobación de la misma. Los nodos receptores de la propuesta invocan al contrato inteligente para producir una respuesta tentativa a esa transacción (propuesta de actualización de *ledger*), agregan su firma electrónica con su llave privada, y la devuelven a la aplicación. Esto permite trazar con exactitud que una respuesta R1 a la transacción T1 fue creada por

el nodo P1 de la organización O1. Este paso es realizado en paralelo por los distintos nodos destinatarios, y todos envían su respuesta a dicha aplicación.

En la Figura 14 se puede observar como la Aplicación 1 envía 2 copias de la transacción propuesta PT1 a los nodos *Peer node 1* y *Peer node 2*. El nodo *Peer node 1* procesa la transacción utilizando el *chaincode 1* para producir una respuesta de transacción RT1. Esta respuesta está firmada con la autorización A1 y se envía de vuelta a la Aplicación 1. Lo mismo ocurre en paralelo en el nodo *Peer node 2*. Todo esto ocurre en el Canal 1.

Al recibir propuestas de respuestas de todos los nodos involucrados, la aplicación las procesa para verificar que todas las respuestas sean consistentes. En caso de que exista alguna inconsistencia, la aplicación rechaza las transacciones y puede solicitar una nueva respuesta a los nodos. Si las respuestas son todas consistentes, la aplicación las envía al *ordering node*.

El MSP que se encuentra en el *ordering node*, es el mecanismo que permite que cada identidad sea reconocida y válida por el resto de la red. Al contener las llaves públicas de todos los nodos, verifica que las transacciones hayan sido firmadas de manera fidedigna, pero sin revelar ninguna llave privada. Este servicio también es quien asigna los roles y permisos para cada identidad, por ende verifica que la acción que cada actor quiere realizar esté dentro de sus capacidades autorizadas. Dentro de los permisos que concede, se encuentra el de participar en los distintos canales de la red.

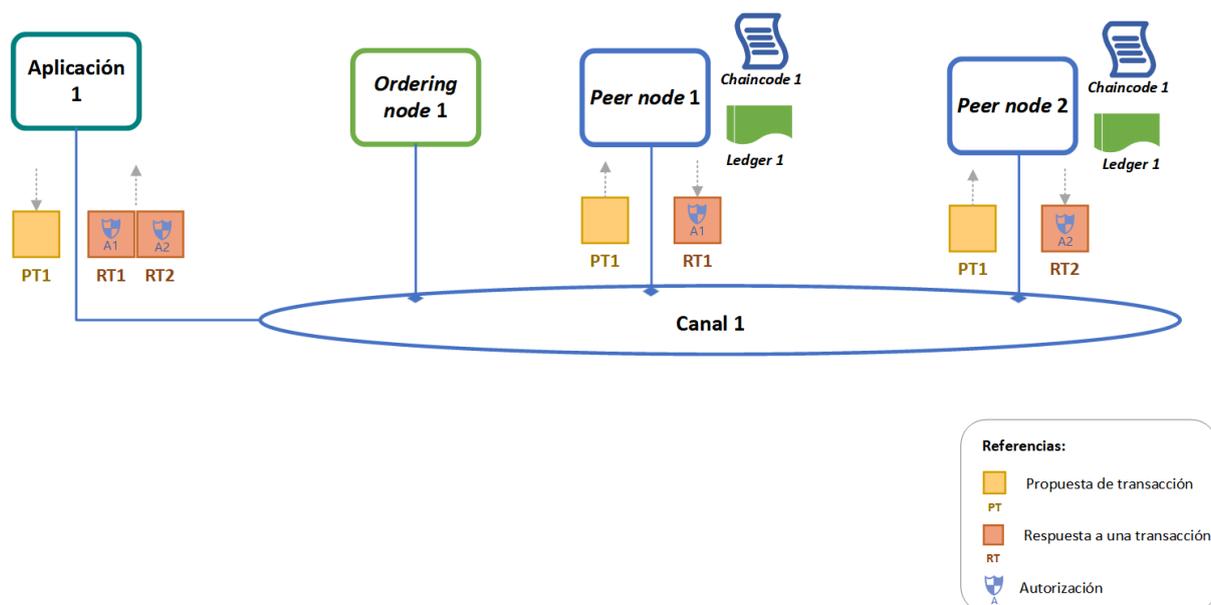


Figura 14 - Esquema de propuesta de transacción y respuesta

Luego de que el MSP valide las identidades y acciones solicitadas en cada transacción, el *ordering node* crea bloques de información para ejecutar transacciones acordadas, y los envía a todos los

nodos del canal para una validación final. Cabe destacar que en este punto también se involucran los nodos del canal que no están en la *Endorsement policy* de la transacción.

Esta validación ocurre en 2 pasos. En primera instancia cada nodo verifica que se haya cumplido la *Endorsement Policy*, es decir que las transacciones estén firmadas por todos los nodos relevantes. Luego, se realiza una verificación de la consistencia del *ledger* para corroborar que las transacciones sigan siendo compatibles y evitar, por ejemplo, que hayan quedado invalidadas por la concreción de otra transacción previa durante el proceso de verificación de las transacciones actuales. Luego de validarlas, los nodos agregan el bloque a su *ledger*.

El procesamiento de los bloques es independiente en cada nodo, pero se realiza de igual forma en cada uno de ellos, para que, al aceptarlo en todos los nodos, el *ledger* final sea consistente. Si algunas de las transacciones de un bloque no son validadas, se identifican como inválidas dentro del mismo, para que no se apliquen al *ledger*. Esto permite que estas transacciones inválidas estén disponibles para auditar.

Esto mismo se puede observar en la Figura 15 , donde el *ordering node* O1 envía el bloque B2 -que contiene varias transacciones- a los nodos P1 y P2. Al aprobarlas, cada nodo agrega el nuevo bloque B2 al *ledger* L1, confirmando las transacciones y actualizando el *ledger* del canal.

Con esta lógica, las redes de *blockchain* de *Hyperledger* aseguran la fiabilidad de la información gracias a que cada nodo dentro del canal cuenta con una copia de la información (*ledger*), y si un nodo modifica la información, ésta no coincidirá con la información en el resto de los nodos, invalidando dicho cambio.

A modo de resumen, se presenta la Figura 16 que describe la interacción completa entre la aplicación que solicita la transacción y los nodos del canal, demostrando cómo los nodos y los *ordering nodes* aseguran que el *ledger* siempre esté actualizado.

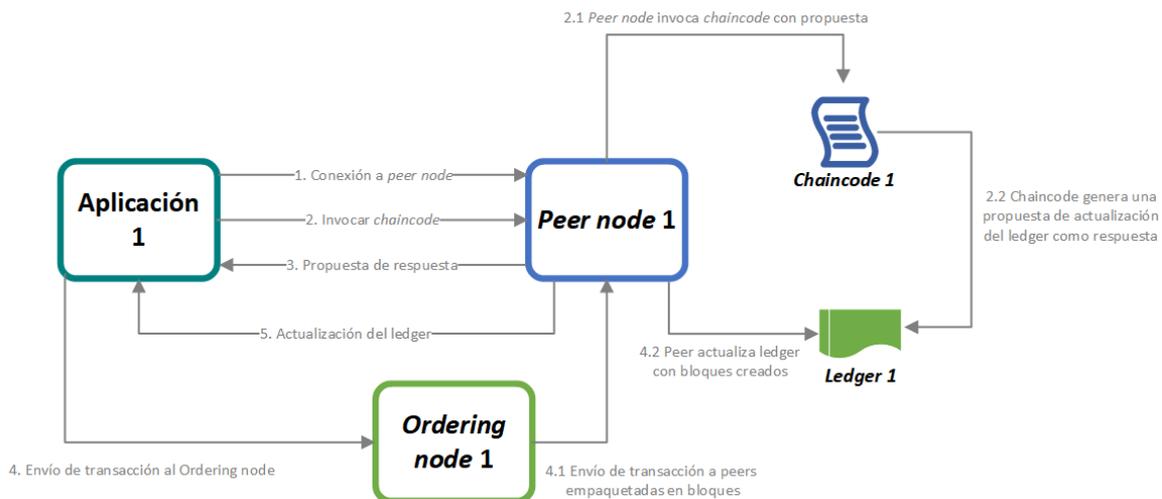


Figura 16 - Esquema de proceso completo de propuesta e inclusión al ledger de una transacción

Luego de profundizar acerca de la lógica de ejecución de transacciones en *Hyperledger Fabric*, se procedió a realizar una prueba de operación más acotada, siguiendo los pasos que se presentan en la **figura 17**.

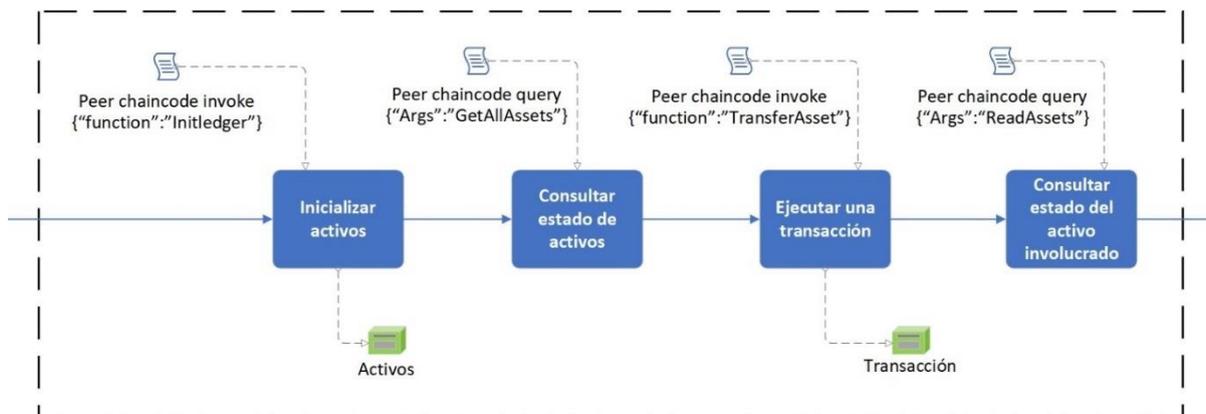


Figura 17 - Proceso de prueba de operación en el sistema como parte de la prueba de concepto

Todas las operaciones fueron llevadas a cabo desde *el peer 0* de la organización 1, con *localhost* número 7051. La serie de comandos para determinar el nodo en el que se iba a trabajar puede ser visto en la **Figura 56** del *Anexo VIII*.

Inicialización de activos

Para que los nodos puedan interactuar en el sistema, es importante contar con activos que puedan ser registrados, transferidos y consultados. En rasgos generales, toda transacción involucra una alteración en cierto activo del sistema. En el caso de la *test network* en cuestión, se ejecutó el comando "*peer chaincode invoke*" que invoca a la función *InitLedger* del *chaincode*, tal como se ve en la **Figura 57** del *Anexo VIII*, para determinar los estados iniciales de los activos.

Dichos activos pueden ser vistos en la Figura 18, que presenta el código de la función en el *chaincode*, donde se definen los 6 activos (*asset1* a *asset6*) y se asigna el color, tamaño, dueño y valor (*Color*, *Size*, *Owner*, *AppraisedValue*) de cada uno. Se nota también que no hay argumentos de entrada para la función.

```
// InitLedger adds a base set of assets to the ledger
func (s *SmartContract) InitLedger(ctx contractapi.TransactionContextInterface) error {
    assets := []Asset{
        {ID: "asset1", Color: "blue", Size: 5, Owner: "Tomoko", AppraisedValue: 300},
        {ID: "asset2", Color: "red", Size: 5, Owner: "Brad", AppraisedValue: 400},
        {ID: "asset3", Color: "green", Size: 10, Owner: "Jin Soo", AppraisedValue: 500},
        {ID: "asset4", Color: "yellow", Size: 10, Owner: "Max", AppraisedValue: 600},
        {ID: "asset5", Color: "black", Size: 15, Owner: "Adriana", AppraisedValue: 700},
        {ID: "asset6", Color: "white", Size: 15, Owner: "Michel", AppraisedValue: 800},
    }

    for _, asset := range assets {
        assetJSON, err := json.Marshal(asset)
        if err != nil {
            return err
        }

        err = ctx.GetStub().PutState(asset.ID, assetJSON)
        if err != nil {
            return fmt.Errorf("failed to put to world state. %v", err)
        }
    }

    return nil
}
```

Figura 18 - Función *InitLedger*

Luego de inicializar los 6 activos, se invocó a la función *GetAllAssets* perteneciente al *chaincode* a través del comando “*peer chaincode query*” para realizar una consulta acerca de los activos actuales, como se ve en la Figura 58 en el Anexo VIII. A través de esta consulta se busca confirmar que los valores de cada activo hayan sido inicializados correctamente y que coincidan con los especificados en el *chaincode*. A modo informativo, la función *GetAllAssets*, detallada en la Figura 19, itera y obtiene todas las entradas en el *array* llamado *assets*.

```

// GetAllAssets returns all assets found in world state
func (s *SmartContract) GetAllAssets(ctx contractapi.TransactionContextInterface) ([]*Asset, error) {
    // range query with empty string for startKey and endKey does an
    // open-ended query of all assets in the chaincode namespace.
    resultsIterator, err := ctx.GetStub().GetStateByRange("", "")
    if err != nil {
        return nil, err
    }
    defer resultsIterator.Close()

    var assets []*Asset
    for resultsIterator.HasNext() {
        queryResponse, err := resultsIterator.Next()
        if err != nil {
            return nil, err
        }

        var asset Asset
        err = json.Unmarshal(queryResponse.Value, &asset)
        if err != nil {
            return nil, err
        }
        assets = append(assets, &asset)
    }

    return assets, nil
}

```

Figura 19 - Función GetAllAssets

Ejecución de transacciones. Múltiples *smart contracts* pueden ser empaquetados en un *chaincode* para ser desplegados en la red *blockchain*. En los *smart contracts* se encuentra la política de validación o *Endorsement Policy* que determina cuáles organizaciones deberán aprobar las transacciones ejecutadas. Cada *smart contract* podrá ejecutar distintos tipos de transacciones, por lo que es posible que dos transacciones distintas se ejecuten con 2 *smart contracts* distintos, y que cada una requiera la aprobación de distintas organizaciones para agregarse al *ledger*. Para poder ejecutar un *smart contract*, el *chaincode* debe ser instalado en cada *peer* y debe ser definido en el canal. La definición del *chaincode* en el canal incluye el nombre del *chaincode*, la versión y su *Endorsement Policy*. Cada *Endorsement Policy* aplica por igual en todos los *smart contracts* de la *chaincode*. Por defecto, cuando la mayoría de las organizaciones participantes han aprobado la misma definición del *chaincode*, ésta se confirma en el canal.

Para instalar el *chaincode* llamado “*basic*” en los nodos *Peer1* y *Peer2* y posteriormente en el canal *mychannel*, se ejecuta el comando *deployCC*. El lenguaje del *chaincode* es *go* y la ruta para el archivo es “*../asset-transfer-basic/chaincode-go*”. De esta forma, tal como se puede ver en la **Figura 52** del *Anexo VII* el comando utilizado es:

```
“./network.sh deployCC -ccn basic -ccp ../asset-transfer-basic/chaincode-go -ccl go” .
```

La política de definición del canal exige que ambas organizaciones aprueben su configuración, por lo que se evalúa la misma primeramente desde la organización 1 y se aprueba, para luego hacer lo mismo con la organización 2.

Prueba de operación en el sistema

Habiendo desarrollado la lógica de levantamiento de una red en *Hyperledger Fabric*, y luego de detallar sus prerequisites, se procede a explicar en profundidad el funcionamiento de una transacción en *Hyperledger*, para luego exponer acerca de la prueba de operación ejecutada como parte de la prueba de concepto.

Las aplicaciones desarrolladas por cada organización se conectan con los *peers* para acceder al *chaincode* y al *ledger*, con la posibilidad de realizar consultas (*query*) o actualizar su estado. Una transacción que busca actualizar el *ledger* de un canal se diferencia de una transacción de consulta, puesto que, si bien ambas pueden ser ejecutadas por un único usuario, la primera precisa del consentimiento de otros usuarios justamente por buscar actualizar el *ledger*, mientras que la segunda busca únicamente conocer el *world state* pero sin realizar ninguna modificación.

El flujo de creación y aprobación de este tipo de transacciones comienza cuando una aplicación de cliente desea crear una nueva transacción. Esta propuesta de transacción es enviada desde la aplicación a los nodos de las organizaciones que estén indicadas por la *Endorsement Policy*, para comenzar con el proceso de aprobación de la misma. Los nodos receptores de la propuesta invocan al contrato inteligente para producir una respuesta tentativa a esa transacción (propuesta de actualización de *ledger*), agregan su firma electrónica con su llave privada, y la devuelven a la aplicación. Esto permite trazar con exactitud que una respuesta R1 a la transacción T1 fue creada por el nodo P1 de la organización O1. Este paso es realizado en paralelo por los distintos nodos destinatarios, y todos envían su respuesta a dicha aplicación.

En la Figura 14 [32] se puede observar como la Aplicación 1 envía 2 copias de la transacción propuesta PT1 a los nodos *Peer node 1* y *Peer node 2*. El nodo *Peer node 1* procesa la transacción utilizando el *chaincode 1* para producir una respuesta de transacción RT1. Esta respuesta está firmada con la autorización A1 y se envía de vuelta a la Aplicación 1. Lo mismo ocurre en paralelo en el nodo *Peer node 2*. Todo esto ocurre en el Canal 1.

Al recibir propuestas de respuestas de todos los nodos involucrados, la aplicación las procesa para verificar que todas las respuestas sean consistentes. En caso de que exista alguna inconsistencia, la aplicación rechaza las transacciones y puede solicitar una nueva respuesta a los nodos. Si las respuestas son todas consistentes, la aplicación las envía al *ordering node*.

El MSP que se encuentra en el *ordering node*, es el mecanismo que permite que cada identidad sea reconocida y válida por el resto de la red. Al contener las llaves públicas de todos los nodos, verifica

que las transacciones hayan sido firmadas de manera fidedigna, pero sin revelar ninguna llave privada. Este servicio también es quien asigna los roles y permisos para cada identidad, por ende verifica que la acción que cada actor quiere realizar esté dentro de sus capacidades autorizadas. Dentro de los permisos que concede, se encuentra el de participar en los distintos canales de la red.

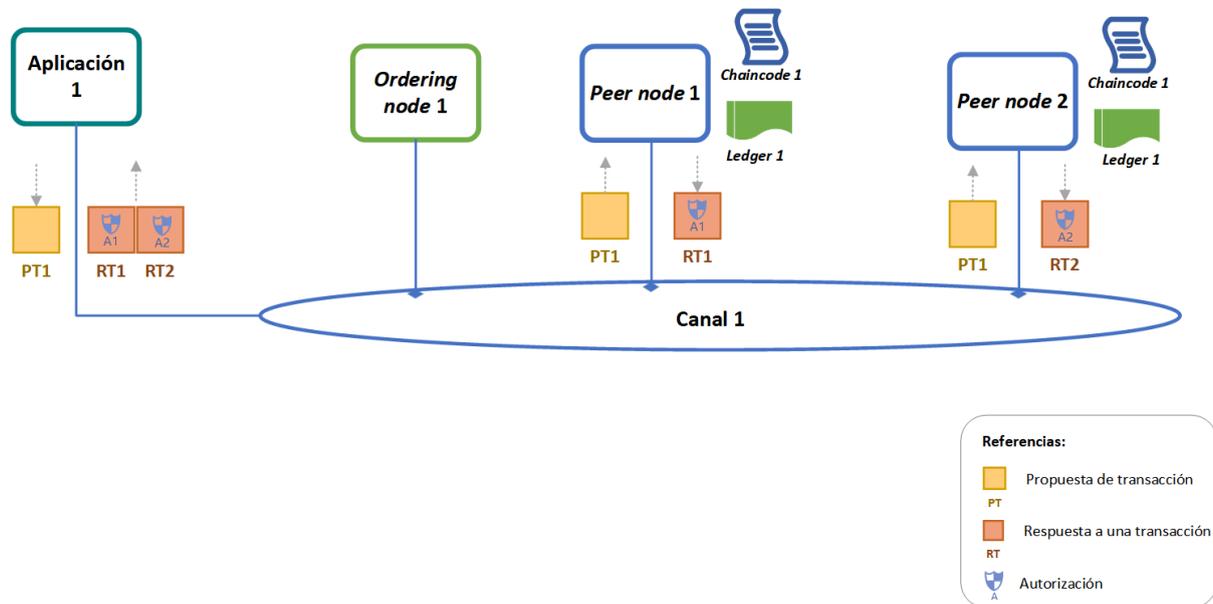


Figura 14 - Esquema de propuesta de transacción y respuesta

Luego de que el MSP valide las identidades y acciones solicitadas en cada transacción, el *ordering node* crea bloques de información para ejecutar transacciones acordadas, y los envía a todos los nodos del canal para una validación final. Cabe destacar que en este punto también se involucran los nodos del canal que no están en la *Endorsement policy* de la transacción.

Esta validación ocurre en 2 pasos. En primera instancia cada nodo verifica que se haya cumplido la *Endorsement Policy*, es decir que las transacciones estén firmadas por todos los nodos relevantes. Luego, se realiza una verificación de la consistencia del *ledger* para corroborar que las transacciones sigan siendo compatibles y evitar, por ejemplo, que hayan quedado invalidadas por la concreción de otra transacción previa durante el proceso de verificación de las transacciones actuales. Luego de validarlas, los nodos agregan el bloque a su *ledger*.

El procesamiento de los bloques es independiente en cada nodo, pero se realiza de igual forma en cada uno de ellos, para que, al aceptarlo en todos los nodos, el *ledger* final sea consistente. Si algunas de las transacciones de un bloque no son validadas, se identifican como inválidas dentro del mismo, para que no se apliquen al *ledger*. Esto permite que estas transacciones inválidas estén disponibles para auditar.

Esto mismo se puede observar en la Figura 15 [32], donde el *ordering node* O1 envía el bloque B2 - que contiene varias transacciones- a los nodos P1 y P2. Al aprobarlas, cada nodo agrega el nuevo bloque B2 al *ledger* L1, confirmando las transacciones y actualizando el *ledger* del canal.

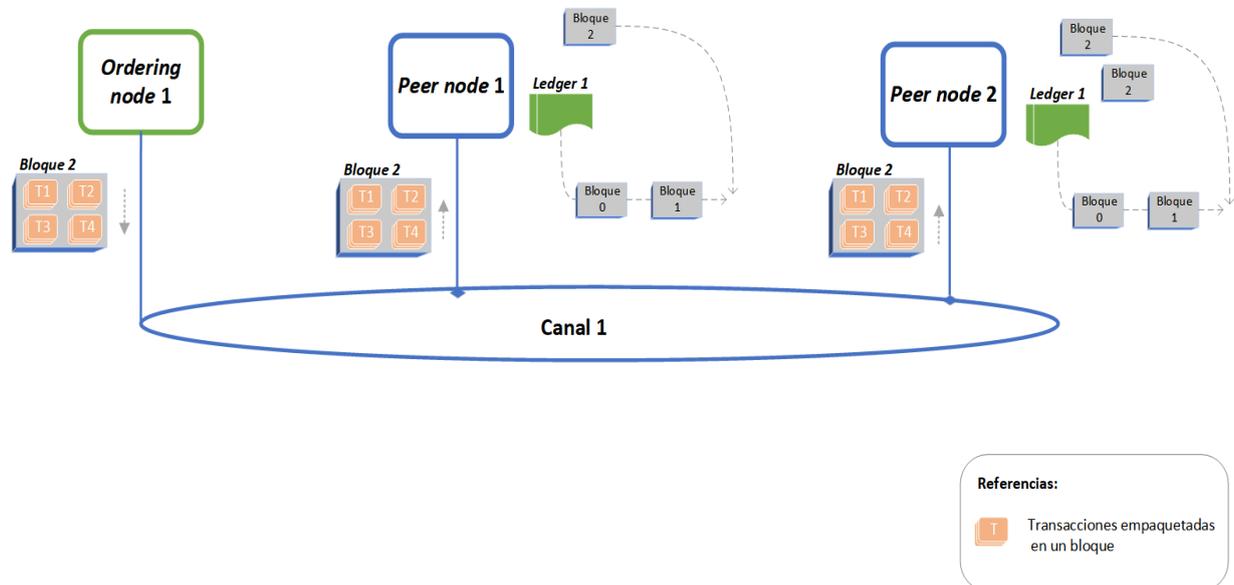


Figura 15 - Esquema de incorporación de un bloque con transacciones al ledger

Con esta lógica, las redes de *blockchain* de *Hyperledger* aseguran la fiabilidad de la información gracias a que cada nodo dentro del canal cuenta con una copia de la información (*ledger*), y si un nodo modifica la información, ésta no coincidirá con la información en el resto de los nodos, invalidando dicho cambio.

A modo de resumen, se presenta la Figura 16 que describe la interacción completa entre la aplicación que solicita la transacción y los nodos del canal, demostrando cómo los nodos y los *ordering nodes* aseguran que el *ledger* siempre esté actualizado.

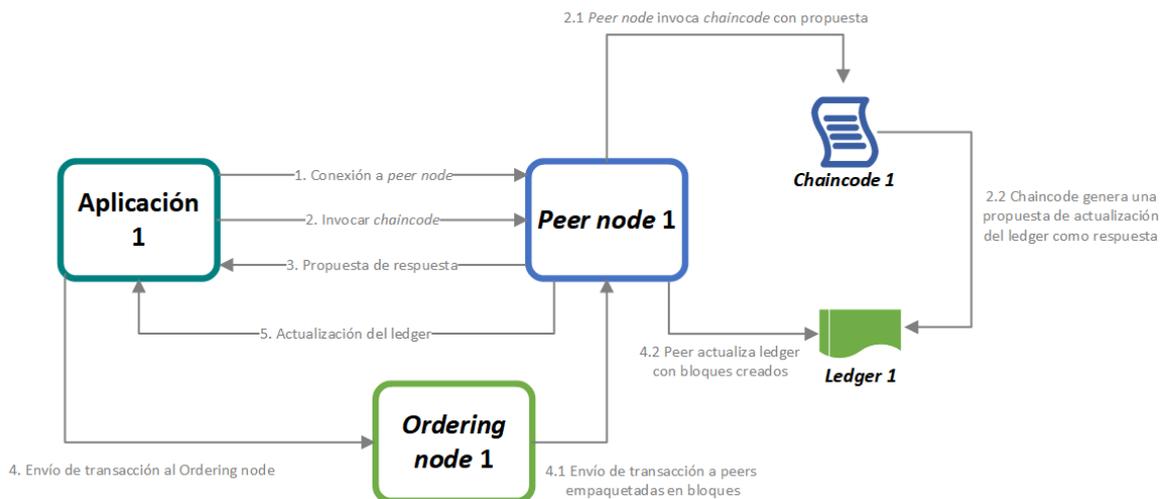


Figura 16 - Esquema de proceso completo de propuesta e inclusión al ledger de una transacción

Luego de profundizar acerca de la lógica de ejecución de transacciones en *Hyperledger Fabric*, se procedió a realizar una prueba de operación más acotada, siguiendo los pasos que se presentan en la **figura 17**.

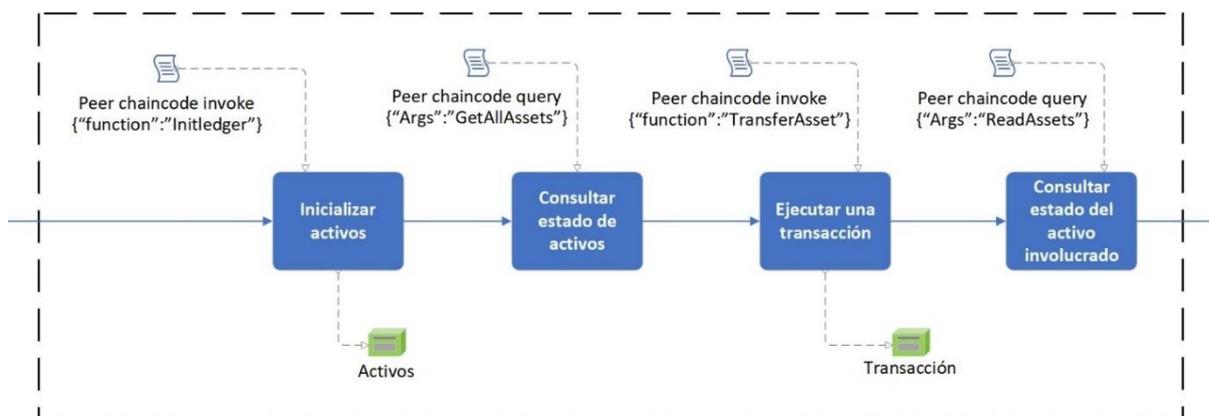


Figura 17 - Proceso de prueba de operación en el sistema como parte de la prueba de concepto

Todas las operaciones fueron llevadas a cabo desde *el peer 0* de la organización 1, con *localhost* número 7051. La serie de comandos para determinar el nodo en el que se iba a trabajar puede ser visto en la **Figura 56** del *Anexo VIII*.

Inicialización de activos

Para que los nodos puedan interactuar en el sistema, es importante contar con activos que puedan ser registrados, transferidos y consultados. En rasgos generales, toda transacción involucra una alteración en cierto activo del sistema. En el caso de la *test network* en cuestión, se ejecutó el comando "*peer chaincode invoke*" que invoca a la función *InitLedger* del *chaincode*, tal como se ve en la **Figura 57** del *Anexo VIII*, para determinar los estados iniciales de los activos.

Dichos activos pueden ser vistos en la Figura 18, que presenta el código de la función en el *chaincode*, donde se definen los 6 activos (*asset1* a *asset6*) y se asigna el color, tamaño, dueño y valor (*Color*, *Size*, *Owner*, *AppraisedValue*) de cada uno. Se nota también que no hay argumentos de entrada para la función.

```
// InitLedger adds a base set of assets to the ledger
func (s *SmartContract) InitLedger(ctx contractapi.TransactionContextInterface) error {
    assets := []Asset{
        {ID: "asset1", Color: "blue", Size: 5, Owner: "Tomoko", AppraisedValue: 300},
        {ID: "asset2", Color: "red", Size: 5, Owner: "Brad", AppraisedValue: 400},
        {ID: "asset3", Color: "green", Size: 10, Owner: "Jin Soo", AppraisedValue: 500},
        {ID: "asset4", Color: "yellow", Size: 10, Owner: "Max", AppraisedValue: 600},
        {ID: "asset5", Color: "black", Size: 15, Owner: "Adriana", AppraisedValue: 700},
        {ID: "asset6", Color: "white", Size: 15, Owner: "Michel", AppraisedValue: 800},
    }

    for _, asset := range assets {
        assetJSON, err := json.Marshal(asset)
        if err != nil {
            return err
        }

        err = ctx.GetStub().PutState(asset.ID, assetJSON)
        if err != nil {
            return fmt.Errorf("failed to put to world state. %v", err)
        }
    }

    return nil
}
```

Figura 18 - Función *InitLedger*

Luego de inicializar los 6 activos, se invocó a la función *GetAllAssets* perteneciente al *chaincode* a través del comando “*peer chaincode query*” para realizar una consulta acerca de los activos actuales, como se ve en la Figura 58 en el Anexo VIII. A través de esta consulta se busca confirmar que los valores de cada activo hayan sido inicializados correctamente y que coincidan con los especificados en el *chaincode*. A modo informativo, la función *GetAllAssets*, detallada en la Figura 19, itera y obtiene todas las entradas en el *array* llamado *assets*.

```

// GetAllAssets returns all assets found in world state
func (s *SmartContract) GetAllAssets(ctx contractapi.TransactionContextInterface) ([]*Asset, error) {
    // range query with empty string for startKey and endKey does an
    // open-ended query of all assets in the chaincode namespace.
    resultsIterator, err := ctx.GetStub().GetStateByRange("", "")
    if err != nil {
        return nil, err
    }
    defer resultsIterator.Close()

    var assets []*Asset
    for resultsIterator.HasNext() {
        queryResponse, err := resultsIterator.Next()
        if err != nil {
            return nil, err
        }

        var asset Asset
        err = json.Unmarshal(queryResponse.Value, &asset)
        if err != nil {
            return nil, err
        }
        assets = append(assets, &asset)
    }

    return assets, nil
}

```

Figura 19 - Función GetAllAssets

Ejecución de transacciones

Una vez fijados los valores iniciales de cada activo, se procedió a realizar una transacción que cambie el propietario de uno de estos activos. Particularmente, se invocó a la función *TransferAsset* del *chaincode* como se ve en la Figura 20. La transacción de prueba consiste en transferir el activo *asset6* a la persona llamada “Christopher”. Como se puede ver se utiliza el comando *invoke* para invocar la función llamada “TransferAsset” del *chaincode*. Además, se puede observar que se apunta a ambas organizaciones *org1* y *org2*, con el comando *--peerAddresses* seguido de la dirección de cada organización, puesto que, tal como se establece en la *Endorsement Policy*, ambas organizaciones deben firmar la transacción. Por otro lado, se referencian los certificados *TLS* de cada nodo utilizando el comando *-tlsRootCertFiles*.

```

juan@juan-VirtualBox:~/fabric-samples/test-network$ peer chaincode invoke -o lo
calhost:7050 --ordererTLSHostnameOverride orderer.example.com --tls --cafile ${
PWD}/organizations/ordererOrganizations/example.com/orderers/orderer.example.co
m/msp/tlscacerts/tlsca.example.com-cert.pem -C mychannel -n basic --peerAddress
es localhost:7051 --tlsRootCertFiles ${PWD}/organizations/peerOrganizations/org
1.example.com/peers/peer0.org1.example.com/tls/ca.crt --peerAddresses localhost
:9051 --tlsRootCertFiles ${PWD}/organizations/peerOrganizations/org2.example.co
m/peers/peer0.org2.example.com/tls/ca.crt -c '{"function":"TransferAsset","Args
":["asset6","Christopher"]}'
2021-05-07 20:56:47.501 -03 [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 C
haincode invoke successful. result: status:200

```

Figura 20 - Ejecución de la función TransferAsset

Al analizar la función en el *chaincode* (Figura 21) se puede visualizar que los dos argumentos de entrada de la misma son el *asset* relacionado a la transacción (*id*) y el nuevo dueño de ese *asset* tras la transacción (*NewOwner*).

```
// TransferAsset updates the owner field of asset with given id in world state.
func (s *SmartContract) TransferAsset(ctx contractapi.TransactionContextInterface, id string, newOwner string) error {
    asset, err := s.ReadAsset(ctx, id)
    if err != nil {
        return err
    }

    asset.Owner = newOwner
    assetJSON, err := json.Marshal(asset)
    if err != nil {
        return err
    }

    return ctx.GetStub().PutState(id, assetJSON)
}
```

Figura 21 - Función TransferAsset

Luego, para visualizar únicamente el estado del activo transferido, se invocó a la función del *chaincode* *ReadAsset* para el *asset6*, como se observa en la Figura 22. Al comparar el estado del *asset6* previa y posteriormente a la ejecución de la transacción, entre la Figura 18 y la Figura 22, se puede observar que la posesión del *asset6* efectivamente pasó de Michael a Christopher. En Figura 23 se ve la definición de dicha función.

```
juan@juan-VirtualBox:~/fabric-samples/test-network$ peer chaincode query -C myc
channel -n basic -c '{"Args":["ReadAsset","asset6"]}'
{"ID":"asset6","color":"white","size":15,"owner":"Christopher","appraisedValue":800}
```

Figura 22 - Visualización del activo luego de la transacción

```
// ReadAsset returns the asset stored in the world state with given id.
func (s *SmartContract) ReadAsset(ctx contractapi.TransactionContextInterface, id string) (*Asset, error) {
    assetJSON, err := ctx.GetStub().GetState(id)
    if err != nil {
        return nil, fmt.Errorf("failed to read from world state: %v", err)
    }
    if assetJSON == nil {
        return nil, fmt.Errorf("the asset %s does not exist", id)
    }

    var asset Asset
    err = json.Unmarshal(assetJSON, &asset)
    if err != nil {
        return nil, err
    }

    return &asset, nil
}
```

Figura 23 - Función ReadAsset

Gracias a la exitosa ejecución de esta prueba de concepto, que es simple pero funcional, la elección de la tecnología *blockchain* y del tipo *Hyperledger Fabric* queda respaldada para aplicar en el caso de estudio. A partir de esto, se puede proceder en el diseño del sistema que se propone para aplicar en la cadena de suministro cárnica.

Diseño del sistema

En esta sección se presentará el diseño de un sistema informático que mejore la cadena de suministro del complejo cárnico, utilizando el tipo de *blockchain Hyperledger Fabric*. Para esto, se define la siguiente metodología para definir el sistema en su totalidad:

1. Identificar los principales actores del proceso. Se hará un relevamiento de cada actor. Su rol en la cadena será evaluado para determinar si es necesaria su participación en la cadena como nodo. Estos nodos serán los encargados de cargar y visualizar la información de la *blockchain* de forma activa.
2. Determinar los documentos e información requerida en la cadena.
3. Estudiar los procesos de la industria para evaluar las funcionalidades aplicables.
4. Definir los canales de comunicación. Detallar los nodos participantes y la información incluida en cada canal.
5. Determinar las reglas de gobernanza.

A continuación, se desarrolla la aplicación de los puntos anteriores a este caso particular.

1. Identificación de los principales actores del proceso.

En esta sección se detallan los distintos actores de la cadena de suministro cárnica, con la visión de que cada actor tomaría el rol de una organización en el sistema. Cada una de ellas contaría con al menos un nodo de los tipos (*ordering, peer, client*) mencionados en la sección *Hyperledger Fabric*.

- **Productor Ganadero:** Es el primer eslabón de la cadena, que produce la materia prima en cuestión (ganado en pie). La misma será comercializada y transportada a lo largo de la cadena hasta una planta de faena en donde comenzará su proceso de transformación hacia un producto terminado. Gran parte de la documentación almacenada y compartida en el sistema está referida al ganado en este estado.
- **Sistema Nacional de Información Agropecuaria (SNIA)/Sistema Nacional de Información Ganadera (SNIG):** Sistemas de información enfocados en el mantenimiento y almacenamiento de todos los registros relacionados al agro. A través de estos se emiten y registran los documentos necesarios para la circulación y comercialización de ganado.
- **INAC:** Organismo público no estatal cuyos cometidos son la proposición y asesoramiento de la política nacional de carnes [33]. La misma es determinada por el poder ejecutivo, y, en parte, ejecutada por el INAC. En lo que respecta al proceso en cuestión, el INAC cumple un rol relevante en el componente industrial de la trazabilidad. Según la normativa vigente (Ley 17.997), al INAC se le comitió establecer un sistema de trazabilidad industrial que permitiera mantener la individualidad de los animales identificados por el SNIG a lo largo del proceso industrial. Para ello, el INAC estableció una serie de puestos de captura de datos en el proceso de faena que permiten mantener la identificación del animal que da origen en los productos a lo largo del proceso. Para garantizar seguridad a los productores ganaderos, se estableció que el INAC tome los registros en cada uno de los cuatro puntos de control mencionados, con

hardware y software propio. Esto se conoce como el “sistema de cajas negras”, y tal denominación se debe a que el sistema busca ser inviolable por parte de las plantas de faena, lo que da garantías al proveedor de materia prima de que la información registrada se corresponde con la realidad.

- **Planta de Faena:** Industria encargada del proceso de producción de cortes cárnicos, utilizando como insumo el animal en pie de los productores ganaderos.
- **Ministerio de Ganadería Agricultura y Pesca:** Departamento del Gobierno Nacional dedicado al desarrollo permanente de los sectores agropecuario, agroindustrial y pesquero, en este caso con el cometido de generar los instrumentos normativos y operacionales que permitan a los agentes económicos desarrollar sus actividades en condiciones adecuadas de información, transparencia y equidad, entre otras cosas [34]. Particularmente, implementó el sistema de identificación universal y obligatoria que requiere la colocación de un dispositivo identificador numerado de manera individual, como máximo a los seis meses de edad, que se mantiene a lo largo de la vida del animal. Esa identificación también es utilizada por el INAC. El sistema establecido y gestionado por el MGAP incluye el registro obligatorio de todos los movimientos de animales ya sea que se realicen entre distintos establecimientos de producción ganadera, o que se destinen a faena para procesamiento industrial. El sistema además prevé el registro de determinados eventos relevantes, por ejemplo, raza y sexo al momento del nacimiento, notificación en caso de ingreso a sistemas de alimentación con granos, o determinados controles respecto del uso de determinados específicos veterinarios.
- **Despachante de Aduana:** Son los autorizados por el Ministerio de Economía y Finanzas para llevar a cabo los trámites de las distintas operaciones aduaneras, entre ellas las de importación, exportación y tránsito de la carne vacuna, en este caso [35].
- **Aduana:** Servicio Gubernamental encargado de controlar el cumplimiento de las normativas relacionadas a las mercancías que atraviesan las fronteras del país, y de efectuar el cobro de los gravámenes pertinentes [36].
- **Agencia Marítima:** El agente marítimo realiza las funciones vinculadas al ingreso, permanencia, aprovisionamiento y salida del buque transportador de bienes como, en este caso, la carne [37]. Es el representante del armador, capitán o dueño del barco en algún puerto determinado. Se encarga de supervisar las operaciones de recepción, carga, descarga y entrega de las mercaderías, dentro de las condiciones detalladas en el Booking Note (ver sección *Determinación de documentos e información (datos relevantes) requerida en la cadena*).
- **Navieras:** Empresa encargada de transportar por vía marítima los productos deseados, desde un puerto a otro.
- **Banco:** Agentes financieros que garantizan que se efectúen correctamente las transacciones monetarias relacionadas a la compraventa del producto en cuestión, de acuerdo a las especificaciones acordadas por ambas partes.
- **Comprador:** Cliente interesado en la compra del producto, usualmente para comercializarlo.
- **Consumidor final:** Último participante de la cadena, interesado en el consumo del producto.
- **Ventanilla Única de Comercio Exterior (VUCE):** Instrumento que centraliza la gestión y el procesamiento de todos los trámites y solicitudes de importación, exportación o tránsito, que proceden de cualquier empresa particular, despachantes de aduana, etc. Esta centralización permite que el Estado intervenga para hacer los procesos de comercio exterior de manera

más eficiente y simple sin descuidar la seguridad de los controles que se deben llevar a cabo en la actividad [38].

En dicho sistema, las distintas organizaciones se conectan de manera descentralizada -como se visualiza en la Figura 24- por la naturaleza de la *blockchain*, más allá de los canales de comunicación privados que se determinan en la subsección *Definición de canales de comunicación*.

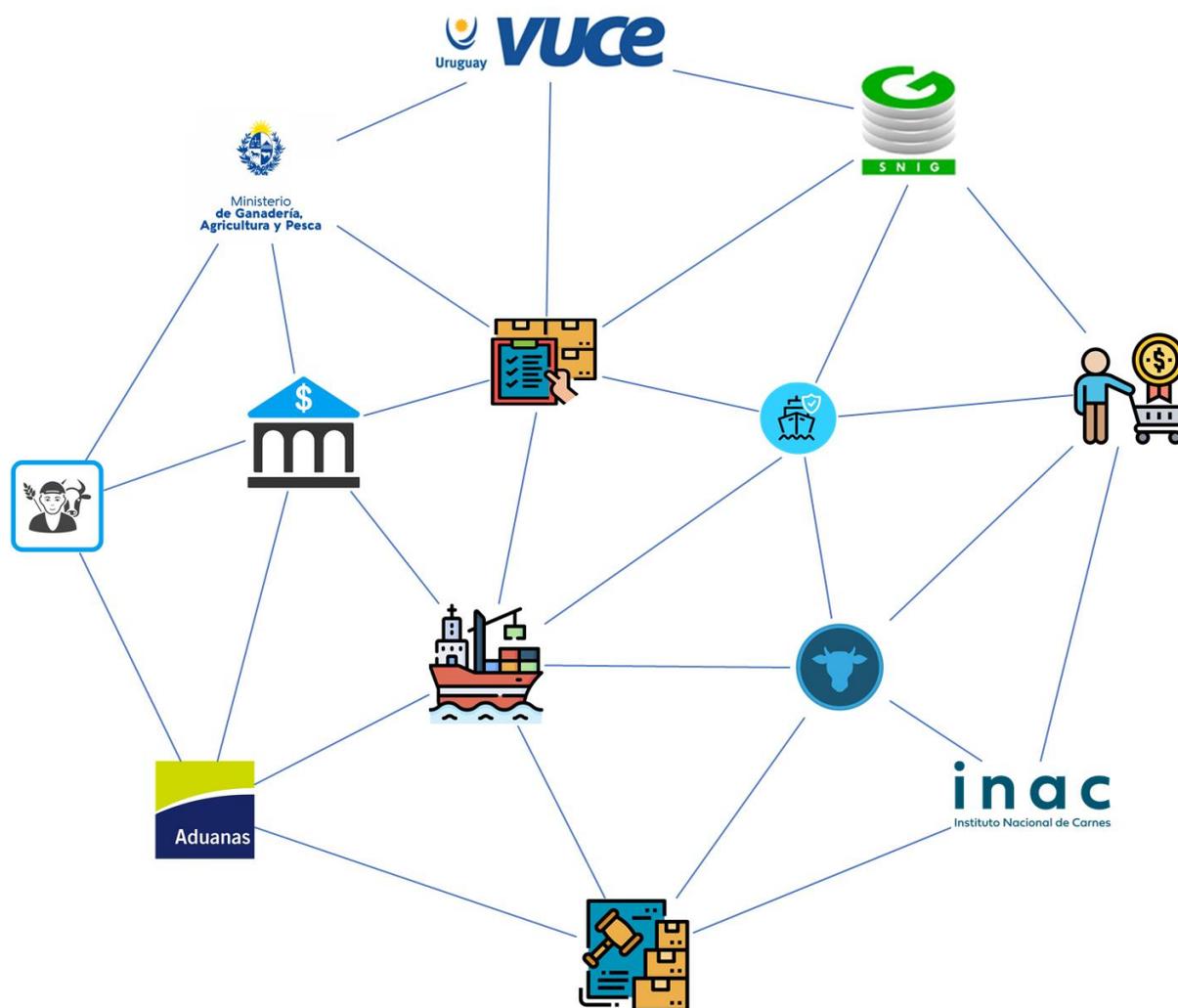


Figura 24 - Conexión entre nodos

2. Determinación de documentos e información (datos relevantes) requerida en la cadena

A continuación, se destacan los documentos e informaciones relevantes a considerar en el diseño del sistema en cuestión. En las siguientes secciones, se continuará desarrollando el rol de estos documentos en la cadena productiva actual, y la gestión propuesta de los mismos en el nuevo sistema.

- **Guía de Propiedad y Tránsito:** Se utiliza para documentar todo tipo de operación que involucre movimientos de haciendas, cambios de propiedad o consignaciones de las mismas con o sin movimiento físico. Es un instrumento legal y administrativo para el control de existencias y movimientos de ganado [39].
- **Carta de Crédito:** Una carta de crédito es un medio de pago utilizado comúnmente en transacciones comerciales internacionales, debido al nivel de seguridad que ofrece al vendedor en cuestión [40]. El fundamento detrás de la utilización de una carta de crédito es garantizar seguridad al momento de realizar una compraventa internacional, especialmente cuando no hay altos niveles de confianza entre las partes. En el caso de la exportación de cortes cárnicos, se realiza un contrato de compraventa entre el cliente y el vendedor, el cual es seguido por la solicitud de apertura de un crédito documentario por parte del cliente internacional a un banco de su país (Banco Emisor). Cuando el banco del vendedor (Banco Notificador) recibe la notificación de la apertura de la carta de crédito por parte del banco emisor, se lo notifica al vendedor, que expedirá los productos al cliente, y los documentos que detallan las condiciones de la transacción al banco notificador, que los envía al banco emisor. Si se cumplen las condiciones pactadas, el banco emisor libera el pago, y el cliente podrá retirar la mercadería, presentando la respectiva documentación. De esta forma, el cliente se asegura que efectuará el pago sólo si el vendedor cumple ciertas condiciones preestablecidas, y además, el vendedor obtiene la certeza de que, al cumplir con las condiciones, obtendrá el pago correspondiente.
- **VSOL:** Este documento funciona como certificado de exportación de productos cárnicos, y valida la autorización para la exportación definitiva de carne [41]. Es tramitado por el despachante de aduana y lo emite el INAC. En él se detallan:
 - Datos del beneficiario: Rut, Razón Social, Dirección, Teléfono, Email.
 - Datos de la mercadería: Número de solicitud de importación, número de pase frontera, información acerca del certificado sanitario, información acerca del establecimiento de origen, fecha de importación, cantidad de bultos, cantidad importada, destino de la mercadería, entre otros.
 - Datos del importador: Nombre y dirección
 - Datos del depósito: Nombre y dirección

Este documento debe ser completado previo al Documento Único Aduanero.

- **Constancia Oficial de Calidad Comercial (COCC):** Se trata de un requisito indispensable para habilitar exportaciones, establecido en 1984 mediante la misma ley que crea al INAC (Ley Nº 15.605) [42]. La conformidad en distintos controles de producción (control a materias primas,

control a procesos y control a empaques) e inspecciones a productos terminados determina el otorgamiento de dicha constancia. Una vez que se obtenga esta constancia, la misma se deberá especificar en el VSOL.

- **Documento Único Aduanero (DUA):** La Dirección Nacional de Aduanas define que este documento fue creado como formato estándar y único para declarar operaciones aduaneras de entrada, salida y tránsito de mercaderías [43]. Al completar el VSOL, se procede a completar el DUA con una numeración identificatoria, donde se declaran, en este caso, las operaciones aduaneras de la carne.
- **Caravana de identificación de ganado:** Esta caravana funciona como dispositivo electrónico de identificación universal de cada animal para cumplir con lo establecido por la Ley 17.997. La misma determina que la identificación bovina es obligatoria, universal, individual y a partir de -como máximo- los 6 meses de edad. Cada una de estas caravanas contiene un código nacional que identifica a cada animal en una base de datos oficial, para llevar registro de los *“movimientos, cambios de propiedad y demás eventos productivos y sanitarios relevantes”* y de esa forma, posibilitar la obtención de un *“informe de toda su historia, desde el nacimiento hasta su muerte”* [6]. La caravana como entidad en sí es de interés en el estudio, puesto que es la clave primaria para la información del ganado, a la que se le asocia todo tipo de información a lo largo de la vida del animal. De esta forma, también interesa centrarse en la información que se le asocia a la caravana como lo son las pesadas en campo, vacunas administradas y demás aplicaciones veterinarias, cambios de propiedad, e ingreso a distintos sistemas de producción, entre otros. En la planta, se asocian datos como la dentición, el peso a la llegada a la planta, o el código del Canal que continuará la trazabilidad interna (ver siguiente subsección).
- **Etiquetas internas de planta:** A medida que la res se subdivide en cortes más pequeños, algunos de los nuevos cortes se identifican con una etiqueta particular. Las etiquetas usadas actualmente para este propósito son la etiqueta del Canal (para la res entera), la etiqueta de la Media Canal (para cada media res), la etiqueta del Cuarto Delantero, la etiqueta del Cuarto Trasero y la etiqueta del Asado. La etiqueta del Canal contiene el ordinal de faena, un código interno que se asocia al número de caravana y al que se referencian las etiquetas de las siguientes subdivisiones (Media Canal, Cuartos y Asado). Una vez más, interesa estudiar cada una de estas etiquetas por sí solas, pero además interesa la información que se les asocia. A modo de ejemplo, esta información incluye, entre otros, el grado de terminación en grasa, los resultados de los distintos controles de calidad y el peso en los 4 puestos de control.
- **Contrato compra venta entre planta de faena y cliente:** El contrato de compraventa también resulta de interés en este estudio. El mismo se gestiona en el proceso de emisión de una carta de crédito, que fue descrito anteriormente.
- **Documentos VUCE:** La VUCE exige la completitud de ciertos documentos:
 - Declaración Jurada de Negocio Concertado
 - Autorización de Exportación
 - Certificado de Calidad
 - Certificado Oficiales de Transferencia de Exportación
 - Certificado Pase de Frontera
 - Exportación de Carnes

- **Documentos a presentar en la aduana:**
 - DUA
 - Título de transporte directo con el que se transporta la carne hacia el exterior
 - Factura comercial certificada por el exportador
- **Declaración de mercadería:** Mediante este documento se otorga un canal de revisión a la mercadería.
- **Booking note:** Documento que detalla condiciones para la exportación, establecidas entre la compañía naviera y el exportador. El mismo especifica la fecha y las horas de salida y llegada, además de indicar la agencia marítima contratada [44].
- **Conocimiento de Embarque o Bill of Lading:** Documento que establece reglas y condiciones a cumplirse entre el expedidor de mercadería (vendedor), el destinatario (cliente) y el transportista. Según el Código Aduanero Uruguayo, es de utilidad para acreditar el recibo de las mercaderías a bordo y representa “el derecho para disponer de las mercaderías” (Código Aduanero Uruguayo, Art. 70) [45]. También cumple las funciones de recibo de las mercancías en el puerto de origen y de título de propiedad para liberar la mercancía en el puerto de destino.
- **Canal de revisión para la declaración de mercadería:** al momento de declarar la mercadería en la Aduana, se pueden dar tres escenarios distintos, que son los canales de revisión verde, naranja o rojo. Los detalles de este proceso se detallan en la sección *Desarrollo práctico de aplicación en cadena de suministro*.
- **Información del establecimiento productivo:** Acerca de los distintos establecimientos productivos, interesa registrar la localidad, el nombre del productor a cargo, las distintas certificaciones que se hayan otorgado, y los tipos de producción ganadera que se practican, entre otros. En la sección *Agregado de valor a la cadena de suministro*, se detallan algunas certificaciones que se podrían registrar para cada establecimiento productivo.
- **Información de la planta de faena:** Acerca de las plantas de faena, interesa registrar el nombre, la localidad, las certificaciones que se otorgaron a cada una de ellas, las marcas con las que se trabaja, y los tipos de producción que se llevan a cabo, entre otros. En la sección *Agregado de valor a la cadena de suministro* se detallan las distintas certificaciones que se podrían registrar para cada planta.
- **Planillas de Bienestar Animal (BA):** En este tipo particular de producción -que se desarrolla en profundidad en la sección *Agregado de valor a la cadena de suministro*- se deben mantener planillas para predios rurales, empresas transportistas y plantas de faena, que garantizan el cumplimiento de distintos requisitos. El registro de estas planillas es de interés para incluir en el sistema propuesto.
- **Información de condiciones de viaje de exportación:** En la subsección *Sinergia entre IoT y la trazabilidad con blockchain* se menciona una funcionalidad particular que se podría ejecutar a través del sistema que se propone. Para esto, resultan de interés los datos acerca de las condiciones en que se realiza el viaje de exportación de carne; registros puntuales y periódicos de temperatura y presión de contenedores a lo largo del viaje, registros puntuales y periódicos de ubicación y tiempo, y fecha de salida del origen, llegada a destino y de paradas intermedias, entre otros.

3. Desarrollo práctico de aplicación en cadena de suministro

3.1. Proceso estándar de producción de cortes cárnicos con *blockchain*

A continuación, se describen las actividades básicas e indispensables del proceso de producción de cortes cárnicos propuesto a partir de la introducción de la tecnología en cuestión. Dicho proceso comienza con la producción de materia prima en un establecimiento rural, y termina con la exportación del producto terminado. En el desarrollo del proceso, se pondrá especial énfasis en los documentos involucrados que se transfieren entre los distintos actores, con el objetivo de dejar explicitadas las funcionalidades que se plantean en el sistema diseñado con *blockchain*. Esta sección propone un funcionamiento alternativo al proceso de exportación actual.

Producción de materia prima (animales en pie).

La producción de la materia prima, es decir, la cría de ganado se realiza en establecimientos rurales. Los animales son identificados de manera única desde su nacimiento mediante la colocación de una caravana numerada. En este punto, comenzaría la recolección de información mediante la creación de un registro en la *blockchain*, con el número de caravana de cada animal como referencia. A lo largo del proceso, se le asociarán los distintos documentos e información relevante que se establecieron en la sección correspondiente.

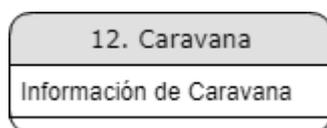


Figura 25 - Nuevo registro creado en la blockchain

Por otro lado, se considera importante también registrar movimientos de ganado entre productores (cambios de propiedad) previo a la venta final hacia una planta de faena. En el momento de la venta del ganado a la planta de faena, se realiza un nuevo intercambio de información entre actores de la cadena. Tanto para el cambio de propiedad, como para trasladar el ganado desde el establecimiento hasta la planta de faena, se necesita la confección de la Guía de Propiedad y Tránsito.

Para el traslado del ganado, se necesitan cuatro vías de la Guía de Propiedad y Tránsito. La vía original y el duplicado acompañan a la carga en su transporte, la tercera vía queda en posesión de la comisaría para enviar a DICOSE posteriormente y la última la conserva el productor oferente de ganado. A pesar de que esto logra disponibilizar la información para cada participante de manera confiable, resulta en papeleo excesivo y la tarea podría ser optimizada. Con la aplicación del modelo que se propone, una sola Guía en formato digital es necesaria para ser cargada a la *blockchain* para estar en simultáneo a disposición de los actores interesados mencionados. Con esto, se ahorra tiempo, papel y dinero, y se evitan riesgos de extravío o daño en el manipuleo.

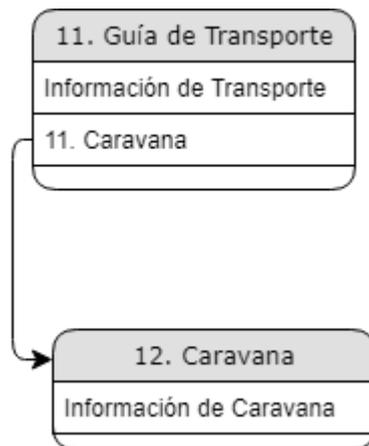


Figura 26 - Nuevo registro creado en la blockchain

Producción industrial de cortes cárnicos

Actualmente, al arribar a la planta de faena un lote de ganado, se leen las caravanas a través de un lector, registrando la fecha y hora de su llegada. Posteriormente, se lleva a cabo el proceso de faena del animal. Se propone que este registro viaje directamente a la *blockchain*, y así se añada a la información ya existente de cada caravana. De esta forma, esta recolección de datos podrá estar disponible para el MGAP para su visualización. Luego, son emitidas y registradas etiquetas a medida que se fracciona la res: al animal entero se le coloca una etiqueta correspondiente al “Canal”. Esta etiqueta contiene una codificación interna (Ordinal de Faena) y se registra el número de caravana del animal vivo del que provino esa carcasa. Luego, la carcasa (res entera) se divide en dos medias reses y se le coloca a cada media res una etiqueta denominada “Media Canal”. Esta etiqueta se codifica internamente, con un código del cual se puede deducir el ordinal de faena original. Por último, cada Media Canal se divide en un Cuarto Delantero, un Cuarto Trasero y un Asado, y a cada uno de estos se les coloca la última etiqueta que contiene una codificación interna que se referencia con la codificación de la media canal original. De esta forma, cada cuarto se puede rastrear hacia atrás, hasta llegar al número de caravana del animal en pie. Es decir que se puede identificar de qué Media Res proviene un Cuarto Delantero, y a su vez de qué Res proviene esa Media Res, y a cuál fue el número de caravana original del animal en cuestión. Cada etiqueta contiene las referencias mencionadas, y además puede incluir otra información como la dentición (indicador de la edad del animal), o el grado de terminación en grasa, entre otros. Al momento de emitir cada una de las etiquetas, una interoperabilidad con el sistema de la planta de faena permitiría agregarlas en simultáneo a los registros de la *blockchain*, así como cualquiera de los datos que se mencionan.

Posteriormente, los cuartos son fraccionados en distintos cortes cárnicos (e.g.: colita de cuadril, peceto, asado de nalga, etc.). En Uruguay algunas plantas de faena identifican los grupos de cortes a nivel de lote, es decir que no necesariamente se puede conocer qué corte provino de qué cuarto, sino que se sabe que un grupo de cortes provino de un grupo de cuartos. Otras plantas de faena sí realizan la trazabilidad a nivel de corte individual.

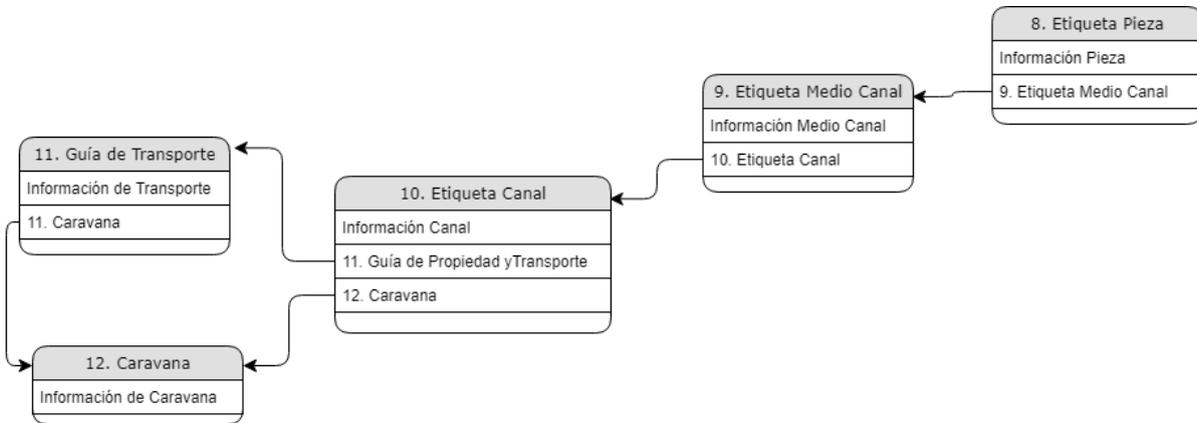


Figura 27 - Nuevo registro creado en la blockchain

Se podría escalar aún más esta lógica de codificación interna ya implementada en plantas de faena para obtener mayor profundidad aún en la trazabilidad. Particularmente, se propone cargar a la *blockchain* también una codificación del envase (caja) en el cual se embalan los cortes, y eventualmente incluir un código QR como mecanismo de acceso a toda la información que haya sido registrada en el sistema hasta ese momento.

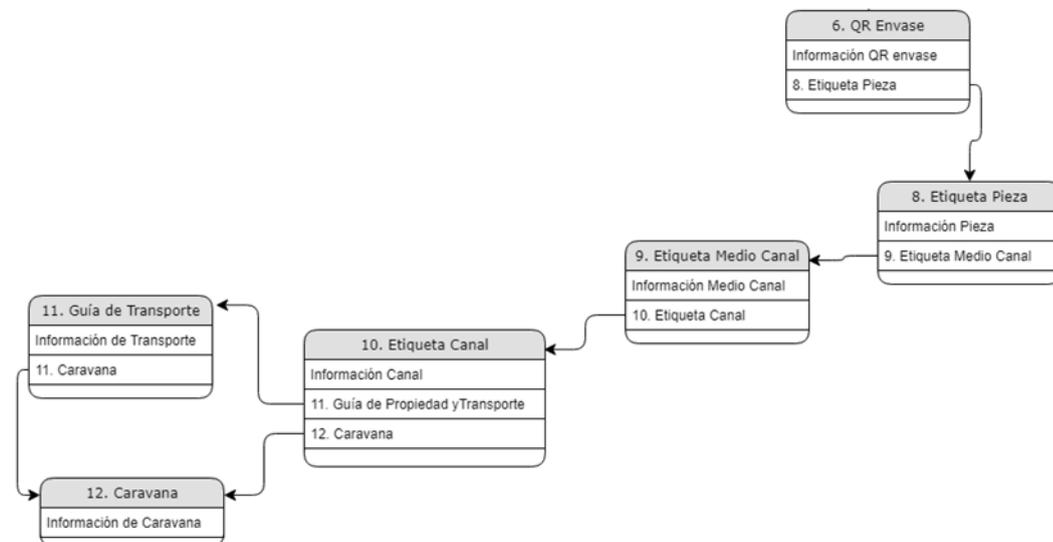


Figura 28 - Nuevo registro creado en la blockchain

Otra actividad relevante en el proceso es la captura de datos en cuatro instancias, que funcionan como puntos de control. Específicamente, se registra:

- el peso del animal vivo (por lotes de animales),
- el peso de las dos medias canales provenientes de cada animal una vez finalizado el proceso de faena,
- el peso de las dos medias canales una vez finalizado el proceso de emprolijamiento o *dressing*,
- el peso del Cuarto Delantero y Cuarto Trasero en el momento de ingresar al proceso de desosado.

Las balanzas que realizan dichos controles son gestionadas por el software del INAC (sistema de cajas negras). Se propone el desarrollo -por parte del área tecnológica de la planta de faena- de una serie de consultas que permitan importar esta información a la *blockchain*, desde el software del INAC.

Todo el proceso descrito anteriormente se mapea en el diagrama del *Anexo I*.

Exportación de cortes cárnicos producidos

La planta de faena negocia la venta de las piezas de carne con los clientes. Para la mayor completitud del modelo, se asume que todos los compradores en cuestión se encuentran en el extranjero. La negociación se materializa en un contrato de compraventa entre las partes, en las cuales quedan definidos los términos y condiciones de la compra y el instrumento de pago a emplearse. Cada forma de pago sea a través de un crédito documentario, una cobranza bancaria o un pago en cuenta corriente, implica un rol distinto por parte del banco del cliente y del exportador [46]. Habitualmente, para garantizar la mayor seguridad posible en una transacción entre partes con poca confianza, se utiliza una carta de crédito, y a efectos de este modelo también se utilizará la misma [47]. La carta de crédito compromete al banco del cliente (banco emisor) a efectuar el pago una vez se haya cumplido con los términos y condiciones de la entrega. La carta de crédito es notificada al vendedor a través de un banco notificador. Ambas partes quedan satisfechas dado que el cliente tiene la garantía de que se cumplirá con lo establecido, y el exportador tiene certeza del cobro de la exportación. Al incorporar *blockchain* en el proceso, existen dos alternativas:

1. El banco emisor carga la carta de crédito en el sistema, creando un respaldo del documento y una comunicación directa con el cliente sin la participación del banco notificador. Este proceso se mapea en el diagrama del *Anexo II*.
2. Se reemplaza la carta de crédito a través de un *smart contract* en la *blockchain*. En el *smart contract* se define un tipo de transacción que involucra como argumentos de entrada el código de los contenedores involucrados en la transacción, junto con el precio y demás atributos pertinentes. El comprador envía el dinero a una cuenta controlada por el *smart contract*, que libera el dinero al exportador automáticamente, solamente si se corrobora el cumplimiento de los términos y condiciones del *smart contract*. El cumplimiento de los términos es sencillamente corroborado al recolectar la información almacenada a través de los RFID de los contenedores, como se profundiza en la sección *Sinergia entre IoT y la trazabilidad con blockchain*. Por otro lado, la aduana de origen debe controlar que los contenedores involucrados y comprometidos en la transacción del *smart contract* no sean liberados al

cliente o a un tercero, hasta que dicha función de transacción haya sido ejecutada exitosamente. Con este rol de la aduana, también se evita que los contenedores puedan ser vendidos a otra persona externa que no participe de la transacción. Hasta que ambas partes no manifiestan su conformidad con el resultado de la transacción, el comprador no puede retirar la mercadería y el vendedor no puede cobrar su dinero. De esta forma ambos participantes están interesados en la resolución de la situación. Si ambos participantes deciden acordar la rescisión de la transacción, el dinero se envía nuevamente al cliente, y los contenedores pueden ser vendidos a cualquier tercero. Todo este proceso se encuentra mapeado en el diagrama del *Anexo III*.

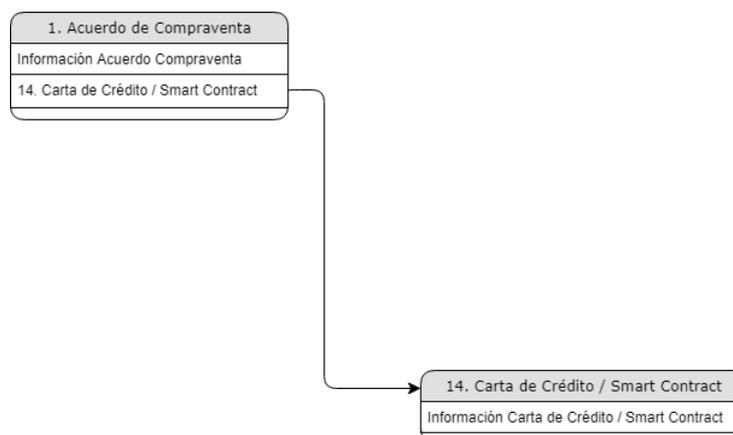


Figura 29 - Nuevo registro creado en la blockchain

Posteriormente, para el cruce de frontera de la carne hacia el exterior, es necesario llevar a cabo una serie de actividades para que finalmente la aduana autorice la exportación [48]. En un primer lugar se debe contar con un despachante de aduana para realizar los trámites. Se propone que cada despachante esté registrado en el sistema con su información, incluyendo habilitaciones y certificados, para que los exportadores tengan un listado fiable de empresas y personas con quien trabajar, y un contacto directo con las mismas.

En línea con esta propuesta, los despachantes de aduana podrán descargar los documentos de exportación obtenidos de la plataforma de la VUCE, para almacenarlos en la *blockchain* y disponibilizarlos a los interesados. Las notificaciones de aprobación/rechazo de cada uno de estos documentos (notificaciones que genera VUCE) se podrán imitar en la *blockchain* mediante cambios de estado en cada uno de los documentos. Es decir, al crear una entidad por cada uno de estos documentos, y al asignarle un atributo a cada entidad -que represente un “estado”-, se podrá notificar a los interesados cuando alguno de los participantes cambia el estado de algún documento (e.g.: una notificación que indique que el VSOL pasó del estado “pendiente de aprobación” al estado “aprobado” podrá ser vista automáticamente por todos los nodos del canal).

Si bien actualmente la plataforma de la VUCE se encarga de enviar documentos entre los participantes, un primer alcance de la implementación del sistema de *blockchain* se limitaría a permitir la carga de

estos documentos y gestionar las notificaciones a los usuarios registrados. Eventualmente, se debería analizar una integración entre la *blockchain* y la plataforma mencionada.

El despachante de aduana debe tramitar el VSOL, que es emitido por el INAC. Una vez aprobados los documentos, el INAC transmite de forma automática, a través de VUCE, los documentos a la aduana que contienen la siguiente información:

1. Número de certificado
2. Tipo y número de documento exportador
3. Nomenclatura Común del Mercosur (Para la carne bovina fresca o refrigerada es 0201 y para la carne bovina congelada 0202)
4. Unidad Física autorizada (UVF que en el caso de kilos sería 10)
5. Cantidad física autorizada
6. País destino
7. Fecha de inicio y fin

Posteriormente, inspectores capacitados del INAC realizan un control de producción e inspección del producto terminado para otorgar la Constancia Oficial de Calidad Comercial (COCC) que se adjunta al VSOL.

Con la certificación VSOL, se procede a completar el DUA con una numeración identificatoria, donde se declara de forma estandarizada las operaciones aduaneras de entrada, salida y tránsito de mercaderías, incluida en la carne. Habitualmente, son impresas seis vías, distribuidas dos para la aduana, una para el exportador, el declarante, el transportista y una vía “cero” de uso común. Con el fin de evitar la burocracia de las reimpressiones y brindar mayor accesibilidad este documento estará siempre disponible para estos actores en la *blockchain*. Una vez más, la carga de estos documentos a la *blockchain* sería tarea de los despachantes de aduana.

Luego, el Sistema Lucia (Sistema Informático de la Dirección Nacional de Aduanas) corrobora que coincida la información proporcionada en ambos documentos y que corresponda con la realidad.

La documentación que presentar en la aduana junto con el DUA es la siguiente:

1. Copia del título de transporte directo con el que se transporta la carne hacia el exterior.
2. Copia de la factura comercial certificada por el exportador.

Idealmente, se buscaría simplemente cargar estos documentos a la *blockchain* dejándolos a disposición de la aduana para evitar el trámite de presentación física de los mismos.

Superadas estas etapas, se decreta un canal de revisión para la declaración de mercadería, cuyo resultado también será almacenado en el sistema para conocimiento de todos los participantes y para futuro control [49]. La mercadería puede tener los siguientes destinos [50]:

- Canal Verde: se dará el cumplimiento automático, pudiendo procederse al retiro de la Mercadería.
- Canal Naranja: se debe realizar un análisis documental previo al retiro de la mercadería

- Canal Rojo: la mercadería debe superar un análisis documental y revisión física para luego ser retirada.

El flujo mencionado anteriormente puede representarse a través del diagrama de la Figura 30, tomado de la Dirección Nacional de Aduanas [48].

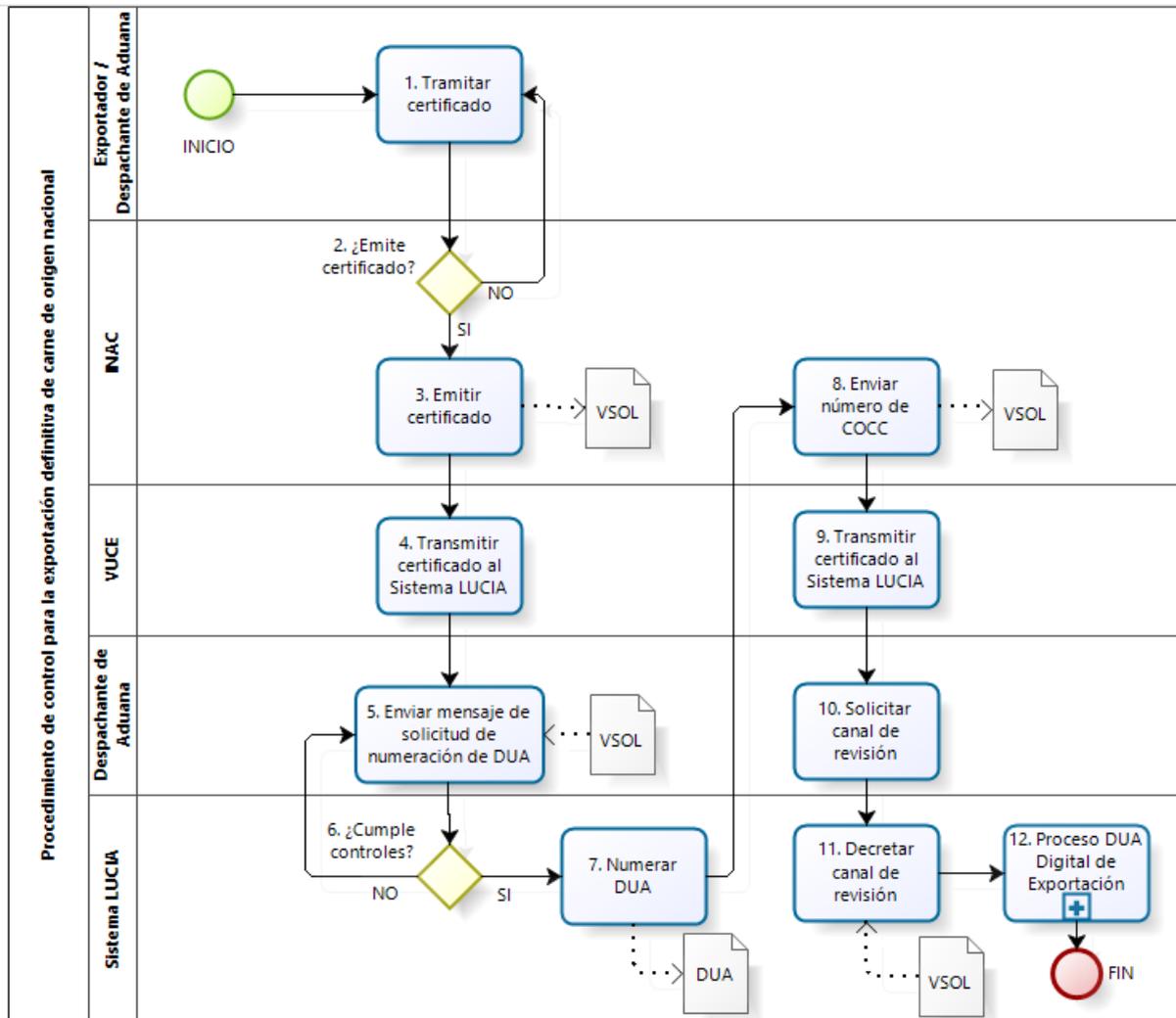


Figura 30 - Procedimiento de control para la exportación de carne

Al finalizar la etapa de revisión, se pagan los impuestos y aranceles correspondientes y la carne estará lista para ser embarcada para su transporte al país de destino. El exportador se comunica con las navieras para el transporte por vía marítima, y el acuerdo entre ambas partes se materializa en el *Booking Note*. Este documento garantiza un espacio para la mercadería dentro de los contenedores marítimos del barco, y detalla fecha y hora de salida y llegada, así como la agencia marítima contratada [44]. Las agencias marítimas supervisan la recepción, carga, descarga y entrega de las mercaderías, según las condiciones detalladas en el *Booking Note*. Tras la carga en los buques, la empresa naviera se encarga de emitir el *Conocimiento de Embarque* o *Bill of Lading* que funciona como un contrato de transporte reconocido internacionalmente entre la naviera y el expedidor. Es emitido por la naviera, además, a través del mismo se constata la recepción de la mercancía para ser transportada al puerto

de destino a bordo de determinado buque y en las condiciones pactadas entre el vendedor y el comprador del producto. Puesto que este documento incluye la información acerca de los contenedores en los cuales se enviará la mercadería, nuevamente se presenta una oportunidad de escalar la información trazada. En este caso, se propone cargar a la *blockchain* -por parte de la naviera- una codificación del contenedor en el cual se transportarán los envases, e incluir en el registro los códigos de dichos envases. Eventualmente se podría incluir nuevamente un código QR, pero en el contenedor, como mecanismo de acceso a toda la información que haya sido registrada en el sistema hasta ese momento. Esto permitirá conectar directamente el historial de los lotes de cortes cárnicos - que hasta este punto era desde el campo hasta la industria- con el historial que se seguirá generando en el proceso de exportación, para impactar definitivamente en el alcance total de la trazabilidad del sistema.

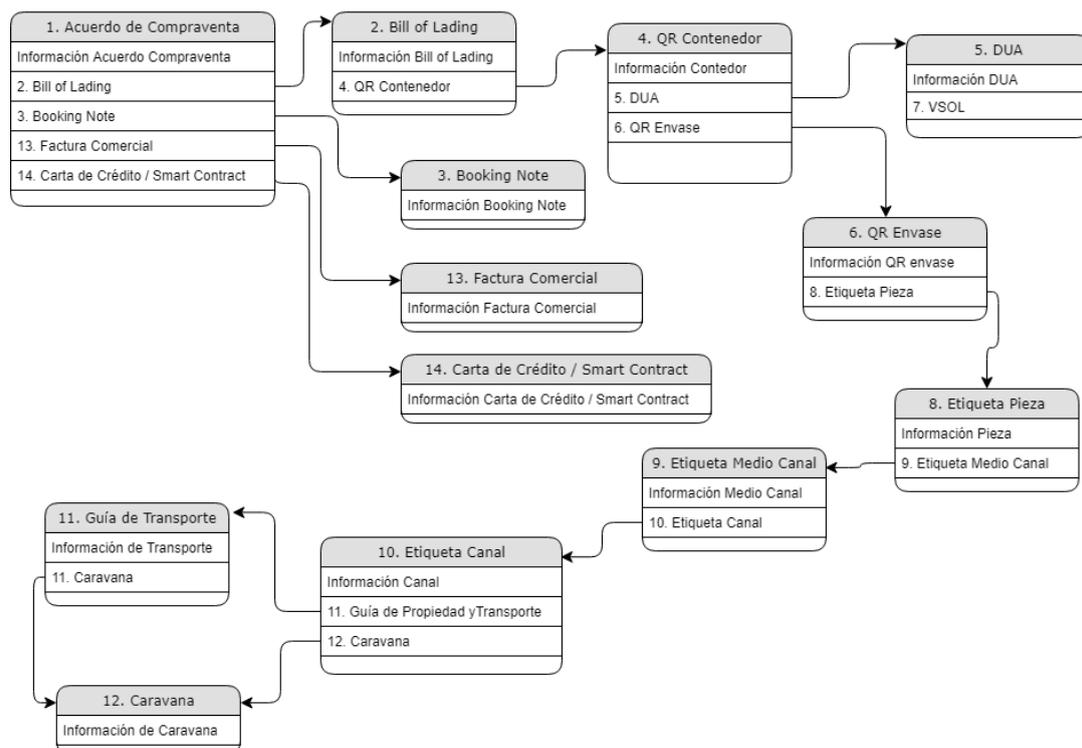


Figura 31 - Nuevo registro creado en la blockchain

Siguiendo con el proceso de exportación, al arribar al puerto de destino, la carga atravesará un proceso similar de importación adaptado a las normativas del país. Sin embargo, con toda la información de los pasos anteriores ya almacenada en la *blockchain*, es muy probable que el trámite de ingreso sea más rápido y eficiente, ya que se habilitaría sencillamente la visualización de los documentos necesarios a la aduana extranjera.

Por esto, la lógica del modelo consiste en almacenar y compartir de forma segura a través de *blockchain*, todos los documentos necesarios que fueron detallados en esta sección.

4. Relación lógica entre documentos

En forma de síntesis, a través del siguiente diagrama se puede visualizar de forma esquemática la trazabilidad de documentos que permitiría el sistema. Esto permite, por ejemplo, que al acceder a un *Bill of Lading*, se puedan visualizar y acceder, en caso de pertenecer a los canales correspondientes, a los distintos contenedores que se relacionan con ese *Bill of Lading* original. Una aplicación particular que se logra a través de esta estructura es, por ejemplo, que se pueda escanear el código QR de un contenedor para visualizar una lista de los distintos envases que el mismo contiene, y su vez toda la información que puede desencadenar este envase, siguiendo las conexiones entre bloques sucesivos. Esto se puede aplicar partiendo de cualquier bloque que se tome.

5. Definición de canales de comunicación

Hasta ahora se ha hecho la simplificación de que cada tipo de actor (e.g. las plantas de faena, los despachantes de aduana, etc) tiene un comportamiento y rol determinado en la cadena de suministro, sin entrar en detalles acerca de las distintas organizaciones que pueden asumir cada rol particular. En la práctica, puede haber varias organizaciones correspondientes a un mismo tipo de actor, que corresponden a las empresas que abarcan el mismo rubro o negocio. Por ejemplo, para el actor genérico “Planta de Faena”, existen varias organizaciones -con sus respectivos nodos- que son las distintas plantas que se desempeñan en el rubro. De esta forma, cada combinación de organizaciones -una correspondiente a cada actor- genera una cadena de suministro distinta.

El principal propósito de los canales es mantener la privacidad de las organizaciones respecto a su competencia, en cuanto a información sensible. Por lo general, cada canal de comunicación corresponderá a las organizaciones involucradas en la cadena de suministro de un producto particular establecido por el acuerdo de compraventa entre la planta de faena y el cliente, como se puede ver en el siguiente diagrama:

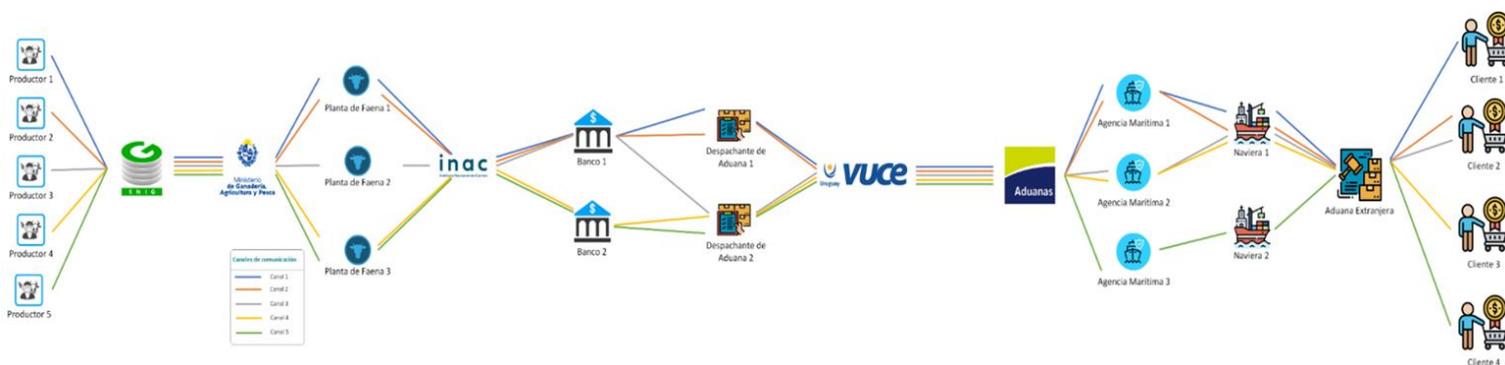


Figura 32 - Canales de comunicación en la blockchain

Cabe destacar también, que aún para un mismo canal, existen sub-canales determinados por los documentos involucrados en la cadena de suministro, ya que cierta privacidad debe ser mantenida inclusive entre las distintas organizaciones de un mismo canal. A continuación, una visualización gráfica de lo mencionado:

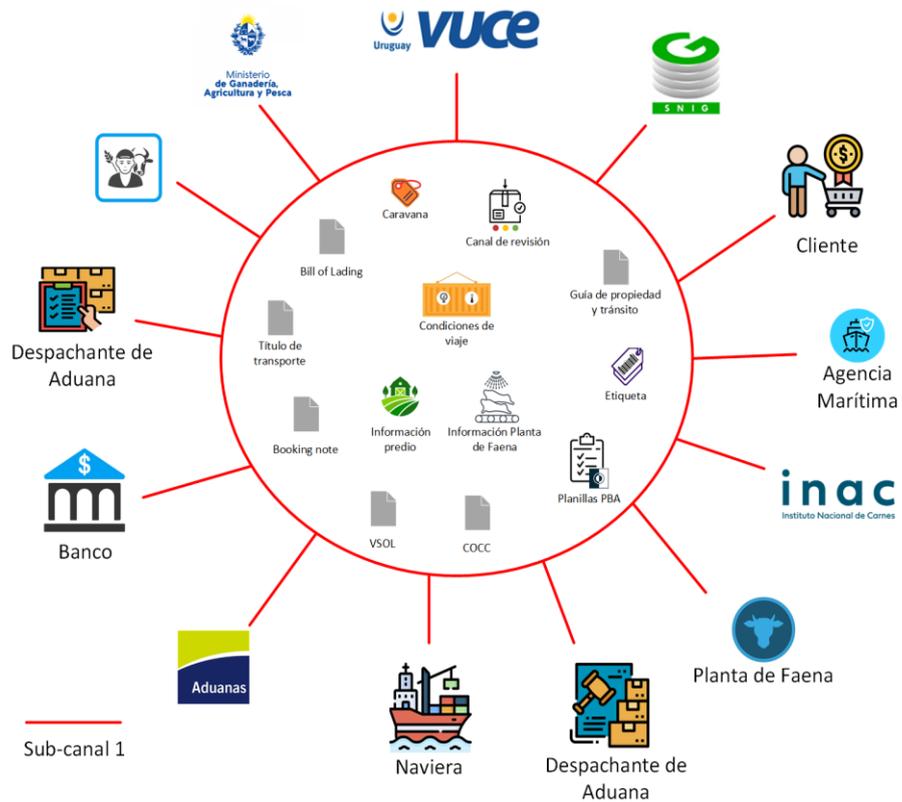


Figura 33 - Sub-canal 1 en la blockchain

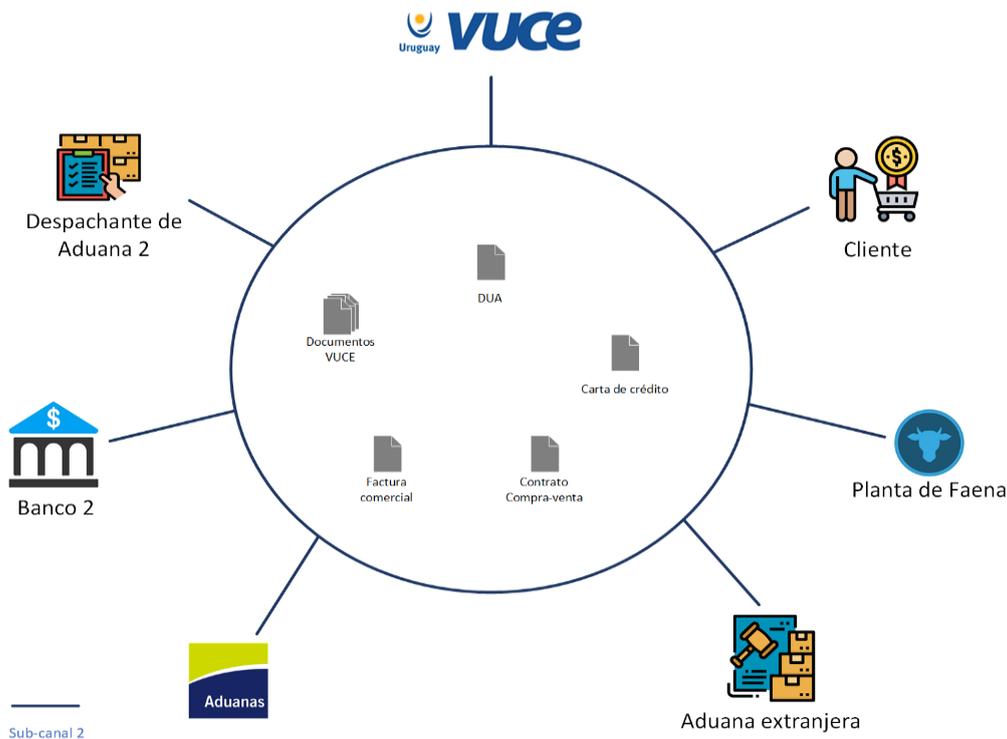


Figura 34 - Sub-canal 2 en la blockchain

A pesar de la existencia de sub-canales, se busca que existan la menor cantidad posible, dado que uno de los principales fundamentos del proyecto es la transparencia y la integración de la cadena de suministro. La creación de muchos sub-canales no brindaría el diferencial que se busca con relación a la situación actual del negocio. Por este motivo, se optó por la posibilidad de que cada actor tenga a su disposición mucha información que no es habitualmente de su interés en lugar de restringir el acceso a la misma. La única información que se consideró como sensible o privada, y por ende deber su sub-canal entre las partes involucradas, es aquella que involucra a los precios, montos y pagos relacionados al negocio.

6. Establecimiento de la gobernanza

Como se ha mencionado, los principales pilares de la aplicación de *blockchain* son la descentralización y la confianza en un sistema gestionado por todos los participantes. En el establecimiento de las reglas de gobernanza es cuando se reafirman estos conceptos y se determina el grado de descentralización que la *blockchain* puede alcanzar. La gobernanza consiste en la estructura aceptada por los participantes del sistema. En el marco teórico, se entiende que en la gobernanza existen tres factores fundamentales: los gobernantes, las reglas y los participantes [51]. La relación entre los tres consiste en la capacidad de los gobernantes de establecer las reglas en función de lo que los participantes necesiten.

En *blockchain*, para poder garantizar el correcto funcionamiento del sistema y satisfacer las demandas de sus participantes, se debe tener la capacidad de adaptar las reglas al compás de los avances del

dinámico mundo tecnológico. Por ejemplo, en el caso de *Bitcoin*, se adoptó la utilización de los BIP (*Bitcoin Improvement Proposals*) para brindarle a la comunidad la posibilidad de evolucionar gradualmente *Bitcoin*. Los BIP son documentos que contienen propuestas de mejora al sistema. Las mismas son evaluadas por la comunidad en busca de consenso acerca de la decisión a tomar. Se pueden incluir cambios en los protocolos de red o en las reglas de validez de bloque, entre otras [52].

Específicamente, la gobernanza de una *blockchain* puede ser categorizada como *on-chain* u *off-chain* [53]. Por un lado, la gobernanza *on-chain* busca democratizar la toma de decisiones con un mecanismo de votación interno de la *blockchain*, de forma que los usuarios participen activamente en el futuro de la red. Se unifican los roles de participantes y gobernantes del sistema. Un ejemplo, es la *blockchain* DAO, que a través del protocolo *MakerDAO* se otorga la posibilidad a los propietarios del *token Maker*, de votar acerca del destino de la tecnología [54]. La gobernanza *off-chain* divide el poder de forma equilibrada y preestablecida, entre distintos *stakeholders* de las *blockchains*, como por ejemplo los desarrolladores, mineros, usuarios y entidades comerciales. Teóricamente tiene la desventaja de no distribuir totalmente el poder de decisión, ya que muchos participantes son dejados por fuera en estos procesos.

De todos modos, cualquiera sea el método de gobernanza, lo que siempre se debe alcanzar es el consenso de los usuarios, dado que, de otro modo, consecuencias negativas como un éxodo de usuarios o un *hard fork* podrían desvalorizar significativamente la cadena en cuestión, ya que reduciría la seguridad y el rendimiento del sistema. Un *fork* puede ser *soft* o *hard* y en términos generales puede describirse como bifurcación en la *blockchain*, principalmente a través de actualizaciones en las reglas de consenso. La diferenciación entre ambos se halla en la compatibilidad de los nodos actualizados y los desactualizados. Los *soft fork* no llevan a cabo grandes cambios y por ende permiten la compatibilidad con los nodos que utilizan el software antiguo, pero no les posibilita la utilización de nuevas características. Por otro lado, los *hard fork* no reconocen a los nodos desactualizados y en estos casos la *blockchain* se divide en dos, con una cadena en común hasta el momento de la actualización [55].

En la aplicación del modelo del proyecto, las principales decisiones de gobernanza se relacionan a la gestión de los participantes del sistema, la privacidad de la información y las actualizaciones del *chaincode*, funcionalidades y rendimientos del sistema [56]. Estas reglas especificadas anteriormente se establecen concretamente a través de *polícies* de configuración en *Hyperledger Fabric*, pero pueden ser alteradas a medida que la red evoluciona.

Las *polícies* en *Hyperledger Fabric* son la forma de administrar la infraestructura del sistema y representan la gobernanza mencionada. Existen tres instancias desde donde se establecen las distintas *polícies*, cada instancia con un alcance distinto, como se muestra en la Figura 35. En la instancia del *system channel configuration* se definen qué tipos de nodos puede tener cada organización y las acciones que puede desarrollar cada tipo de nodo. Con respecto a las definiciones sobre la gobernanza, también se establece cuáles organizaciones tienen la capacidad de crear un canal y cómo se procede para modificar las *polícies* establecidas. En este sentido, se propone que cualquier organización pueda crear un canal, y que para alterar una *policy* la mayoría de las organizaciones deben estar de acuerdo.

En una segunda instancia, en la *application channel configuration* se determina la capacidad de agregar o eliminar participantes de un canal, y el criterio para aceptar la adopción de un nuevo *chaincode*. En el sistema propuesto, ambas situaciones precisan del consenso de la mayoría de las organizaciones.

Por último, en la configuración de la lista de control de acceso (*Access control lists*) se determina en un grado mayor la privacidad y el acceso a información específica.

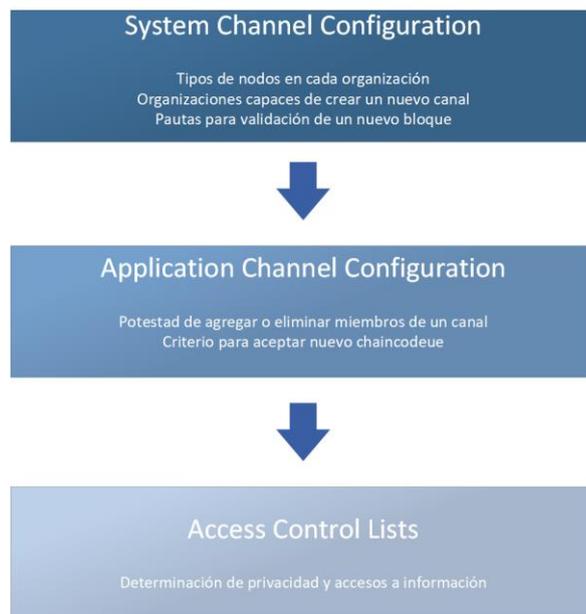


Figura 35 - Instancias de establecimientos de las políticas

Agregado de valor a la cadena de suministro

Las secciones anteriores plantean la utilización de *blockchain* para complementar algunas de las tareas que se llevan a cabo en los procesos mencionados. La mayoría de las funcionalidades se basan en interacciones simples entre los sistemas oficiales y la *blockchain*. Si bien lograr una integralidad completa a través de *blockchain* sería lo más beneficioso, es actualmente un planteo muy difícil de materializar. Por esta razón, el apartado anterior se limita únicamente a describir el uso de la *blockchain* como complemento de algunas tareas particulares.

Más allá de estas funcionalidades básicas ya existentes -que se plantean modificar parcialmente con la utilización de *blockchain*-, la tecnología puede ser utilizada para agregar valor al sistema mediante el desarrollo de funcionalidades no existentes en los sistemas actuales. Lo destacable de las mismas es que se centran en la satisfacción de nuevas demandas del cliente, lo que naturalmente hace su desarrollo más rentable, materializa los beneficios de manera más clara y logra agregar valor a la cadena de suministro, impactando positivamente en uno o más nodos, además de en la cadena como conjunto. Para estos casos, se considera al consumidor final como nuevo actor final en el sistema, además de ser hacia quién está destinada la generación de valor.

A continuación, se describen algunas de las oportunidades de agregado de valor que se consideran interesantes para el futuro del rubro cárnico. Para adoptar cada uno de estos tipos de producción mencionados a continuación, se deberá hacer un análisis diligente de los mercados actuales, para identificar cuáles son los más rentables hoy en día y eventualmente evaluar cómo será conveniente adaptar el portfolio de cada empresa. Luego, se deberá trabajar profundamente -desde una perspectiva mercadotécnica- en la construcción de marcas para atrapar el interés de esos consumidores y terminar de consolidar los nichos de mercado.

Producción de cortes orgánicos

Tal como fue descrito en el análisis contextual, las nuevas tendencias de la sociedad se basan en exigir una mayor transparencia en las metodologías de producción, para poder elegir productos con una confiable conciencia ambiental.

Según la *Codex Alimentarius Commissio* la agricultura orgánica *“es un sistema global de gestión de la producción que fomenta y realza la salud de los agroecosistemas, incluyendo la diversidad biológica, los ciclos biológicos y la actividad biológica del suelo. Hace hincapié en la utilización de prácticas de gestión, con preferencia a la utilización de insumos no agrícolas (...). Esto se consigue aplicando, siempre que es posible, métodos agronómicos, biológicos y mecánicos, en contraposición a la utilización de materiales sintéticos, para desempeñar cualquier función específica dentro del sistema.”* [57]

A su vez, la *Food and Agriculture Organization (FAO)* de la Organización de las Naciones Unidas plantea tres características relevantes de la producción orgánica [58]:

- **El sistema de producción debe estar orientado a los procesos y más que a los productos.**

- **El proceso de producción agrícola orgánica exige ciertas restricciones que pueden elevar costos de producción y comercialización.** En este caso, se restringe la utilización de fertilizantes y plaguicidas sintéticos para la producción de cultivos y forraje, así como productos sanitarios sintéticos, estimulantes y hormonas para el crecimiento en la producción de los animales de cría, u organismos genéticamente modificados en todas las etapas de la cadena alimenticia.
- **Los consumidores compran este tipo de productos por considerar que aportan a la salud personal, a la seguridad en los alimentos y al cuidado del medio ambiente.**

Estas características son difíciles de comprobar para el consumidor final. Además, existen muchos productos con certificaciones que pueden parecer similares (e.g.: certificación de animales criados a cielo abierto o certificación de productos ecológicos, entre otros) pero que no garantizan un control tan estricto como los productos orgánicos. A modo de ejemplo, según la *Mintel Press Office*, solamente el 26% de los consumidores de productos orgánicos confía en que las características de los productos se condicen con su etiqueta, y sólo un 13% de dicha población cree que este tipo de producción está altamente regulado. Por otro lado, considerando que la producción orgánica en general trae un aumento de costos comparada con la producción tradicional, se debe garantizar una certificación confiable -y que por ende facilite un respaldo de consumidores fieles- para que el nicho de mercado pueda sobrevivir, y no ser absorbido por otros productos con certificación de poco reconocimiento o respaldo, y menos costosas.

El INAC cuenta con dos certificaciones, una para establecimientos ganaderos y otra para plantas de faena. Actualmente, en Uruguay se produce carne orgánica principalmente para exportación a mercados como el europeo y estadounidense. En estos países existe una gran demanda por este tipo de productos y cotiza con un elevado precio de mercado, por lo que se reconoce una oportunidad de importantes beneficios económicos.

De esta forma se observa una gran oportunidad para ofrecer una solución definitiva a la cuestión a través de *blockchain*. Muchas de las validaciones a considerar en este mecanismo de producción, implican un control del día a día de las actividades de establecimientos ganaderos, lo que en principio se puede tornar complejo. Por esta razón, se propone registrar estos hitos relevantes en la vida del animal (vacunaciones, tipos de alimentación, análisis de sangre en búsqueda de presencia de hormonas) en el sistema, y de esa forma poder garantizar el cumplimiento de las normas de producción orgánica. Por normativa del MGAP, estos procesos deben ser validados por un veterinario. El mismo podría registrarse en el sistema como veterinario certificado, lo que agrega confiabilidad a futuros poseedores del ganado o plantas de faena a las cuales se destinará la producción, además de cumplir con las disposiciones del MGAP.

De esta forma se podría validar que no existieron, por ejemplo, aplicaciones de hormonas, para cumplir con los requisitos orgánicos, o se podrían visualizar los resultados de los posibles análisis de sangre, entre otros. Esto permite mapear toda la información exigida para la certificación de establecimientos orgánicos. Luego, se procedería a hacer lo propio en las plantas de faena.

Toda esta información podrá ser registrada en la *blockchain* como información asociada al establecimiento, que se relaciona a la caravana de cierto animal como entidad, para luego poder ser

accedida por el consumidor al hacer la trazabilidad hacia atrás de la cadena de producción de un corte particular. Los entes públicos podrán, inicialmente, trabajar por fuera del sistema y que el propio productor se encargue de cargar la información al mismo (incluso adjuntar el certificado en formato digital) como tipo de certificado, fecha de obtención del certificado, tipo de sistema de producción, tipo de sistema de alimentación, etc. En un futuro, considerando una escalabilidad completa del sistema a públicos y privados, estos entes podrán funcionar como nodos particulares que validen la información directamente en el sistema.

Carne producida a bajo carbono

La industria cárnica no tiene una producción exenta de emitir gases de efecto invernadero. Según las notas del curso de Elementos de Ingeniería Ambiental - Fing, *“La emisión de metano se asocia con los procesos de degradación anaerobia. A nivel mundial, se considera que un 17% (proviene) de la fermentación entérica del ganado. (...) Algunas tecnologías actualmente en uso contribuyen fuertemente con las emisiones de metano a la atmósfera y dificultan su control. Tal es el caso, por ejemplo, de los establecimientos de cría intensiva de ganado (feed-lots), donde coexisten problemas de emisiones de gases malolientes y GEI”*. Además, también se asocia el Óxido nitroso a la producción ganadera, *“Proviene principalmente del sector agropecuario por excretas de animales y utilización de fertilizantes nitrogenados, que representa a nivel mundial el 62% de la emisión.”*

En la actualidad se emplea el *Global Warming Potential (GWP)* para comparar el impacto de diferentes gases en la intensificación del efecto invernadero natural. Esta escala representa *“la cantidad de calor que puede ser absorbido por una unidad de masa de un gas en un cierto período de tiempo, en relación al que absorbe la misma masa de CO₂ en el mismo lapso de tiempo”*. [59]

Un indicador ambiental que busca cuantificar la totalidad de gases de efecto invernadero emitidos por efecto directo o indirecto de una entidad es denominado Huella de Carbono. La misma se mide en la unidad *CO₂ equivalente (CO_{2eq})* que corresponde a la multiplicación entre la masa del gas contaminante y su GWP. Esta es una medición universal que permite comparar fácilmente el impacto de distintas actividades en la intensificación del efecto invernadero. Existen distintas metodologías y protocolos para medir la huella de carbono de una actividad productiva, aunque para algunos casos particulares, esto puede tornarse engorroso y puede ser difícil de llevar a cabo.

En Uruguay existe un único antecedente del cálculo de la huella de carbono para la producción de carne. El Ministerio de Ganadería Agricultura y Pesca se asoció con la Universidad de la República, el Instituto Nacional de Investigación Agropecuaria y el Laboratorio Tecnológico del Uruguay para realizar el *Primer Estudio de la Huella de Carbono de tres cadenas agroexportadoras del Uruguay: Carne vacuna, lácteos, arroz*. En el informe final de dicho estudio se menciona que *“En los últimos años, la creciente preocupación internacional por los impactos adversos del cambio climático, ha impulsado a las organizaciones e instituciones a profundizar su conocimiento respecto a las emisiones de gases de efecto invernadero (GEI) y su mitigación. A esto se suma que la mayoría de las cadenas de producción de alimentos, en los últimos años, están recibiendo señales desde los consumidores en relación con la calidad de los productos y los impactos ambientales relacionados a su producción y*

distribución. (...) Especialistas en industrias alimenticias pronostican que la huella de carbono puede ser un factor más de decisión de compra por parte de los consumidores, como forma de contribuir a reducir las emisiones de GEI.” [60]

La Norma PAS 2050:2008 denominada *Specification for the assessment of the life cycle greenhouse gas emissions of good and services* identifica algunas fuentes de emisión que deben ser consideradas en el cálculo de la huella de carbono de la producción cárnica. El estudio mencionado anteriormente, se basa en esta norma para establecer las fuentes de emisión que se tuvieron en cuenta para los cálculos. [61] Algunas de ellas son:

- Emisiones derivadas de procesos biológicos y excretas de animales
- Transporte, refinación y combustión del petróleo, así como el transporte del combustible luego utilizado en la producción
- Insumos agropecuarios como fertilizantes y agroquímicos con su propia emisión por manufactura
- Transporte de ganado al predio y a planta de faena
- Transporte de producto terminado desde plantas de faena a puerto y luego a país destino

Este estudio arrojó resultados interesantes que se presentan a continuación. En la Figura 36 [60] se puede observar cómo, dentro del sistema de cría, los subsistemas de recría e internada son los que registran mayores emisiones de GEI. Además, como se visualiza en la Figura 37 [60], en los sistemas productivos de campo natural, la fermentación entérica tiene asociada la mayor cuota de emisión, pero a medida que el sistema se torna más mecanizado, otras emisiones entran en juego como las emisiones por fertilización o utilización de maquinaria. Por último, otro resultado interesante es que al analizar la huella de carbono de la producción de cortes cárnicos, incluyendo todas las etapas productivas y de transporte, donde las emisiones en el establecimiento productivo tienen un peso casi totalitario por sobre las emisiones por el transporte o la producción industrial, como se ve en la Figura 38 [60].

Sistema	Sub - Sistema	Emisiones Sistema Criador Base 100 (%)
Cría (para prod. 1 ternero)		100
Recriador (150 – 350 kg)	Recría Corta 17 meses	38.9
	Recría Larga 24 meses	57.1
Internada (350- 486 kg)	Novillos Campo Natural (CN)	72.2
	Novillos Past. + Supl. (P+S)	29.4
	Novillos Feedlot (FL)	21.3
Internada (366- 415 kg)	Vacas	45.4

Figura 36 - Emisiones de GEI por Sub - Sistema

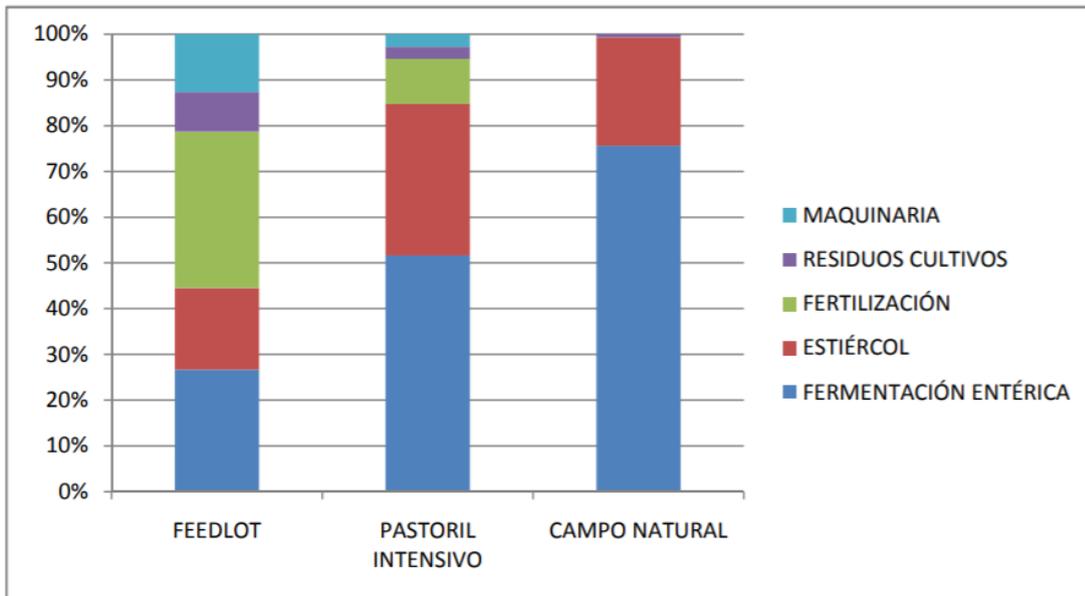


Figura 37 - Distribución de fuentes de emisión por sistema

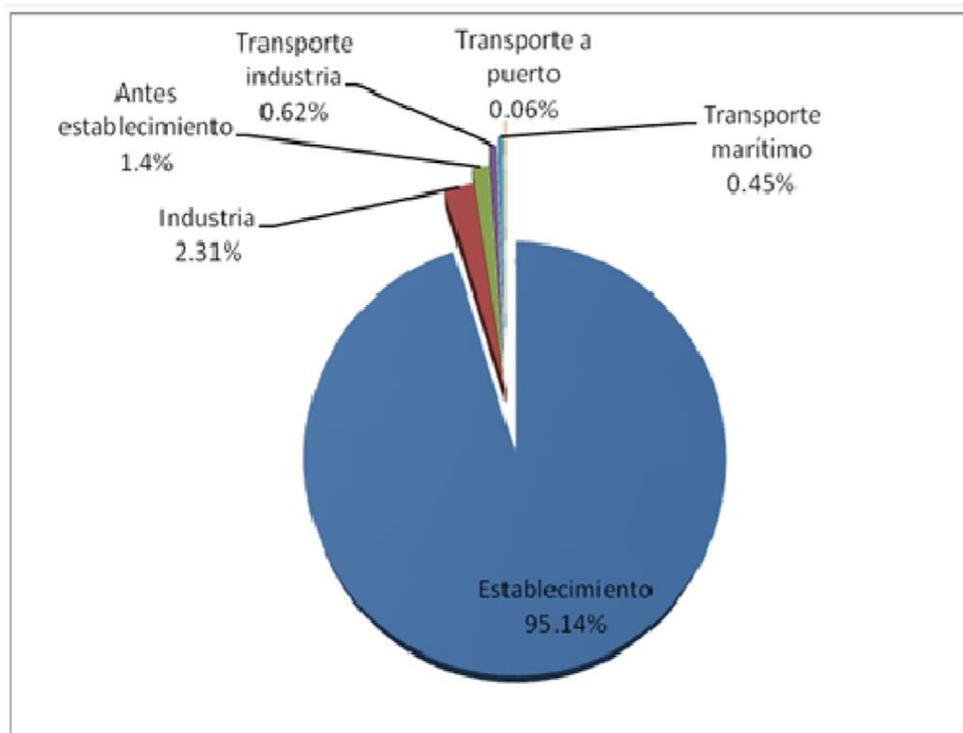


Figura 38 - Aportes a la emisión total de la industria por etapa productiva

A partir de la toma de conciencia de estos resultados tan determinantes, se genera la oportunidad de robustecer los sistemas de mediciones y captura de datos existentes. De hecho, en el informe se menciona que *“el desarrollo y aplicación de técnicas de medición y monitoreo de emisiones y capturas es una prioridad, tanto para reducir las incertidumbres asociadas a las estimaciones como para trabajar en mejora continua y poder reportar los avances. Las mencionadas incertidumbres en las estimaciones asociadas al uso de algunos factores de emisión importantes son muy relevantes”* [60].

Se tomó contacto con el Ing. Agr. Agustín Inthamoussu, quien fue gerente general de la empresa Carbosur -dedicada a brindar servicios especializados en el área del cambio climático- e integrante de la *United Nations Framework Convention on Climate Change* para profundizar acerca de la realidad del Uruguay en el tema. Dicho profesional manifestó que, si bien no es una realidad actual, están dadas las condiciones para producir carne bajo carbono en Uruguay. La falta de incentivos radica en que los consumidores aún no exigen este tipo de productos con determinación, pero sin embargo existen probabilidades altas de que en el mediano plazo esta situación se revierta, generando una nueva oportunidad de agregado de valor al mercado. Si se cumplen dichos pronósticos, aquellos productores que hayan adquirido el *know-how* adecuado con anterioridad, se podrán destacar sobre otros competidores. Además, más allá de las exigencias de los consumidores, este atributo en la carne está tomando mayor relevancia en la negociación de nuevas cuotas exportadoras, o incluso algunos atributos medioambientales del estilo se transformarán en nuevas exigencias de las cuotas existentes.

En este contexto, se considera que se está ante una oportunidad de poder potenciar esta certificación mediante el robustecimiento de las tecnologías que actualmente la soportan. Nuevamente la utilización de *blockchain* es adecuada para este cometido, permitiendo una digitalización rápida e inmutable de datos claves, que podrá ser accesible fácilmente por el resto de los actores de la cadena y sobre todo, podrá ser visualizada y analizada en conjunto con otros tipos de datos relevantes de los demás nodos del sistema.

Esto fue visto con una confiada expectativa por parte del Ing. Agr. Inthamoussu, quien comentó que actualmente la captura de datos en campo se utiliza para procesar la información y otorgar dicha certificación, pero estos datos en general no son compartidos hacia adelante en la cadena productiva. Teniendo en cuenta este aspecto, se considera que justamente estos datos pueden ser de gran valor para afirmar la confiabilidad de la certificación, y aumentar la fidelidad de las plantas de faena hacia sus proveedores, y luego, de los consumidores hacia las distintas marcas.

De esta forma, al ingresar algunos resultados claves de las auditorías ambientales de un predio ganadero a la *blockchain* (e.g.: cuota de emisión de carbono / cantidad de animales, hectáreas totales de forestación, porcentaje de preñez del rodeo, porcentaje de parición del rodeo, tipo de sistemas productivos llevados adelante -asociados a un lote de ganado-, ganancia de kilogramos por año, etc.), los restantes nodos de la cadena no sólo podrán validar la certificación de producción bajo carbono, sino también profundizar en los indicadores ambientales correspondientes, tanto como se desee. Incluso una idea que resulta interesante de implementar es que, al momento de acceder al sistema para visualizar la información ambiental del predio, se puedan ver los registros históricos para evaluar el desempeño del mismo en la mejora continua hacia una producción más amigable con el medio ambiente.

Este agregado de valor es comentado por Daniel de Matos, asesor de la directiva de la planta de faena BPU Meat Uruguay [20]. El mismo manifiesta que una correcta gestión del balance de carbono es clave para la industria, y que la información asociada se puede incorporar rápidamente a los sistemas informáticos para generar valor. También comenta que Uruguay no tiene todo resuelto, pero sí una gran parte del camino recorrido, donde se puede diferenciar de sus competidores regionales.

Debido a que se profundizó acerca de las emisiones de GEI en la industria cárnica, que por sí solas impactan negativamente en la preservación del medio ambiente, se considera oportuno dejar constancia que, más allá de estas puntualizaciones, la ganadería en Uruguay es muy sustentable comparada con otros países, y colabora de distintas formas a la conservación de hábitats naturales. Esto es un diferencial competitivo destacado del país que es altamente valorado en los mercados internacionales. En el *Anexo IV* se profundiza acerca de la contribución de la ganadería en Uruguay para preservar el medio ambiente [62].

Producción de carne *Kosher*

La cultura judía considera que los alimentos deben cumplir ciertos requisitos, que se resumen como alimentos *Kosher* [63]. Todos los alimentos consumidos por la tradición judía, así como los medicamentos deben ser certificados de manera oficial. Los procesos de certificación incluyen la inspección de materias primas, la inspección de los procesos de producción y la inspección de estado de las instalaciones productivas. En lo que respecta a la producción cárnica, el principal objetivo de esta tradición es que los animales que serán sacrificados no sufran [64].

En Uruguay, la mayor cantidad de productos cárnicos *kosher* son destinados al mercado estadounidense e israelí. Si bien el negocio en sí puede brindar una utilidad mucho mayor que la producción de cortes comunes, los moderados precios de venta en Uruguay no lo hacen un negocio tan rentable. De esta forma, se presenta una oportunidad para poder potenciar este tipo de producción mediante la búsqueda de nuevas eficiencias en el proceso productivo. Los cortes *kosher* pueden ser de cualquier parte del animal (en general no se consumen los cortes del nervio ciático) y su diferencia con los cortes tradicionales radica en el proceso de producción en sí.

Luego de realizar una entrevista a un rabino, y consultar a distintos encargados de procesos de plantas de faena, se tomó conocimiento detallado de las distintas etapas de este proceso productivo. Para empezar, los bovinos sacrificados deben estar sanos, y no deben sufrir ni estresarse en el proceso de llegada a la planta de faena. El sacrificio -ritual llamado *Shejita*- debe ser realizado por un rabino calificado, y se debe efectuar en una zona del cuello donde se conjuntan nervios, arterias y venas, con el fin de que el animal pierda conocimiento rápidamente y no sufra la muerte. Además, se requiere de un cuchillo particular que debe ser afilado por el propio rabino que efectúa el sacrificio. Por otro lado, los cortes cárnicos a producir no deben contener restos sanguíneos, por lo que las carcasas se someten a un proceso de salado -proceso no efectuado para producir cortes tradicionales- que asegura la remoción de toda la sangre del cuerpo. Por último, se lleva adelante un control biopsico de algunos órganos como pulmones y estómago para asegurar la ausencia de hormonas en los animales que evidencien que los mismos hayan pasado por episodios de estrés o sufrimiento.

En las plantas de faena, estos procesos no son realizados por el personal habitual, sino que se llevan a cabo por rabinos habilitados. Además, se debe asegurar el cumplimiento de estos requisitos mediante controles periódicos en las distintas etapas del proceso. Los puestos de control particulares se dan en las etapas de:

- degollado,
- limpieza de carcasas,
- control de estado de pulmones, estómago y demás órganos,
- salado,
- desosado,
- empaque.

Todos estos procesos deben ser certificados de manera confiable y segura por el rabinato de Israel mediante la otorgación de un sello de validez de carne del tipo *Kosher*.

Si bien estos procesos de certificación en Uruguay funcionan de manera correcta, el diálogo con autoridades de distintas plantas de faena evidenció un cierto grado de interés en poder mejorar las herramientas de apoyo tecnológico que garantizan la certificación. De esta forma, se propone utilizar el sistema de *blockchain* para completar los distintos registros y brindar mayor confiabilidad a los clientes que deseen adquirir estos productos. Sería interesante incluir a rabinos como usuarios en el sistema para que ellos mismos registren la información correspondiente, e incluso que se puedan cargar las habilitaciones de los rabinos para brindar mayor confiabilidad. Estas consideraciones logran validar automáticamente la información ingresada. De esta forma, el cliente -o consumidor final- tendrá acceso a un historial completo de cómo se llevó a cabo la producción *kosher*.

Certificaciones de bienestar animal

El Instituto Nacional de Carnes diseñó el Programa de Bienestar Animal del Uruguay (PBA) con el objetivo de que sea utilizado *“como estrategia de trabajo, y comercial ante clientes, el área de Estándares, Protocolos y Programas, de la Dirección de Control y Desarrollo de Calidad de INAC”* [65]. El programa se basa en tres tipos de certificaciones; certificaciones a **predios agropecuarios**, certificaciones a **empresas transportistas** y certificaciones a **plantas de faena**. Un corte de carne puede ser certificado bajo el sello del PBA si y sólo si proviene de animales que se criaron en predios certificados, que fueron trasladados por transportistas certificados y cuyos cortes de carne fueron producidos en plantas certificadas.

Protocolo de certificación del PBA para predios agropecuarios

La certificación para predios agropecuarios consta de varios requisitos -con distinto nivel criticidad- que deben ser cumplidos por el predio [66]. Existen varias instituciones que se dedican a verificar su cumplimiento como LSQA, SGS Uruguay, CONTROL UNION o el propio INAC. Los requisitos que establece el INAC se agrupan en las siguientes categorías:

- **Empresa:** requisitos que exigen el compromiso e interés de la empresa con el Bienestar Animal.

- **Personal:** exigencia de capacidades, entrenamiento y competencias del personal en Buenas Prácticas del Manejo Animal.
- **Aspectos ambientales:** el hábitat debe responder a necesidades biológicas de los animales (disponibilidad de agua, protección contra fenómenos meteorológicos peligrosos, espacio disponible por animal).
- **Instalaciones:** las instalaciones deben ser seguras y facilitar el manejo de los animales (dimensiones de embarcaderos, tubos y cepos, mantenimiento adecuado de los mismos).
- **Manejo animal:** entre otros, la estadía mínima de un animal en el predio debe ser de 90 días, las aplicaciones de medicamentos deben ser supervisadas por veterinarios y deben ser autorizados, se debe disponer de zonas para aislamiento de animales enfermos o lesionados, se deben eliminar los animales agresivos del rodeo, los inyectables deben ser aplicados minimizando accidentes o lesiones, los destetes se deben realizar en condiciones de mínimo estrés, se debe establecer una rutina de inspección del ganado, el sacrificio de los animales debe respetar condiciones humanitarias y se debe evitar el sufrimiento innecesario.
- **Embarque de hacienda:** los animales deben cumplir ciertas condiciones de descanso previo al embarque, se debe completar la planilla de BA (PLA-BA 02), los embarques deben ser en horarios alejados del mediodía en estaciones calurosas, se debe evitar el uso de perros y elementos punzantes.

Protocolo de certificación del PBA para empresas transportistas

De la misma forma, existen requisitos que se deben cumplir para obtener la certificación como empresas transportistas [67]. Los requisitos exigidos por el INAC se agrupan en las siguientes categorías:

- **Empresa:** requisitos que exigen el compromiso e interés de la empresa con el Bienestar Animal.
- **Personal:** exigencia de capacidades, del personal en Buenas Prácticas del Manejo Animal en el transporte de hacienda.
- **Equipo de transporte:** los vehículos deben estar habilitados por el Ministerio de Transporte y Obras Públicas (MTOP), deben presentar evidencia de mantenimiento, deben tener escaleras y pasarelas que faciliten inspecciones y permitan auxiliar animales en caso de que sea necesario, se deben respetar las reglamentaciones de cantidad de animales por jaula según la Asociación Uruguaya de Transportistas de Hacienda, los vehículos deben tener el comprobante de equipo certificado (Figura 39).
- **Manejo de la hacienda:** sólo se deben transportar aquellos animales que se pueden mantener en pie y no tienen miembros fracturados, se debe limitar el uso de la picana eléctrica a un 25% de los animales, se deben evitar actos abusivos y maltratos, se debe dar un tiempo a los animales para que se acomoden dentro del vehículo, se debe completar y firmar la planilla de BA (PLA-BA 02), el tiempo de transporte se debe minimizar, y no debe ser mayor a 8 hs, el transportista debe inspeccionar a los animales en intervalos de 2 hs, y la primera inspección debe ser dentro de los primeros 30 minutos de comenzado el viaje.

Protocolo de certificación del PBA para plantas de faena

Los requisitos para la certificación de plantas de faena que exige INAC son los siguientes [68]:

- **Empresa:** requisitos que exigen el compromiso e interés de la empresa con el Bienestar Animal.
- **Personal:** exigencia de capacidades, del personal en Buenas Prácticas del Manejo Animal en Planta de Faena.
- **Instalaciones:** las instalaciones deben ser seguras y deben facilitar la descarga, la espera y el manejo en general de los animales.
- **Manejo prefaena:** el encargado de Bienestar Animal debe estar presente en la Planta de Faena para recibir los animales, la descarga debe ser ordenada y cuidadosa (limitar uso de picana eléctrica al 25% de los animales, evitar esperas de animales mayores a 60 minutos), los animales deben ser manejados con Buenas Prácticas Operativas (BPO) por ejemplo controlando la cantidad de animales que se caen, reduciendo el tiempo de espera en corrales (según registro de tiempos en planilla).
- **Faena:** debe existir un manual de procedimientos redactado por la empresa (incluir detalles de procedimientos de insensibilización, equipos utilizados, criterios de chequeo) el cual debe ser conocido por el personal a cargo, el grado de efectividad de la primera insensibilización no debe ser menor al 95%, el equipo debe ser mantenido correctamente, en el riel de sangrado no deben existir animales sensibles, el intervalo transcurrido entre la insensibilización y el sangrado no debe ser mayor a 60 segundos.

Al verificar el cumplimiento de estos requisitos, se otorga el logo identificatorio del programa (Figura 39 [69]). Como fue mencionado anteriormente, un producto certificado implica que el establecimiento ganadero, las empresas transportistas y la planta de faena involucrados en su producción están certificados.



Figura 39 - Sellos otorgados por certificación de bienestar animal

Se decidió consultar a autoridades del INAC acerca de la aplicabilidad de esta certificación hoy en día. Las mismas manifestaron que, si bien el certificado de bienestar animal es moneda corriente en la producción para exportación (a mercados europeos principalmente), las plantas de faena eligen en general a otras instituciones distintas del INAC-con distintos requisitos- para validar su certificación. De hecho, al consultar acerca de la cantidad de empresas certificadas por el INAC, se tomó conocimiento de que en la actualidad existen solamente siete predios ganaderos, dos empresas transportistas y cuatro plantas de faena. Ante esta realidad, se considera que se está ante una buena oportunidad de buscar mecanismos que permitan conseguir una certificación que registre de forma más precisa y eficiente el cumplimiento de cada uno de sus requisitos, e incluso conocer los valores de aquellos que se basen en mediciones. Al cargar los distintos requisitos y planilla de BA en el sistema propuesto con *blockchain*, se podría registrar -mediante una funcionalidad particular disponible en una API a la que se registren y accedan productores, operarios de plantas de faena y operadores de empresas transportistas, y en la que las distintas instituciones certificadoras accedan para validar la información- fácilmente cuáles fueron los requisitos que cumplió una empresa particular -ya sea un predio ganadero, una empresa transportista o una planta de faena-, y cuál fue el grado de cumplimiento de cada uno de ellos. Esta información se debería asociar a la información ya registrada como número de caravana, etiqueta de canal, etiqueta particular de envase, etc.

De esta forma, cualquier organización en la cadena de suministro podrá tener acceso a la información acerca de los protocolos de BA utilizados hasta el momento. A modo de ejemplo, una planta de faena podrá evaluar el grado de cumplimiento de protocolos de BA para un lote de ganado particular y así evaluar sus insumos y proveedores. Además, el consumidor final podría acceder a esta información al momento de elegir sus productos en la góndola, como se desarrolla en la subsección [Registro de hitos relevantes durante la producción de carne](#).

Registro de hitos relevantes durante la producción de carne

Más allá de las certificaciones particulares que fueron desarrolladas en puntos anteriores, existen registros que agregan valor a la cadena y no necesariamente pertenecen a una certificación particular.

Tener conocimiento certero de la historia de vida del animal puede agregar valor de distintas formas a la cadena de suministro. A modo de ejemplo, se consideran hitos importantes como pesadas, cambios de propiedad, formas de producción en campo y aplicaciones veterinarias al ganado. En consulta con expertos, los mismos manifestaron que el registro preciso de estos datos puede tornarse dificultoso, debido a la gran incertidumbre intrínseca a muchas de las tareas manuales en campo abierto. De todas formas, se considera que existe una buena oportunidad para lograr capturar estos datos de manera segura y confiable utilizando *blockchain*. La metodología sugerida en este caso implica que el productor responsable cuente con un acceso web a una API que se conecte a la capa de transporte de la *blockchain* a través de la cual pueda completar los distintos registros, siempre referidos a un número de caravana inicialmente ingresado.

Algunos de estos registros necesitan ser validados por un veterinario oficial. Para esto, se propone que los veterinarios existan como usuarios en el sistema, y que los mismos registren aquellas aplicaciones

accediendo a la API mencionada. El hecho de que los veterinarios ingresen estos registros es condición suficiente para certificar su validez. De esta forma se puede generar una lista confiable de veterinarios en el sistema a partir de la cual un productor particular puede realizar la contratación de sus servicios (de la misma forma que se genera la lista confiable de despachantes de aduana mencionada en la sección *Desarrollo práctico de aplicación en cadena de suministro*).

Toda esta información -junto con la información recolectada en el proceso de producción frigorífico-mencionada en la sección anterior- podrá ser desplegada de manera ordenada y accesible por distintos actores especialmente seleccionados en la cadena. Esto permite, por ejemplo, que el productor ganadero comparta un link con información filtrada sobre el lote que ofrece a una planta de faena. Desde la planta de faena se podrá visualizar en detalle toda la información de los animales, permitiendo una profunda y confiable evaluación de proveedores. Los beneficios obtenidos pueden ser, entre otros, evaluar riesgos involucrados por la selección de animales no aptos, proteger la reputación de la marca o mejorar las exigencias hacia el proveedor con el fin de aumentar las exigencias en la cadena entera. Cabe destacar que, debido al tipo de información recolectada en todo el proceso, este tipo de evaluaciones se podrá realizar también por parte de los clientes, visualizando información acerca de la cría del ganado y del trato dentro de la planta de faena.

Por otro lado, si se considera la inclusión del consumidor final en la cadena de suministro, éste puede obtener un gran valor agregado, que actualmente no recibe. Al incluir un código QR en el envase del corte cárnico, el consumidor podrá escanearlo para acceder a un *dashboard* que muestre información relevante como puede ser:

- año de nacimiento,
- raza,
- sexo,
- establecimiento rural de cría (ubicación, productor responsable, fotografías, entre otros),
- tipo de sistema de producción (corral, pasto natural, pradera, terminada a grano, etc.),
- fecha de faena,
- planta de faena (ubicación, certificaciones, fotografías, entre otros),
- marca,
- grado de terminación en grasa.

Además, cualquier certificación que tenga el corte en sí (como lo pueden ser las certificaciones descritas en las subsecciones anteriores) podrá ser informada en esta instancia. Una consideración no menor es el costo que implica desarrollar y ofrecer este servicio.

En la actualidad, existen distintos esfuerzos para brindar servicios similares, pero en un restaurante, por ejemplo. El corte de carne podrá traer un código QR para que el cliente acceda a toda la información de producción. Este emprendimiento se quiso llevar adelante con carne uruguaya, hasta ahora sin éxito.

Sinergia entre IoT y la trazabilidad con *blockchain*

Considerando la sinergia entre las tecnologías *blockchain* e IoT mencionadas en la sección *Casos de Uso*, es importante aprovechar los recursos que IoT puede ofrecer para la cadena de suministro. El sistema descrito busca desarrollar la trazabilidad desde el campo hasta la carga de contenedores para exportación. Gran parte del proceso consiste en la movilización del producto, incluyendo transporte terrestre o marítimo. En consulta con despachantes de aduana expertos en la exportación de carne y en el desarrollo de sistemas de *blockchain*, se sugirió, entre varias opciones, la incorporación de *RFIDs*, que a través de IoT, permitan aumentar la granularidad en la trazabilidad del proceso de exportación.

Los RFID (*radio frequency identifiers*) consisten en una etiqueta que comunica la identidad y demás información de un objeto a través de radio frecuencias. Contienen un chip y una antena que permite enviar, alterar y sobrescribir información existente a un receptor distanciado, incluyendo también la posibilidad de encriptar la información que así lo requiera. Dicho receptor envía la información a la *blockchain* y la misma puede ser consultada por los usuarios interesados.

Entonces, en las cadenas de suministro, la inclusión de *RFIDs* en los contenedores permitirá compartir con certeza la evolución de la temperatura y presión del contenedor durante el viaje para respetar las cadenas de frío, las fechas de partida y arribo, la ubicación en tiempo real y garantías de cerrado de contenedor comparables con la utilización de precintos de seguridad [70]. Los *smart contracts* permiten que los dispositivos de IoT negocien y ejecuten acciones preestablecidas de manera automática, habilitando muchas nuevas funcionalidades y casos de uso para soluciones IoT. Particularmente en este caso, se puede lograr un mayor nivel de automatización en la recolección y comunicación de datos, en determinados puntos cruciales de la cadena de suministro, lo que potencia el valor agregado inicial aportado por *blockchain* a la cadena. En conjunto, se elimina la necesidad de que cada participante de la cadena tenga que trazar un bien en su propia base de datos. La utilización de base de datos independientes dificulta la transparencia, colaboración y verificabilidad de la información entre partes. Al recolectar y almacenar de forma segura con *blockchain*, los procesos de certificación y controles sanitarios serían considerablemente más fidedignos y eficientes, creando consecuentemente un impacto favorable en los clientes.

Trazabilidad hacia atrás y logística de retiro de productos

La logística inversa se basa en planificar, controlar y hacer efectivo el flujo de información y materiales desde el punto de consumo hasta el punto de origen, para recobrar parte del valor de los materiales o eliminarlos [71]. Un caso particular de la logística inversa se da cuando un producto ya distribuido se encuentra defectuoso, implica un riesgo para la seguridad del consumidor o no cumple con alguna normativa vigente. La logística involucrada en el retiro de estos productos se llama *recall* [72].

Para poder responder ante este tipo de imprevistos de manera rápida y certera, se debe planificar el *recall* desde un principio, al momento de diseñar las estructuras de la cadena de suministro. Este diseño debe asegurar que las herramientas tecnológicas seleccionadas se puedan integrar para recolectar información que estará desperdigada por todos los nodos.

Actualmente muchos de los sistemas informáticos de los distintos nodos resultan incompatibles entre sí, limitando el flujo de información a una comunicación fragmentada entre nodos, lo que dificulta la correcta ejecución de la logística inversa. De hecho, los productos que deben ser retirados del mercado por problemas de salud e inocuidad, sólo un 43% de los mismos son trazados [73]. En este contexto, se torna evidente que la efectividad y eficiencia del *recall* dependerá de la calidad de información recabada a lo largo del proceso productivo, y su grado de accesibilidad en los distintos nodos. Por esta razón, se considera que la utilización de un sistema de *blockchain* puede ser la solución indicada para respaldar los procesos de *recall* de la industria cárnica.

En las secciones anteriores se describió una gran variedad de registros en la *blockchain* que acompañan el proceso productivo propuesto. Estos registros permitirán realizar el proceso de *recall* de manera ágil. A modo de ejemplo, un productor podría descubrir que algunos de sus animales -ya faenados- no cumplieron con alguna medida sanitaria. De la misma forma, la planta de faena se podría alertar por un lote que fue liberado sin pasar todos los controles de calidad. Cualquiera de estos escenarios dispararía rápidamente la logística de *recall*. La planta de faena podría ingresar el número de lote al sistema para observar a qué cliente fue vendido. El cliente podrá trazar las distintas partidas que ha vendido a partir de ese lote, e identificar las tiendas que vendieron esos productos. Las tiendas se podrían comunicar con los clientes que adquirieron específicamente un lote de producción de una fecha de producción particular para que desechen los productos. En caso de que eso no logre alertar al 100% de los clientes, se podría emitir un comunicado a la sociedad civil alertando acerca de la situación, y una vez más indicando específicamente el número de lote, fecha de producción y demás detalles que acotan la cantidad de productos a retirar. De esta forma se logra un retiro efectivo y puntual, evitando tener que retirar grandes cantidades de productos por contar con mayor incertidumbre.

Esta misma lógica se podría aplicar en sentido inverso, al momento de querer trazar los productos desde el consumidor final hasta el productor. Toda la información estará disponible en un mismo sistema, lo que acelera de manera exponencial la búsqueda del origen de una posible falla de calidad. De esta forma, y a modo de ejemplo, un consumidor en el exterior podrá reportar a su minorista que su producto se encuentra en mal estado. El minorista contará con la información del lote de producción y podrá informar al importador que se podrá comunicar con la planta de faena. La propia planta de faena podrá acceder a la *blockchain* para conocer todos los detalles del transporte de sus productos para determinar, por ejemplo, que la falla se produjo gracias a una ruptura de la cadena de frío al exportar el producto. De la misma manera, la falla se pudo haber generado por el productor rural, y se podrá investigar rápidamente si el mismo aplicó todas las vacunas obligatorias a ese lote de animales, por ejemplo.

Con este tipo de procedimientos no será necesario utilizar sistemas paralelos e informales, así como documentación a papel, puesto que una gran cantidad de información crítica de cada nodo se encontrará en un mismo sistema. Esto permitirá una rápida búsqueda de las causas que llevan a que un producto sea no conforme.

Eventualmente, esto facilitará la aplicación de multas específicas y justas al actor de la cadena que haya incumplido algún requisito, elevando de manera continua el estándar sanitario de la cadena completa. Esto no quiere decir necesariamente que el estándar sanitario actual sea pobre -de hecho,

es una gran fortaleza del sector cárnico uruguayo-, pero si se presenta una oportunidad de mejora en cuanto a la rapidez con que se pueden encontrar causas para una producción no conforme. Además, estos análisis podrían ser de utilidad para revisar y actualizar las normativas vigentes o requisitos mínimos de calidad.

Estos aspectos son de vital importancia para la cadena de suministro y definitivamente agregan un valor extra. Se debe trabajar fuertemente para evitar lo más posible exponerse a situaciones de esta índole, y en caso de que estas situaciones no se logren evitar, que las consecuencias sean lo más tenues posibles. Algunas desventajas de un retiro de productos de mercado son el deterioro de la imagen de la empresa ante el cliente, así como su relación de confianza con la marca, el costo logístico e informático implicado en una campaña de retiro, el eventual costo de desecho de productos no aptos para consumo, la amenaza de no cumplimiento con nuevas fechas de entrega por avocar recursos materiales, humanos y tiempo al proceso de retiro de productos [74]. De esta forma, al enfrentarse con la necesidad de realizar un retiro de productos, la rápida ejecución del proceso permitirá mitigar las consecuencias en mayor medida.

Análisis de implementación

Luego de realizar el relevamiento de la cadena cárnica, escoger y validar el tipo de *blockchain Hyperledger Fabric* a utilizar -a través de la prueba de concepto-, se procede a analizar la implementación de dicho sistema.

Para empezar, debido al gran alcance y la cantidad de actores involucrados en un proceso de modernización tan extenso como el presentado, se propone una implementación escalonada comenzando por la inclusión de unos pocos, pero cruciales participantes en la cadena de suministro, para progresivamente ir incluyendo más.

Resulta fácil observar que los actores del sector privado tienen mayor flexibilidad para emprender cambios tecnológicos -y adaptar su operativa a estos cambios- que los actores del sector público. En este caso, se considera que la participación inicial de actores como el MGAP, el INAC, la Aduana, o cualquier otro ente público, sería poco viable. En cambio, se propone inicialmente incluir solamente tres tipos de actores en la *blockchain*: Plantas de Faena, Despachantes de Aduana y Clientes. Cada uno de estos actores corresponderá a una organización, y cada una tendrá distintos tipos de nodos según lo que se planteó anteriormente, pero no necesariamente todos, ya que, por ejemplo, algunas organizaciones menores podrían no estar interesadas en instalar *ordering nodes*. Las distintas organizaciones podrán intercambiar los documentos correspondientes a través de los canales, así como realizar distintos tipos de registros en la *blockchain*, según lo descrito a lo largo del trabajo. Cabe destacar que esta determinación de alcance inicial fue validada por despachantes de aduana, plantas de faena y desarrolladores de *software*, como se comenta en la subsección *Retroalimentación Plantas de Faena* y la subsección *Retroalimentación Jaume & Seré y Concepto*.

En esta etapa inicial, el mayor enfoque del sistema será la reducción de papeleo, tiempo, duplicación de la información, costos de documentación y el registro de certificaciones en la *blockchain* (limitado a actividades en plantas de faena), puesto que el resto de valor se obtiene con la inclusión de otros

actores. Lo que se busca es una mejora en la eficiencia operativa de estos tres participantes de la cadena de suministro, para derivar en una mejora en el servicio ofrecido por los despachantes y una ventaja competitiva del producto en cuestión. Eventualmente, se podrán integrar otro tipo de actores hasta llegar al sistema integrado completo que se plantea en este trabajo. Ese será el punto en el que se verán ventajas exponenciales para la industria, y el sistema podrá ofrecer todas las funcionalidades planteadas, y muchas otras aún por idearse, para ofrecer un sólido diferencial competitivo sobre la región.

En sintonía con las posibles alternativas que se presentarán a lo largo de la maduración de un proyecto de gran escala como el propuesto, se deberían seguir muy de cerca los avances vinculados a IoT. Por su profunda compatibilidad con *blockchain*, grandes oportunidades de mejora estarán sin duda relacionadas a esta tecnología, con el fin de brindar al consumidor la mejor experiencia posible y la rentabilidad al mercado.

En lo que respecta a la viabilidad de las propuestas planteadas, se considera que será necesario evaluar la evolución del mercado cárnico en el futuro. Según los expertos, es probable que muchos de los atributos que hoy en día se consideran como atributos excepcionales (e.g.: carne bajo carbono, carne orgánica, producción con bienestar animal, etc) puedan ser imprescindibles posteriormente por demanda del consumidor o políticas estatales [20]. En ese escenario, será necesario que todo aquel que quiera sobrevivir en el mercado cárnico pase a adoptar este tipo de producciones en su día a día, en lugar de que sea una especialización, como hoy en día.

El camino hacia una completa integración digital de la cadena de suministro es largo y definitivamente traerá muchos desafíos. Aun así, se considera que la industria cárnica uruguaya tiene una oportunidad única de adelantarse a los cambios y emprender hacia esta dirección en un futuro cercano, para superar esas etapas desafiantes de manera temprana en comparación con el resto del mundo. Esto permitirá que al momento de que estas exigencias sean inminentes en el mercado, la industria uruguaya ya esté pronta para adaptarse al mismo y así convertirse en un pionero en la materia.

Retroalimentación Plantas de Faena

Marfrig Uruguay

En el marco del desarrollo del proyecto, se contactó a los directivos Marfrig - Frigorífico Tacuarembó S.A., para intentar incluir sus conocimientos en el rubro y evaluar la viabilidad del proyecto en el mercado nacional. La empresa se caracteriza por estar en la vanguardia de la innovación, asumiendo un rol protagónico en la industria cárnica regional, y por ese motivo se valoró mucho la receptividad e interés que se obtuvo con relación a las propuestas presentadas. Además, la misma otorga gran importancia al control de origen, a la compra responsable, sostenibilidad y al aseguramiento de la calidad, directrices altamente compatibles con el uso de *blockchain*, por lo que se entendió desde un principio que el proyecto tendría una favorable compatibilidad con la empresa.

Con relación a los encuentros y reuniones con dicha parte, manifestaron su valoración positiva con relación a *blockchain*, pero recalcaron la necesidad de justificar el uso de la tecnología con un impacto en el agregado de valor y en el consumo de los clientes. Por este motivo, se elaboró la sección

Agregado de valor a la cadena de suministro, que incursiona en un enfoque más comercial del proyecto.

Otras plantas de faena

Resulta importante destacar que también se realizó un contacto con el Ing. Agr. José Ignacio Gamio, CEO de Athena Foods, empresa que en Uruguay opera tres plantas de faena de su propiedad: Frigorífico PUL S.A., Frigorífico Canelones S.A. y Frigorífico Carrasco S.A. Al exponer los detalles acerca del sistema propuesto por los estudiantes, este profesional manifestó que un sistema de estas características se adapta a las necesidades actuales del rubro. Además, expuso su interés en estudiar la viabilidad de implementar un sistema de estas características en un mediano plazo.

Retroalimentación Jaume & Seré y Concepto

También se entró en contacto con las empresas Jaume & Seré y Concepto. Jaume & Seré cuenta con 65 años de experiencia como despachante de aduana, y además, junto con las empresas Arnaldo Castro y *Power Ledger*, desarrolló el primer sistema de *blockchain* en Uruguay para la compañía forestal Montes del Plata. Complementariamente, se accedió a la ayuda del Gerente de Desarrollo de la empresa Concepto, especializada en soluciones integrales de comercio exterior, también con varios proyectos basados en *blockchain*. Se valoran enormemente sus opiniones, no solo en lo que respecta al rol de los despachantes de aduana y el proceso de exportación, sino también en la experiencia acerca de sistemas de *blockchain*.

Particularmente, el Gerente de TI de Jaume y Seré, Fernando Thul, y el Gerente de Desarrollo de Concepto, Alexander Wolff, brindaron su visión acerca del sistema propuesto. Al contar con experiencia en el área, el principal aporte de dichas partes consistió en apoyar el proceso de planificación y creación de una *blockchain* desde sus inicios, así como evacuar consultas técnicas a la hora de desplegar la prueba de concepto. Además, reconocieron las oportunidades de mejora que se pueden presentar al aplicar *blockchain* en la cadena de suministro cárnica.

Una vez validado ese aspecto, Alexander Wolff aprobó la propuesta de que se utilice *Hyperledger Fabric* para implementar el sistema propuesto, por adecuarse mejor a los requerimientos y necesidades del mismo. Esto también se pudo notar a la hora de ejecutar exitosamente la prueba de concepto de dicha plataforma.

En lo que respecta a la implementación del sistema, los expertos realizaron especial énfasis en que el alcance inicial para implementar la solución sería involucrando únicamente a plantas de faena, despachantes de aduana y clientes, para garantizar su viabilidad. En ese sentido, se comentó acerca de la dificultad de involucrar a los entes públicos en el sistema, algo que no se proyecta como posible para el corto y mediano plazo, pero que de concretarse pondría a la industria en una gran revolución tecnológica. Cabe mencionar también, que a diferencia de Marfrig, debido a sus funciones en la cadena de suministro, la parte en cuestión valora más los beneficios operacionales que brindaría la aplicación de la tecnología, como los referidos a la eficiencia y velocidad en las comunicaciones y el ahorro de recursos innecesarios.

Conclusiones

A lo largo del proyecto “Mejora de la cadena de suministro por aplicación de *blockchain*”, se presentaron en líneas generales los fundamentos de la tecnología *blockchain* y se estudió acerca de la logística y estructura de las cadenas de suministro. Partiendo de esa base teórica, se buscó el caso más relevante de aplicación, a través de un análisis del contexto nacional. Se concluyó que la cadena cárnica ofrecía posibilidades de mejora muy interesantes, con capacidad de lograr un verdadero impacto en el mercado. Para lograr la adaptación de la tecnología se debió aprender en profundidad acerca de los procesos de exportación de la carne, de los procesos industriales correspondientes, de la producción de ganado, y de variadas funciones de apoyo en la cadena, a través de intercambios con profesionales consagrados en el rubro. Por último, se analizó la viabilidad y la forma de materialización del proyecto en el futuro. De todos modos, para dar cierre al proyecto, se evaluó, en retrospectiva, la evolución del mismo, para rememorar las enseñanzas y desafíos que se han presentado a lo largo del camino y corroborar el cumplimiento de metas y objetivos planteados en un principio.

En primer lugar, se valora la posibilidad brindada a través del proyecto de investigar y aprender sobre *blockchain*, una tecnología novedosa de la actualidad. Una de las principales interrogantes surgidas ha sido analizar cómo promocionar esta tecnología disruptiva e innovadora, de funcionamiento complejo, a la gran variedad de integrantes de la cadena de suministro. Para esto, ha sido importante visualizar el proyecto desde distintas perspectivas a medida que el mismo era presentado a las partes involucradas, dado que su fuente de valor variaba considerablemente en base a los intereses de cada uno. Por este motivo, a pesar de los evidentes beneficios para la cadena de suministro como un conjunto, se tuvo que analizar el contexto y el propósito de cada actor para poder encontrar y destacar las características del proyecto que mejor solucionen sus necesidades particulares. Por el lado de Marfrig, se pudo captar que la principal razón para la implementación de *blockchain* reside en poder garantizar a través de la misma un agregado de valor al producto que tenga un impacto positivo en su participación en el mercado, mientras que en Jaume & Seré se encontró el diferencial en la posibilidad de garantizar un flujo dinámico de información para una mejora operativa en la exportación de carne.

En base a lo mencionado anteriormente, el proyecto se desarrolló en torno a dos ideas centrales. En primer lugar, se estudió en detalle el procedimiento de exportación de la carne desde el productor hasta el consumidor final. Fue necesario interiorizarse en las actividades llevadas a cabo por cada actor de la cadena. En todo momento se debió evaluar la participación de los mismos con un sentido crítico para poder encontrar las posibilidades de mejora con la inclusión de *blockchain*. Parte de esta investigación inicial consistió en comprender la normativa vigente como también los documentos involucrados. En función a lo anterior, se concluyó que la *blockchain* aportaría un rol fundamental en la integración de la cadena de suministro, al facilitar la tarea de gestión de información y documentación entre partes de forma segura. Al hacerlo, se busca eliminar el fraude, mejorar la eficiencia de las interacciones entre actores, reducir los tiempos de entrega y los costos de información.

En segundo lugar, se busca aumentar la participación de los involucrados en el mercado, a través de la implementación de procesos que garanticen un agregado de valor al consumidor. El proyecto plantea la posibilidad de incursionar a través de *blockchain* en la producción a bajo carbono,

producción orgánica y producción de carne Kosher, entre otras, y así crear un impacto positivo en los ingresos e imagen de las partes involucradas. Existe la posibilidad incluso, de que, en un futuro, nuevas normativas exijan de forma imperativa distintas certificaciones relacionadas a la producción, para permitir la participación en ciertos mercados, por lo que una adopción de tecnologías como la mencionada pasaría de ser una ventaja competitiva a una necesidad.

Se puede concluir también que la mayor incertidumbre relacionada al proyecto es la coordinación entre públicos y privados de forma que pueda potenciar al sector para el beneficio de todos. El máximo potencial del sistema se logra al alcanzar el mayor número de tipos de actores involucrados y la sinergia del sector productivo con el Estado. Sin embargo, llegar a ese punto de maduración puede llevar un período largo de tiempo, por lo que se cree que la mejor forma de iniciar este desarrollo es enfocándose en algunas funcionalidades específicas para algunos actores privados. Es un camino complejo pero los pasos a seguir están claros y sería interesante que se empiecen a ejecutar en el mediano plazo porque estos desarrollos definitivamente apalancarán la producción y desarrollarán el sector por el camino indicado, según las tendencias de los próximos años.

Con respecto a la aplicación práctica basada en el despliegue de una red de prueba de *Hyperledger Fabric*, se valora la posibilidad de acercarse a la programación y desarrollo informático de esta tecnología. Esto permitió comprender el funcionamiento de la misma, a tal punto que se pudo interactuar con ella hasta ejecutar un producto sencillo pero funcional. La experiencia permitió potenciar la base de conceptos generales de computación adquiridos en la carrera, y del sistema operativo Ubuntu de Linux, dejando un precedente para el futuro profesional de los estudiantes. Además, la actividad fue importante para materializar y visualizar la teoría desarrollada, cerrando el ciclo de aprendizaje y consolidando los conocimientos que en principio se habían investigado únicamente de manera teórica. Por otro lado, se lograron entender algunas de las posibles problemáticas que pueden afrontar los informáticos en un proyecto similar.

Con relación a lo personal, resultó de gran satisfacción haber podido interactuar de forma fluida con figuras referentes en su rubro. Se pudo aprovechar la experiencia comercial de los representantes de distintas empresas, para aprender acerca de la forma de gestionar y materializar una idea, algo que sin duda es fundamental para el desarrollo profesional de cualquier estudiante. La apertura de las partes mencionadas con relación a sus proyectos y proyecciones permitió asimilar hacia dónde avanzará el mercado.

Todo el proyecto en sí permitió ensayar el proceso necesario para la realización de un nuevo emprendimiento, ya que todo lo planteado fue diseñado con intenciones de plasmarlo más allá de fines académicos. Con referencia a este proceso, se cumplieron los plazos estipulados para la concreción de cada etapa. Aun así, dado el largo período de tiempo en cuestión, se encuentra cierta dificultad en mantener un nivel constante de motivación. Por fortuna, en las reuniones con las contrapartes, se encontraba el ímpetu necesario para avanzar. Por sobre todas las cosas, se valora la aplicación de los conceptos desarrollados en distintas asignaturas a lo largo de la carrera, siendo las más relevantes Fundamentos de Ingeniería de Software, Elementos de Gestión Logística, Teoría Algoritmos y Aplicaciones de Gestión Logística, Planeamiento Estratégico y Estrategia Competitiva, Administración de Operaciones y Elementos de Ingeniería Ambiental. De todas formas, más allá de los conceptos particulares obtenidos en las distintas materias, el proyecto sirvió para tomar conciencia

de todas las herramientas con las que se contaban como eventuales Ingenieros en Producción para llevar adelante y gestionar un proyecto.

Bibliografía

- [1] «Elementos de Gestión Logística - Eva Fing,» Facultad de Ingeniería, 10 Marzo 2020. [En línea]. Available: <https://eva.fing.edu.uy/enrol/index.php?id=50>. [Último acceso: 20 Setiembre 2020].
- [2] «Schroeder,» de *Administración de operaciones - Conceptos y casos contemporáneos*, Estados Unidos, The McGraw-Hill Companies, 2011, p. 210.
- [3] «Introducción a la Logística,» de *Clase 1 - Introducción a la Logística*, Montevideo, 2020.
- [4] R. Schroeder, S. Goldstein y J. Rungtusanatham, de *Administración de operaciones - Conceptos y casos contemporáneos*, Estados Unidos, The McGraw - Hill Companies, 2011, p. 230.
- [5] S. Mecaluz, «La trazabilidad deja huella,» 1 abril 2014. [En línea]. Available: <https://www.mecaluz.com.uy/articulos-de-logistica/trazabilidad-deja-huella>. [Último acceso: 3 agosto 2020].
- [6] Registro Nacional de Leyes y Decretos., «Ley N° 17997 de 2006,» Montevideo, 8 de agosto de 2006.
- [7] T. L. World, «Recall, clave para proteger al consumidor,» 2020. [En línea]. Available: <https://thelogisticsworld.com/historico/recall-clave-para-protger-al-consumidor/>. [Último acceso: 3 febrero 2021].
- [8] B. Singhal, G. Dhameja y P. Sekhar Panda, «Centralized vs. Decentralized Systems,» de *Beginning Blockchain - A Beginner's Guide to Building Blockchain Solutions*, Nueva York, Springer Science - Business Media New York, 2018, pp. 11-17.
- [9] D. Drescher, de *Blockchain Basics - A Non-Technical Introduction in 25 Steps*, Nueva York, Springer Science + Business Media New York, 2017, p. 15.
- [10] B. Singhal, G. Dhameja y P. Sekhar Panda, «Properties of Blockchain Solutions,» de *Beginning Blockchain - A Beginner's Guide to Building Blockchain Solutions*, Nueva York, Springer Science - Business Media New York, 2018, p. 124.
- [11] B. Singhal, G. Dhameja y P. Sekhar Panda, «Blockchain Transaction,» de *Beginning Blockchain - A Beginner's Guide to Building Blockchain Solutions*, Nueva York, Springer Science - Business Media New York, 2018, p. 129.
- [12] D. Drescher, «Hashing Data,» de *Blockchain Basics - A Non-Technical Introduction in 25 Steps*, Nueva York, Springer Science + Business Media New York, 2017, pp. 71-79.
- [13] B. Singhal, G. Dhameja y P. Sekhar Panda, «Cryptography,» de *Beginning Blockchain - A Beginner's Guide to Building Blockchain Solutions*, Nueva York, Springer Science - Business Media New York, 2018, pp. 34-102.
- [14] F. d. Ingeniería, «Fundamentos de Ingeniería de Software - Fing,» May 2020. [En línea]. Available: <https://eva.fing.edu.uy/enrol/index.php?id=787>. [Último acceso: May 2020].
- [15] B. Singhal, G. Dhameja y P. Sekhar Panda, «Layers of Blockchain,» de *Beginning Blockchain - A Beginner's Guide to Building Blockchain Solutions*, Nueva York, Springer Science - Business Media New York, 2018, pp. 17-22.

- [16] B. Singhal, G. Dhameja y P. Sekhar Panda, «Distributed Consensus Mechanisms,» de *Beginning Blockchain - A Beginner's Guide to Building Blockchain Solutions*, Nueva York, Springer Science - Business Media New York, 2018, pp. 130-133.
- [17] G. Iredale, «List Of Top 50 Companies Using Blockchain Technology,» 101 Blockchains, 26 diciembre 2020. [En línea]. Available: 101blockchains.com/companies-using-blockchain-technology/. [Último acceso: 20 febrero 2021].
- [18] F. Knirsch y A. Unterweger, «Implementing a blockchain from scratch: why, how, and what we learned.,» Springer Nature, 2019.
- [19] W. H. Organization, «Carga mundial de enfermedades de transmisión alimentaria: estimaciones de la OMS,» 2015. [En línea]. Available: https://www.who.int/foodsafety/areas_work/foodborne-diseases/fergonepager_es.pdf?ua=1. [Último acceso: 30 marzo 2021].
- [20] B. y. Asociados, «Webinar Ganadería 2021: La próxima década, trazabilidad y blockchain en la ganadería uruguaya,» Montevideo, 2020.
- [21] «Por primera vez INAC asiste a la feria de alimentos más grande del sur de China,» El Observador, 21 abril 2021. [En línea]. Available: <https://www.elobservador.com.uy/nota/por-primera-vez-inac-asiste-a-la-feria-de-alimentos-mas-grande-del-sur-de-china-202142119120>. [Último acceso: 24 abril 2021].
- [22] M. High, «Supply chain insight: Inside IBM's Food Trust Blockchain system,» Supply Chain, 17 mayo 2020. [En línea]. Available: <https://supplychaindigital.com/technology-4/supply-chain-insight-inside-ibms-food-trust-blockchain-system>. [Último acceso: 18 setiembre 2020].
- [23] «Plataforma de trazabilidad Ampliada sobre Blockchain,» Carnes Validadas, [En línea]. Available: https://www.carnesvalidadas.com/index_es.php#quescv. [Último acceso: 18 setiembre 2020].
- [24] «The Leading Blockchain Solution for Global Beef Supply Chain,» Beef Ledger, [En línea]. Available: <https://beefledger.io>. [Último acceso: 18 setiembre 2020].
- [25] N. Rodriguez, «Árbol de Decisión de Blockchain Definitivo,» 27 diciembre 2018. [En línea]. Available: <https://101blockchains.com/es/necesitas-una-solucion-blockchain/>. [Último acceso: 30 marzo 2021].
- [26] A. Grakov, «A blockchain platforms comparison,» vironIT, 27 agosto 2018. [En línea]. Available: <https://vironit.com/a-blockchain-platforms-comparison/>. [Último acceso: 2 febrero 2021].
- [27] M. Holovský, «Unhyped comparison of Blockchain Platforms,» Medium, 25 enero 2021. [En línea]. Available: <https://medium.com/coinmonks/unhyped-comparison-of-blockchain-platforms-679e122947c1>. [Último acceso: 3 febrero 2021].
- [28] A. Hertig, «Ethereum 101,» condesk, 3 diciembre 2020. [En línea]. Available: <https://www.coindesk.com/learn/ethereum-101/what-is-ethereum>. [Último acceso: 20 marzo 2021].
- [29] G. Araujo, «Hyperledger Fabric: Conceptos y tipos de nodos,» BABEL, 5 agosto 2019. [En línea]. Available: <https://www.coindesk.com/learn/ethereum-101/what-is-ethereum>. [Último acceso: 20 marzo 2021].

- [30] Hyperledger, «How Fabric networks are structured,» Hyperledger Fabric, 2020. [En línea]. Available: <https://hyperledger-fabric.readthedocs.io/en/release-2.3/network/network.html> . [Último acceso: 30 abril 2021].
- [31] N. Abramov, «How R3 Corda Works,» MEDIUM, 28 marzo 2019. [En línea]. Available: <https://nickavramov.medium.com/how-r3-corda-works-24d9285059a2> . [Último acceso: 5 febrero 2021].
- [32] Hyperledger, «Peers,» Hyperledger Fabric, 2020. [En línea]. Available: <https://hyperledger-fabric.readthedocs.io/en/release-2.3/peers/peers.html>. [Último acceso: 10 mayo 2021].
- [33] I. N. d. Carnes, «Breve Historia,» [En línea]. Available: <https://www.inac.uy/innovaportal/v/1110/17/innova.front/breve-historia#:~:text=El%20Instituto%20Nacional%20de%20Carnes,determinaci%C3%B3n%20corresponde%20al%20Poder%20Ejecutivo..> [Último acceso: 10 diciembre 2020].
- [34] A. y. P. Ministerio de Ganadería, «Cometidos,» [En línea]. Available: <https://www.gub.uy/ministerio-ganaderia-agricultura-pesca/institucional/cometidos>. [Último acceso: 10 diciembre 2020].
- [35] D. N. d. Aduanas, «Glosario,» [En línea]. Available: <https://www.aduanas.gub.uy/innovaportal/v/227/8/innova.front/glosario.html> . [Último acceso: 13 diciembre 2020].
- [36] M. d. E. y. Finanzas, «Dirección Nacional de Aduanas,» [En línea]. Available: <https://www.gub.uy/ministerio-economia-finanzas/institucional/estructura-del-organismo/direccion-nacional-aduanas>. [Último acceso: 12 diciembre 2020].
- [37] M. Barone, «El agente marítimo, sus funciones y la responsabilidad en los reclamos de índole laboral,» *Anales - Facultad de Ciencias Jurídicas y Sociales*, nº 48-2018.
- [38] V. Ú. d. C. Exterior, «¿Qué es VUCE?,» [En línea]. Available: <https://vuce.gub.uy/acerca-de-vuce/#:~:text=La%20Ventanilla%20C3%9Anica%20de%20Comercio,de%20importaci%C3%B3n%20exportaci%C3%B3n%20y%20tr%C3%A1nsito..> [Último acceso: 20 diciembre 2020].
- [39] S. N. d. I. Ganadera, «Guías de Propiedad y Tránsito,» [En línea]. Available: <https://www.snig.gub.uy/principal/snig-trazabilidad-traz-grupal-guia-de-propiedad-y-transito-generalidades?es>. [Último acceso: 8 enero 2021].
- [40] «¿Qué es y para qué sirve una carta de crédito?,» EAE Business School, 24 octubre 2018. [En línea]. Available: <https://retos-directivos.eae.es/que-es-y-para-que-sirve-una-carta-de-credito/>. [Último acceso: 30 noviembre 2020].
- [41] V. Ú. d. C. Exterior, «VSOL/COCC - INAC: Certificación de INAC para la Exportación de Carnes,» [En línea]. [Último acceso: 28 noviembre 2020].
- [42] Registro Nacional de Leyes y Decretos., «Ley N° 15605 de 1984, Art. 3°.,» Montevideo, 27 de julio de 1984.
- [43] D. N. d. Aduanas, «Documento Único Aduanero,» Dirección Nacional de Aduana, [En línea]. Available: <https://www.aduanas.gub.uy/innovaportal/v/2602/8/innova.front/documento-unico-aduanero.html>. [Último acceso: 10 noviembre 2020].
- [44] C. Moldtrans, «Descubre la importancia del Booking Note para el transporte marítimo,» Grupo Moldtrans, 18 enero 2019. [En línea]. Available: <https://www.moldtrans.com/descubre-la->

- importancia-del-booking-note-para-el-transporte-maritimo/. [Último acceso: 12 diciembre 2020].
- [45] Registro Nacional de Leyes y Decretos, «Ley N° 19.276 de 19/04/2014, artículo 1.,» Montevideo, 19 de abril de 2014.
- [46] Uruguay XXI, «Guía del Exportador,» [En línea]. Available: <https://www.uruguayxxi.gub.uy/es/quiero-exportar/herramientas/guia-del-exportador/>. [Último acceso: 20 noviembre 2020].
- [47] E. B. School, «¿Qué es y para qué sirve una carta de crédito?,» EAE Business School, 24 octubre 2018. [En línea]. Available: <https://retos-directivos.eae.es/que-es-y-para-que-sirve-una-carta-de-credito/>. [Último acceso: 29 enero 2021].
- [48] Aduanas, «Procedimiento de control para la exportación definitiva de carne de origen nacional,» 5 febrero 2019. [En línea]. Available: <https://aplicaciones.aduanas.gub.uy/wikiprocpod/hwiki.aspx?Procedimiento+de+control+para+la+exportaci%c3%b3n+definitiva+de+carne+de+origen+nacional>. [Último acceso: 25 noviembre 2020].
- [49] Aduanas, «Asignación de canal de Importación,» 17 setiembre 2012. [En línea]. Available: <https://aplicaciones.aduanas.gub.uy/wikiprocpod/hwiki.aspx?Asignaci%c3%b3n+de+canal+Imp+ortaci%c3%b3n>. [Último acceso: 30 noviembre 2020].
- [50] Dirección Nacional de Aduanas, «Procedimiento de exportación definitiva,» Montevideo, 7 de febrero de 2003.
- [51] N. Rodriguez, «Principios de gobernanza blockchain,» 13 setiembre 2020. [En línea]. Available: <https://101blockchains.com/es/principios-de-gobernanza-blockchain/>. [Último acceso: 20 febrero 2021].
- [52] «¿Qué es un BIP - Bitcoin Improvement Proposal?,» bit2me ACADEMY, [En línea]. Available: <https://academy.bit2me.com/que-es-bip-bitcoin/>. [Último acceso: 8 abril 2021].
- [53] J. Maldonado, «Gobernanza, la clave de la descentralización y desarrollo de proyectos blockchain,» Cointelegraph, 5 noviembre 2020. [En línea]. Available: <https://es.cointelegraph.com/explained/governance-the-key-to-decentralization-and-development-of-blockchain-projects>. [Último acceso: 20 febrero 2021].
- [54] «Gestión y gobernanza de blockchains,» Ripio, [En línea]. Available: <https://launchpad.ripio.com/guias-capitulos/gestion-y-gobernanza-de-blockchains> . [Último acceso: 4 febrero 2021].
- [55] G. López, «Hard fork y soft fork. En qué consisten y cuáles son sus diferencias,» Coin Telegraph, 26 abril 2017. [En línea]. Available: <https://es.cointelegraph.com/news/hard-fork-y-soft-fork-en-que-consisten-y-cuales-son-sus-diferencias-20170426>. [Último acceso: 10 abril 2021].
- [56] A. R. Jaramillo, «La gobernanza en las redes privadas de blockchain,» Covalent, 17 enero 2019. [En línea]. Available: <https://medium.com/covalentxhq/la-gobernanza-en-las-redes-privadas-de-blockchain-56e943fe0505> . [Último acceso: 20 enero 2021].
- [57] F. a. A. Organization, «Novedades en el mercado de la carne y los productos lácteos orgánicos: Repercusiones para los países en desarrollo,» FAO, 29 agosto 2002. [En línea]. Available: <http://www.fao.org/3/y6976s/y6976s.htm#:~:text=Los%20productos%20etiquetados%20como>

%20%22org%C3%A1nicos,de%20producci%C3%B3n%20org%C3%A1nica%20claramente%20definidos.&text=En%20otras%20palabras%20el%20t%C3%A9rmino,no%20al%20producto%20en%20s%C3%AD.. [Último acceso: 3 marzo 2021].

- [58] F. a. A. Organization, «Características relevantes de la agricultura orgánica,» FAO, [En línea]. Available: <http://www.fao.org/3/y4137s/y4137s0d.htm>. [Último acceso: 2 febrero 2021].
- [59] E. d. I. Ambiental, «Notas del Curso,» Facultad de Ingeniería , 2019.
- [60] G. Becoña y W. Oyhantcabal, «Primer estudio de la huella de carbono de tres cadenas agroexportadoras del Uruguay: carne vacuna, láctea, arroceras,» Ministerio de Ganadería, Agricultura y Pesca, Montevideo, 2013.
- [61] B. S. Institutions, «Specification for the assessment of the life cycle greenhouse gas emissions of goods and services,» BSI, Londres, 2011.
- [62] Instituto Nacional de Investigación Agropecuaria, «Producción Ganadera - Hábitats Naturales - Bienestar Humano,» *Producir carne preservando hábitats naturales e impactando positivamente en el bienestar humano.*, 2021.
- [63] M. Selhi, «Carne Kosher en Argentina: ¿Qué es, cómo se produce y adónde va?,» Sitio Argentino de Producción Animal, 2018. [En línea]. Available: https://www.produccion-animal.com.ar/informacion_tecnica/carne_y_subproductos/205-kocsher.pdf. [Último acceso: 10 abril 2021].
- [64] «Producción kosher en Uruguay: ¿qué requiere?,» Uruguay Natural, 8 julio 2020. [En línea]. Available: <https://marcapaisuruguay.gub.uy/produccion-kosher-en-uruguay-que-requiere/>. [Último acceso: 10 abril 2021].
- [65] Instituto Nacional de Carnes, «Programa de Bienestar Animal,» 11 marzo 2015. [En línea]. Available: <https://www.inac.uy/innovaportal/v/10844/2/innova.front/programa-de-certificacion-de-bienestar-animal-pba#:~:text=El%20Programa%20de%20certificaci%C3%B3n%20fue,el%20uso%20del%20LOGO%20BA..> [Último acceso: 20 marzo 2021].
- [66] Instituto Nacional de Carnes, «Protocolo de Bienestar Animal - Predio agropecuario,» 7 octubre 2020. [En línea]. Available: <https://www.inac.uy/innovaportal/file/11637/1/protocolo-inac-ba-bovino---predio-1.pdf>. [Último acceso: 2 abril 2021].
- [67] Instituto Nacional de Carnes, «Protocolo de Bienestar Animal - Empresa de Transporte,» 6 marzo 2019. [En línea]. Available: <https://www.inac.uy/innovaportal/file/11638/1/protocolo-inac-ba-bovino--transporte.pdf>. [Último acceso: 3 abril 2021].
- [68] Instituto Nacional de Carnes, «Protocolo de Bienestar Animal - Planta de Faena,» 6 marzo 2019. [En línea]. Available: <https://www.inac.uy/innovaportal/file/11640/1/protocolo-inac-ba-v6-bovino---planta-2.pdf>. [Último acceso: 3 abril 2021].
- [69] Instituto Nacional de Carnes, «Logo identificadorio del Programa,» enero 2021. [En línea]. Available: <https://www.inac.uy/innovaportal/v/11827/14/innova.front/logo-indentificadorio-del-programa>. [Último acceso: 3 abril 2021].
- [70] A. Rayes y S. Salam, Internet of Things From Hype to Reality, Switzerland: Springer Nature, 2019.
- [71] «Hawks, Karen. VP Supply Chain Practice, Navesink.Reverse Logistics Magazine, Winter/Spring (2006)».

- [72] T. México, «Retiro de Productos (Recall),» An Amwins Group Company, 27 diciembre 2017. [En línea]. Available: <https://www.thbmexico.com/post/2017/12/26/retiro-de-productos-recall>. [Último acceso: 2 abril 2021].
- [73] «Recall, clave para proteger al consumidor,» The Logistics World, [En línea]. Available: <https://thelogisticsworld.com/historico/recall-clave-para-proteger-al-consumidor/>. [Último acceso: 3 abril 2021].
- [74] S. Lasserre, «Retirada de productos: ¿qué impacto tiene para su línea de producción?,» Locabri Solutions Modulaires, 14 febrero 2019. [En línea]. Available: <https://www.locabri.com/es/blog/retirada-de-productos-impacto-l%C3%ADnea-de-producci%C3%B3n>. [Último acceso: 30 marzo 2021].

Anexo I – flujo de procesos desde ingreso de ganado a planta hasta envasado de cortes cárnicos

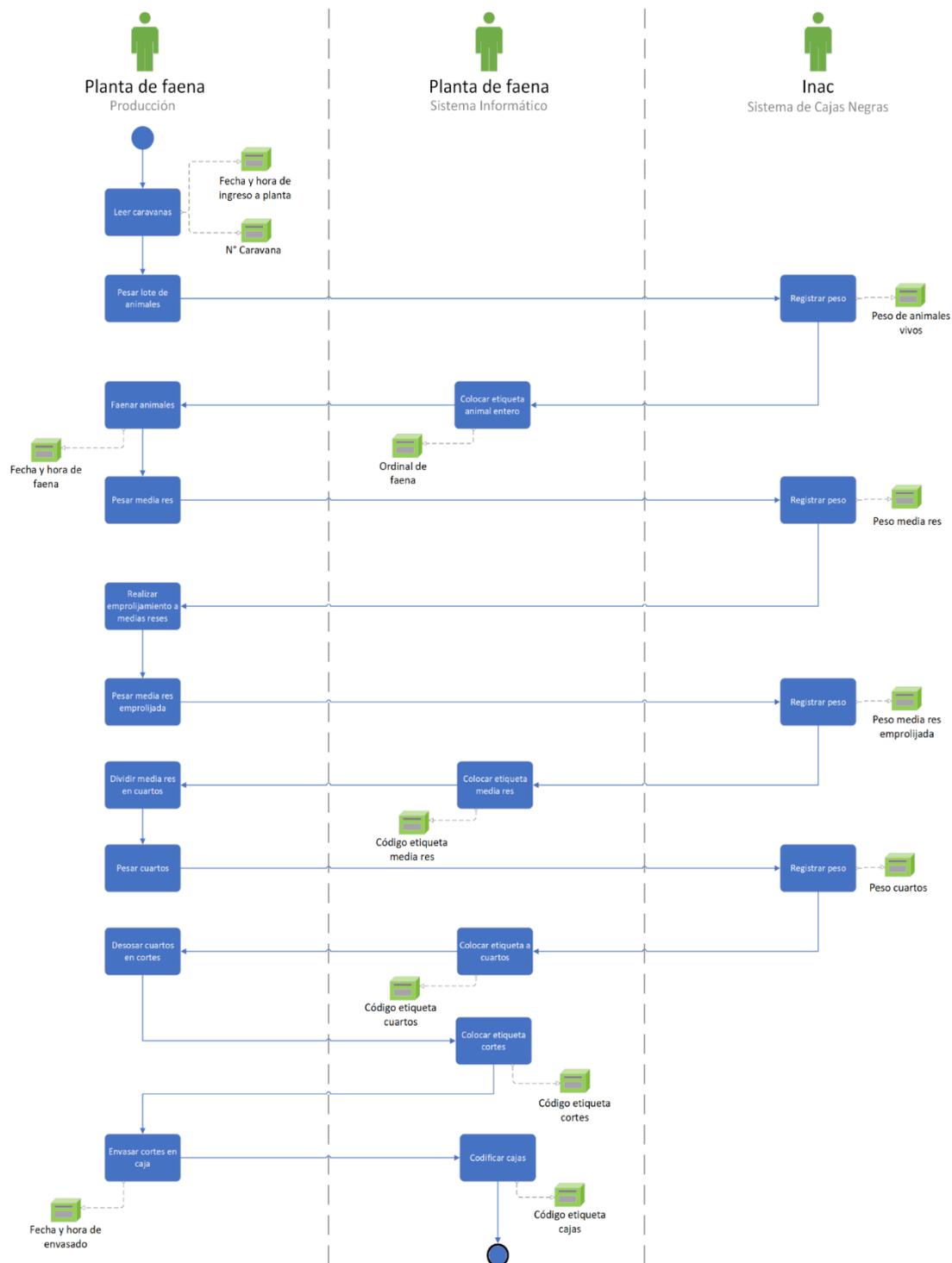


Figura 40 - Flujo de procesos desde el ingreso de ganado a planta hasta envasado de cortes cárnicos

Anexo II – flujo de procesos correspondientes a la negociación entre planta de faena y cliente

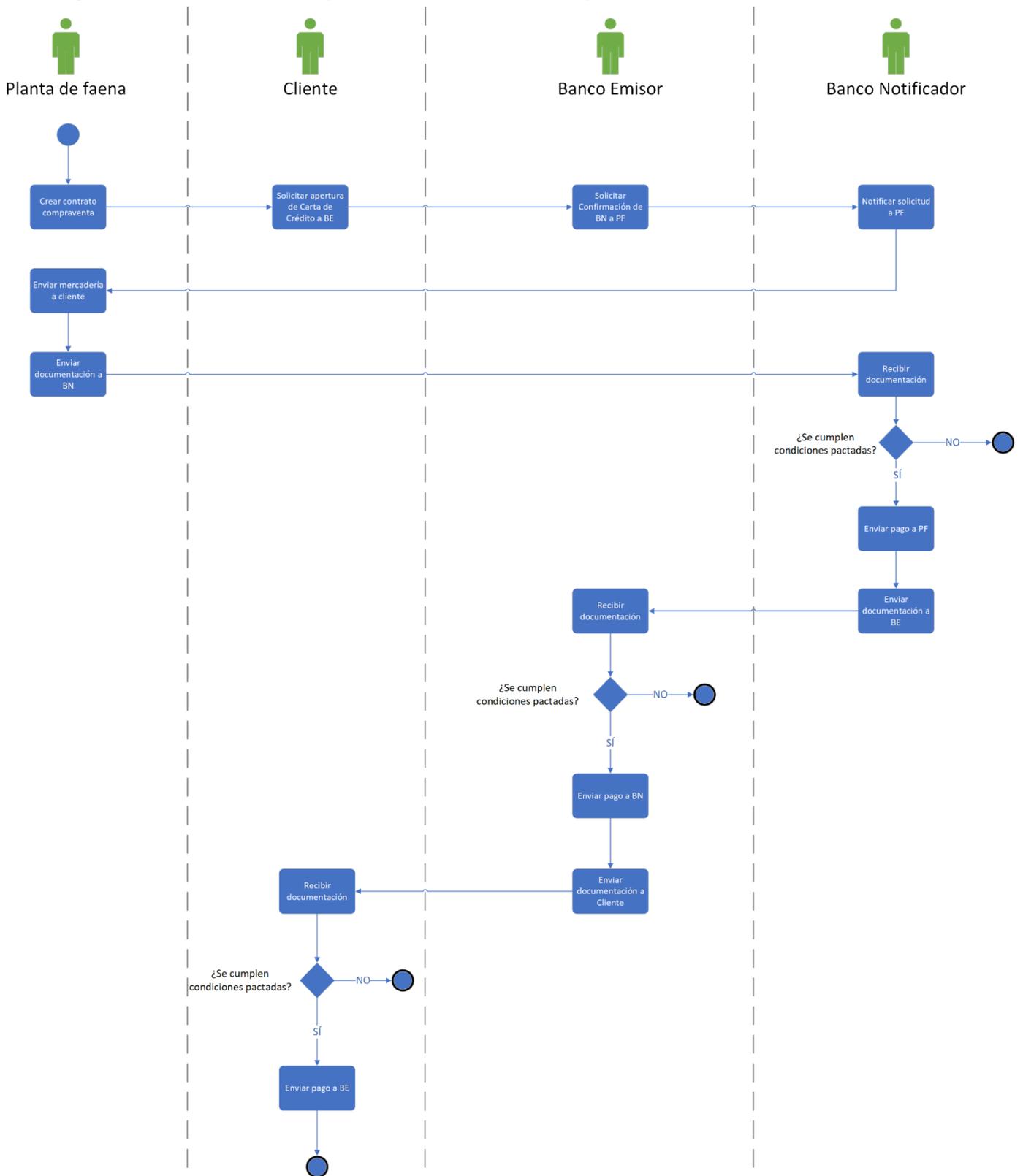


Figura 41 - Flujo de procesos correspondiente a la negociación entre planta de faena y cliente

Anexo III – funcionamiento del *smart contract* como sustituto de la carta de crédito

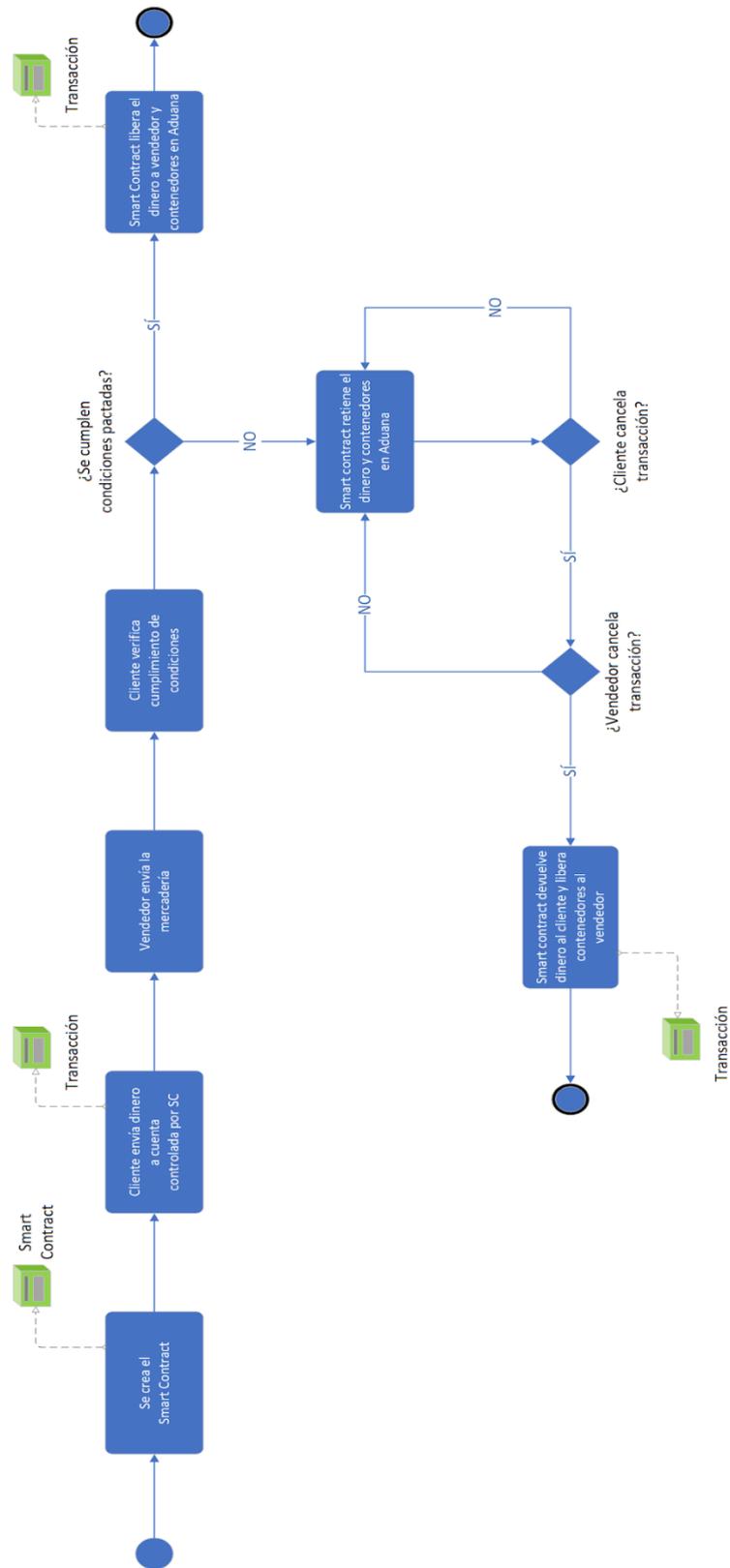


Figura 42 - Funcionamiento del smart contract como sustituto de la carta de crédito

Anexo IV – la ganadería uruguaya y el cuidado del medio ambiente

El mencionado informe del Instituto Nacional de Investigación Agropecuaria [62] sostiene que los cuestionamientos a la sostenibilidad ambiental de la ganadería se asocian a tres aspectos que son la producción en sistemas confinados, la destrucción de hábitats naturales y el cambio climático. Sin embargo, Uruguay se encuentra en una posición segura y destacable en estos aspectos, puesto que la producción en sistemas confinados se da en cantidades menores, porque la ganadería uruguaya ayuda a preservar ciertos hábitats naturales amenazados y porque su impacto al cambio climático, comparado con otros países, es bajo. A continuación, se profundiza en los puntos que destaca el informe mencionado.

Los pastizales en regiones sub-húmedas son uno de los biomas más amenazados del planeta

Los pastizales son altamente valorados por impactar positivamente en el bienestar humano (proveer Servicios Ecosistémicos) a través de la conservación del suelo y nutrientes, del mantenimiento de la biodiversidad, de la mitigación de las emisiones de GEI y de la regulación hídrica.

La ganadería uruguaya preserva un hábitat natural amenazado

Como se observa en la Figura 43, una gran cuota de la producción ganadera del país se lleva adelante en campo natural (pastizales perennes). Lejos de desplazar bosques o humedales, la ganadería preserva el pastizal natural y los bosques nativos, hábitats amenazados en todo el mundo. Además, es interesante observar los siguientes datos acerca de la ganadería nacional:

- La cría de terneros utiliza casi en su totalidad el campo natural como base forrajera. En el caso de la recría, esto se da en un 45% de los casos, y en la invernada de un 29% de los casos.
- Casi el 33% de los animales faenados utilizan solamente el campo natural.
- En 2020, un 14% de los animales faenados se terminaron a corral en los últimos 60-90 días

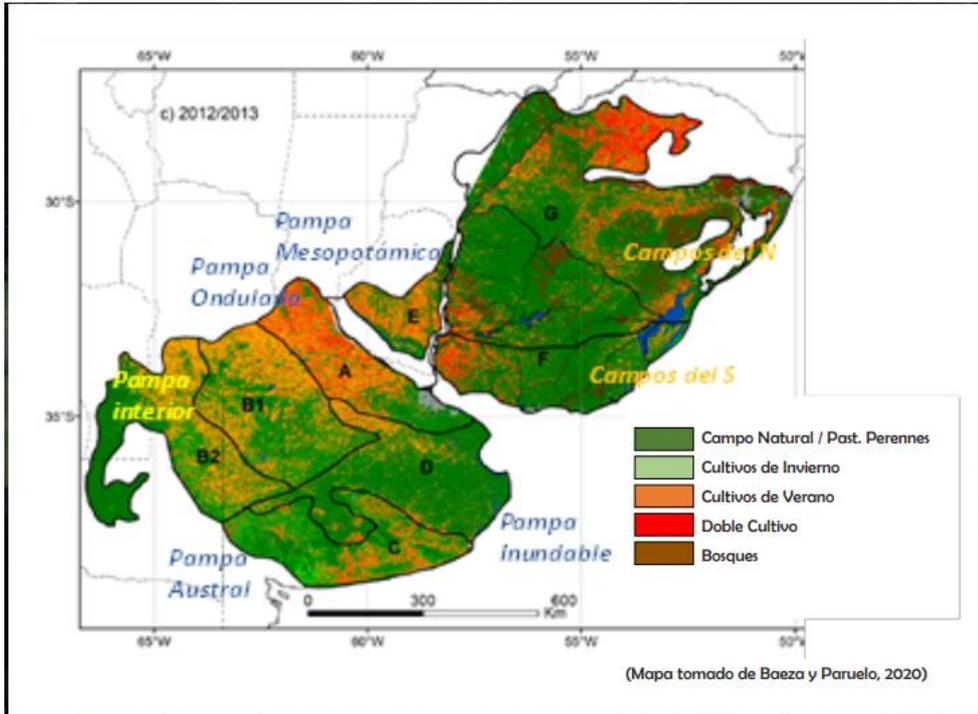
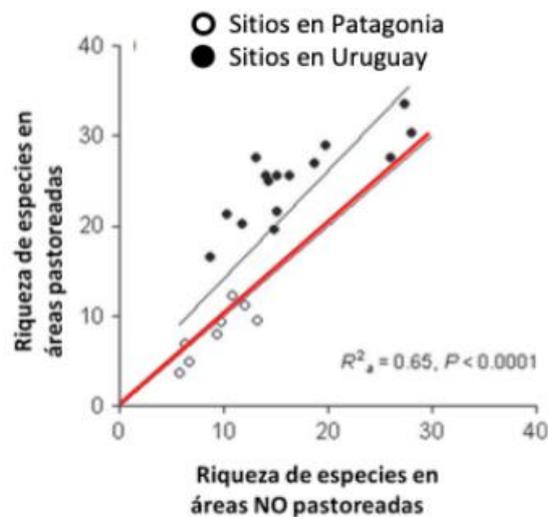


Figura 43 - Mapa de sistemas productivos de la región

La ganadería uruguaya promueve la biodiversidad

La ganadería uruguaya preserva hábitats naturales promoviendo la presencia de mayor cantidad de especies que si se eliminara el pastoreo. De esta forma, el pastoreo tiene una alta influencia en la conservación de la biodiversidad. Como se observa en la siguiente gráfica (Figura 44), la riqueza de especies es mayor en áreas pastoreadas.



Comparación entre la riqueza (número total) de especies vegetales nativas en áreas no-pastoreadas y pastoreadas contiguas. Los puntos negros corresponde a pares en los pastizales del Río de la Plata. Cuando la cantidad de especies está por encima de la línea roja la riqueza fue mayor en condiciones de pastoreo.

Modificado de Lezama et al. (2013)

Figura 44 - Comparación de riqueza de especies en áreas protegidas pastoreadas y no pastoreadas

La ganadería uruguaya es la actividad con menor impacto sobre los ecosistemas

Si se comparan todas las actividades agropecuarias, la ganadería es la que extrae menor cantidad de carbono fijado por los ecosistemas. Al comparar la extracción de carbono de campo natural bajo uso ganadero con la agricultura, se destaca que la primera extrae un 30% de carbono mientras que la segunda un 50%.

El sistema de ciencia y tecnología uruguayo desarrolló protocolos auditables para medir el impacto ambiental de la ganadería

Uruguay elaboró diversos protocolos para asegurar una confiable evaluación de la oferta de Servicios Ecosistémicos, de la integridad ecosistémica, del nivel de conservación del campo natural y de la biodiversidad.

Anexo V – Proceso de prueba de concepto en Hyperledger Fabric

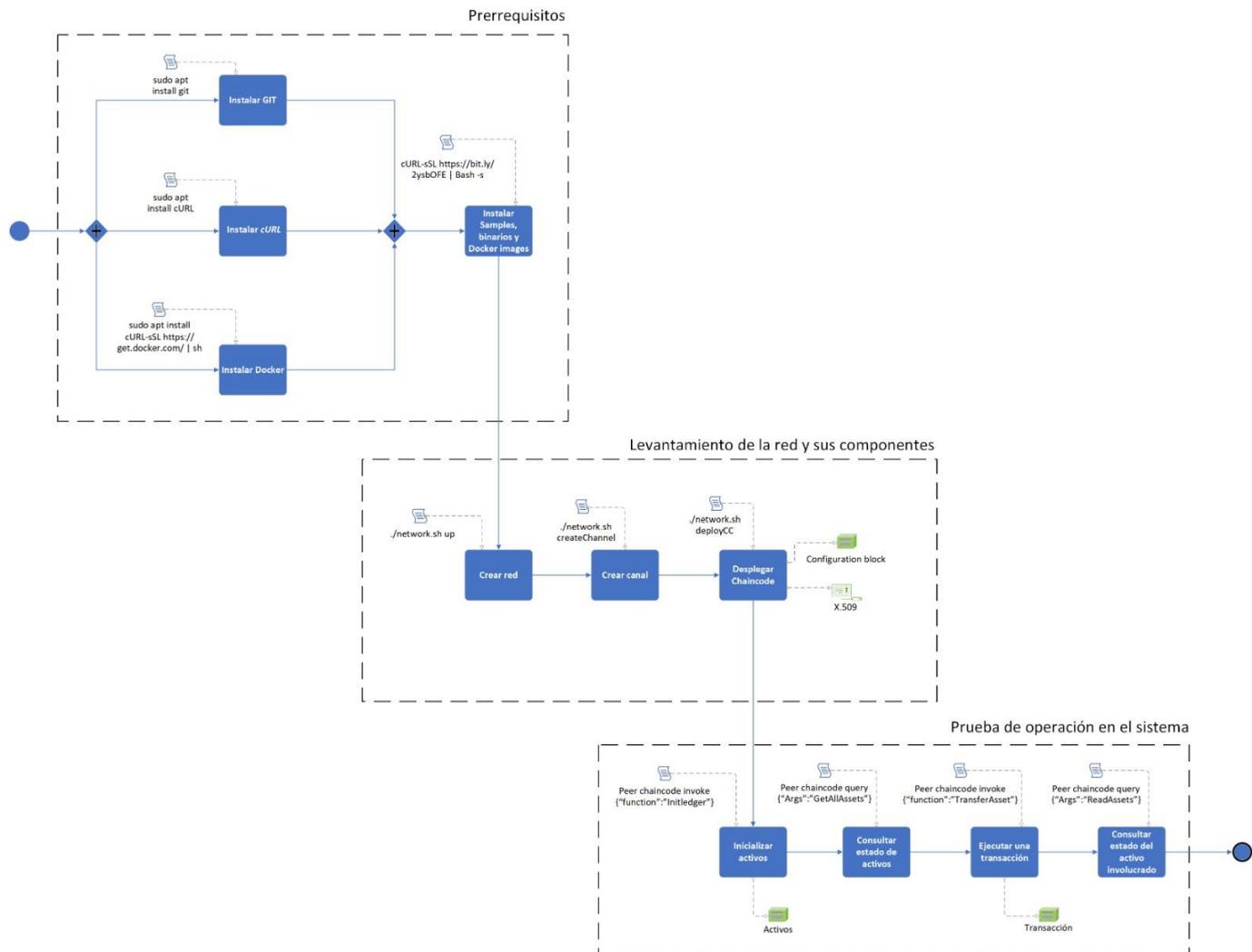


Figura 45 - Proceso completo de la prueba de concepto ejecutada

Anexo VI – Ejecución de instalación de Prerrequisitos Hyperledger Fabric

```
juan@juan-VirtualBox:~$ sudo apt install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-el git-email git-gui gitk
  gitweb git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 150 not upgraded.
Need to get 5.468 kB of archives.
After this operation, 38,4 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://uy.archive.ubuntu.com/ubuntu focal/main amd64 liberror-perl all 0.17029-1 [26,5 kB]
Get:2 http://uy.archive.ubuntu.com/ubuntu focal-updates/main amd64 git-man all 1:2.25.1-1ubuntu3.1 [884 kB]
Get:3 http://uy.archive.ubuntu.com/ubuntu focal-updates/main amd64 git amd64 1:2.25.1-1ubuntu3.1 [4.557 kB]
Ign:3 http://uy.archive.ubuntu.com/ubuntu focal-updates/main amd64 git amd64 1:2.25.1-1ubuntu3.1
Get:3 http://security.ubuntu.com/ubuntu focal-updates/main amd64 git amd64 1:2.25.1-1ubuntu3.1 [4.557 kB]
Fetched 5.034 kB in 2min 29s (33,9 kB/s)
Selecting previously unselected package liberror-perl.
(Reading database ... 182825 files and directories currently installed.)
Preparing to unpack .../liberror-perl_0.17029-1_all.deb ...
```

Figura 46 - Descarga e instalación del software de repositorio del sistema

```
juan@juan-VirtualBox:~$ sudo apt install curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libcurl4
The following NEW packages will be installed:
  curl
The following packages will be upgraded:
  libcurl4
1 upgraded, 1 newly installed, 0 to remove and 149 not upgraded.
Need to get 395 kB of archives.
After this operation, 411 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://uy.archive.ubuntu.com/ubuntu focal-updates/main amd64 libcurl4 amd64 7.68.0-1ubuntu2.5 [234 kB]
Get:2 http://uy.archive.ubuntu.com/ubuntu focal-updates/main amd64 curl amd64 7.68.0-1ubuntu2.5 [161 kB]
Fetched 395 kB in 1s (702 kB/s)
(Reading database ... 183760 files and directories currently installed.)
Preparing to unpack .../libcurl4_7.68.0-1ubuntu2.5_amd64.deb ...
Unpacking libcurl4:amd64 (7.68.0-1ubuntu2.5) over (7.68.0-1ubuntu2.4) ...
Selecting previously unselected package curl.
Preparing to unpack .../curl_7.68.0-1ubuntu2.5_amd64.deb ...
Unpacking curl (7.68.0-1ubuntu2.5) ...
Setting up libcurl4:amd64 (7.68.0-1ubuntu2.5) ...
Setting up curl (7.68.0-1ubuntu2.5) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
```

Figura 47 - Instalación de cURL

```

juan@juan-VirtualBox:~$ curl -sSL https://get.docker.com/ | sh
# Executing docker install script, commit: 7cae5f8b0decc17d6571f9f52eb840fbc13b
2737
Warning: the "docker" command appears to already exist on this system.

If you already have Docker installed, this script can cause trouble, which is
why we're displaying this warning and provide the opportunity to cancel the
installation.

If you installed the current Docker package using this script and are using it
again to update Docker, you can safely ignore this message.

You may press Ctrl+C now to abort this script.
+ sleep 20
+ sudo -E sh -c apt-get update -qq >/dev/null
+ sudo -E sh -c DEBIAN_FRONTEND=noninteractive apt-get install -y -qq apt-trans
port-https ca-certificates curl >/dev/null
+ sudo -E sh -c curl -fsSL "https://download.docker.com/linux/ubuntu/gpg" | apt
-key add -qq - >/dev/null
Warning: apt-key output should not be parsed (stdout is not a terminal)
+ sudo -E sh -c echo "deb [arch=amd64] https://download.docker.com/linux/ubuntu
 focal stable" > /etc/apt/sources.list.d/docker.list
+ sudo -E sh -c apt-get update -qq >/dev/null
+ [ -n ]
+ sudo -E sh -c apt-get install -y -qq --no-install-recommends docker-ce >/dev/
null
+ [ -n 1 ]
+ sudo -E sh -c DEBIAN_FRONTEND=noninteractive apt-get install -y -qq docker-ce
juan@juan-VirtualBox:~$ sudo systemctl start docker
juan@juan-VirtualBox:~$ sudo usermod -a -G docker jua

```

Figura 48 - Instalación de Docker

```

juan@juan-VirtualBox:~$ curl -sSL https://bit.ly/2ysb0FE | bash -s

Clone hyperledger/fabric-samples repo

====> Changing directory to fabric-samples
fabric-samples v2.3.2 does not exist, defaulting main

Pull Hyperledger Fabric binaries

====> Downloading version 2.3.2 platform specific fabric binaries
====> Downloading: https://github.com/hyperledger/fabric/releases/download/v2.3.2/hyperledger-fabric-linux-amd64-2.3.2.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100  649    100    649     0     0    935     0  --:--:-- --:--:-- --:--:--    933
100 73.5M   100 73.5M     0     0 5016k     0  0:00:15 0:00:15 --:--:-- 5601k
==> Done.
====> Downloading version 1.5.0 platform specific fabric-ca-client binary
====> Downloading: https://github.com/hyperledger/fabric-ca/releases/download/v1.5.0/hyperledger-fabric-ca-linux-amd64-1.5.0.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100  652    100    652     0     0    846     0  --:--:-- --:--:-- --:--:--    845
100 20.4M   100 20.4M     0     0 4253k     0  0:00:04 0:00:04 --:--:-- 5954k
==> Done.

Pull Hyperledger Fabric docker images

FABRIC_IMAGES: peer orderer ccenv tools baseos
====> Pulling fabric Images
====> hyperledger/fabric-peer:2.3.2
2.3.2: Pulling from hyperledger/fabric-peer
339de151aab4: Pull complete
b4bf7ae190fe: Pull complete
10fe799bdafa: Pull complete
15f2887b5ef0: Pull complete
a13b95531ea2: Pull complete
e7da33d025ba: Pull complete
Digest: sha256:f39281832923fc98695e3aebd998619e4ad3eec5acb861d2636a9be296b519d8
Status: Downloaded newer image for hyperledger/fabric-peer:2.3.2
docker.io/hyperledger/fabric-peer:2.3.2
====> hyperledger/fabric-orderer:2.3.2
2.3.2: Pulling from hyperledger/fabric-orderer
339de151aab4: Already exists
b4bf7ae190fe: Already exists
ed8a60a97f32: Pull complete
449433bcd453: Pull complete
3043f4effeca: Pull complete
9ea245af5804: Pull complete
36869231524e: Pull complete
Digest: sha256:50f2c36e5d11a5ae9b266cf062299e538a0f5e95289b736f3c16108697a7bb13
Status: Downloaded newer image for hyperledger/fabric-orderer:2.3.2
docker.io/hyperledger/fabric-orderer:2.3.2
====> hyperledger/fabric-ccenv:2.3.2
2.3.2: Pulling from hyperledger/fabric-ccenv
801bfaa63ef2: Pull complete
ee0a1ba97153: Pull complete

```

Figura 49 - Instalación de samples, binarios y docker images de Hyperledger Fabric

Anexo VII- Creación de la red Hyperledger Fabric

```
juan@juan-VirtualBox:~/fabric-samples/test-network$ ./network.sh up
Starting nodes with CLI timeout of '5' tries and CLI delay of '3' seconds and u
sing database 'leveldb' with crypto from 'cryptogen'
LOCAL_VERSION=2.3.2
DOCKER_IMAGE_VERSION=2.3.2
/home/juan/fabric-samples/test-network/./bin/cryptogen
Generating certificates using cryptogen tool
Creating Org1 Identities
+ cryptogen generate --config=./organizations/cryptogen/crypto-config-org1.yaml
--output=organizations
org1.example.com
+ res=0
Creating Org2 Identities
+ cryptogen generate --config=./organizations/cryptogen/crypto-config-org2.yaml
--output=organizations
org2.example.com
+ res=0
Creating Orderer Org Identities
+ cryptogen generate --config=./organizations/cryptogen/crypto-config-orderer.y
aml --output=organizations
+ res=0
Generating CCP files for Org1 and Org2
Creating network "fabric_test" with the default driver
Creating volume "docker_orderer.example.com" with default driver
Creating volume "docker_peer0.org1.example.com" with default driver
Creating volume "docker_peer0.org2.example.com" with default driver
Creating orderer.example.com ... done
Creating peer0.org2.example.com ... done
Creating peer0.org1.example.com ... done
Creating cli ... done
CONTAINER ID        IMAGE                                     COMMAND                  CREATED
STATUS            PORTS
NAMES
4e87b79aa794      hyperledger/fabric-tools:latest        "/bin/bash"            1 second
ago              Up Less than a second
cli
f75d9735eda8      hyperledger/fabric-orderer:latest      "orderer"              4 second
s ago           Up 1 second          0.0.0.0:7050->7050/tcp, 0.0.0.0:7053->7053/tcp
orderer.example.com
698b4fe59a74      hyperledger/fabric-peer:latest         "peer node start"      4 second
s ago           Up 2 seconds         0.0.0.0:7051->7051/tcp
peer0.org1.example.com
002a4d916861      hyperledger/fabric-peer:latest         "peer node start"      4 second
s ago           Up 1 second          7051/tcp, 0.0.0.0:9051->9051/tcp
peer0.org2.example.com
```

Figura 50 - Levantamiento de la red

```
juan@juan-VirtualBox:~/fabric-samples/test-network$ ./network.sh createChannel
Creating channel 'mychannel'.
If network is not up, starting nodes with CLI timeout of '5' tries and CLI dela
y of '3' seconds and using database 'leveldb'
Generating genesis block 'mychannel.block'
/home/juan/fabric-samples/test-network/./bin/configtxgen
+ configtxgen -profile TwoOrgsApplicationGenesis -outputBlock ./channel-artifac
ts/mychannel.block -channelID mychannel
2021-05-07 20:44:54.847 -03 [common.tools.configtxgen] main -> INFO 001 Loading
configuration
2021-05-07 20:44:54.874 -03 [common.tools.configtxgen.localconfig] completeInit
ialization -> INFO 002 orderer type: etcdraft
2021-05-07 20:44:54.874 -03 [common.tools.configtxgen.localconfig] completeInit
ialization -> INFO 003 Orderer.EtcdRaft.Options unset, setting to tick_interval
:"500ms" election_tick:10 heartbeat_tick:1 max_inflight_blocks:5 snapshot_inter
val_size:16777216
2021-05-07 20:44:54.874 -03 [common.tools.configtxgen.localconfig] Load -> INFO
004 Loaded configuration: /home/juan/fabric-samples/test-network/configtx/conf
igtx.yaml
2021-05-07 20:44:54.888 -03 [common.tools.configtxgen] doOutputBlock -> INFO 00
5 Generating genesis block
2021-05-07 20:44:54.889 -03 [common.tools.configtxgen] doOutputBlock -> INFO 00
6 Creating application channel genesis block
2021-05-07 20:44:54.889 -03 [common.tools.configtxgen] doOutputBlock -> INFO 00
7 Writing genesis block
+ res=0
Creating channel mychannel
2021-05-07 23:45:06.302 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser an
d orderer connections initialized
2021-05-07 23:45:06.341 UTC [channelCmd] update -> INFO 002 Successfully submit
ted channel update
Anchor peer set for org 'Org2MSP' on channel 'mychannel'
Channel 'mychannel' joined
```

Figura 51 - Creación de un canal en la red

```

juan@juan-VirtualBox:~/fabric-samples/test-network$ sudo ./network.sh deployCC
-ccn basic -ccp ../asset-transfer-basic/chaincode-go -ccl go
[sudo] password for juan:
deploying chaincode on channel 'mychannel'
executing with the following
- CHANNEL_NAME: mychannel
- CC_NAME: basic
- CC_SRC_PATH: ../asset-transfer-basic/chaincode-go
- CC_SRC_LANGUAGE: go
- CC_VERSION: 1.0
- CC_SEQUENCE: 1
- CC_END_POLICY: NA
- CC_COLL_CONFIG: NA
- CC_INIT_FCN: NA
- DELAY: 3
- MAX_RETRY: 5
- VERBOSE: false
Vendoring Go dependencies at ../asset-transfer-basic/chaincode-go
/home/juan/fabric-samples/asset-transfer-basic/chaincode-go /home/juan/fabric-s
amples/test-network
/home/juan/fabric-samples/test-network
Finished vendoring Go dependencies
+ peer lifecycle chaincode package basic.tar.gz --path ../asset-transfer-basic/
chaincode-go --lang golang --label basic_1.0
+ res=0
Chaincode is packaged
Installing chaincode on peer0.org1...
Using organization 1

```

Figura 52 - Despliegue del chaincode

```

+ peer lifecycle chaincode install basic.tar.gz
+ res=0
2021-05-07 20:46:31.400 -03 [cli.lifecycle.chaincode] submitInstallProposal ->
INFO 001 Installed remotely: response:<status:200 payload:"\nJbasic_1.0:0788b09
dbb0681d835dad50a770a6f51aabdf53f0ad5da4135d776ad585ea48d\022\tbasic_1.0" >
2021-05-07 20:46:31.400 -03 [cli.lifecycle.chaincode] submitInstallProposal ->
INFO 002 Chaincode code package identifier: basic_1.0:0788b09dbb0681d835dad50a7
70a6f51aabdf53f0ad5da4135d776ad585ea48d
Chaincode is installed on peer0.org1
Install chaincode on peer0.org2...
Using organization 2
+ peer lifecycle chaincode install basic.tar.gz
+ res=0
2021-05-07 20:46:55.867 -03 [cli.lifecycle.chaincode] submitInstallProposal ->
INFO 001 Installed remotely: response:<status:200 payload:"\nJbasic_1.0:0788b09
dbb0681d835dad50a770a6f51aabdf53f0ad5da4135d776ad585ea48d\022\tbasic_1.0" >
2021-05-07 20:46:55.867 -03 [cli.lifecycle.chaincode] submitInstallProposal ->
INFO 002 Chaincode code package identifier: basic_1.0:0788b09dbb0681d835dad50a7
70a6f51aabdf53f0ad5da4135d776ad585ea48d
Chaincode is installed on peer0.org2
Using organization 1
+ peer lifecycle chaincode queryinstalled
+ res=0
Installed chaincodes on peer:
Package ID: basic_1.0:0788b09dbb0681d835dad50a770a6f51aabdf53f0ad5da4135d776ad5
85ea48d, Label: basic_1.0
Query installed successful on peer0.org1 on channel

```

Figura 53 - Instalación del chaincode en cada peer

```

Anchor peer set for org 'Org1MSP' on channel 'mychannel'
Setting anchor peer for org2...
Using organization 2
Fetching channel config for channel mychannel
Using organization 2
Fetching the most recent configuration block for the channel
+ peer channel fetch config config_block.pb -o orderer.example.com:7050 --ordererTLSHostnameOverride orderer.example.com -c mychannel --tls --cafile /opt/gopath/src/github.com/hyperledger/fabric/peer/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem
2021-05-07 23:45:05.756 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2021-05-07 23:45:05.761 UTC [cli.common] readBlock -> INFO 002 Received block: 1
2021-05-07 23:45:05.761 UTC [channelCmd] Fetch -> INFO 003 Retrieving last config block: 1
2021-05-07 23:45:05.764 UTC [cli.common] readBlock -> INFO 004 Received block: 1
Decoding config block to JSON and isolating config to Org2MSPconfig.json
Checking the commit readiness of the chaincode definition successful on peer0.org1 on channel 'mychannel'
Using organization 2
Checking the commit readiness of the chaincode definition on peer0.org2 on channel 'mychannel'...
Attempting to check the commit readiness of the chaincode definition on peer0.org2, Retry after 3 seconds.
+ peer lifecycle chaincode checkcommitreadiness --channelID mychannel --name basic --version 1.0 --sequence 1 --output json
+ res=0
{
  "approvals": {
    "Org1MSP": true,
    "Org2MSP": false
  }
}
Checking the commit readiness of the chaincode definition successful on peer0.org2 on channel 'mychannel'
Using organization 2
+ peer lifecycle chaincode approveformyorg -o localhost:7050 --ordererTLSHostnameOverride orderer.example.com --tls --cafile /home/juan/fabric-samples/test-network/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem --channelID mychannel --name basic --version 1.0 --package-id basic_1.0:0788b09dbb0681d835dad50a770a6f51aabdf53fad5da4135d776ad585ea48d --sequence 1
+ res=0

```

Figura 54 - Instalación del chaincode - Aprobación MSP Org1

```

2021-05-07 20:47:06.502 -03 [chaincodeCmd] ClientWait -> INFO 001 txid [e334e4a7c28a102c454480a92eac81be5910d197155ed4bf9ef1114d1879c789] committed with status (VALID) at localhost:9051
Chaincode definition approved on peer0.org2 on channel 'mychannel'
Using organization 1
Checking the commit readiness of the chaincode definition on peer0.org1 on channel 'mychannel'...
Attempting to check the commit readiness of the chaincode definition on peer0.org1, Retry after 3 seconds.
+ peer lifecycle chaincode checkcommitreadiness --channelID mychannel --name basic --version 1.0 --sequence 1 --output json
+ res=0
{
  "approvals": {
    "Org1MSP": true,
    "Org2MSP": true
  }
}
Checking the commit readiness of the chaincode definition successful on peer0.org1 on channel 'mychannel'
Using organization 2
Checking the commit readiness of the chaincode definition on peer0.org2 on channel 'mychannel'...
Attempting to check the commit readiness of the chaincode definition on peer0.org2, Retry after 3 seconds.
+ peer lifecycle chaincode checkcommitreadiness --channelID mychannel --name basic --version 1.0 --sequence 1 --output json
+ res=0
{

```

Figura 55 - Instalación del chaincode - Aprobación MSP Org2

Anexo VIII- Ejecución de prueba de operación del sistema Hyperledger Fabric

```
juan@juan-VirtualBox:~/fabric-samples/test-network$ export PATH=${PWD}/../bin:$
PATH
juan@juan-VirtualBox:~/fabric-samples/test-network$ export FABRIC_CFG_PATH=$PWD
/./config/
juan@juan-VirtualBox:~/fabric-samples/test-network$
juan@juan-VirtualBox:~/fabric-samples/test-network$ export CORE_PEER_TLS_ENABLE
D=true
juan@juan-VirtualBox:~/fabric-samples/test-network$ export CORE_PEER_LOCALMSPID
="Org1MSP"
juan@juan-VirtualBox:~/fabric-samples/test-network$ export CORE_PEER_TLS_ROOTCE
RT_FILE=${PWD}/organizations/peerOrganizations/org1.example.com/peers/peer0.org
1.example.com/tls/ca.crt
juan@juan-VirtualBox:~/fabric-samples/test-network$ export CORE_PEER_MSPCONFIGP
ATH=${PWD}/organizations/peerOrganizations/org1.example.com/users/Admin@org1.ex
ample.com/msp
juan@juan-VirtualBox:~/fabric-samples/test-network$ export CORE_PEER_ADDRESS=lo
calhost:7051
```

Figura 56 - Establecimiento de peer0.org1 para operar

```
juan@juan-VirtualBox:~/fabric-samples/test-network$ peer chaincode invoke -o lo
calhost:7050 --ordererTLSHostnameOverride orderer.example.com --tls --cafile $(
PWD)/organizations/ordererOrganizations/example.com/orderers/orderer.example.co
m/msp/tlscacerts/tlsca.example.com-cert.pem -C mychannel -n basic --peerAddress
es localhost:7051 --tlsRootCertFiles $(PWD)/organizations/peerOrganizations/org
1.example.com/peers/peer0.org1.example.com/tls/ca.crt --peerAddresses localhost
:9051 --tlsRootCertFiles $(PWD)/organizations/peerOrganizations/org2.example.co
m/peers/peer0.org2.example.com/tls/ca.crt -c '{"function":"InitLedger","Args":[
]}'
2021-05-07 20:54:25.196 -03 [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 C
haincode invoke successful. result: status:200
```

Figura 57 - Inicialización de estados de los activos

```
juan@juan-VirtualBox:~/fabric-samples/test-network$ peer chaincode query -C myc
hannel -n basic -c '{"Args":["GetAllAssets"]}'
[{"ID":"asset1","color":"blue","size":5,"owner":"Tomoko","appraisedValue":300},
{"ID":"asset2","color":"red","size":5,"owner":"Brad","appraisedValue":400},{"ID
":"asset3","color":"green","size":10,"owner":"Jin Soo","appraisedValue":500},{"
ID":"asset4","color":"yellow","size":10,"owner":"Max","appraisedValue":600},{"I
D":"asset5","color":"black","size":15,"owner":"Adriana","appraisedValue":700},{
"ID":"asset6","color":"white","size":15,"owner":"Michel","appraisedValue":800}]
```

Figura 58 - Visualización del estado de cada activo