UNIVERSIDAD DE LA REPÚBLICA

FACULTAD DE INGENIERÍA

Instituto de Computación - InCo

PROYECTO DE GRADO

Plataformas blockchain y escenarios de uso

Autores:

Mauricio Pereira
Marcos Toscano
Paula Villar

Tutores:

Ing. Javier Barreiro
Ing. Guzmán Llambías

Montevideo, Uruguay
Marzo 2019

Índice

Resumen

En un inicio, la tecnología blockchain estuvo fuertemente asociada a Bitcoin. Hoy en día, es claro que esta tecnología puede ser de gran utilidad para otros contextos de aplicación. A su vez, distintas implementaciones ya se encuentran disponibles, cada una de ellas buscando optimizar diferentes aspectos funcionales o no funcionales.

Los problemas que promete resolver y la idea innovadora detrás de blockchain, han despertado interés en diferentes sectores de la sociedad. Sin embargo, la complejidad intrínseca y el dinamismo característico de esta tecnología, aún relativamente nueva, se presentan como obstáculos a la hora de decidir si blockchain es solución a un problema a resolver y en caso de serlo, qué implementación resulta apropiada para su construcción.

En este proyecto se analizan cincuenta y un plataformas de blockchain, y se realizan pruebas de concepto sobre Hyperledger Fabric, Corda y NEM. Además, se identifican y estudian más de treinta escenarios de negocio e implementaciones que utilizan o proponen la utilización de blockchain, clasificados en ocho grandes áreas de aplicación. El conocimiento adquirido en este proceso, permitió obtener como resultado una taxonomía que clasifica plataformas blockchain según veintidós características, constituyendo el principal aporte del proyecto, así como también un procedimiento que, utilizando la taxonomía, permite determinar un conjunto de plataformas de blockchain a utilizar para la implementación de un escenario dado.

Se realizan cinco tareas de validación de la taxonomía definida que permiten verificar su pertinencia y utilidad en función de los objetivos planteados. Las tareas de validación realizadas son: aplicación del procedimiento de selección de plataformas a doce escenarios de negocio, estudio de estándares y taxonomías existentes, contacto con expertos, análisis de proyectos de estudiantes de Facultad de Ingeniería, Udelar e implementación de un escenario. Esta última tarea, consiste en el diseño e implementación de un escenario de trazabilidad de productos lácteos, utilizando herramientas provistas por la plataforma NEM; lo que permite no solo validar la taxonomía, sino mostrar un caso de uso en dónde se utiliza blockchain para la auditabilidad de procesos y trazabilidad en cadenas de suministro.

Palabras clave: Blockchain, Plataforma Blockchain, Taxonomía, Corda, Hyperledger Fabric, NEM.

1. Introducción

Blockchain adquirió popularidad tras la publicación del artículo: “Bitcoin a peer-to-peer electronic cash system” [1] en el año 2008. Desde entonces, esta tecnología es utilizada principalmente para la implementación de sistemas de dinero electrónico basados en criptomonedas. De todos modos, desde la publicación del artículo de Bitcoin, se ha puesto especial interés en blockchain y cómo puede aprovecharse en diferentes áreas de negocio; siendo tema central en los principales eventos de tecnología del mundo, de particular interés para diferentes organizaciones y objeto de estudio para la academia. Los esfuerzos relativos a esto provienen principalmente de organizaciones, como son bancos, gobiernos, y empresas de tecnología y no tanto de emprendimientos o propuestas individuales como se menciona en el artículo “Evolution of blockchain technology” publicado por Deloitte Insights [2].

El creciente interés por la tecnología en cuestión y su potencial de brindar confianza en ambientes donde los participantes no necesariamente confían entre sí, ha motivado a diferentes empresas, organizaciones, y gobiernos de todas partes del mundo a incluir blockchain como parte de la solución a problemas existentes. Esto, a su vez, ha impulsado el desarrollo de diferentes herramientas que asistan en el desarrollo de aplicaciones distribuidas que utilizan blockchain, es decir, plataformas de blockchain.

La complejidad que caracteriza a la tecnología en cuestión, dificulta en algunos casos la adopción de la misma o lleva a la elaboración de conceptos erróneos, incluso y en particular debido a su gran popularidad, motiva el planteo de soluciones que sugieren la utilización de blockchain en escenarios en donde su aplicación no resulta justificada. Por estos motivos, se han desarrollado artículos y propuestas que asisten en el proceso de determinar cuándo es útil utilizar una blockchain y cuando no [3] [4].

Existen hoy en día más de cincuenta plataformas de blockchain, muchas de las cuales difieren significativamente en sus características tecnológicas así como también en su grado de madurez. Si bien hay mecanismos que dan soporte a la toma de decisiones respecto a la utilización de la tecnología blockchain para la resolución de problemas o escenarios particulares, una vez determinado que es conveniente utilizar una blockchain es necesario definir cuál de las más de medio centenar de plataformas se adapta mejor a las necesidades propias de la solución a implementar. Actualmente, se encuentran en

desarrollo estándares y propuestas de clasificación de plataformas de blockchain que resulten de utilidad para la definición de qué plataforma utilizar, pero aún no han sido publicadas o abarcan aspectos específicos de las mismas, lo cual resalta la oportunidad y pertinencia de este proyecto.

La motivación principal del proyecto es proporcionar un mecanismo para clasificar plataformas blockchain y un procedimiento que permita, dado un escenario de negocio, obtener un conjunto de plataformas posibles para su implementación. De esta forma, se pretende proveer una herramienta que asista en el proceso de diseño e implementación de una solución que utilice blockchain.

1.1 Objetivos

El objetivo del proyecto es identificar, catalogar y analizar distintas plataformas basadas en la tecnología blockchain, poniendo foco en relacionar estas plataformas con los escenarios de negocio que mejor resuelvan. Para ello, se plantea un conjunto de objetivos específicos:

- Estudiar las principales características de la tecnología blockchain.
- Identificar y catalogar diferentes plataformas de blockchain.
- Identificar escenarios de uso/negocio donde estas plataformas aportan valor.
- Realizar un estudio de beneficios y oportunidades de mejora en cada plataforma en escenarios identificados.
- Diseñar y construir una taxonomía que permita clasificar las plataformas analizadas en función de sus características principales.
- Elaborar un procedimiento que permita mediante la utilización de la taxonomía y dado un escenario de uso/negocio específico, obtener un conjunto de plataformas de blockchain sugeridas para su implementación.
- Implementar prototipos en escenarios seleccionados.

2. Marco conceptual

En este capítulo se presentan los conceptos principales utilizados en el transcurso del proyecto. Se describe el proceso realizado para obtener las definiciones utilizadas y las razones que motivan a la especificación de las mismas.

2.1 Blockchain

Durante el proceso de investigación respecto al estado actual de la tecnología, se analizan las definiciones de blockchain existentes, identificando diferencias significativas entre cada una de ellas. Por estas razones, se construye una definición de blockchain, basada en los conceptos relevados, que contempla todos los aspectos de interés a ser utilizados para la realización del proyecto.

Para el diccionario de Oxford, una blockchain es: “un sistema en el cual un registro de transacciones de bitcoins u otras criptomonedas es mantenido en varias computadoras enlazadas entre sí en una red peer-to-peer” [5]. Si se analiza esta definición, la misma incorpora el concepto de red P2P, pero no aplica totalmente a este proyecto debido a que se enfoca únicamente en transacciones de criptomonedas.

Según Michael Crosby (Google), Nachiappan (Yahoo), Pradhan Pattanayak (Yahoo), Sanjeev Verma (Samsung Research America), Vignesh Kalyanaraman (Fairchild Semiconductor), una blockchain es: “esencialmente una base de datos distribuida de registros o libro mayor[1] de transacciones o eventos que hayan sido ejecutados y compartidos entre participantes. Cada transacción en el libro mayor es verificada por consenso de la mayoría de los participantes en el sistema. Una vez que la información es ingresada en el sistema, no puede ser nunca eliminada” [6]. En esta definición se incorporan conceptos clave tales como “base de datos distribuida” o “libro mayor”, además de la idea de información que no puede ser eliminada, así como el concepto de verificar transacciones por consenso. Sin embargo, cuando se menciona el concepto de consenso, se restringe al caso de consenso de la mayoría de participantes en el sistema, lo cual aplica generalmente en blockchains públicas pero no siempre en privadas, clasificación sobre la cual se

[1] Libro mayor: Término utilizado en contabilidad que hace referencia al registro de partidas importantes o globales [7]

profundiza en este informe.

Por otro lado, en el sitio web de Hyperledger, blockchain se define como “libro mayor distribuido en una red *peer-to-peer,* definido fuertemente por el consenso combinado con “smart contracts” y otras tecnologías” [8]. En esta definición, también se mencionan los conceptos de libro mayor, red P2P, y consenso. Si bien también presenta el término contratos inteligentes (definido en la sección 2.3.2), este no aplica a todas las plataformas.

En el libro “Blockchain basics: Introduction to distributed ledgers” de IBM se define que “es un libro mayor digital, distribuido, que registra transacciones en una red peer-to-peer pública o privada. Este libro mayor registra permanentemente los registros/historial de transacciones entre dos nodos, en una cadena secuencial de bloques enlazados mediante hashes criptográficos y se distribuye a todos los nodos de la red. Todas las transacciones confirmadas y validadas son enlazadas entre sí y colocadas en la cadena. La cadena de bloques actúa como una única fuente de verdad, y los miembros de la red solo pueden ver aquellas transacciones que son relevantes para ellos” [9]. Esta definición hace referencia a conceptos como libro mayor, red P2P, hash criptográfico, almacenamiento permanente, única fuente de verdad y la distinción entre redes públicas o privadas. Por otra parte, también menciona que los miembros de la red solo pueden ver transacciones relevantes para ellos, lo cual aplica únicamente a algunas redes privadas. Además, menciona que las transacciones son entre pares, siendo que en algunas plataformas, como Corda [103] por ejemplo, las transacciones pueden incluir a más participantes.

Como puede observarse en las definiciones estudiadas, muchas de ellas son incompletas o no incluyen aspectos relevantes [5][6][8][9] que otras definiciones si lo hacen, o se encuentran orientadas a escenarios de utilización de criptomonedas [5] y no a casos de uso generales. Por ello, se construye la siguiente definición, la cual es utilizada para el desarrollo de todas las etapas del proyecto:

“Una blockchain es un libro mayor, implementado como una base de datos distribuida en una red, la cual puede ser pública o privada. En ella, se almacenan de forma permanente (inmutable) un historial de transacciones mediante la utilización de nodos, los cuales pueden contar con diferentes permisos sobre la red.

La blockchain garantiza la consistencia de los registros almacenados utilizando diferentes mecanismos de validación y consenso, actuando como una única fuente de verdad (canónica).”

Principales características

Existen determinadas características que hacen a blockchain una tecnología prometedora capaz de proporcionar nuevas soluciones a ciertos problemas [10], como las transferencias de dinero internacionales sin una autoridad central que haga de intermediario o la auditabilidad de las cadenas de suministro garantizando su inmutabilidad, por citar algunos de los ejemplos más conocidos. De las características que es posible identificar en la bibliografía se destacan las siguientes [11][12]:

- **Descentralización**: las transacciones en una red de blockchain pueden efectuarse entre pares de la misma sin necesidad de contar con la intervención de una autoridad central.
- **Inmutabilidad**: las transacciones que se intercambian a través de la red atraviesan un proceso de validación, confirmación, y almacenamiento distribuido en diferentes nodos de la red, de tal modo que resulta casi imposible modificar las transacciones almacenadas.
- **Auditabilidad**: consultando las transacciones almacenadas en la blockchain, participantes de la red y/o usuarios de aplicaciones que interactúan con la blockchain pueden verificar y llevar una trazabilidad de registros almacenados.
- **Procedencia**: provee de una forma de trazar el origen de cada transacción.
- **Red P2P**: los nodos participantes se comunican directamente entre sí, sin ninguna entidad ni nodo central o intermediario.
- **Base de datos distribuida**: cada nodo participante tiene acceso a una base de datos distribuida que ningún par individual controla y cualquiera de ellos puede verificarla o regenerarla en caso de ser necesario, sin ningún intermediario central.

2.2 Plataforma blockchain

De modo similar a lo que sucede con el término blockchain, el estudio del estado actual de la tecnología presentó un desafío en cuanto al análisis de este concepto ya que resulta complejo, sin contar con una definición precisa y consensuada, determinar si un producto es una plataforma blockchain o no lo es. Se realiza sin éxito un relevamiento en artículos, diccionarios, revistas y sitios de tecnología, entre otros, en búsqueda de una definición para el concepto en cuestión. Por estas razones, como resultado del estudio del estado actual de la tecnología y comparación preliminar de las soluciones existentes, se construye la siguiente definición de plataforma blockchain, la cual es utilizada para el desarrollo de todas las etapas del proyecto:

"Una plataforma blockchain es un conjunto de herramientas que permiten desarrollar aplicaciones distribuidas que utilizan la tecnología blockchain".

2.3 Terminología relacionada con la tecnología blockchain

A continuación, se definen términos utilizados para la elaboración de la taxonomía y sus aplicaciones, que son característicos de la tecnología blockchain y su comprensión resulta fundamental para el entendimiento del proyecto.

2.3.1 Red P2P

Según Bisconti, para la enciclopedia Salem Press [13], una red P2P (*peer-to-peer*) es un método para compartir archivos a través de internet, constituyendo un tipo específico de una red descentralizada. En este tipo de redes no existe un servidor central, y cada nodo de la red utiliza software especializado para conectarse con el resto de los nodos.

Dentro de las ventajas de la utilización de este tipo de redes se destaca la redundancia. En comparación con estructuras en las cuales existe un servidor central, si un nodo de la red P2P deja de estar disponible, el sistema puede continuar en funcionamiento con el resto de los nodos que se encuentran disponibles. Debido a que uno de los objetivos y características principales de la tecnología blockchain es proveer de una solución en dónde se pueda garantizar confianza a sus participantes, sin contar con una autoridad central que regule el funcionamiento de los sistemas a construir, una red P2P contribuye al cumplimiento de dicho objetivo. Esto se debe principalmente a que en este tipo de redes

todos los pares son iguales y ningún par o grupo de pares es crítico para la salud del sistema [14].

2.3.2 Mecanismos de consenso

El consenso, en términos generales, refiere al acuerdo u opinión de la mayoría respecto a determinado tema. Según la Real Academia Española, es el acuerdo producido por consentimiento entre todos los miembros de un grupo o entre varios grupos [15]. En blockchain, el consenso es el proceso mediante el cual los nodos (distribuidos) de la red llegan a un acuerdo respecto al estado de la cadena de bloques (su histórico y el estado final).

Como se menciona en “Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus” [16], el consenso es el proceso mediante el cual una red de nodos garantiza el orden correcto de las transacciones y valida los bloques que las contienen.

Siempre que exista una propuesta de actualización de la cadena, es necesario llegar a un acuerdo respecto a la legitimidad de dicha actualización entre nodos de la red, utilizando para ello un mecanismo de consenso. Algunos ejemplos de mecanismos de consenso utilizado son prueba de trabajo [17], prueba de participación [18], prueba de importancia [19] y prueba de participación delegada [20].

Las diferencias entre los mecanismos de consenso utilizados en las plataformas de blockchain impactan en un gran número de atributos, como la velocidad a la que se ejecutan las transacciones, la eficiencia energética, la escalabilidad y la capacidad de la plataforma de evitar manipulaciones maliciosas del libro mayor.

2.3.3 Contratos inteligentes

Análogamente a lo mencionado anteriormente en relación con el concepto de blockchain, no existe una definición consensuada respecto a qué es un contrato inteligente. De la bibliografía consultada, se destacan las siguientes definiciones:

En el contexto de blockchain, según Robert Crown en “Back to Blockchains … This Time in the Context of “Smart Contracts”” [21], un contrato inteligente, “es un código destinado a contribuir, verificar o implementar la negociación o realización de un acuerdo; contienen información acerca de los términos del contrato y ejecutan un conjunto de acciones

programadas de forma automática. Permiten realizar transacciones confiables sin la necesidad de contar con un intermediario. Esto es posible ya que estos contratos son trazables e irreversibles en una blockchain". De esta definición, se destaca la idea que un contrato inteligente es un código trazable e irreversible, además del concepto de verificación o implementación de un acuerdo, es decir, una transacción en la cadena.

Por otra parte, en el artículo "Smart Contracts –How will Blockchain Technology Affect Contractual Practices?" [22], se define a un contrato inteligente como "un programa digital, basado en la arquitectura de consenso de blockchain, que se ejecuta automáticamente cuando se cumplen los términos especificados en el contrato. Debido a la estructura descentralizada de estos contratos son a prueba de manipulación". De esta definición se destaca la idea que, un contrato se ejecuta automáticamente cuando se cumplen los términos especificados en el mismo.

En el marco de este proyecto, a partir de las definiciones presentadas, se define contrato inteligente como: *una porción de código trazable e irreversible, que se ejecuta automáticamente cuando se cumplen los términos especificados en el mismo, con el fin de verificar o ejecutar una transacción en la cadena de bloques*.

2.3.4 Minería

Como se menciona en el sitio web oficial de NEM [19], dependiendo de la plataforma, existen diferentes conceptos tales como "mining" o "harvesting", los cuales tienen pequeñas variaciones en cada caso, pero en general, se encuentran asociados al concepto que en este proyecto se menciona como "minería" de bloques. Según [19] la minería es: *"el proceso por el cual se verifican las transacciones que se propone agregar a la cadena de bloques, y se construyen dichos bloques"*

2.3.4 Plataforma NEM: Terminología específica

La plataforma NEM es utilizada en este proyecto para la implementación de un escenario, como mecanismo de validación de la taxonomía definida. En esta sección se presentan los principales conceptos necesarios para la comprensión del capítulo 5.

Cuentas

Las cuentas en NEM pueden conceptualizarse como un contenedor de activos en la cadena de bloques. Una cuenta puede representar, por ejemplo, un depósito de *tokens* o también

un objeto que debe ser único y actualizable (un paquete a enviar, una escritura, etc). Cada cuenta tiene asociada una dirección.

Cuentas de firma múltiple

Este tipo de cuentas, permiten especificar restricciones respecto a las formas en las que se puede compartir, actualizar y transferir su contenido.

Mosaicos

Los mosaicos son activos fijos en la blockchain y representan un conjunto de objetos idénticos que no pueden ser modificados. Estos objetos pueden ser transferibles o no y comúnmente representan *tokens*, acciones, votos, sellos de seguridad, entre otros. Si es posible transferirlos, la transferencia se efectúa mediante una transacción entre cuentas.

Espacio de nombres

Este concepto hace referencia al nombre que recibe un espacio en la blockchain en el cual se almacenan los activos de una organización, individuo o entidad en particular. En la documentación de NEM se compara un espacio de nombres con lo que es un dominio en internet.

Subespacio de nombres

Continuando con la analogía de dominios de internet, un subespacio de nombres es un subdominio de un espacio de nombres en NEM. Por ejemplo si se tiene el espacio de nombres “miempresa” un subespacio de nombre puede ser “sector1.miempresa”.

Transacciones

Como fue mencionado, las transacciones de transferencia se utilizan para enviar mosaicos entre dos cuentas.

Transacciones agregadas

Las transacciones agregadas permiten unir múltiples transacciones en una sola. Cuando todas las cuentas involucradas firman la transacción agregada, se ejecutan al mismo tiempo, las transacciones que la componen.

Xem

Xem es la criptomoneda propia de NEM, utilizada en las transacciones.

2.4 Arquitectura de blockchain

En la presente sección se describen las características técnicas de una blockchain, específicamente sus componentes y las relaciones entre ellos.

Como lo indica su nombre, una blockchain como estructura de datos, es una secuencia de bloques la cual permite almacenar una lista completa de registros de transacciones. Utilizando Bitcoin como ejemplo, y al igual que sucede en una gran cantidad de implementaciones, cada bloque contiene un cabezal en el cual se almacena el *hash* que identifica al bloque anterior de la cadena. Al primer bloque de la cadena comúnmente se le denomina bloque génesis y es el único que no contiene una referencia a un bloque anterior. En la imagen 1 se puede observar un ejemplo de estructura de bloques en donde cada uno contiene el *hash* que identifica al bloque de la cadena anterior, una marca de tiempo, un campo *nonce* utilizado en Bitcoin para el cálculo del *hash* del bloque y la secuencia de transacciones agregadas en el bloque actual. De todos modos, la estructura específica de cada bloque difiere según las diferentes implementaciones y los conceptos que en ellas se utilizan.

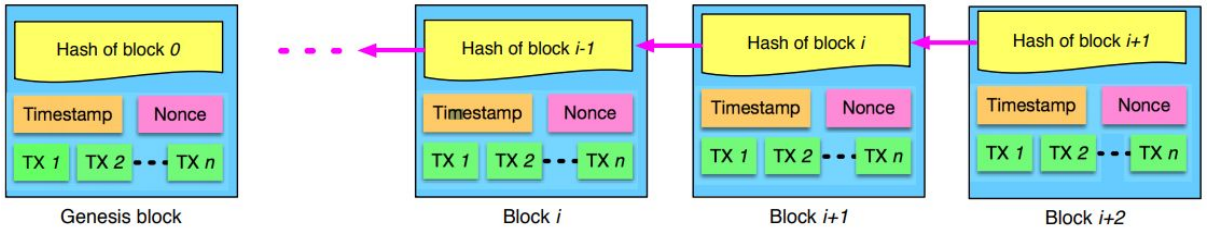


Imagen 1 - Ejemplo de blockchain ilustrada en [11]

En el artículo “Cloud Customer Architecture for Blockchain” [12] se ilustra en alto nivel la estructura de una red blockchain, la cual puede observarse en la imagen 2. En la imagen es posible identificar cinco componentes principales de la arquitectura: los usuarios (*User*) , los nodos (*Node*), la cadena de bloques (*ledger*) y los mecanismos de seguridad (llave) y comunicación utilizados (enlaces).

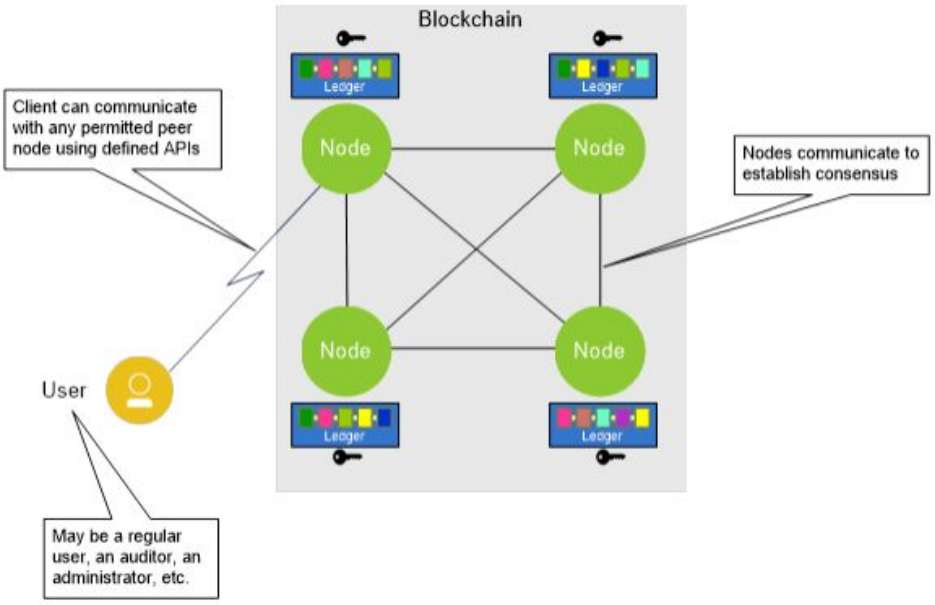


Imagen 2 - Vista en alto nivel de una red blockchain [12]

La cadena de bloques es construida y mantenida en conjunto por los nodos de la red, los cuales almacenan la totalidad o porciones de la cadena localmente, dependiendo esto también de cada implementación particular. Los usuarios (individuos o agentes de software), realizan solicitudes de transacciones, típicamente utilizando APIs, para efectuar diferentes operaciones que el sistema se encuentra diseñado para proveer. Los nodos, se comunican entre sí para verificar la validez de las transacciones y determinar qué bloques son insertados en la cadena. Como se detalla en la sección 2.3, en la red se utiliza lo que se denomina un mecanismo de consenso y hace referencia al mecanismo utilizado por los nodos para determinar qué bloques insertar en la cadena y el orden de los mismos. Una vez que se efectúa una transacción y se registra en un bloque, esta nunca puede ser modificada o eliminada, garantizando la inmutabilidad. En relación a la seguridad, tanto de la información almacenada en la blockchain, como en la comunicación entre nodos, se utiliza criptografía. Mediante la utilización de parejas de claves públicas y privadas se garantiza la integridad de los mensajes intercambiados entre nodos, así como también el hecho que determinadas operaciones sean efectuadas por entidades autorizadas.

Por otra parte, en “A Reference Model for Blockchain-Based Distributed Ledger Technology” [23] de Andreas Ellervee, se propone un modelo de referencia que pretende asistir a analistas de negocio y sistemas, en el desarrollo de nuevas plataformas o implementaciones de la tecnología. Para ello, en dicho artículo, se analizan cuatro plataformas de blockchain, haciendo hincapié en sus propiedades a nivel de negocio

identificando los siguientes componentes: actores, roles, servicios, procesos y modelo de datos. El modelo de referencia propuesto por Andreas Ellervee resulta apropiado para la presentación de la arquitectura de una blockchain en este proyecto ya que surge del análisis de plataformas existentes, construyendo un modelo con un alto grado de generalización. Este modelo propone una descripción de la arquitectura que no hace referencia a una implementación en particular, como sucede en otros artículos analizados [11] o disponibles en la bibliografía, que presentan propuestas para la solución de problemas específicos.

En la imagen 3 se presenta el modelo propuesto por Ellervee y en la tabla 1 la descripción de sus componentes.

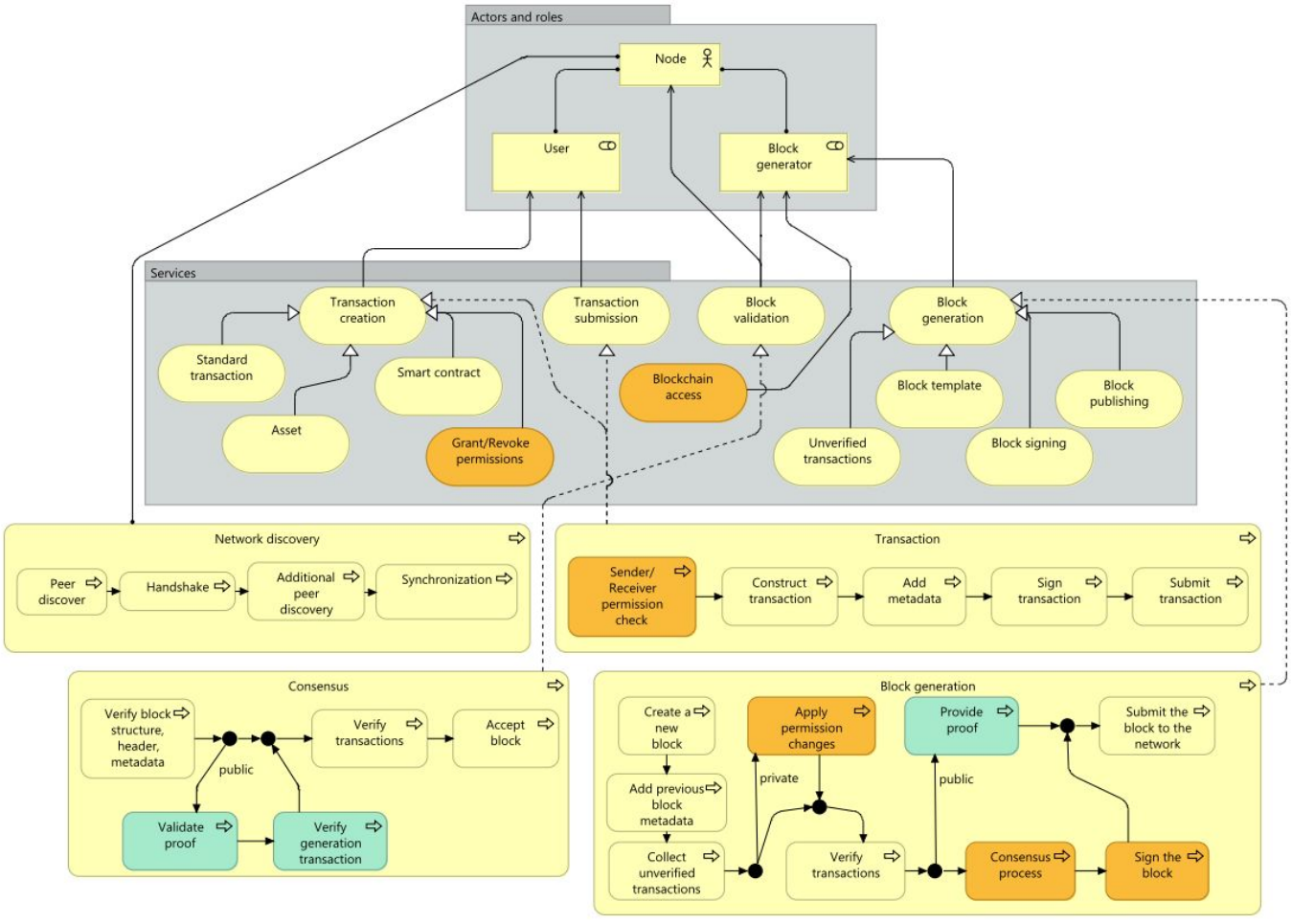


Imagen 3 - Modelo de referencia propuesto por Andreas Ellervee [23]

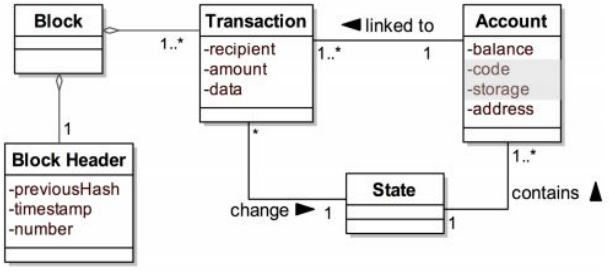
Actores	Desde una perspectiva de negocio se definen dos actores: **Usuarios**: quienes interactúan con la red de nodos realizando transacciones. **Generador de bloques**: responsable de la verificación y validación de transacciones, construcción de nuevos bloques y publicación de bloques en la red.
Servicios	Refiere a los servicios provistos por la red y se definen los siguientes: **Creación de transacciones:** utilizado para que los usuarios puedan agregar información a la blockchain **Envío de transacciones:** este servicio es utilizado para realizar el envío de las transacciones y la firma de las mismas. **Validación de bloques:** servicio utilizado por los nodos para validar y decidir qué bloques se insertan en la cadena **Generación de bloques:** hace referencia al proceso de minería presentado en la sección 2.3 En la imagen 3, en color naranja, se destacan servicios específicos utilizados en redes privadas, concepto sobre el cual se profundiza más adelante.
Procesos	Refiere a los procesos que se ejecutan en este tipo de aplicaciones, en el modelo de referencia se proponen cuatro: **Descubrimiento de la red:** Permite a los nodos que ingresan a la red conectarse a los pares existentes y conocer la red. **Crear y enviar transacciones a la red:** Proceso de crear una transacción con sus metadatos, firmarla y enviarla a la red para su posterior validación **Consenso**: como fue mencionado y se profundiza en la sección 2.3 hace referencia al mecanismo utilizado por los nodos para determinar qué bloques insertar en la cadena y el orden de los mismos. **Generación de bloques**: Refiere al proceso asociado al servicio de generación de bloques presentado. En la imagen 3 es posible observar los componentes propuestos en el marco de referencia.
Modelo de datos	El modelo de referencia propone un modelo de datos basado en el modelo de dominio propuesto por la plataforma de blockchain Ethereum. Describe los bloques, como estos se componen de transacciones y su relación con las cuentas (en el contexto de blockchain típicamente refiere a un contenedor de los recursos, no necesariamente criptomonedas, de un usuario de la red condicionando su posibilidad de efectuar transacciones). 

Tabla 1 - Componentes del modelo de referencia propuesto por Andreas Ellervee [23]

2.4.1 Arquitectura de soluciones que utilizan blockchain

El objetivo de esta sección es presentar cómo se utiliza una blockchain en una solución en particular y qué rol ocupa en la arquitectura de este tipo de sistemas; para ello se analizan las propuestas de Cloud Standards Customer Council de OMG [12], IBM [24] y cómo proponen integrar blockchain a sus soluciones Microsoft Azure [25] y Amazon Web Services [26].

En términos generales, en este tipo de soluciones, se utiliza una blockchain para registrar transacciones mediante la utilización de una API (correspondiente al servicio de creación de transacciones presentado en esta sección) desde una aplicación cliente, así como también realizar consultas sobre los registros almacenados en la blockchain.

En el artículo Cloud Customer Architecture for Blockchain [12] se presenta un modelo general, similar al propuesto por IBM, siendo incluso los principales contribuyentes del artículo disponible en [12] integrantes del equipo de IBM. Sin embargo, la arquitectura de referencia propuesta en Cloud Customer Architecture no hace referencia a un escenario o plataforma de blockchain en particular, especificando los componentes de la misma de forma genérica.

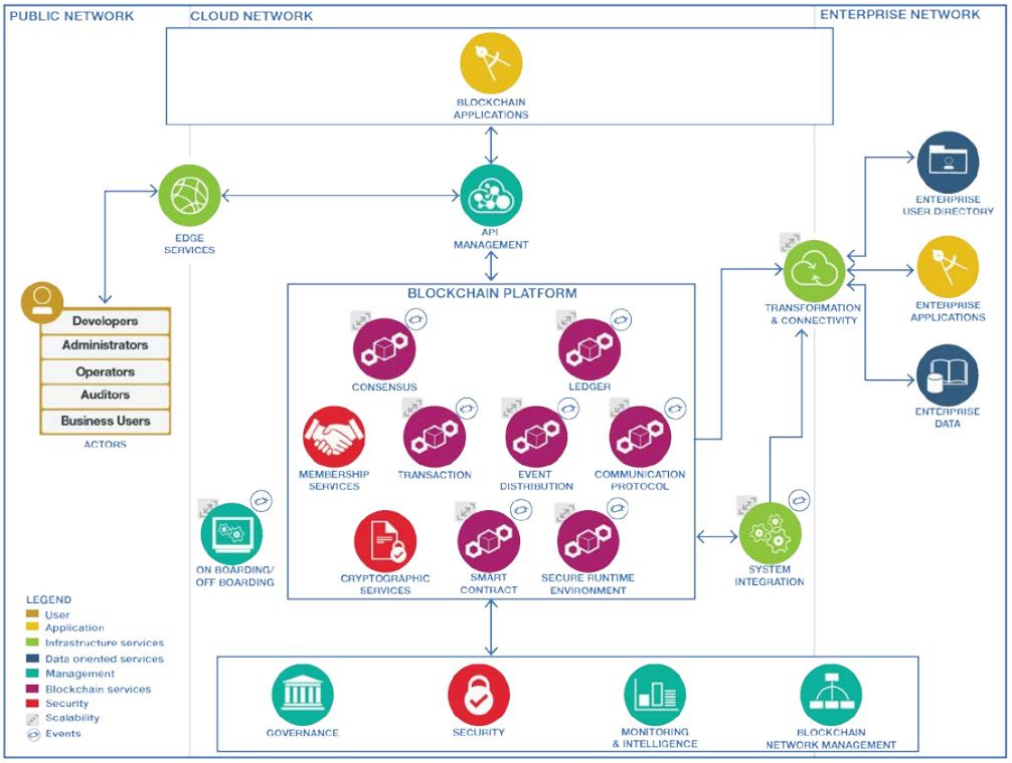


Imagen 4 - Arquitectura de referencia propuesta por el Cloud Standards Customer Council de OMG [12]

Esta propuesta organiza las diferentes prestaciones en función de la red en la cual se ubican: red pública, nube y red empresarial. Sin embargo, se menciona que cada uno de los componentes pueden ubicarse en las diferentes redes en función de las necesidades así como también, si bien se recomienda la utilización de computación en la nube para dar soporte a la plataforma de blockchain y sus servicios, este no es un requisito excluyente.

En la tabla 2 se presentan los componentes ilustrados en la imagen 4 y sus respectivos roles.

Usuarios	Refiere a quienes crean, distribuyen y mantienen aplicaciones así como también quienes realizan operaciones utilizando la blockchain. Comprende desarrolladores, administradores de la red de blockchain, equipo de operaciones, auditores y usuarios finales de las aplicaciones desarrolladas.
Servicio de borde	Refiere a los servicios de borde típicos: firewalls, balanceadores de carga, servidores DNS, etc.
Aplicaciones blockchain	Son las aplicaciones construidas que utilizan la blockchain y se comunican con esta mediante las APIs provistas por cada plataforma.

Administración de las APIs	Es el componente que publica los catálogos de servicios y actualiza las APIs utilizadas por las aplicaciones para comunicarse con la blockchain, en los diferentes entornos de despliegue.
Plataforma blockchain	Como fue mencionado, refiere al conjunto de herramientas que permiten el desarrollo de aplicaciones que utilizan blockchain. Como se menciona en este informe, una plataforma blockchain cuenta con procesos o mecanismos de consenso, el libro mayor, servicios que permiten gestionar el control de acceso y manejo de identidad en la red, protocolos de comunicación, servicios criptográficos, etc. Cada plataforma puede implementar estos componentes de forma diferente como se verá más adelante.
Integración con otros sistemas	La plataforma blockchain puede integrarse con sistemas empresariales existentes utilizando para ello APIs o ESBs.
Transformación y conectividad	Permite establecer conexiones seguras con sistemas empresariales existentes así como también filtrar, agregar o modificar datos o su formato para la comunicación de los componentes de la blockchain y los sistemas empresariales.
Gobernanza	Refiere a procedimientos y políticas que gobiernan la operativa de la red blockchain
Seguridad	Políticas de seguridad y estándares definidos para garantizar la seguridad de la plataforma blockchain
Monitoreo e inteligencia	Herramientas de análisis, automatización y monitoreo que permiten responder ante cambios en la plataforma y el entorno.
Administración de la red blockchain	Componente que provee datos respecto a las operaciones de la blockchain, su performance y métricas relativas a los procesos de negocio.

Tabla 2 - Componentes de la arquitectura de referencia propuesta por el Cloud Standards Customer Council de OMG [12]

La arquitectura de referencia propuesta por IBM se encuentra accesible en [24] y el diagrama de dicha arquitectura se muestra en la imagen 5.

Esta propuesta se encuentra fuertemente relacionada con escenarios de negocio que involucran dinero electrónico ya que asumen que el usuario interactúa con el sistema a través de una aplicación de billetera para su intercambio y es específica para la plataforma de blockchain Hyperledger Fabric.

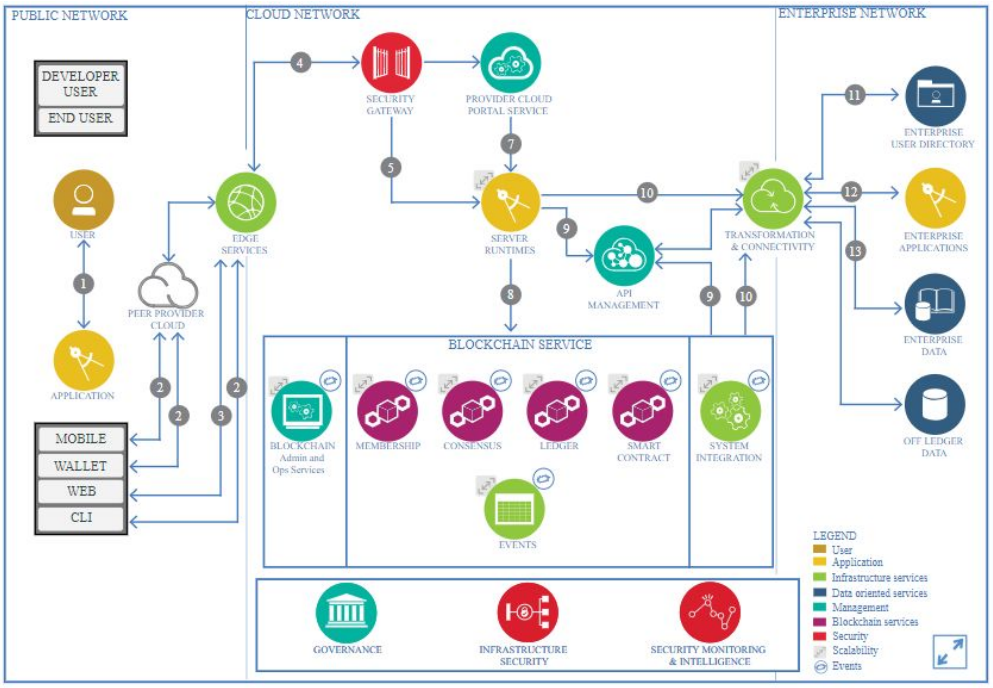


Imagen 5 - Referencia de arquitectura propuesta por IBM [24]

Por otra parte, en [25] y [26] es posible observar la propuesta de arquitectura respecto a la integración de blockchain a los productos y soluciones ofrecidos por Microsoft Azure y Amazon Web Services respectivamente. Si bien los componentes provistos por Microsoft y Amazon difieren, en ambas propuestas se destaca la posibilidad de integrar una blockchain con los diferentes productos que proveen, como cualquier otro de los componentes disponibles. La comparación de ambas soluciones queda por fuera del alcance del proyecto.

2.5 Casos de aplicación

Hasta el momento, se presentan los conceptos básicos para comprender qué es una blockchain, su arquitectura y componentes y cómo estos pueden diferir según las diferentes plataformas. Como fue mencionado, uno de los objetivos del proyecto es determinar y analizar escenarios en lo cuales la utilización de una blockchain resulta pertinente para brindar una solución a un problema particular. A modo introductorio, en esta sección se presenta un análisis de los esfuerzos realizados por diferentes organizaciones para la implementación de soluciones utilizando blockchain con el objetivo de ilustrar qué tipo de problemas esta tecnología puede y pretende resolver. En el Anexo 2 se presentan ejemplos de casos de uso concretos.

Según un estudio realizado por Deloitte Insights en noviembre de 2017 [2], en GitHub, existían al momento 86034 proyectos que utilizan blockchain pero solo un 8% se encontraban activos. Varios de estos proyectos corresponden a la creación de plataformas que permitan desarrollar aplicaciones utilizando blockchain.

IBM es una de las organizaciones que se ha dedicado a realizar acuerdos con diferentes compañías e implementar casos de uso que utilicen la tecnología blockchain. Ejemplo de ello es su asociación con Walmart, empresa con la cual se encuentran desarrollando un prototipo que permita rastrear el origen de los alimentos que se venden en la cadena de supermercados de forma transparente, con el objetivo de garantizar la seguridad de los mismos a los consumidores [27][28]. Otro ejemplo, es el resultado de su asociación con Hejia, con quienes desarrollaron una red basada en blockchain entre proveedores del mercado farmacéutico, sistema que se encuentra actualmente en producción. Además, IBM cuenta con un acuerdo con la Food and Drug Administration (FDA) con quienes planifican comenzar a realizar un proyecto para garantizar el intercambio seguro de registros de salud [27][29] y con “Energy Blockchain Labs” con el objetivo de utilizar blockchain para hacer más eficiente la generación de insumos de carbono reduciendo su impacto en el medio ambiente [27][30].

Las instituciones financieras también han demostrado especial interés por la tecnología en cuestión. A modo de ejemplo, J.P Morgan lanzó en Octubre de 2017 una red basada en blockchain para el procesamiento de pagos. El sistema fue construido utilizando Quorum, plataforma desarrollada por J.P Morgan utilizando Ethereum [31]. Otra de las implementaciones existentes relativas a este rubro son TEMPO Money Transfer [32], Bank innovation [33] y Guild One [34][35] que permiten realizar transferencias de criptomonedas, pagos de poco valor monetario como alternativa a las tarjetas de crédito y pagos de regalías respectivamente. Se profundiza sobre estos casos de aplicación en siguientes secciones así como también se analizan implementaciones relativas a la filantropía (donaciones), la industria del entretenimiento (juegos y apuestas) y sistemas de validación (identidad, voto electrónico y diplomas universitarios), entre otros.

2.6 Trabajo relacionado

Durante el desarrollo del proyecto, se identifican y estudian diferentes artículos y publicaciones de trabajos que apuntan a objetivos similares tales como otras clasificaciones,

estándares y taxonomías. Las referencias a los trabajos estudiados y su análisis se detallan en la sección 4.2 de este informe.

Al ser blockchain una tecnología relativamente nueva, en general, los trabajos encontrados al respecto son muy recientes o están en pleno desarrollo. En particular, los artículos que definen una clasificación de plataformas lo hacen a partir de la selección de un subconjunto reducido de ellas, sin especificar una clasificación genérica que aplique a todo tipo de plataformas existentes.

Existen varias instituciones y entidades encargadas de la creación de estándares tales como la ISO, IEEE, W3C, Administración de estándares de China y Standards Australia que se encuentran actualmente trabajando para estandarizar aspectos básicos como terminología y formatos de datos a utilizarse en tecnologías relacionadas a blockchain, sin embargo, estos trabajos tienen fechas previstas de finalización que van hasta el año 2022.

En términos generales, como resultado del análisis mencionado, es posible concluir que si bien existen propuestas de estándares y taxonomías que proponen clasificaciones de plataformas de blockchain, existe cierto grado de heterogeneidad en los artículos. No es posible encontrar un estándar claro en cuanto a cuáles son las características más importantes en una plataforma; lo cual, como fue mencionado, constituye uno de los objetivos principales de este proyecto y destaca su pertinencia.

3. Desarrollo de la taxonomía

En el presente capítulo se presenta uno de los aportes centrales del proyecto: una taxonomía que permite clasificar plataformas blockchain, con el objetivo de dar soporte a la toma de decisiones respecto a qué plataforma utilizar a la hora de implementar un proyecto que involucre la tecnología blockchain. Para ello, se describe la metodología utilizada para definir y validar la taxonomía así como también la especificación de las características de la misma. Este trabajo se encuentra orientado a un público de carácter técnico, es decir, se pretende que la taxonomía a describir sea utilizada por profesionales del área de las tecnologías de la información.

3.1 Metodología

Debido a que no se encuentra una metodología de referencia para la definición de una taxonomía en este contexto, se define la propia, la cual se presenta en esta sección y es utilizada para la elaboración de la taxonomía.

La definición de la taxonomía se construye en base al estudio de las plataformas de blockchain existentes y propuestas académicas de clasificación de las mismas. Para llegar al estado actual de la taxonomía, se realizan distintas etapas, iterando sobre ellas a lo largo del proyecto.

En primer lugar se realiza un estudio del estado actual de la tecnología, así como también la identificación de escenarios de negocio en donde se propone la utilización de blockchain para resolver determinados problemas como la trazabilidad, transparencia, garantizar la inmutabilidad, entre otros.

Luego de identificar un conjunto de plataformas, sus principales características y los escenarios de negocio en los cuales son utilizadas, se procede a realizar pruebas de concepto sobre tres plataformas seleccionadas con el objetivo de profundizar sobre sus similitudes, las características que las diferencian y su curva de aprendizaje, por mencionar algunos ejemplos.

Una vez realizados los pasos mencionados, recolectando a través de los mismos las características que permiten clasificar a las plataformas, se procede a definir la taxonomía.

El último paso de la metodología realizada consiste en validar la taxonomía construida, para ello se verifica que cumpla con el objetivo de poder clasificar plataformas así como también que se encuentre en la misma línea respecto a trabajos similares existentes.

La metodología propuesta resulta en un proceso de cinco etapas el cual se resume en la imagen 6 y es detallado a continuación.

Imagen 6 - Metodología utilizada para definición y validación de la taxonomía

3.1.1 Estudio del estado de la tecnología e identificación de escenarios de negocio

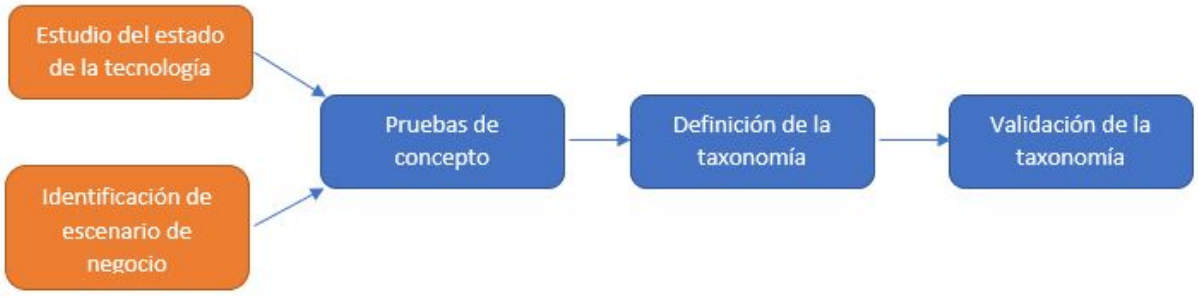


Imagen 7 - Estudio del estado de la tecnología e identificación de escenarios de negocio

Como primer paso, se estudia el estado del arte, es decir, el estado actual de las tecnologías relacionadas a blockchain, lo cual implica un relevamiento inicial sobre las aplicaciones y plataformas de blockchain existentes, la identificación de características y conceptos generales, con el objetivo de evaluar su relevancia y el impacto que estas tienen a la hora de seleccionar una plataforma. Además, se estudian diferentes formas de clasificar plataformas.

En esta etapa se identifican y analizan más de cincuenta plataformas de blockchain (ver “Plataformas relevadas” en el Anexo 1) para las cuales se identifican sus características principales. Dichas características, junto a las sugerencias de los tutores y aquellas

destacadas a partir de los conocimientos preliminares adquiridos acerca de la temática, son utilizadas como base para establecer una clasificación inicial o primera versión de la taxonomía. De las plataformas identificadas se descartan aquellas cuya documentación es muy limitada o inexistente. De las restantes, se identifican los valores de sus características en función de la clasificación definida y se ordenan según su popularidad, medida en base a la cantidad de estrellas en sus respectivos repositorios en GitHub así como también teniendo en cuenta su presencia en la comunidad como ser foros, redes sociales, proyectos implementados con dichas tecnologías y propuestas de las principales compañías y organizaciones de la industria y academia.

De las plataformas identificadas, se seleccionan siete de ellas para ser estudiadas en mayor profundidad. Esta selección se realiza en base a la popularidad de cada plataforma, el nivel de soporte y documentación brindado, y además buscando heterogeneidad entre las mismas, es decir, que difieran en las características relevadas. En una primera instancia se seleccionan Ethereum, Corda e Hyperledger Fabric para dicho estudio.

En iteraciones siguientes se agregan más plataformas al conjunto de las estudiadas con mayor profundidad, más precisamente EOS, Cardano, Stellar y NEM, lo cual implica la necesidad de modificar las características de plataformas seleccionadas como más relevantes así como también agrupar algunas características relacionadas entre sí, como por ejemplo aquellas relacionadas al desempeño, en un mismo grupo.

Por otra parte, se investigan áreas en las cuales es posible implementar proyectos utilizando blockchain, especificando para cada una de ellas ejemplos de casos de uso particulares que la tecnología en cuestión puede resolver. Las áreas identificadas para el análisis son: salud, gobierno, cadenas de suministro, arte, filantropía, identidad, sector financiero, juegos y apuestas, bolsa de trabajo y redes sociales; dicho análisis se encuentra especificado en el Anexo 2. Los requisitos particulares de los escenarios de negocio, como puede ser la necesidad de contar con mecanismos de control de acceso o restringir el acceso al libro mayor a determinados participantes, contribuyen a la identificación de características de las plataformas a tener en cuenta para su clasificación.

El estudio realizado en esta etapa se resume en la imagen 8. En la tabla 3 se detallan sus entradas y salidas.

Entradas del proceso	Salidas del proceso
Documentación oficial de las plataformas identificadas, conjunto de escenarios de negocio en los cuáles se utiliza o propone la utilización de blockchain	Clasificación inicial de plataformas

Tabla 3 - Entradas y salidas del estudio del estado de la tecnología e identificación de escenarios de negocio

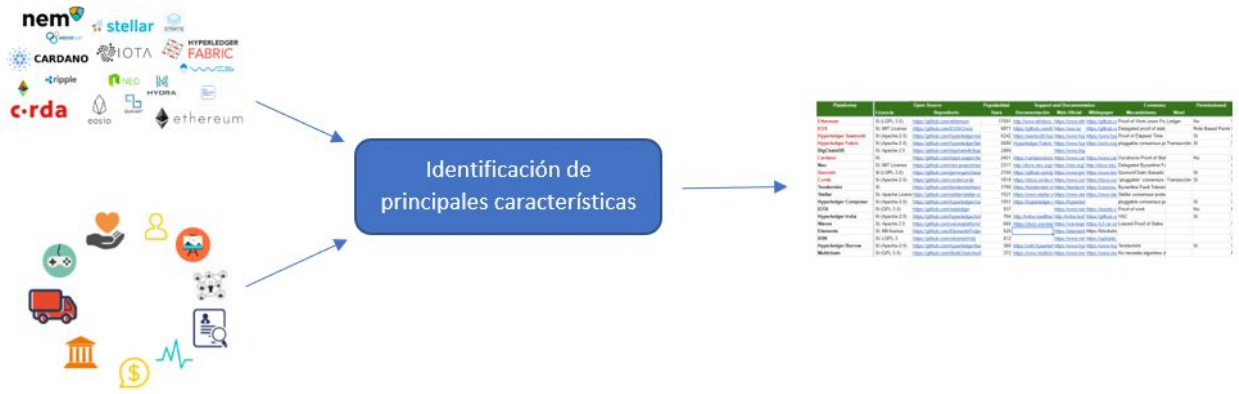


Imagen 8 - Etapa “estudio actual de la tecnología e identificación de escenarios de negocio”

En la imagen 9 es posible observar algunas de las plataformas y características de la clasificación inicial de plataformas. Esta clasificación incluye cincuenta y dos plataformas para las cuales se identifican treinta y dos características, entre ellas si la plataforma es de código abierto o no, si es permisionada, si cuenta con contratos inteligentes, si utilizan criptomonedas, el mecanismo de consenso utilizado y enlaces a su documentación y comunidad, entre otros. Como fue mencionado, la tabla con la clasificación se encuentra accesible en el Anexo 6 en donde las columnas contienen las características y las filas las plataformas relevadas. En la imagen 9 se muestra una porción de dicha tabla.

Plataforma	Open Source		Consenso
	Licencia	Repositorio	Mecanimismo
Ethereum	Si (LGPL-3.0)	https://github.com/ethereum	Proof of Work (soon PoS)
Corda	Si (Apache-2.0)	https://github.com/corda/corda	“pluggable” consensus (se puede elegir según necesidad). Verification y Uniqueness
EOS	Si, MIT License	https://github.com/EOSIO/eos	Delegated proof of stake
Hyperledger Fabric	Si (Apache-2.0)	https://github.com/hyperledger/fabric	pluggable consensus protocols
Cardano	Si	https://github.com/input-output-hk/cardano-sl	Ouroboros Proof of Stake https://www.cardano.org/en/ouroboros/
Nem	Si, MIT License	https://github.com/NemProject/nem.core	Proof of Importance
Stellar	Si, Apache Licens	https://github.com/stellar/stellar-core	Stellar consensus protocol (https://www.stellar.org/developers/guides/concepts/scp.html
BigChainDB	Si, Apache 2.0	https://github.com/bigchaindb/bigchaindb	
Neo	Si, MIT License	https://github.com/neo-project/neo	Delegated Byzantine Fault Tolerant
Quorum	Si (LGPL-3.0)	https://github.com/jpmorganchase/quorum	QuorumChain (basado en votación)
Hyperledger Sawtooth	Si (Apache-2.0)	https://github.com/hyperledger/sawtooth-core	Proof of Elapsed Time
Tendermint	Si	https://github.com/tendermint/tendermint	Byzantine-Fault Tolerant
Hyperledger Composer	Si (Apache-2.0)	https://github.com/hyperledger/composer	pluggable consensus protocols

Imagen 9 - Resumen de la clasificación de plataformas relevadas

3.1.2 Pruebas de concepto

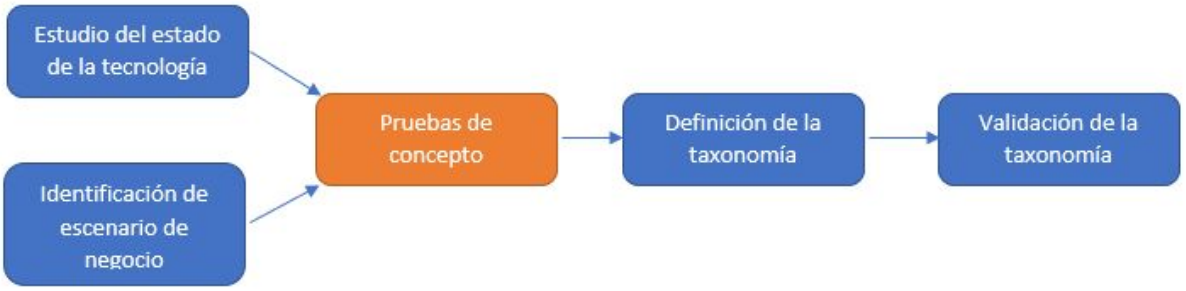


Imagen 10 - Pruebas de concepto

En una segunda etapa del proceso, con el objetivo de conocer en profundidad las implementaciones particulares de las diferentes características relevadas, una vez identificadas y priorizadas las plataformas, se procede a seleccionar un conjunto de tres de ellas para realizar un estudio en mayor profundidad. En este estudio se hace hincapié en los conceptos más relevantes, tales como tipos de nodos, mecanismos de consenso, soporte de contratos inteligentes, entre otros. Se seleccionan Corda, Ethereum e Hyperledger por ser de parte de las siete plataformas más relevantes del conjunto seleccionado, así como también porque se diferencian entre sí respecto a las características relevadas, por ejemplo, cada una utiliza un mecanismo de consenso diferente, y Ethereum es pública mientras que Hyperledger y Corda son privadas. Para estas tres plataformas, se analizan sus características particulares (tipos de nodos, estructura de las transacciones, APIs provistas, por mencionar algunos ejemplos) y se realizan pruebas de concepto, las cuales se detallan en el Anexo 2. Se recomienda su lectura para obtener mayor información acerca de las pruebas de concepto realizadas.

Como resultado de esta etapa, se elabora una nueva versión de la clasificación inicial de plataformas que incluye, por ejemplo, la clasificación por tipo de nodos (oráculo, ordenador, verificador); se eliminan características que no contribuyen a la clasificación, como las URLs a documentación o repositorios y se adquiere mayor conocimiento respecto a conceptos típicos relativos a las plataformas a ser utilizados en la definición de la taxonomía, por ejemplo, el consenso, el control de acceso al libro mayor, entre otros.

Las actividades realizadas en esta etapa se resumen en la imagen 10. En la tabla 4 se detallan sus entradas y salidas.

Entradas del proceso	Salidas del proceso
Clasificación inicial de plataformas	Pruebas de concepto Nueva versión de la clasificación inicial de plataformas

Tabla 4 - Entradas y salidas de las pruebas de concepto

Imagen 11 - Etapa “pruebas de concepto”

3.1.3 Definición de la taxonomía

Imagen 12 - Definición de la taxonomía

Tomando como entrada el resultado de los puntos anteriores, se procede a definir cuáles son las características más relevantes a la hora de seleccionar una plataforma blockchain dado un escenario de uso, para el cual se sepa previamente que es posible utilizar blockchain.

En esta etapa se define la taxonomía, que como fue mencionado, es uno de los puntos centrales del proyecto, y está definida por una tabla, donde cada fila representa una plataforma blockchain, cada columna indica una característica, y cada celda indica el valor de dicha característica para la plataforma correspondiente. La imagen 13 ilustra lo mencionado.

Plataforma	Interoperabilidad		Desempeño		Contratos inteligentes		Manejo de identidad	
	Implícita	Explícita	Tiempo de confirmación	Transacciones por segundo	Turing completos	Verificables	Control de accesso a la red	Identidad
Ethereum	×	✓	3 minutos	15	✓	✓	×	×
Hyperledger Fabric	✓	✓	< 1 segundo	3500+	✓	×	Intercambiable: LDAP, Open Id	✓
Cardano	×	En desarrollo	?	?	✓	✓	N/A	×
Corda	✓	✓	?	1000-1800	✓	×	LDAP, Active directory	✓
Stellar	×	✓	3-5 segundos	1000-10000	×	×	N/A	×
Nem	×	×	20 segundos	3000	N/A	N/A	N/A	✓

Imagen 13 - Estructura de la taxonomía

Si al aplicar la clasificación propuesta en la taxonomía para la plataforma en cuestión no existen datos disponibles, se utiliza un signo de interrogación “?” para indicar que no fue posible encontrar información respecto a la característica analizada. Una “✖” representa que la plataforma no cuenta con el mecanismo o propiedad correspondiente y, contrariamente, el “✔” representa que la plataforma si cuenta con el mecanismo o propiedad.

En esta etapa además, se elabora un documento que define cada una de las características y los posibles valores que puede adoptar.

Si bien se presenta la definición de la taxonomía como etapa posterior a las definidas en las secciones 3.1.1 y 3.1.2, la misma se construye a partir de la clasificación inicial de plataformas realizada en la etapa correspondiente a la sección 3.1.1. Las pruebas de concepto realizadas resultaron de especial utilidad para la definición de la taxonomía ya que generaron la necesidad de modificar la lista de características a tener en cuenta en la taxonomía. Respecto a la clasificación utilizada como punto de partida, se agregan nuevas características, por ejemplo los diferentes tipos de nodos de la red y otras se definen de forma más precisa, como es la característica “control de acceso al libro mayor bajo “Seguridad y privacidad”.

En la tabla 5 se detallan sus entradas y salidas.

Entradas del proceso	Salidas del proceso
Nueva versión de la clasificación inicial de plataformas	Primer versión de la taxonomía (tabla, especificación y definiciones de las características)

Tabla 5 - Entradas y salidas de la definición de la taxonomía

Como fue mencionado, se vuelve analizar la tabla 4 obtenida en la etapa anterior y se busca refinarla para maximizar la utilidad de la misma a la hora de comparar entre diferentes plataformas. Dicho refinamiento implica agrupar características, por ejemplo, los mecanismos de manejo de identidad tanto para acceder a la red como para el acceso al libro mayor; especificar con mayor profundidad otras de las características, por ejemplo, se sustituye la característica “gobernanza” por las características “proveedor” y “gobernanza abierta” así como también se eliminan características que no aportan a la clasificación como por ejemplo el lenguaje de programación en el cual se encuentra implementada la plataforma.

La primer versión de la taxonomía se compone de la tabla resultado del análisis mencionado así como también de un documento con la especificación de las características en dónde se define cada una de ellas y los valores que pueden adoptar.

Imagen 14 - Etapa “Definición de la taxonomía”

3.1.4 Verificación y validación de la taxonomía

Imagen 15 - Validación de la taxonomía

Una vez definida la taxonomía se procede a verificar su pertinencia, utilidad y simplicidad. Para ello, se estudian taxonomías existentes, estándares y se aplica el proceso definido en la sección 3.3 (que dadas las características de una aplicación, retorna un conjunto de

plataformas sugeridas para su implementación) a un conjunto concreto de escenarios de negocio.

En el proceso de validación se obtiene la especificación de un escenario de negocio para su implementación (descripto en el capítulo 5) y la generalización del procedimiento anteriormente mencionado, que oficia como guía a la hora de seleccionar una plataforma blockchain para la implementación de un caso de uso particular, dicho procedimiento se encuentra definido en la sección 3.3 del presente informe.

En la tabla 6 se detallan las entradas y salidas de esta etapa.

Entradas del proceso	Salidas del proceso
Primer versión de la taxonomía, descripción de doce casos de uso que utilizan plataformas blockchain, artículos y propuestas de estándares relacionados con la clasificación de plataformas blockchain, especificación de un escenario de trazabilidad a implementar.	Procedimiento de selección de plataformas dado un escenario de negocio. Especificación de un escenario de negocio para su implementación. Versión final de la taxonomía.

Tabla 6 - Entradas y salidas de la validación de la taxonomía

Con los pasos antes mencionados se verifica la validez de la taxonomía.

3.2 Taxonomía de plataformas blockchain

Como resultado de las tareas de investigación y análisis antes mencionadas se construye una taxonomía que permite clasificar plataformas de blockchain, constituyendo el principal aporte del proyecto.

En esta sección se presentan las características que permiten clasificar a las plataformas blockchain. Como fue mencionado, el objetivo principal de la taxonomía es proveer de un mecanismo que asista en el proceso de selección de una plataforma a la hora de implementar un escenario que utilice blockchain; por estos motivos se propone una clasificación de las características que faciliten dicho proceso. Las clasificación definida se presenta a continuación.

- **Características duras**: permiten clasificar una plataforma para luego contribuir a determinar si dicha plataforma es apropiada para la implementación de un caso de uso particular. Por ejemplo, si en un caso de uso particular se requiere procesar las transacciones en un tiempo menor a un minuto, cualquier plataforma que no cumpla con esta restricción debe ser descartada. En la tabla 7 se listan las características duras.
- **Características blandas**: aportan información adicional de interés acerca de la plataforma, pero no permiten clasificarlas. Estas características son de especial utilidad para diferenciar dos plataformas que clasifican igual según las características duras. Por ejemplo, si una vez vistas todas las características duras, aún queda por decidir entre dos plataformas, se puede optar por la que se considere más madura o por la que sea provista por una organización de confianza. En la tabla 8 se listan las características blandas.

Características duras:

Característica	**Descripción**
Permisionada	Si existen restricciones de ingreso a la red, o si, por el contrario, cualquier nodo que pretenda unirse puede hacerlo.
Interoperabilidad	Capacidad de comunicación con otros sistemas externos a la red.
Desempeño	Tiempo de confirmación de una transacción y cantidad de transacciones que se pueden ejecutar por segundo.
Tolerancia a fallas	Capacidad de continuar funcionando en caso de ocurrir eventos inesperados, garantizando la confiabilidad, validez y seguridad de la información almacenada en el libro mayor.
Contratos inteligentes	Si la plataforma maneja o no el concepto de contratos inteligentes, y en caso de hacerlo se especifica si son turing completos y si son verificables.
Manejo de identidad	Mecanismos de control de acceso a la red, y capacidad de la plataforma de validar organizaciones, atributos o datos de un nodo, que permitan identificarlo de cierta forma.

Seguridad de la información y privacidad	Mecanismos para preservar la confidencialidad, integridad y disponibilidad de la información. Incluye mecanismos de encripción así como de control de acceso al libro mayor. El control de acceso al libro mayor se diferencia del control de acceso a la red en que este último refiere a los mecanismos utilizados para acceder a la infraestructura y el acceso al libro mayor referencia al acceso a los datos almacenados en la cadena de bloques.
Involucra criptomoneda	Si involucra o no una criptomoneda tanto para el intercambio de bienes como incentivo a los mineros o para ejecutar contratos inteligentes.
Consenso	Mecanismos de consenso utilizados (algoritmos) y si es posible intercambiarlos.
Protocolo de comunicación	Protocolo de comunicación utilizado entre los nodos de la red.
Incentivos	Incentivos a los nodos que se encargan de la minería para que validen transacciones.
Despliegue	Mecanismos disponibles para realizar el despliegue de los nodos de la red. Se especifica si se facilita el despliegue en la nube mediante servidores pre-configurados, si se brindan imágenes de Docker o si se tiene otros métodos de despliegue.
Entorno de ejecución	Entorno de ejecución de los nodos tales como la Ethereum Virtual Machine o la Java Virtual Machine.
Tipos de nodos	Si existen nodos con determinados roles específicos en la red.
Costo	Costos monetarios involucrados en la utilización de la plataforma, ya sea por construir una red, por acceder a una API que permite implementar aplicaciones sobre blockchains preexistentes o por ejecutar transacciones.

Tabla 7 - Características duras

Características blandas:

Característica	**Descripción**
Usabilidad	Tipo de API (lenguaje de programación y/o protocolo de comunicación utilizado por la API provista), y existencia de GUI que permita al dueño del nodo interactuar con el mismo.

Áreas de investigación / Proyectos	Referencia de proyectos o áreas de investigación abordados utilizando la plataforma en cuestión.
Soporte y documentación	Si la plataforma es de código abierto o no, si existe documentación técnica accesible en internet, si existe un whitepaper asociado y se cuenta con una comunidad (conjunto de personas que se encuentran utilizando la tecnología y mantienen una plataforma de intercambio accesible tal como Twitter, Slack o GitHub, entre otros).
Madurez	Fecha del primer y último commit.
Bifurcación de	Si la plataforma surge como una bifurcación de otra plataforma existente.
Proveedor	Entidad u organización que provee la plataforma.
Gobernanza abierta	Si la plataforma es gobernada de forma abierta o si es gobernada por una entidad u organización.

Tabla 8 - Características blandas

La especificación en profundidad de las características presentadas y los valores que puede adquirir cada uno de los atributos se especifican en el Anexo 4. Se recomienda su lectura para comprender la clasificación definida.

3.3 Cómo utilizar la taxonomía

En esta sección se presenta cómo utilizar la taxonomía tanto para conocer las principales características de las plataformas más relevantes identificadas y cómo estas se diferencian, así como también para determinar, dadas las características de un escenario de negocio o aplicación, las plataformas apropiadas para su implementación.

3.3.1 Utilización de la taxonomía

Como se menciona en la sección 3.1, la taxonomía se encuentra definida por una tabla donde cada fila representa una plataforma blockchain, cada columna indica una característica, y cada celda indica el valor de dicha característica para la plataforma correspondiente. Para evaluar las características de una plataforma en particular se debe seleccionar la fila correspondiente a la plataforma y las celdas, para cada columna, permiten determinar sus principales características. La tabla se encuentra ordenada de modo que las características duras se ubican en las primeras columnas y las blandas en las últimas. Por ejemplo, si se selecciona la plataforma Corda para su análisis, es posible determinar, como

se indica en la imágen 16, que es permisionada. Además, dispone de mecanismos que permiten la interoperabilidad implícita y explícita, cuenta con la posibilidad de implementar contratos inteligentes (Turing completos) y es posible controlar el acceso a la red utilizando LDAP, así como también la posibilidad de validar organizaciones, atributos o datos de un nodo que permitan identificarlo de cierta forma, entre otros.

Plataforma	Permisionada	Interoperabilidad		Desempeño		Contratos inteligentes		Manejo de identidad	
		Implicita	Explicita	Tiempo de confirmación	Transacciones por segundo	Turing completos	Verificables	Control de accesso a la red	Identidad
Ethereum 3	×	×	✓	3 minutos	15	✓	✓	×	×
EOS	×	×	×	1 segundo	3000+	×	×	×	Si (para los 21 nodos que validan los bloques)
Hyperledger Fabric 1.1.0	✓	✓	✓	< 1 segundo	3500+	✓	×	Intercambiable: LDAP, Open Id	✓
Cardano 1.3	×	×	En desarrollo	?	?	✓	✓	N/A	×
Corda 2.0	✓	✓	✓	?	1000-1800	✓	×	LDAP, Active directory	✓
Stellar 9.2	×	×	✓	3-5 segundos	1000-10000	×	×	N/A	×
Nem 2	Ambas	×	×	20 segundos	3000	N/A	N/A	N/A	✓

Imagen 16 - Análisis plataforma Corda

Como puede verse en la imagen 16, a medida que se analizan las características de una plataforma en particular, es posible compararla con el resto de las plataformas.

Existen celdas de la taxonomía que tienen asociadas notas que especifican en mayor profundidad el valor adquirido para la característica asociada o incluyen referencias a las fuentes para poder profundizar en caso de así desearlo.

3.3.2 Procedimiento de selección de plataformas

Motivación

Para validar la taxonomía, uno de los mecanismos utilizados consiste en seleccionar un conjunto de soluciones existentes que utilizan blockchain y estudiar sus características. Cada una de estas soluciones es implementada utilizando una plataforma en particular y el objetivo del análisis en cuestión es verificar que, para cada uno de los escenarios, dadas sus características, la taxonomía sugiere la plataforma con la cual dicho escenario fue implementado. Los mecanismos de validación de la taxonomía se especifican en profundidad en el capítulo 4 del presente informe.

El análisis mencionado motiva la definición de un procedimiento que permita obtener plataformas sugeridas para futuros escenarios planteados. Para ello, se generalizan los pasos realizados al validar la taxonomía para los doce escenarios, obteniendo como

resultado un procedimiento que, dada una idea, implementación o escenario de negocio, permita determinar un conjunto de plataformas de blockchain para su implementación.

Procedimiento

El siguiente diagrama ilustra el proceso definido:

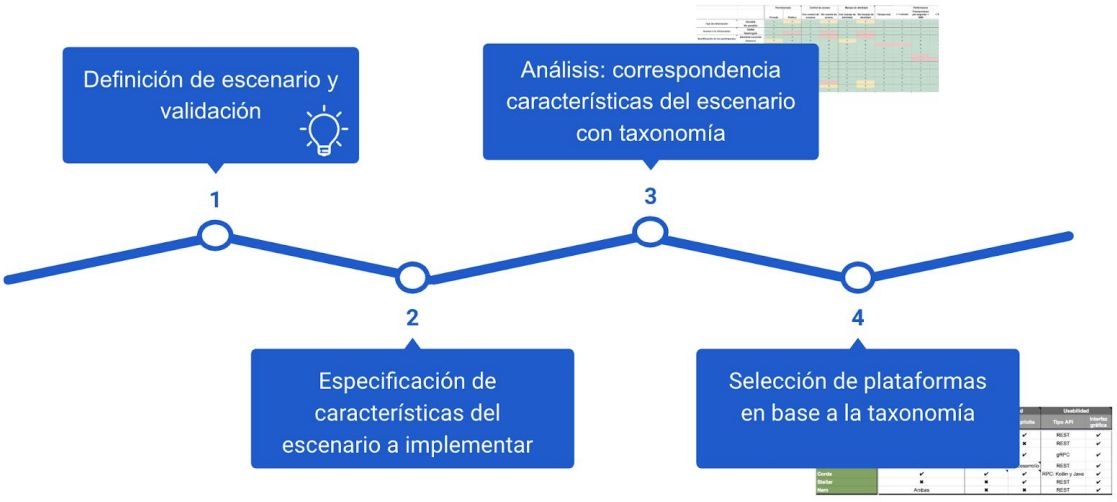


Imagen 17 - Procedimiento para dado un escenario de negocio obtener una plataforma para su implementación

3.3.2.1 Definición de escenario y validación

Es el paso inicial del proceso en el cual se selecciona la idea, implementación o escenario de negocio a evaluar. Dicho escenario debe pasar previamente por alguna validación que determine la viabilidad y el aporte de utilizar blockchain tales como los procesos sugeridos en “Do you need a blockchain?” por Morgen E. Peck [3] y Blockchain beyond the hype [4], pero esta validación está por fuera del alcance de este proyecto.

3.3.2.2 Especificación de características del escenario a implementar

Refiere al proceso de identificar las características de la idea, implementación o escenario especificada en el punto 3.3.2.1. Las características a determinar se encuentran definidas en base al análisis de las características de la taxonomía presentadas en la sección 3.2, de modo que existe una relación entre ambas.

En la tabla 9 se especifican las características a identificar para el análisis de los escenarios.

Característica	**Descripción**	**Valores posibles**
Tipo de información	Refiere a la sensibilidad de la información que es necesario intercambiar entre los nodos de la red.	- Sensible: debido al tipo de información manejada, la misma no debería ser leída por cualquiera, sino que solo puede ser vista por determinados usuarios. - No sensible: el tipo de información manejada no implica ninguna restricción en cuanto a quienes pueden leerla.
Acceso a la información	Esta característica refiere a si, para el problema a resolver, existe la necesidad que la información intercambiada sea conocida por un subconjunto particular de actores o el acceso a la misma es global por parte de todos las entidades involucradas.	- Global: es necesario que la información esté disponible para todos los usuarios. - Restringido: la visibilidad de la información se restringe a usuarios determinados.
Identificación de los participantes	Refiere a la necesidad de contar con un mecanismo que permita identificar a los diferentes actores del sistema. En este punto se pretende identificar si es necesario contar con una entidad certificadora o mecanismo que permita verificar la identidad de los participantes.	- Identidad conocida: se necesita un relación entre cada nodo de la red y la identidad de la persona o entidad que lo controla. - Anónimo: no se identifica quién controla cada nodo de la red y todos tienen un mismo nivel de privilegios sobre la blockchain.

Velocidad de las transacciones	Esta característica permite identificar requisitos de desempeño de la solución a implementar, en función del tiempo requerido para el procesamiento de transacciones.	- Tiempo real: las transacciones deben ser confirmadas en un tiempo de hasta un minuto. - > 1 minuto: no existe restricción en cuanto al tiempo de confirmación de las transacciones.
Volumen de transacciones	Permite en cierto modo determinar requisitos relativos a la escalabilidad de la solución a implementar en función de la cantidad de transacciones por segundo que se requiere procesar	- vt < 1000: el escenario no requiere más de mil transacciones por segundo. - 1000 <= vt < 3000: el escenario requiere entre mil y tres mil transacciones por segundo - vt >= 3000: el escenario impone como restricción soportar tres mil o más transacciones por segundo
Interoperabilidad con sistemas existentes	Refiere a la necesidad que la aplicación a implementar requiera de la comunicación con otros sistemas ya existentes.	- Si: el escenario necesita la interacción con otros sistemas externos. - No: el escenario no impone restricciones de interoperabilidad con otros sistemas.
Necesidad de utilizar su propia criptomoneda	Existen aplicaciones orientadas a la utilización de criptomonedas. Esta característica refiere a la necesidad que, la solución a implementar, permita utilizar una criptomoneda en particular.	- Si: el escenario necesita utilizar una criptomoneda para funcionar. - No: no se precisa la utilización de criptomonedas.

Participación voluntaria	En función de los escenarios analizados, existen aplicaciones para las cuales la participación en la red a implementar no es opcional, es decir, existe algún tipo de regulación que obliga a determinadas organizaciones/entidades pertenecer a la red. Ejemplos de este tipo de aplicaciones pueden ser: escenarios de salud en los cuales el estado impone la necesidad que prestadores de salud se incorporen a un sistema o escenarios de trazabilidad en los cuales diferentes compañías solicitan a proveedores la utilización de un sistema/solución en particular.	- Si: se tiene la libertad de elegir participar o no de la red. - No: la participación en la red es obligatoria para determinadas organizaciones o entidades.
Tolerancia a fallas	Refiere en cierta forma a la criticidad del escenario y la magnitud del impacto de una falla en el sistema.	- Alto impacto: una eventual falla del sistema puede implicar repercusiones con impacto considerable (ej: interferir en tratamientos médicos, pérdida de dinero, etc) - Bajo impacto: las repercusiones derivadas de fallas en el sistema son menores.

Tabla 9 - Características a especificar para el análisis de un escenario

3.3.2.3 Análisis de correspondencia entre las características del escenario y la taxonomía

En esta etapa se identifica la correspondencia entre las características del escenario definidas en el punto 3.3.2.2 con las características de la taxonomía, definiendo qué características debe tener una plataforma de blockchain para ser compatible con el escenario elegido.

Para la realización de este punto se implementa una tabla de decisión (imagen 18 y disponible en el Anexo 6) que permite restringir las características de una potencial plataforma a utilizar para implementar la solución a partir de las características del escenario.

		Permisionada		Control de acceso		Manejo de identidad		Desempeño					Interoperabilidad	
		Privada	Pública	Con control de accesso	Sin control de acceso	Con manejo de identidad	Sin manejo de identidad	Tiempo real	> 1 minuto	Transacciones por segundo < 1000	< 3000	>= 3000	Si	No
Tipo de información	Sensible	+	?	+	?	+	?	+	+	+	+	+	+	+
	No sensible	+	+	+	+	+	+	+	+	+	+	+	+	+
Acceso a la infromación	Global	+	+	+	+	+	+	+	+	+	+	+	+	+
	Restringido	+	-	+	-	+	-	+	+	+	+	+	+	+
Identificación de los participantes	Identidad conocida	+	+	+	?	+	-	+	+	+	+	+	+	+
	Anónimo	?	+	?	+	?	+	+	+	+	+	+	+	+
Velocidad de las transacciones	Tiempo real	+	+	+	+	+	+	+	-	+	+	+	+	+
	> 1 minuto	+	+	+	+	+	+	+	+	+	+	+	+	+
Volumen de transacciones	<1000	+	+	+	+	+	+	+	+	+	+	+	+	+
	<3000	+	+	+	+	+	+	+	+	-	+	+	+	+
	>=3000	+	+	+	+	+	+	+	+	-	-	+	+	+
Interoperabilidad con sistemas existentes	Si	+	+	+	+	+	+	+	+	+	+	+	+	-
	No	+	+	+	+	+	+	+	+	+	+	+	+	+
Necesidad de utilizar su propia criptomoneda	Si	+	+	+	+	+	+	+	+	+	+	+	+	+
	No	+	+	+	+	+	+	+	+	+	+	+	+	+
Participación voluntaria	Si	+	+	+	+	+	+	+	+	+	+	+	+	+
	No	+	?	+	?	+	-	+	+	+	+	+	+	+
Tolerancia a fallas	Alto Impacto	+	+	+	?	+	?	+	+	+	+	+	+	+
	Bajo impacto	+	+	+	+	+	+	+	+	+	+	+	+	+

Imagen 18 - Vista de la tabla de decisión

Para utilizar la tabla se parte de las características del escenario especificadas en las primeras dos columnas, y para cada característica se selecciona uno de los posibles valores. Para cada uno de esos valores se debe revisar su fila correspondiente (referente a características de la plataforma en la taxonomía) hasta encontrar celdas en rojo (con el valor “-”). En base a dichas celdas, se descartan valores que puede tomar una plataforma en la característica correspondiente en la taxonomía. Por ejemplo, la imagen 19 muestra el caso particular de la característica “Acceso a la información”, el cual, en caso de ser restringido, el procedimiento sugiere que se descarte el uso de plataformas públicas.

		Permisionada	
		Privada	Pública
Acceso a la infromación	Global	+	+
	Restringido	+	-

Imagen 19 - Si el escenario requiere que el acceso a la información almacenada en la blockchain sea restringido a un conjunto de participantes, entonces no se recomienda la utilización de una plataforma pública

Por otra parte, el símbolo “?” representa que se sugiere estudiar en profundidad el costo-beneficio de utilizar una plataforma que cuente con la característica señalada para el escenario que está siendo utilizado. Por ejemplo, si el escenario maneja información sensible, la tabla indica un símbolo “?” bajo la característica “pública”, lo cual indica que si bien es posible implementar el escenario en una plataforma con dicha característica, no es lo más recomendable debido a que puede suponer un costo extra de implementación.

		Permisionada	
		Privada	Pública
Tipo de información	Sensible	+	?
	No sensible	+	+

Imagen 20 - Si el escenario requiere involucrar el uso de información sensible se sugiere evaluar con mayor profundidad la utilización de una plataformas públicas.

El símbolo “+” representa que es posible (y preferible) utilizar una plataforma con dicha característica para el escenario en cuestión.

Luego de este proceso, para cada característica de la taxonomía se debería tener uno o más posibles valores sin descartar (en rojo). En caso contrario, es decir, si para alguna característica se tienen todos sus posibles valores en rojo, esto quiere decir que para el escenario dado no es conveniente utilizar blockchain.

3.3.2.4 Selección de plataforma en base a la taxonomía

Una vez que se tienen las características de la taxonomía definidas, resta, utilizando la taxonomía, descartar las plataformas incompatibles (determinadas en el paso anterior) en base a las características duras, y del conjunto de plataformas restantes, elegir la más adecuada en base a las características blandas.

Plataforma	Permisionada	Interoperabilidad		Usabilidad	
		Implícita	Explícita	Tipo API	Interfaz gráfica
Ethereum	✖	✖	✔	REST	✔
EOS	✖	✖	✖	REST	✔
Hyperledger Fabric	✔	✔	✔	gRPC	✔
Cardano	✖	✖	En desarrollo	REST	✔
Corda	✔	✔	✔	RPC: Kotlin y Java	✔
Stellar	✖	✖	✔	REST	✔
Nem	Ambas	✖	✖	REST	✔

Imagen 21 - Taxonomía

En el Anexo 7 se presentan ejemplos concretos de aplicación del procedimiento presentado en esta sección. Por otra parte, en la sección 4.1 se presenta la aplicación del procedimiento para las doce implementaciones seleccionadas y en el Anexo 8 el resultado del análisis en formato de tabla.

4. Verificación y validación de la taxonomía

Con el objetivo de validar la taxonomía definida se realizan un conjunto de actividades las cuales se describen en el presente capítulo.

En esta etapa, se relevan implementaciones existentes que utilizan blockchain estudiando las características que motivan a estos proyectos. Adicionalmente se investigan y analizan taxonomías y estándares que permiten clasificar plataformas blockchain. Además, se estudia el análisis sobre blockchain realizado en la asignatura “Taller de Evaluación de Tecnologías de la Información (Facultad de Ingeniería, UdelaR)”; se contacta expertos en la temática, concretando una reunión en la Agencia de Gobierno electrónico y Sociedad de la Información y Conocimiento (Agesic) y se especifica e implementa un escenario de negocio como mecanismo adicional de validación de la taxonomía.

Las actividades realizadas se ilustran en la imagen 22.

Imagen 22 - Actividades de verificación y validación de la taxonomía

A continuación se describen las etapas realizadas.

4.1 Análisis de escenarios relevados

Uno de los mecanismos utilizados para verificar la correctitud y la facilidad respecto a la utilización de la taxonomía es la aplicación del proceso definido en la sección 3.3 a escenarios de negocio o aplicaciones que se encuentran en producción actualmente. Estos escenarios se encuentran implementados utilizando una plataforma en particular y el objetivo del proceso es verificar que la taxonomía sugiere, para cada una de las implementaciones, la plataforma con la cual fue construido el sistema.

Los escenarios analizados se describen en la tabla 10.

Escenario	**Descripción**	**Plataforma**
Validación de identidad [36]	Este escenario consiste en la identificación de usuarios de forma eficiente y segura (en contraposición a los sistemas tradicionales como mostrar documentación física). Se basa en la confianza que tienen entre sí diferentes instituciones financieras, gubernamentales y proveedoras de servicios. Cuando una de ellas requiere la identificación de un nuevo usuario consulta en la aplicación por información que tengan las demás.	Hyperledger Fabric
Transferencias internacionales [32]	Consiste en transferencias de dinero a través de criptomonedas.	Stellar
Micropagos [33]	Pagos de poco valor monetario, como alternativa más segura a tarjetas de crédito.	Stellar
CryptoKitties [37]	Juego donde se coleccionan, compran y venden gatos virtuales.	Ethereum
Apuestas [38]	Alternativa más transparente/confiable que un casino en línea centralizado.	EOS
Sistema de votos [39]	Sistema de votación electrónica.	Dash
Validación de diplomas universitarios [40]	Aplicación con la que se valida la autenticidad de títulos y diplomas universitarios, aprovechando la inmutabilidad de la información en la blockchain.	Cardano
Pago de regalías [34][35]	Aplicación que permite gestionar, aprovechando la transparencia que provee una solución utilizando blockchain, los pagos de regalías.	Corda

Pagos de préstamos sindicados [41]	Sistema que permite gestionar préstamos sindicados. Este tipo de préstamos involucra a múltiples actores y se propone aprovechar la blockchain como solución distribuida, la inmutabilidad de los registros y la privacidad que provee una plataforma como Corda para gestionar este tipo de préstamos de gran complejidad.	Corda
Cambios de monedas [42]	Aplicación que implementa un sistema de cambio de criptomonedas.	EOS
DNS [43]	Se propone la utilización de una blockchain para brindar un servicio de DNS pretendiendo proveer de una solución que minimice los riesgos de las implementaciones actuales. La utilización de un registro distribuido pretende resolver la vulnerabilidad de los sistemas actuales en cuanto a la posibilidad de modificar registros redireccionando el tráfico a sitios equivocados.	NEM
Donaciones [44]	Solución que permite gestionar y trazar donaciones. Esta propuesta permite conectar entidades interesadas en realizar donaciones con aquellas en necesidad de recibirlas, garantizando la transparencia del proceso.	NEM

Tabla 10 - Escenarios analizados

En la imagen 23 es posible observar el resultado del análisis de las doce implementaciones seleccionadas, identificando para cada una de ellas sus características principales. En la segunda columna es posible observar la plataforma con la cual fue implementada la aplicación y en la última columna, el conjunto de plataformas sugerido, resultado de la aplicación del procedimiento basado en la taxonomía. Para leer la tabla con mayor detalle ver el Anexo 8.

Análisis de los resultados obtenidos

Escenario	Plataforma	Permisionada	Manejo de identidad	Control de acceso al ledger	Velocidad de las transacciones	Volumen de transacciones	Interoperabilidad	Necesidad de utilizar su propia criptomoneda	Participación voluntaria	Tolerancia a fallas	Plataformas sugeridas
Validación de identidad	Fabric	+	+	+	> 1 minuto	> 3000	No necesariamente	No	Si	Bajo impacto	Fabric, NEM
Transferencias internacionales	Stellar	?	?	+	> 1 minuto	> 3000	No necesariamente	Si	Si	Alto impacto	Stellar, NEM
Micropagos	Stellar	?	?	+	Tiempo real	> 3000	No necesariamente	Si	Si	Alto impacto	Stellar, NEM
CryptoKitties (juego)	Ethereum	?	?	+	Tiempo real	> 3000	No necesariamente	Si	Si	Bajo impacto	EOS
Apuestas	EOS	-	-	+	> 1 minuto	>1000	No necesariamente	Si	Si	Alto impacto	EOS, Stellar
Sistema de votos	Dash	?	?	+	> 1 minuto	> 3000	No necesariamente	No	Si	Alto impacto	EOS, NEM, Cardano
Validación de diplomas universitarios	Cardano	?	+	+	> 1 minuto	< 1000	No necesariamente	No	Si	Bajo impacto	Ethereum, EOS, Fabric, Cardano, Corda, Stellar, NEM
Royal payments / Pago de regalias	Corda	?	+	+	> 1 minuto	< 1000	No necesariamente	No, pero una alternativa podría haber sido manejar los pagos en la plataforma utilizando criptomonedas	No	Alto impacto	EOS, Fabric, Corda, NEM
Syndicated loan market	Corda	?	+	+	> 1 minuto	< 1000	No necesariamente	No, pero una alternativa podría haber sido manejar los pagos en la plataforma utilizando criptomonedas	No	Alto impacto	EOS, Fabric, Corda, NEM
Cambios de monedas	EOS	-	+	+	> 1 minuto	>3000	Si	Si	Si	Alto impacto	EOS, NEM, Cardano
DNS	NEM	-	-	-	Tiempo real	>3000		SI	Si	Alto impacto	EOS, NEM
Donaciones	NEM	?	?	?	> 1 minuto	< 1000	No	Si	Si	Alto impacto	Corda, Fabric, NEM, Ethereum

Imagen 23 - Resultado de aplicación del procedimiento definido sobre doce escenarios existentes

Para once de los doce escenarios analizados, el conjunto de plataformas sugeridas al aplicar el procedimiento contienen a la plataforma con la cual dicho escenario fue implementado.

Se detecta una inconsistencia entre los resultados obtenidos y la plataforma en la que se implementó el escenario de CryptoKitties. Este escenario tiene un requerimiento de más de tres mil transacciones por segundo para funcionar de forma adecuada aún en picos de tráfico, pero fue implementado en Ethereum que soporta hasta 15 transacciones por segundo. Esta inconsistencia no se debe a un error en la taxonomía sino a la propia elección de implementar este escenario utilizando Ethereum. Es decir, la plataforma tiene problemas para manejar el volumen de transacciones requerido por el escenario y su performance se ha visto afectada a nivel global debido a esta aplicación. En [45] es posible acceder a una nota periodística publicada por la BBC en la cual se hace referencia al impacto de la aplicación CryptoKitties sobre la red de Ethereum, poniendo en evidencia los problemas que esta plataforma presenta en cuanto a escalabilidad.

Por otra parte, para el caso de uso de validación de diplomas universitarios, en el conjunto de plataformas sugeridas se encuentra Corda como posible plataforma a utilizar. De todos modos, para un escenario en el cual se requiere un acceso global a los registros de libro

mayor, la utilización de Corda como plataforma no es la mejor alternativa debido a que el conocimiento del libro mayor por los participantes de la red es tal que un nodo conoce únicamente las transacciones en las que haya participado. Si bien esto no imposibilita la utilización de Corda, esta plataforma no provee de un mecanismo que permita sobrepasar esta restricción y sería necesario diseñar la red y la aplicación de una forma particular para que todos los nodos tengan acceso a todo el conjunto de transacciones. Este aspecto no se encontraba reflejado en el procedimiento de sugerencia de plataformas. Por este motivo, si un escenario requiere un acceso global a la información y la plataforma cuenta con la posibilidad de utilizar canales privados, se modifica el procedimiento definido en la sección 3.3 para que en vez de recomendar la utilización de dicha plataforma, se sugiera estudiar en profundidad el costo-beneficio de utilizarla (mediante un signo de interrogación “?”).

4.2 Trabajo relacionado: estudio de estándares y taxonomías existentes

Como mecanismo adicional de validación, así como también con el objetivo de mejorar la taxonomía propuesta, se analiza la existencia de estándares aplicables a plataformas blockchain, así como también propuestas de taxonomías para su clasificación.

Existen actualmente diferentes iniciativas en cuanto a la implementación de estándares de blockchain por parte de organizaciones referentes en el área.

Se analizan los siguientes estándares y clasificaciones:

- ISO/TC 307 Blockchain and distributed ledger technologies [46][47]: la International Organization for Standarization (ISO) se encuentra, desde 2016, en proceso de desarrollo del estándar: “ISO/TC 307 Blockchain and distributed ledger technologies”. Ninguno de los borradores del proyecto, con fecha de finalización en el año 2019, se encuentra aún aprobado, muchos de ellos en etapa de propuesta.
- W3C Community & Business Groups. Blockchain Community Group [48]: este grupo tiene el objetivo de generar un estándar para la comunicación/intercambio de mensajes en blockchains en base al estándar ISO20022, proveer pautas para la utilización del almacenamiento y evaluar nuevas tecnologías relacionadas con blockchain. No existen reportes publicados aún.
- Administración de estándares China [49]: Li Ming, director del instituto de investigación de la tecnología blockchain en el Ministerio de Economía chino,

mencionó que dicho país se encuentra en proceso de implementación de un estándar a ser publicado a finales de 2019.

- IEEE Standards Association. Data Format for Blockchain Systems [50]: esta asociación tiene el objetivo de generar un estándar sobre requerimientos en el formato de almacenamiento de datos para sistemas de blockchain incluyendo estructuras de datos, clasificación de datos, tipos de datos, identificadores y largo de los datos. Este proyecto tiene fecha de expiración en diciembre de 2022.
- The W3C's Web Ledger Protocol [51]: describe un modelo de datos y una sintaxis para expresar un conjunto de eventos ordenados en un sistema descentralizado en el que se puede verificar criptográficamente. Si bien no propone una clasificación de plataformas y no se utiliza en este proyecto, en esta propuesta se analizan determinadas características de las mismas (posibilidad de intercambiar el protocolo de consenso e interoperabilidad) y se incluye en este informe como un ejemplo más de los esfuerzos existentes entorno a la estandarización en el contexto de blockchain.
- Standards Australia. Roadmap for *blockchain* standards [52]: la asociación de estándares de Australia elabora un reporte que incluye un relevamiento acerca de las propuestas de estándares para la tecnología blockchain y qué estándares existentes se utilizan en dicho país para la implementación de aplicaciones que utilizan la tecnología (estándares relativos a la implementación de aplicaciones que utilizan la nube, de arquitecturas SOA, entre otros). De todos modos, no se hace referencia a estándares de blockchain existentes; únicamente a la propuesta de estándar ISO/TC 307 mencionado en esta sección.
- IEEE Standards Association. Standard for the Framework of Blockchain Use in Internet of Things (IoT) [53]: esta asociación tiene el objetivo de generar un estándar que brinde un marco común para el uso, implementación e interacción de blockchain en aplicaciones del internet de las cosas (IoT). Este marco apunta a problemas de escalabilidad, privacidad y seguridad. Además incluye el uso de IoT en redes públicas y privadas y contratos inteligentes . El proyecto tiene fecha de expiración en diciembre de 2021. Este estándar puede contribuir al diseño e implementación de escenarios como el propuesto en el capítulo 5, en el cual se registran en una blockchain datos recolectados a partir de sensores de IoT.
- Blockchain Standards for Compliance and Trust [54]: investigadores de la Universidades de Derby y Texas desarrollan una clasificación de plataformas de blockchain haciendo hincapié en los diferentes tipos, principios de seguridad de la

información y características de desempeño de las mismas. Si bien se presenta una clasificación, no se incluye una definición de los atributos estudiados lo que dificulta el estudio comparativo. Con el objetivo de comparar la taxonomía desarrollada con el presente artículo o evaluar aspectos que puedan enriquecer la misma, se obtienen la siguientes conclusiones: existen características similares a las definidas en la taxonomía como son la confidencialidad y la consistencia y características como la tolerancia a fallas, auditabilidad y *liveliness* no aportan a la taxonomía. Esto se debe a que dichas características no permiten clasificar a las plataformas ya que el valor que adopta cada plataforma según esas características coincide para la mayoría de ellas. Existen datos relativos al desempeño de las plataformas que pueden resultar de utilidad incluir en la taxonomía en caso de obtener información precisa acerca de la obtención de dichos datos.

4.3 Análisis de proyectos del Taller de Evaluación de Tecnologías de la Información (Facultad de Ingeniería, UdelaR)

Como mecanismo adicional de validación de la taxonomía propuesta, se analizan proyectos realizados por estudiantes de la carrera Ing. en Computación de la Facultad de Ingeniería, Udelar, para la asignatura “Taller de Evaluación de Tecnologías de la Información”, los cuales consistían en un análisis de plataformas blockchain disponibles en el mercado [55] [56]. Los trabajos consisten en el análisis de dos plataformas de blockchain utilizando la técnica T-Check a partir de un conjunto de hipótesis predefinidas.

En función de las hipótesis planteadas se seleccionan aquellas que permitan clasificar dos plataformas blockchain, descartando aquellas que aportan información común a todas las plataformas de blockchain.

Las hipótesis seleccionadas son:

1. “La plataforma permite implementar seguridad a nivel de blockchain: En caso de ser blockchain privada, la plataforma permite dar de alta nuevos usuarios y brinda mecanismos de autenticación/autorización para acceder a la cadena y a las transacciones.”

Este punto se encuentra reflejado en las características: “Manejo de identidad” y en “Control de acceso al libro mayor”, clasificadas como duras según la taxonomía propuesta. Estas

características refieren a los mecanismos que provee la plataforma para determinar qué nodos pueden unirse a la red y cómo es la política de acceso al libro mayor respectivamente.

2. “La plataforma puede utilizarse de manera sencilla”
   Esta hipótesis comprende los siguientes puntos:
   a. La plataforma puede instalarse en menos de una hora y es posible unirse a una red en menos de 2 horas desde el inicio de la instalación.
   b. La plataforma es de fácil uso y permite que los usuarios desarrollen una interacción efectiva con la misma (ej. es amigable, intuitiva, simple, predecible, familiar, rápida, consistente).
   c. La plataforma cuenta con tutoriales y/o manuales claros.
   d. La plataforma brinda herramientas que permiten la administración de las funcionalidades y el uso de sus recursos.

Este punto se encuentra reflejado en las características: “Usabilidad” y “Soporte y documentación” clasificadas como blandas según la taxonomía propuesta y que contribuyen a seleccionar entre dos o más plataformas cuyas características duras son de gran similaridad. En la taxonomía propuesta no se incluye el tiempo promedio necesario para instalar una red pero podría ser un elemento adicional a incluir en futuras versiones ya que, al menos para las plataformas Hyperledger Fabric, Corda y NEM, se cuenta con la información relativa a los tiempos de instalación.

3. “La plataforma es reconocida y vigente”
   a. La plataforma cuenta con reseñas positivas en sitios o publicaciones especializadas.
   b. Existen blogs y foros sobre la plataforma con actualizaciones periódicas (no más de una semana).
   c. Existen versiones actuales y una planificación en cuanto a la evolución de la plataforma para el próximo año.

Este punto se encuentra reflejado en las características: “Madurez” y “Soporte y documentación” clasificadas como blandas según la taxonomía propuesta.

Además de poder identificar las correspondencias antes mencionadas, se destaca otra de las hipótesis planteadas en los proyectos que no es tenida en cuenta de forma explícita en

la taxonomía propuesta: “La plataforma permite que los bloques sean encriptados, verificando cuáles son los algoritmos utilizados para la encripción”. Esta característica hace referencia a si la plataforma cuenta con un mecanismo nativo que permita encriptar el contenido de lo almacenado en la blockchain, pero no es tenida en cuenta por considerar que no es determinante para la clasificación de plataformas debido a que es posible implementar esta funcionalidad fácilmente en cualquier aplicación.

4.4 Contacto con expertos

Una de las propuestas de validación de la taxonomía consiste en contactar organizaciones o expertos que se encuentren trabajando en la definición de clasificaciones o estandarización de plataformas. En ese marco, se contacta a Alan Sill, integrante del departamento de computación de alto desempeño de la Universidad de Texas, quién contribuyó en la elaboración de “Blockchain Standards for Compliance and Trust” [54] y Emily Dawson, coordinadora del TC 307 [46] analizados en la sección 4.2. Sin embargo, no fue posible realizar un intercambio con ninguno de los expertos contactados.

Por otra parte, la Agencia de Gobierno electrónico y Sociedad de la Información y Conocimiento (Agesic) se interesa en el proyecto descripto en el presente informe, especialmente en la definición de la taxonomía y se concreta una reunión con integrantes del área de tecnología de Agesic en la cual se presenta el proyecto y se intercambian experiencias. El equipo del área de tecnología realiza sugerencias relativas a la definición de la taxonomía y al proceso elaborado que utiliza dicha taxonomía para sugerir plataformas para la implementación de un escenario particular. Respecto a la taxonomía, se sugiere agregar una característica que permita conocer el grado de actualización de la comunidad de una plataforma y re-evaluar la definición de costo propuesta. Estos puntos se detallan en el capítulo 7 (Trabajo futuro). En cuanto al procedimiento que sugiere plataformas, Agesic propone la automatización del proceso, mediante la implementación de un programa que recibe como entrada las características del escenario a implementar y retorna el conjunto de plataformas sugeridas.

4.5 Implementación

Como mecanismo adicional de validación, se especifica un escenario de trazabilidad y se verifica que, dadas las características del mismo, resulta conveniente la utilización de una blockchain y es posible implementar la solución utilizando la plataforma sugerida por la taxonomía aplicando el proceso descripto en la sección 3.3. Este mecanismo de validación

cumple con el objetivo de verificar que es posible implementar un escenario utilizando la plataforma sugerida por dicho procedimiento. Por estos motivos esta etapa no genera modificaciones en la taxonomía.

La documentación de esta tarea de verificación se encuentra disponible en el capítulo 5 del presente informe.

5. Implementación

En este capítulo se describe la etapa de implementación realizada como mecanismo de verificación de la taxonomía. Se describe qué motiva la definición del escenario, su especificación, se aplica el procedimiento definido en la sección 3.3 para determinar la plataforma sugerida para su implementación y en función de dicho resultado se realiza el diseño e implementación del escenario propuesto.

Esta etapa permite validar la taxonomía, mostrando que es posible implementar un escenario utilizando la plataforma sugerida por el procedimiento a partir de su especificación; por estos motivos no se realizan cambios en la taxonomía una vez finalizada esta etapa.

5.1 Introducción

En ecosistemas de producción complejos, los cuales se caracterizan por involucrar múltiples actores, y en particular en la producción de alimentos, resulta crucial contar con un mecanismo que brinde confiabilidad tanto al consumidor y los productores así como también a la entidad encargada de la producción.

Los lácteos son producto que requiere que se cumplan características específicas relativas a su temperatura, pasteurización y otros componentes para su consumo seguro. Aspectos como interrumpir la cadena de frío durante los traslados o recibir un producto desde los tambos que no cumple con los estándares de calidad establecidos, pueden generar grandes pérdidas en el proceso de industrialización o incluso colocar en el mercado productos no aptos para su consumo.

En esta línea de trabajo, se propone la utilización de un sistema basado en blockchain, que permita registrar la trazabilidad en la cadena logística durante todas las etapas de su procesamiento. El propósito de utilizar una blockchain para el escenario planteado es la necesidad de poder llevar un registro inmutable y trazable del cumplimiento de las normas de calidad del producto (temperatura de la leche, etc.) a lo largo de todo su procesamiento hasta que es adquirido por el consumidor. Se pretende, de esta forma, brindar a las empresas un mayor control sobre el proceso y a los usuarios verificar la calidad de los productos que consumen.

5.2 Descripción del problema

El problema particular a resolver en la etapa de la implementación es el hecho de poder contar con un registro inmutable del estado de los productos lácteos durante todo el proceso, desde la obtención de la materia prima en los tambos; durante su procesamiento y hasta que es entregado en los puntos de venta al consumidor.

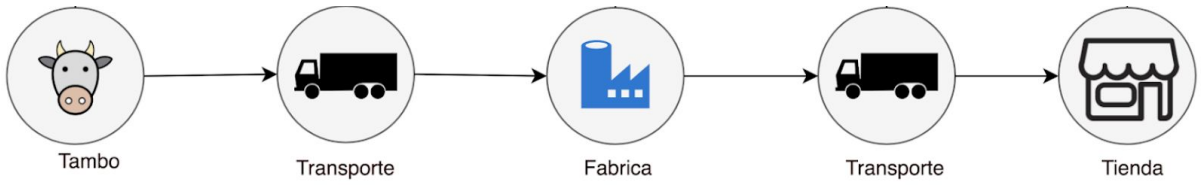


Imagen 24 - Etapas del proceso en las cuales medir los atributos de calidad del producto

Las etapas del proceso a evaluar, ilustradas en la imagen 24, son:

- Extracción de la leche en el tambo: una vez obtenida la materia prima previo a su carga en los camiones que transportan hasta la planta procesadora (Tambo).
- Durante el traslado desde el tambo a la planta procesadora (Transporte).
- Planta procesadora: una vez elaborado el producto final previo a su entrega a los puntos de venta (Fábrica).
- Durante el traslado de la planta procesadora al punto de venta (Transporte).
- Puntos de venta: al arribar a los puntos de venta (Tienda).

Se propone, para cada una de las etapas, que la calidad del producto se encuentre determinada por tres componentes: las mediciones recolectadas por sensores que analizan propiedades de la leche como su porcentaje graso y densidad, sensores de temperatura y operadores, que con una visión general determinen si el producto se encuentra apto para su consumo o no. Debe ser posible que los operadores certifiquen un producto como apto para su consumo, otorgando un sello a los mismos así como también rechazarlos cuando consideran que su calidad impide el consumo. Se define que se otorgue un sello de calidad a un producto si el operador determina que el mismo se encuentra apto para su consumo y si los datos recolectados por el sensor de temperatura o el sensor de densidad/porcentaje graso son correctos.

En la imagen 25 se muestra el flujo completo de validaciones y sellos de calidad/seguridad que recibe un producto

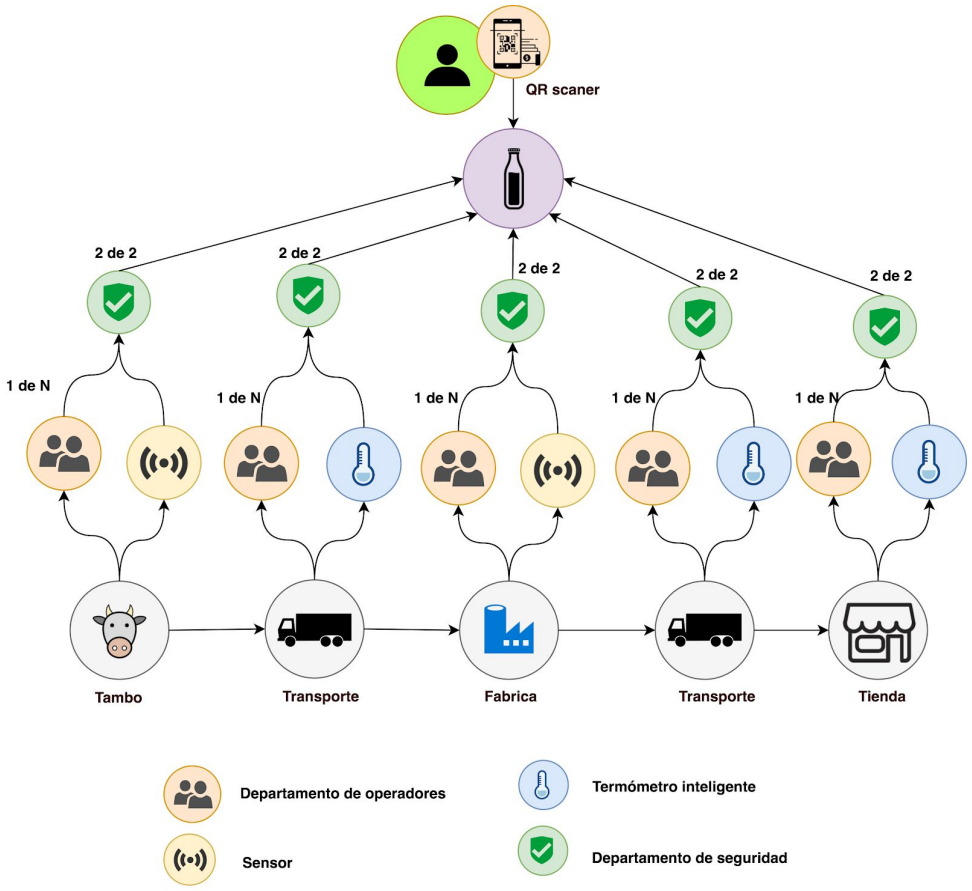


Imagen 25 - Diagrama de aprobación de calidad

El mecanismo de validación está definido de la siguiente manera:

1. La desaprobación de cualquiera de los participantes es condición suficiente para cortar la cadena de suministro. En ese caso, el producto no se encuentra apto para su consumo.
2. El sello de seguridad de cada empresa sólo se obtiene si el departamento de operadores y el sensor/termómetro aprueban el producto. Para obtener la aprobación del departamento de operadores alcanza con que un solo miembro del departamento apruebe el producto.
3. Para que el producto obtenga la validación completa, debe recibir todos los sellos y en el orden definido.

5.3 Análisis

En la tabla 11 se describen los principales componentes del sistema a implementar, descripto en la sección 5.2

Componente	Descripción	Instancias
Actores	Identidades que interactúan con el sistema.	-Operador del tambo. -Conductor del camión que transporta la materia prima del tambo a la fábrica. -Operador fabrica. -Conductor del camión que transporta el producto de la fábrica a la tienda. -Operador de tienda.
Límites	Cómo interactúan los actores con el sistema.	Los operadores y conductores se comunican con el sistema mediante un panel web.
Entidades	Modelos de datos a representar en el sistema.	-Productos. -Sellos de calidad (otorgados por los operadores y conductores cuando los productos se encuentran aptos para su consumo y los sensores determinan que la calidad es correcta). -Eslabones de la cadena: tambo, transportes, fábrica y tienda.
Controladores	Cada actor desencadena acciones que realizarán cambios en las entidades.	Crear producto: Guardar un nuevo producto en el sistema. Enviar sello de seguridad: Después de verificar que el producto pasa el control de seguridad manual, el operador envía un sello de calidad.

Tabla 11 - Componentes y entidades del sistema

Por tratarse de una prueba de concepto, se simplifica la realidad en la cual existen múltiples tambos, plantas y tiendas y se diseña una solución con un tambo, una planta procesadora y una tienda.

5.3.1 ¿Es conveniente utilizar blockchain para este escenario?

Para determinar si efectivamente utilizar una blockchain resulta conveniente, se utilizan los procesos sugeridos en “Do you need a blockchain?” por Morgen E. Peck [3] y Blockchain beyond the hype [4].

Análisis en base a “Do you need a blockchain?”[3]

1. ¿Puede una base de datos tradicional resolver el problema?

Es posible utilizar una base de datos tradicional para resolver el problema ya que permite llevar un registro de las características de la leche en todas las etapas del proceso. Sin embargo, al existir la posibilidad de manipular los registros almacenados en la base de datos, siendo posible realizar modificaciones por parte de la organización propietaria del sistema, contar con una base de datos tradicional para la solución del problema implica que exista confianza entre los diferentes involucrados del sistema y del consumidor final para con ellos, lo cual no puede asumirse en este contexto. Además, no existe actualmente una autoridad central capaz de certificar la calidad de todo el proceso productivo de los productos lácteos, lo cual constituye un problema respecto a qué entidad sería la encargada de administrar la base de datos tradicional que almacene los datos relativos a la calidad del producto durante el proceso.

2. ¿Es necesario que más de un participante actualice los datos?

Si, ya que como fue mencionado, se quiere asegurar el cumplimiento con las normas de calidad de la leche luego de su extracción en el tambo, al ingresar a la planta procesadora, antes de partir de la planta procesadora y al ingresar al punto de venta. Por lo tanto, debe ser posible actualizar los datos desde el tambo, la planta procesadora, los puntos de venta por diferentes actores y los camiones que transportan los productos.

3. ¿Existe confianza entre los actores; del consumidor final en los actores y del dueño de la cadena productiva en los actores?

No, el consumidor no necesariamente conoce a los actores involucrados en el proceso productivo y no necesariamente dichos actores confían entre sí. Además, la calidad de un producto a elaborar en la planta procesadora depende de la calidad de la materia prima proporcionada por el tambo y no necesariamente existe confianza en dichos actores.

4. ¿Todos los participantes confiarían en una tercer parte que regule el proceso?

Hoy en día, en Uruguay los consumidores de cierta forma confían en diferentes empresas proveedoras de leche y productos lácteos. Sin embargo, como fue mencionado, existe una creciente demanda de los mismos por contar con procesos transparentes. Además, sería necesario contar con una organización en la cual tanto los productores, la planta procesadora y los puntos de venta confíen.

Conclusión del análisis

Como resultado de la aplicación del proceso se puede concluir que es adecuada la utilización de una blockchain para resolver el problema planteado

5.3.2 ¿Qué plataforma utilizar?

Para determinar la plataforma de blockchain a utilizar se especifican las características técnicas de la solución a implementar en función de los lineamientos establecidos en el procedimiento descripto en la sección 3.3.2. Estas características se detallan en la tabla 12.

Característica	**Valor**
Tipo de información	No sensible
Acceso a la información	Global
Identificación de los participantes	Identidad conocida
Velocidad de las transacciones	> 1 minuto
Volumen de transacciones	1000 < x < 3000
Interoperabilidad con sistemas existentes	No
Utilizar su propia criptomoneda	No
Participación voluntaria	No

Tabla 12 - Características específicas del escenario a implementar

A partir de dichas características, se aplican los pasos definidos en la taxonomía y las plataformas posibles son: Fabric, Corda y NEM.

Se realiza un análisis para determinar cuál de las tres plataformas sugeridas utilizar:

- El procedimiento alerta respecto a la utilización de una plataforma que brinde un mecanismo de control de acceso al libro mayor distribuido para un escenario con las características del escenario planteado. Corda es una plataforma que cuenta con un mecanismo de control de acceso y por estos motivos se prefiere no utilizarla en este caso. Implementar el escenario planteado utilizando dicha plataforma implica diseñar una estructura de la red que no es natural en Corda, en donde el acceso al libro mayor es tal que cada nodo conoce las transacciones en la cuales ha participado, mientras que en el escenario en cuestión el objetivo es que todos los nodos conozcan todas las transacciones para cumplir con el objetivo de brindar un proceso transparente.
- Una vez descartado Corda para la implementación, se analizan Hyperledger y NEM. Ante un empate, se analiza el resto de las características de la taxonomía en las cuales estas plataformas difieren. Las redes públicas garantizan mayor seguridad en cuanto a la inmutabilidad de la cadena ya que existe una mayor cantidad de mineros. NEM provee la posibilidad de utilizar tanto redes públicas como privadas, por lo que es posible si se requiere, pasar de la red privada a una red pública. En cambio, en Hyperledger Fabric esto no es posible ya que es una red privada y no brinda la opción de utilizar redes públicas. Se decide ponderar la seguridad, por lo tanto, se selecciona NEM2 (relanzamiento de la plataforma NEM, publicada en 2018) como plataforma para realizar la implementación.

5.4 Diseño

En esta sección se presentan los detalles de diseño del sistema de trazabilidad y cómo implementarlo utilizando una plataforma de blockchain.

Para la implementación se utiliza como base el proyecto publicado por la Fundación NEM.io [57]. El mismo que se encuentra publicado en el sitio de NEM como parte del material disponible para el aprendizaje de la herramienta, indicando para ello los pasos a seguir para implementar un escenario de trazabilidad/cadena de suministro.

5.4.1 Diseño de la red

En el proyecto utilizado como base [57] se propone la utilización de dos nodos mineros y un nodo API (permite acceder a los servicios que permiten interactuar con la blockchain desde la aplicación a implementar). Se propone agregar a la solución provista y con el objetivo de brindar mayor confiabilidad al sistema, que cada uno de los actores (tambo, fábrica, tienda y las dos entidades encargadas del transporte) cuente con un nodo minero por actor y un nodo API constituyendo una red P2P. En la imagen 26 se ilustra la estructura de la red P2P en la que cada actor cuenta con sus nodos NEM.

Imagen 26 - Diseño de la red

5.4.2 Correspondencia del escenario y conceptos en NEM

Para la implementación en NEM del caso de uso, se utilizan las correspondencias definidas en la tabla 13.

Elemento de la realidad	Representación en NEM
Producto (materia prima / producto procesado)	Cuenta
Operador	Cuenta
Sensor	Cuenta
Termómetro inteligente	Cuenta
Sello de calidad	Mosaico
Empresa	Espacio de nombres
Subdivisión de la empresa (departamento de seguridad / calidad)	Sub espacio de nombres

Tabla 13 - Mapeo entre elementos del escenario y su representación en la implementación

Productos

Los productos, en la terminología NEM, se pueden representar como activos. Un activo es un objeto que tiene un valor, único, de estado actualizable y que pertenece a alguien. Se decide utilizar cuentas (concepto de NEM) para representar a estos activos, permitiendo identificar a cada producto de forma única y conocer el historial de transacciones y mosaicos enviados. Al representar los productos como cuentas, cualquier actor podría rastrear eventos relacionados con un producto al verificar su dirección.

Operadores

En NEM una cuenta identifica y permite al operador del almacén realizar transacciones.

Sello de seguridad

El sello de seguridad se representa con un *espacio de nombres*, un *sub espacio de nombre* y un *mosaico*. Un *espacio de nombres* identifica a la compañía y un *sub espacio* a la división. El mosaico *empresa.seguridad:sello* representa los sellos de calidad otorgados por el departamento de seguridad/calidad de la empresa "*empresa"*.

Inicialmente, la empresa envía algunos *mosaicos* a la *cuenta* del operador, para que luego este pueda asignar los sellos de calidad a los productos aptos para su consumo. Luego, los operadores envían una transacción de transferencia al producto, con un *mosaico*: *empresa.seguridad:sello*.

Sensores de calidad digitales

Con el objetivo de disminuir los errores humanos y proporcionar una nueva fuente de confianza, se propone la utilización de sensores digitales (capaces de medir las propiedades de la leche antes mencionadas).

Se propone que, además de los sellos de calidad otorgados por los operadores, un producto se encuentre apto para su consumo si los sensores validan que la calidad es correcta. Después que el operador del almacén anuncie la solicitud de sello de calidad, un sensor realiza una inspección digital. El sensor digital confirma o niega la solicitud de sello de seguridad. El sensor digital requiere consignar transacciones, por esta razón se representa al sensor como una cuenta.

Termómetros inteligentes

Para asegurar que las restricciones sobre los productos se cumplan durante el transporte, se propone la utilización de sensores capaces de medir la temperatura. Al igual que el sensor, el termómetro inteligente requiere consignar transacciones y es por esta razón que se representa como una cuenta.

Departamento de operadores

Para cada etapa, se agrupan a los operadores en un departamento. La razón es que se desea que solo se necesite la aprobación de un operador por etapa. Se define al departamento de operadores como una cuenta de firma múltiple, compuesta por dos operadores, en la que solo se requiere la aprobación de uno de sus miembros para aprobar un producto determinado.

Departamento de calidad/seguridad

Los encargados de entregar en última instancia los sellos de calidad en cada etapa son los departamentos de seguridad, que se definen como una cuenta de firma múltiple entre el departamento de operadores y los sensores. En este caso, se requiere la aprobación tanto del departamento de operadores como los sensores.

5.4.3 Arquitectura de la solución

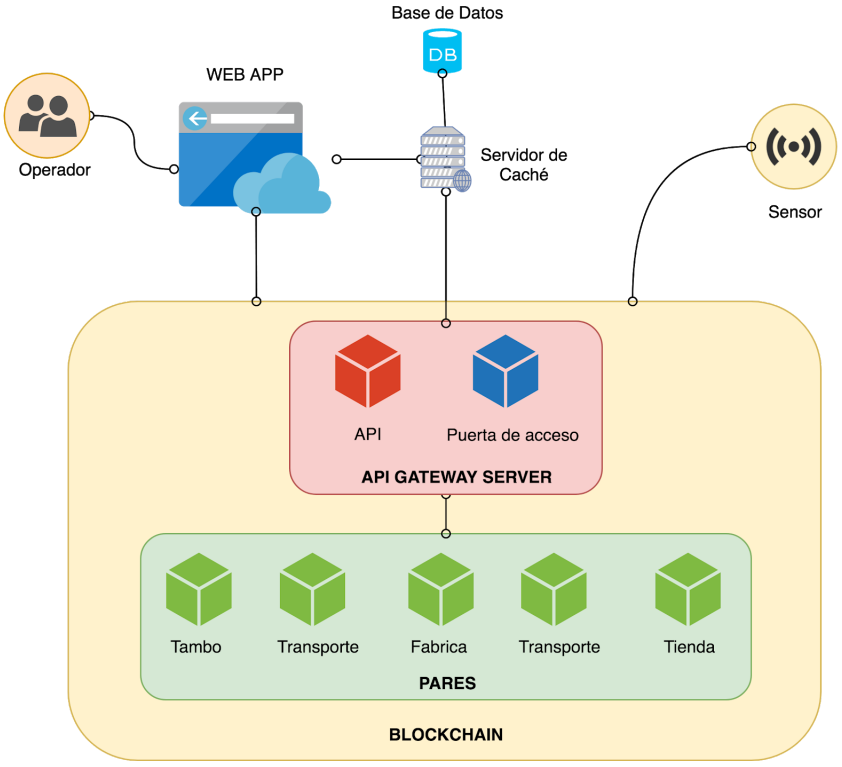


Imagen 27 - Arquitectura de la solución

Como se indica en la imagen 27, los componentes principales de la arquitectura son: la aplicación web, el servidor de caché de la empresa y la base de datos relacional y la red de blockchain.

Los operadores (tanto del tambo, fábrica y tienda), como quienes transportan la materia prima y productos, interactúan con el sistema a través de una aplicación web.

La aplicación es utilizada por los operadores y conductores para enviar los sellos de calidad y permite a consumidores y auditores del proceso, obtener el estado actual de cada producto. La aplicación interactúa con el servidor de caché de la empresa, donde todos los productos son almacenados en una base de datos relacional, con el objetivo de reducir el número de consultas a la blockchain. Además, la aplicación también se comunica, a través de las APIs, con la cadena de bloques, enviando transacciones desde el lado del cliente.

Los sensores se comunican a través de las APIs con blockchain, firmando transacciones agregadas para otorgar sellos de calidad a productos luego de una validación correcta. Para el desarrollo del sistema se simulan los sensores en el servidor cache.

La red blockchain se utiliza en el sistema para mantener el registro inmutable de los estados de los productos a lo largo de su procesamiento, en definitiva para:

- Transferencia y almacenamiento de valor.
- Autorización.
- Trazabilidad.
- Autenticación.

Las tecnologías y servicios utilizados por cada componente se describen en el Anexo 9.

5.4.4 Inicialización del sistema

Una de los principales aportes a destacar es la implementación de un programa que permite, mediante un archivo de configuración YAML, definir la realidad a resolver para el escenario de cadena de suministro. Esto hace que sea posible modelar un conjunto de realidades para este tipo de escenario, pudiéndose configurar las etapas del proceso a auditar y para cada etapa el número de operadores y si se desea utilizar un sensor. De esta

manera se permite definir la estructura del sistema sin tener conocimientos sobre Blockchain.

En el archivo de configuración, se definen los componentes de la cadena de suministro (modelados como empresas en este caso: tambo, fábrica, transportes y tienda) y el orden de los mismos; la cantidad de operadores que pertenecen al departamento de operadores de cada componente de la cadena de suministro y si se utilizan sensores o no en cada componente.

El programa implementado realiza, recibiendo como entrada el archivo YAML, los siguientes pasos para cada componente (empresa) definido:

1. Creación de cuenta de la empresa, utilizando las cuentas creadas en el bloque origen con grandes cantidades de XEM.
2. Creación de espacio de nombres para la empresa.
3. Creación de subespacio del espacio de nombres del paso 2 utilizado para definir los mosaicos (sellos de seguridad) a ser otorgados por el departamento de seguridad.
4. Creación de los mosaicos (sellos de seguridad) de la subdivisión de seguridad.
5. Creación de las cuentas del departamento de operadores y el departamento de seguridad.
6. Creación de las cuentas de operadores, sensores y termómetros inteligentes.
7. Transformación de la cuenta del departamento de operadores a una cuenta de firma múltiple definiendo a los operadores como sus consignatarios.
8. Transformación de la cuenta de departamento de seguridad a una cuenta de firma múltiple definiendo como consignatarios al departamento de operadores y al sensor/termómetro.

De esta forma quedan definidas todas las estructuras dentro de la red. Es importante destacar que estas operación se realizan en ese orden ya que cada etapa depende de las anteriores. Además, es necesario esperar entre cada etapa a que se persistan los datos en la cadena. El tiempo de espera es de 15 segundos ya que es lo que demora la blockchain en confirmar las transacciones.

En el Anexo 9 se muestra el archivo YAML utilizado para la definición de las estructuras del presente proyecto.

5.5 Funcionalidades

Como fue mencionado, los operadores acceden al sistema a través de un portal web desde el cual pueden realizar las siguientes operaciones:

- Crear productos
- Asignar sellos de seguridad a los productos
- Analizar el estado del producto en la cadena de suministro (visualizar los sellos de seguridad otorgados y el conjunto de transacciones almacenadas en la blockchain)

Creación de productos

El proceso a trazar de un producto comienza con su creación. Los operadores pueden crear productos desde la opción “Crear producto” de la barra de navegación superior.

Una vez creado el producto, este es almacenado en la blockchain. En la interfaz, se lista el número del producto, su dirección y clave pública creadas.

Imagen 28 - Creación de productos

Asignar sellos de seguridad a los productos

Para determinar la calidad de un producto, se toman medidas de los atributos del mismo por parte de sensores (simulados como fue mencionado, asignando un valor aleatorio) y operadores.

Cuando los operadores tanto del tambo, de la fábrica, la tienda y los encargados de los transportes determinan que el producto se encuentra dentro de los parámetros de calidad

establecidos (por ejemplo temperatura, porcentaje graso, densidad), estos otorgan los denominados sellos de seguridad al producto.

Los operadores pueden otorgar sellos de seguridad desde la opción “Enviar sello de operador” de la barra de navegación superior. Para ello, deben seleccionar el producto a certificar e ingresar su clave pública y clave privada.

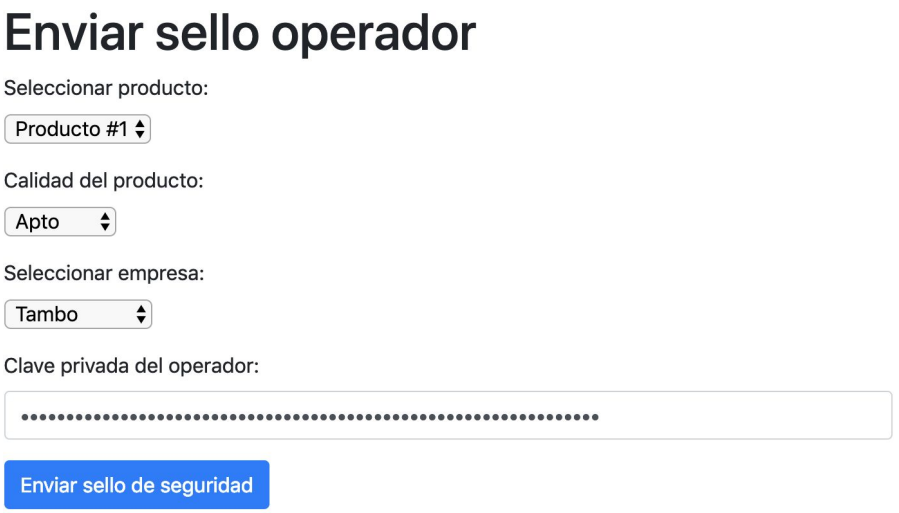


Imagen 29 - Asignar sello de seguridad a un producto

Al otorgar el sello, se crea la transacción que representa la transferencia de un mosaico desde la cuenta del operador que lo emite al producto. Dicha transacción es validada y almacenada en la blockchain. Desde el portal web, el operador puede verificar el ciclo de vida de la transacción.

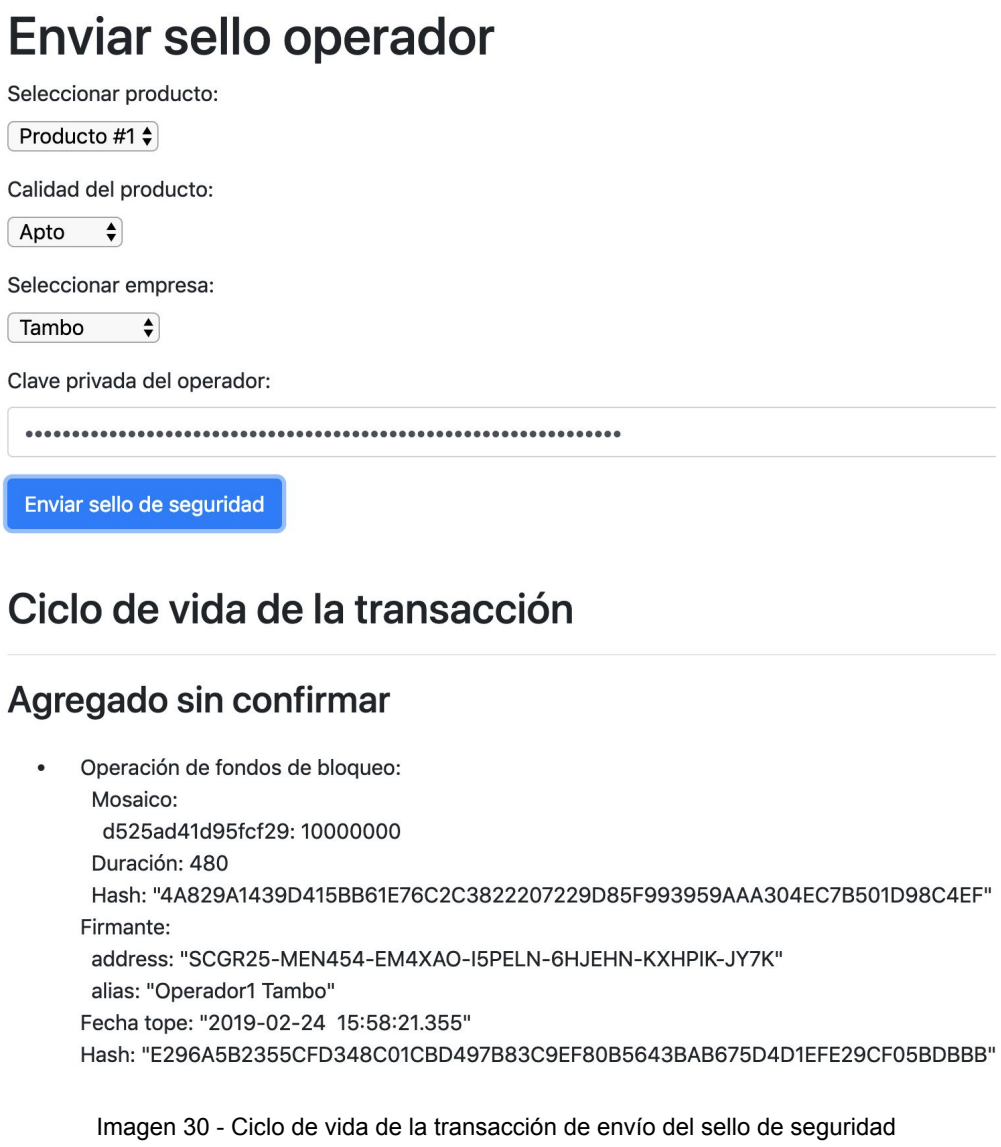


Imagen 30 - Ciclo de vida de la transacción de envío del sello de seguridad

Los estados del ciclo de vida de la transacción son:

- Agregado sin confirmar: Se muestran las transacciones que aún no han sido validadas, es decir, no han sido agregadas a ningún bloque de la cadena.
- Confirmadas: Si las transacciones agregadas sin confirmar son validadas y agregadas a un bloque, se muestran bajo la sección de “Confirmadas”
- Transacciones agregadas consolidadas: Cuando un operador realiza la solicitud de emitir un sello de seguridad, como fue mencionado, para que efectivamente se otorgue dicho sello el sensor correspondiente debe firmar la transacción enviada por el operador. Los sensores se suscriben a las transacciones emitidas por el departamento en el cual se encuentran. Una vez que reciben que se ha emitido una transacción, se simula la inspección y se firma la transacción agregada en caso de

ser correcta o un mensaje de error en caso que la calidad del producto no sea adecuada. Se muestran las transacciones agregadas que fueron consolidadas y agregadas a un bloque.

Analizar el estado del producto en la cadena de suministro

Para cumplir con el objetivo principal del escenario de negocio propuesto, desde el portal web es posible seleccionar un producto por su identificador y visualizar la cantidad de mosaicos/sellos de seguridad recibidos y quién los otorga, la etapa del proceso en la cual se encuentra y las últimas diez transacciones recibidas.

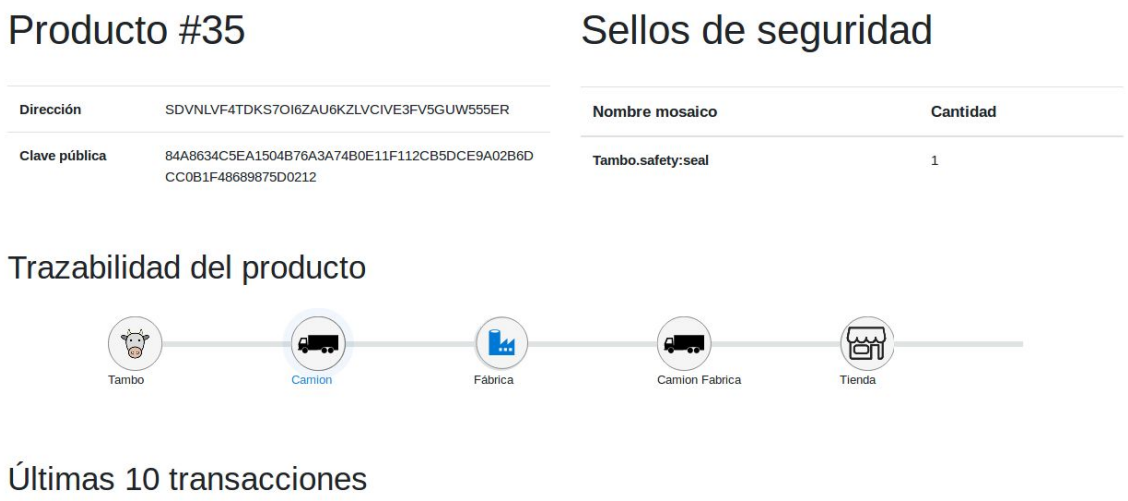


Imagen 31 - Trazabilidad del producto

Como se muestra en la imagen 31 se despliegan los datos del producto, su dirección y clave pública; los sellos de seguridad recibidos, en este caso el otorgado por el tambo y una barra de progreso que indica que el producto se encuentra siendo trasladado del tambo a la fábrica/planta de procesamiento.

Para garantizar que no existan anomalías respecto a el otorgamiento de los sellos de seguridad se valida que el orden de los mosaicos recibidos coincida con el orden en el cual deben enviarse (tambo, camión, fábrica, camión fábrica y tienda). Para ello se verifica el orden de las transacciones y en caso que se emitan sellos de seguridad en un orden incorrecto se informa que el producto no es válido.

Imagen 32 - Orden incorrecto

5.6 Desafíos

Fue necesario, en la etapa de verificar la taxonomía mediante la ejecución de un caso de uso, afrontar diferentes desafíos los cuales se mencionan a continuación.

Documentación

Por ser la tecnología blockchain una tecnología emergente y, en particular la plataforma NEM 2 ser lanzada en 2018, la información, documentación y ejemplos disponibles son escasos, dificultando la comprensión de la plataforma y su integración.

Tecnología

El proyecto utilizado como base para esta etapa se encuentra implementado utilizando herramientas sobre las cuales no se contaba con experiencia, como son TypeScript, Angular y la API de NEM. Además, fue necesario evaluar diferentes versiones del proyecto en cuestión ya que no era posible la correcta ejecución del mismo (en especial la utilización de la interfaz “nem2 client interface”, utilizada para interactuar con la blockchain y fundamental para la creación de las estructuras básicas y versiones de los *scripts* provistos en “catapult-service-bootstrap”) siguiendo los pasos mencionados en la documentación [57].

De modo similar a lo mencionado en el Anexo 3, respecto a la prueba de concepto en Corda, una operación que aparenta ser común en aplicaciones que utilizan blockchain, como es agregar nodos a la red, no resulta intuitiva ni sencilla de realizar además de no contar con documentación oficial respecto a cómo realizar dicha operación.

Modelado

Por otra parte, la API de NEM no cuenta con un mecanismo nativo que permita validar el orden de las transacciones se corresponde con un orden especial a seguir. Para el escenario en cuestión, la existencia de las cuentas de firma múltiple de NEM permite modelar la realidad restringiendo las validaciones necesarias para otorgar un sello de calidad a un producto, sin embargo, no existe un mecanismo que permita validar el orden en el cual se realizan estas validaciones. Por ello, se agrega al proyecto la validación del orden, analizando las transacciones en la blockchain.

6. Gestión del proyecto

En este capítulo se describe el proceso llevado a cabo para la realización del proyecto; incluyendo la planificación inicial, así como las desviaciones y modificaciones sobre la misma.

6.1 Organización

Al comienzo del proyecto, se propone la realización de reuniones de avance con los tutores cada dos semanas, de forma tal que el trabajo quede dividido en iteraciones de corta duración, con el fin de minimizar desviaciones. En cada reunión se plantean objetivos de cara a las siguientes dos semanas, y en la siguiente, se controla el avance hasta el momento.

Si bien se establece la frecuencia esperada para estas reuniones, no se fijan fechas para las mismas, asumiendo que siempre pueden haber imprevistos y que en algunos momentos es difícil mantener la frecuencia pretendida. A pesar de esto, igualmente se aclara desde un comienzo que el trabajo se pone en pausa en determinadas fechas, tales como períodos de parciales o exámenes, así como en licencias prefijadas.

Si bien se intenta seguir la planificación de la mejor manera posible, durante el transcurso del proyecto, ocurren desviaciones tanto en la realización de reuniones que son pospuestas por eventos imprevistos, como en el propio trabajo que no siempre es terminado en los plazos establecidos.

6.2 Planificación

Inicialmente se define una planificación del trabajo que involucra las siguientes cinco fases:

1. Estado del arte: Adquisición de conceptos básicos sobre blockchain, identificación de más de 50 plataformas, generación del marco conceptual del proyecto.
2. Definición de taxonomía, escenarios de negocio y análisis de las plataformas identificadas.
3. Clasificación de las plataformas según la taxonomía definida.
4. Implementación de un caso de uso en una plataforma seleccionada.
5. Documentación: generación del informe final del proyecto.

En la imagen 33 se muestra el diagrama de Gantt de la planificación inicial del proyecto. Los colores se correlacionan uno a uno con las fases mencionadas arriba: estado del arte en verde; definición de la taxonomía, escenarios de negocio y análisis de las plataformas identificadas en azul; clasificación de las plataformas según la taxonomía definida en naranja; implementación de un caso de uso en una plataforma seleccionada en celeste; y documentación en gris.

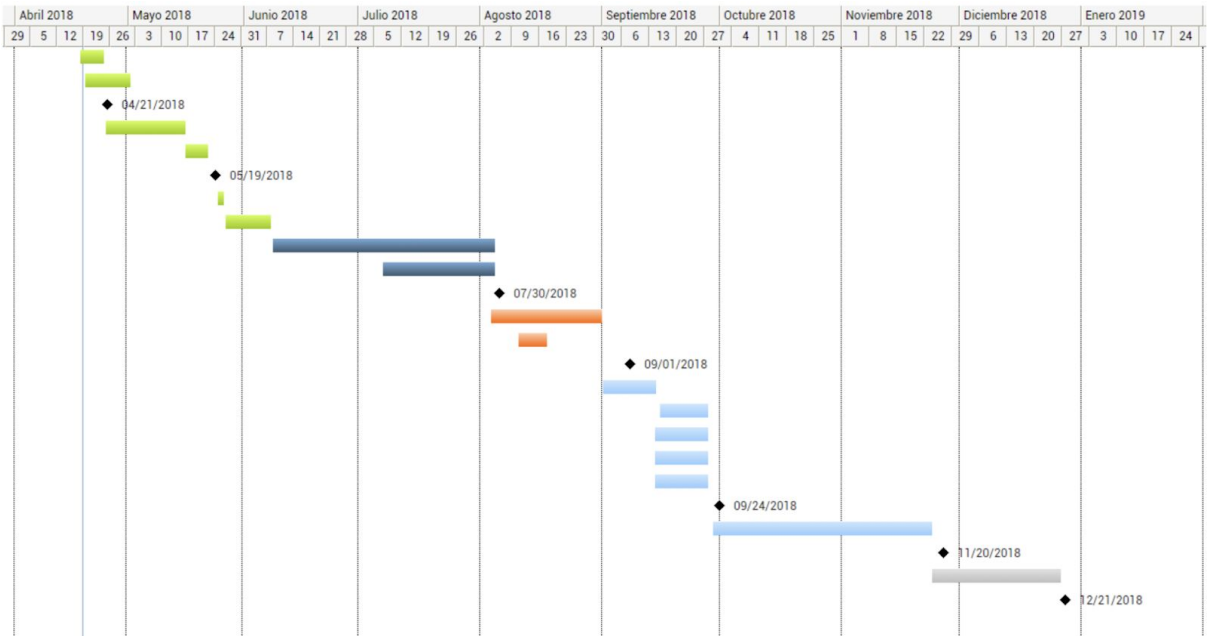


Imagen 33 - Diagrama de Gantt de la planificación inicial del proyecto.

Si bien en la planificación, la tarea de documentación aparece únicamente sobre el final del proyecto, se espera que se trabaje sobre la misma a lo largo de todo el proyecto, y que se dedique sobre el final un período exclusivo para dicha tarea.

Durante el transcurso del proyecto, se realizan modificaciones sobre la planificación inicial, como se puede ver en la imagen 34. Estas modificaciones se deben principalmente a retrasos por dificultad en la coordinación de reuniones tanto internas como con los tutores, y motivos de fuerza mayor.

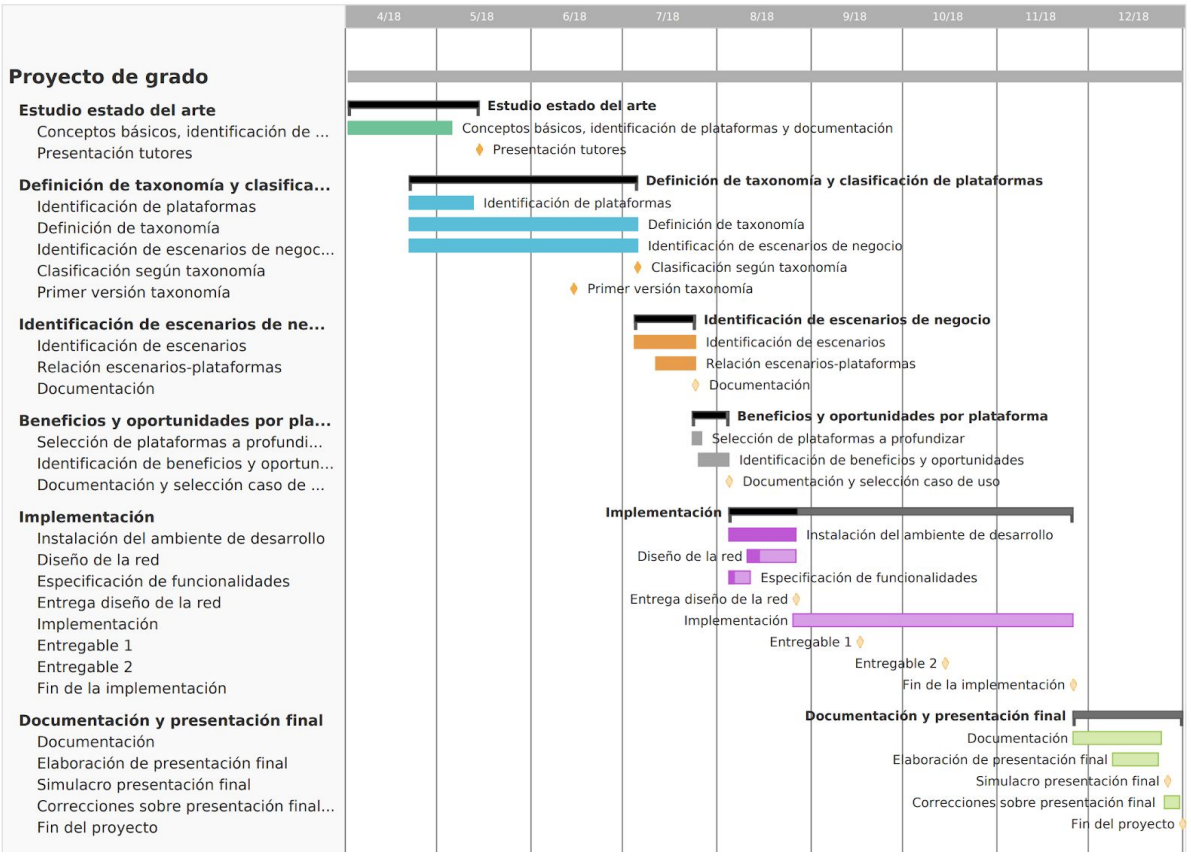


Imagen 34 - Diagrama de Gantt de la planificación actualizada.

6.3 Fases del proyecto

Como se menciona en la planificación, el trabajo realizado se divide en cinco fases. En esta sección, se describe a grandes rasgos cada una de ellas.

6.3.1 Estado del arte

Esta es la etapa inicial del proyecto, en la cual se busca adquirir todos los conocimientos necesarios para cumplir con los objetivos del mismo. Se comienza por estudiar definiciones básicas tales como el concepto de “blockchain” o “consenso”, que luego son incluídas en el marco conceptual. Una vez adquirido el conocimiento básico de la temática, se identifican varias decenas de plataformas y aplicaciones que de algún modo utilizan blockchain, y para ellas, se estudia la documentación disponible.

Al igual que sucede con todas las fases del proyecto, a medida que se avanza con cada tarea, se escriben borradores de las secciones correspondientes en el informe, registrando todas las referencias utilizadas.
Con el objetivo de validar y enriquecer los conocimiento adquiridos, en la etapa inicial se planifica y efectúa una presentación a los tutores del proyecto, en la cual se presentan los conceptos adquiridos y el listado de plataformas relevadas.

6.3.2 Definición de taxonomía, escenarios de negocio y análisis de las plataformas identificadas

Partiendo de lo obtenido en la fase anterior, se analizan las plataformas identificadas y se define una clasificación de las mismas, identificando las características más relevantes. Además, se identifican y estudian escenarios de negocio donde aplica blockchain, con el fin de asociar las características relevadas en las plataformas con características de los escenarios.

Durante la validación del trabajo realizado en esta fase, en una reunión con los tutores, surge la oportunidad de elaborar un procedimiento que sugiera cuál es la mejor plataforma para un escenario dado. Este procedimiento no fue planificado al comienzo del proyecto, pero resulta ser de especial interés debido a que le agrega una utilidad práctica muy clara al elemento central del proyecto, que es la taxonomía. Además, se realizan presentaciones de plataformas seleccionadas y demostraciones de las pruebas de concepto implementadas.

6.3.3 Clasificación de las plataformas según la taxonomía definida

La idea original de esta fase es, dadas las características definidas en la taxonomía, obtener los valores que toman dichas características en un conjunto de plataformas blockchain. En la práctica, esta fase se solapa con la fase anterior, entrando en un círculo de retroalimentación, en el que la propia clasificación de plataformas según la taxonomía motiva la redefinición de algunas características.

La intención inicial es de clasificar todas las plataformas estudiadas según la taxonomía, pero se observa que este trabajo tiene un costo muy elevado, por lo cual, se acota sustancialmente el alcance, comenzando en un principio con tres plataformas clasificadas, e

iterando en etapas posteriores, llegando al final del proyecto a un total de siete plataformas clasificadas.

Para evaluar el proyecto realizado hasta el momento, se coordina una reunión con el Ing. Gustavo Guimerans, en la cual se presenta lo realizado, se responden consultas y se intercambian sugerencias, las cuales son consideradas para etapas posteriores del proyecto. En particular, se analizan estándares relacionados a la temática y se comparan con la taxonomía propuesta, lo que implica agregar tareas adicionales no planificadas al proyecto.

6.3.4 Implementación de un caso de uso en una plataforma seleccionada

Como una de las formas utilizadas para validar la taxonomía, se propone seguir de principio a fin la metodología propuesta. Comenzando por un caso de uso particular, sobre el cual se desea implementar una solución que utilice blockchain, especificar sus características para determinar cuál es la plataforma que mejor se adapta a dicho caso de uso y finalmente realizar la implementación de una prueba de concepto que permita verificar que la plataforma sugerida es apropiada.

6.3.5 Documentación

A lo largo del proyecto, y especialmente sobre el final, se elabora el presente informe con el objetivo de documentar el trabajo realizado, especificando la metodología seguida y la forma de gestionar el proyecto.

Se realizan entregas parciales tanto de la definición de la taxonomía, como también de la especificación de escenarios de negocio, utilizadas como punto de partida para la elaboración del informe final.

Uno de los mecanismos principales de documentación a lo largo del proyecto es la elaboración de presentaciones utilizadas en las diferentes reuniones llevadas a cabo a lo largo del proyecto: reunión con tutores, presentación del proyecto al Ing. Gustavo Guimerans como mecanismo de validación del proyecto y presentación realizada a personal del equipo Tecnología de Agesic. El contenido de las presentaciones fue utilizado también como fuente para la elaboración del presente informe.

7. Trabajo futuro

En el transcurso del proyecto, tanto en la definición de la taxonomía como en los mecanismos utilizados para su verificación, se analizan y evalúan aspectos que pueden complementar o enriquecer el trabajo realizado pero su abordaje queda por fuera del alcance del proyecto. El objetivo de este capítulo es describir las propuestas de mejora e ideas que puedan complementar el proyecto.

Características de la taxonomía

En un principio, se decide incluir la escalabilidad como una característica que permite clasificar plataformas blockchain. Se propone determinar si existen cotas superiores respecto al tamaño de la red (cantidad de nodos) y qué alternativas de almacenamiento del libro mayor se proponen; de todos modos los proveedores de las plataformas no indican de manera específica cómo se resuelve el problema de la escalabilidad. Se considera que en caso de poder obtener esta información por parte de los proveedores o como resultado de analizar las mismas, su inclusión en la taxonomía puede aportar un valor adicional a la misma.

En la reunión realizada con la Agencia de Gobierno Electrónico y Sociedad de la Información (Agesic), el equipo de tecnología sugiere agregar a la taxonomía una característica que permita conocer el grado de actualización de la comunidad de una plataforma y volver a evaluar la definición de costo propuesta. Para conocer el grado de actualización de la comunidad, en instancias posteriores, se podría agregar información relacionada con las fechas de últimas publicaciones en las redes utilizadas por la comunidad o cantidad de proyectos activos por mencionar algunos ejemplos. Respecto a la definición de costo presentada en este proyecto, el equipo de tecnología de Agesic sugiere dividir dicha característica dependiendo si se trata de una plataforma pública o privada y luego que se distinga, por ejemplo, si el costo es relativo al acceso a una API provista por la plataforma o por ejecutar transacciones.

Existen características que fueron relevadas pero no incluidas en la clasificación, que si son propuestas en trabajos relacionados, las cuales puede resultar de interés agregar en un futuro. Por ejemplo, si es posible realizar modificaciones en el protocolo de consenso utilizado (como incrementar el tamaño de los bloques de modo que quepan más transacciones y así reducir el tiempo requerido para la minería impactando en el

desempeño del sistema) o clasificar qué acciones o funcionalidades son provistas por la blockchain o fuera de la cadena. Es conocido que una de las “desventajas” o características de la tecnología blockchain es que no es posible ejecutar la misma cantidad de transacciones por segundo que en otro tipo de sistemas transaccionales y aquí es donde surge el concepto de “dentro de la cadena y fuera de la cadena”. Algunas plataformas han propuesto el intercambio de datos fuera de la cadena, por ejemplo, permitiendo el intercambio de transacciones entre dos pares sin necesidad de incluir cada una de las transacciones en la cadena de bloques (si se agregan estas transacciones a la cadena en un futuro, pero permite el intercambio de transacciones sin que cada una de ellas sea validada hasta cierto momento). Sin embargo, este no es el único contexto en el cual se utiliza dicha terminología, sino que también es utilizada para hacer mención a la capacidad de una plataforma de integrarse con otro tipo de datos fuera de la cadena, por ejemplo, bases de datos o para distinguir qué tipo de información debe almacenarse en la cadena y qué otra puede ser almacenada fuera de ella. Esta capacidad de trabajar conjuntamente dentro y fuera de la cadena puede ser una característica relevante en algunos escenarios.

Por último, existen en la clasificación propuesta, características que para cada una de las plataformas estudiadas adquieren el mismo valor. Por ejemplo, todas las plataformas relevadas brindan o al menos soportan un mecanismo de consenso que tenga tolerancia a fallas bizantinas. Una de las posibles conclusiones respecto a lo antes mencionado, es que esos valores tienden a ser un estándar sin importar la plataforma, por lo cual, si es posible determinar que la tendencia continúa en el tiempo, en el futuro dichas características pueden volverse irrelevantes a la hora de clasificar plataformas de blockchain.

Procedimiento de selección de plataformas

Otra de las propuestas de trabajo futuro es la automatización de los pasos a realizar para determinar, dado un escenario de negocio, qué plataformas son apropiadas para su implementación. En ese sentido, se propone implementar un programa que reciba como entrada las características del escenario de negocio y retorne, como resultado de la utilización de la taxonomía y los pasos descriptos en la sección 3.3.2, el conjunto de plataformas sugeridas.

Implementación

La plataforma NEM tiene la característica de poder ser tanto una red pública como privada. Si se considera la puesta en producción del escenario descripto en la implementación y dado que la información almacenada en la blockchain no es confidencial para este caso, puede resultar conveniente evaluar si utilizar la red pública de NEM ya que permite agregar confiabilidad al proceso, por contar con más nodos capaces de validar las transacciones.

8. Conclusiones

A lo largo del proyecto “Plataformas blockchain y escenarios de uso” se estudian las principales características de la tecnología blockchain, se identifican y catalogan diferentes plataformas y escenarios de uso donde la utilización de estas plataformas aporta valor. Se elabora una taxonomía que permite clasificar a las plataformas blockchain y se define un procedimiento que permite, dado un escenario de uso / negocio específico, obtener un conjunto de plataformas sugeridas para su implementación. En la etapa de elaboración de la taxonomía, se realizan pruebas de concepto y como mecanismo de verificación de la misma, entre otros, se realiza una etapa de implementación utilizando la plataforma NEM. Respecto a los objetivos planteados, se decide junto con los tutores que el abordaje del objetivo “Realizar un estudio de beneficios y oportunidades de mejora en cada plataforma en escenarios identificados” no contribuye al desarrollo del proyecto, por lo que no se realiza el análisis correspondiente. Teniendo en cuenta las actividades realizadas, es posible concluir que se cumplen con los objetivos planteados en el proyecto.

La complejidad de la tecnología blockchain, la diversidad entre plataformas, y el dinamismo que caracteriza al desarrollo de soluciones entorno a esta tecnología, presentó uno de los principales desafíos del proyecto. En el relevamiento inicial de plataformas, fue necesario identificar y filtrar el ruido generado por muchas propuestas en desarrollo, que prometen grandes beneficios sobre otras, pero que en realidad ofrecen muy poco.

Para la elaboración de la taxonomía, se analizan cincuenta y un plataformas de blockchain, seis de ellas en profundidad y se realizan pruebas de concepto sobre Hyperledger Fabric, Corda y NEM. Además, se identifican y estudian más de treinta escenarios de negocio e implementaciones que utilizan o proponen la utilización de blockchain, clasificados en ocho grandes áreas de aplicación. El conocimiento adquirido en este proceso, permitió obtener como resultado una taxonomía que clasifica plataformas blockchain según veintidós características. Estas características, como por ejemplo, el mecanismo de consenso utilizado, el hecho de contar con contratos inteligentes o ser permisionada o no; permiten identificar qué aspectos resulta conveniente analizar a la hora de estudiar una plataforma y considerarla para la implementación de un escenario particular.

La taxonomía, como principal aporte del proyecto, permite contar con una clasificación de plataformas blockchain que asiste a personal del área de tecnologías de la información,

quienes no necesariamente conocen sobre el tema, en el análisis de plataformas y la selección de ellas para la implementación de escenarios de uso. Se destaca la pertinencia del proyecto en relación a este aporte, ya que organizaciones mundialmente reconocidas como ISO, IEEE, W3C, entre otros, se encuentran en proceso de desarrollo de estándares y clasificaciones de este tipo de plataformas.

Para validar la utilidad y correctitud de la taxonomía, se realizan cinco actividades diferentes que permiten analizar la propuesta realizada desde distintos enfoques: aplicación del procedimiento de selección de plataformas a doce escenarios de negocio, estudio de estándares y taxonomías existentes, contacto con expertos, análisis de proyectos de estudiantes de Facultad de Ingeniería, Udelar e implementación de un escenario. La diversidad de estas validaciones, desde el análisis de publicaciones académicas hasta tareas de implementación, permitieron verificar la utilidad de la propuesta.

Se espera que los aportes de este proyecto resulten de utilidad como mecanismos para comprender la tecnología blockchain, así como también las principales características y limitaciones de sus implementaciones. Las herramientas desarrolladas y la experiencia adquirida y documentada durante la realización de las pruebas de concepto, pretenden simplificar el proceso de evaluación de propuestas que utilicen blockchain, acorde a las características específicas de un escenario de negocio o caso de uso particular.

Referencias bibliográficas

[1] Nakamoto, Satoshi. Bitcoin a peer-to-peer electronic cash system. 2008.

[2] «Evolution of blockchain technology». Deloitte Insights, https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html. Accedido febrero de 2019.

[3] Peck, M. E. «Blockchain world - Do you need a blockchain? This chart will tell you if the technology can solve your problem». IEEE Spectrum, vol. 54, n.o 10, octubre de 2017, pp. 38-60. IEEE Xplore, doi:10.1109/MSPEC.2017.8048838.

[4] «Blockchain Beyond the Hype». World Economic Forum, https://www.weforum.org/whitepapers/blockchain-beyond-the-hype/. Accedido febrero de 2019.

[5] Soanes, Catherine, y Angus Stevenson, editores. «Blockchain». Oxford dictionary of English, 2nd ed, Oxford University Press, 2003. Library of Congress ISBN, https://en.oxforddictionaries.com/definition/blockchain.

[6] Crosby, Michael, et al. «BlockChain Technology Beyond Bitcoin». Berkley Engineering, 2015, http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

[7] «libro mayor». Oxford Dictionaries | Español, https://es.oxforddictionaries.com/definicion/libro_mayor. Accedido febrero de 2019.

[8] Hyperledger. https://www.hyperledger.org/. Accedido febrero de 2019.

[9] Brakeville, Sloane, y Bhargav Perepa. Blockchain basics: Introduction to distributed ledgers. IBM, https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html. Accedido febrero de 2019.

[10] Arnold, Andrew. «Blockchain Cannot Solve All The World's Problems, But It Sure Does Help With The Following». Forbes, https://www.forbes.com/sites/andrewarnold/2018/08/30/blockchain-cannot-solve-all-the-worlds-problems-but-it-sure-does-help-with-the-following/. Accedido febrero de 2019.

[11] Zheng, Zibin, et al. «Blockchain Challenges and Opportunities: A Survey». International Journal of Web and Grid Services, vol. 14, n.o 4, 2018, p. 352. Crossref, doi:10.1504/IJWGS.2018.095647.

[12] Cloud Customer Architecture for Blockchain. Cloud Standards Customer Council, 2017, https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-Blockchain.pdf.

[13] Biscontini, Tyler. «Peer-to-peer». Encyclopedia of Science, Salem Press. Accedido febrero de 2019.

[14] Bass, Len, et al. Software architecture in practice. 3rd ed, Addison-Wesley, 2013.

[15] ASALE, RAE. «consenso». Diccionario de la lengua española, Edición del Tricentenario, http://dle.rae.es/?id=AP0O6TO. Accedido febrero de 2019.

[16] «Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus». Hyperledger Architecture, vol. 1, 2017, https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf.

[17] Proof Of Work - Bitcoin Glossary. https://bitcoin.org/en/glossary/proof-of-work. Accedido febrero de 2019.

[18] Moindrot, Olivier, y Charles Bournhonesque. «Proof of Stake Made Simple with Casper». ICME, Stanford University, 2017, http://www.scs.stanford.edu/17au-cs244b/labs/projects/moindrot_bournhonesque.pdf.

[19] NEM – Distributed Ledger Technology (Blockchain) » Cosechar & POI. https://nem.io/es/inversores/la-cosecha-poi/. Accedido febrero de 2019.

[20] Consensus Algorithm (BFT-DPOS). 2017. EOSIO. GitHub, https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md#consensus-algorithm-bft-dpos. Accedido febrero de 2019.

[21] «Back to Blockchains … This Time in the Context of “Smart Contracts”». Robert Crown Law Library Blog, Stanford Law School, 2018, http://liblog.law.stanford.edu/2018/05/back-to-blockchains-this-time-in-the-context-of-smart-contracts/.

[22] Lauslahti, Kristian, et al. «Smart Contracts How Will Blockchain Technology Affect Contractual Practices?» SSRN Electronic Journal, 2017. Crossref, doi:10.2139/ssrn.3154043.

[23] Ellervee, Andreas. A Reference Model for Blockchain-Based Distributed Ledger Technology. University of Tartu, https://comserv.cs.ut.ee/home/files/ellervee_softwareengineering_2017.pdf?study=ATILoputoo&reference=77BCAF0F09164BE4DB593978F449D0B493FFE7BA. Accedido febrero de 2019.

[24] «Blockchain Reference Architecture». IBM, https://www.ibm.com/cloud/garage/architectures/blockchainArchitecture/reference-architecture. Accedido febrero de 2019.

[25] «Azure Blockchain Workbench Architecture». Microsoft Azure, https://docs.microsoft.com/en-us/azure/blockchain/workbench/architecture. Accedido febrero de 2019.

[26] «Blockchain on AWS». Amazon Web Services, Inc., https://aws.amazon.com/partners/blockchain/. Accedido febrero de 2019.

[27] Blockchain use cases. IBM, https://www.ibm.com/blockchain/use-cases/ . Accedido febrero de 2019.

[28] «Blockchain for Food Safety». IBM, 22 de agosto de 2017, https://www-03.ibm.com/press/us/en/pressrelease/53013.wss.

[29] «Watson Health to Study the Use of Blockchain in Healthcare». IBM, 11 de enero de 2017, https://www-03.ibm.com/press/us/en/pressrelease/51394.wss.

[30] «IBM Leverages Blockchain for a Low-Carbon Future». IBM, 20 de marzo de 2017, https://www-03.ibm.com/press/us/en/pressrelease/51839.wss.

[31] «J.P. Morgan Is Launching a Payments Network Using Blockchain». Fortune, http://fortune.com/2017/10/16/jp-morgan-bitcoin-blockchain/. Accedido febrero de 2019.

[32] TEMPO Money Transfer | Send Money Online With Best Rates. https://tempo.eu.com/en. Accedido febrero de 2019.

[33] McCaleb, Jed. «Deloitte Partners with Stellar for Affordable Payments». Stellar, 27 de junio de 2016, https://www.stellar.org/blog/deloitte-launch/.

[34] «Home • GuildOne». GuildOne, https://guild1.co/. Accedido febrero de 2019.

[35] «GuildOne Case Study – Amazon Web Services (AWS)». Amazon Web Services, Inc., https://aws.amazon.com/partners/apn-journal/all/guildone/. Accedido febrero de 2019.

[36] «SecureKey: Building Trusted Identity Networks». SecureKey, https://securekey.com/. Accedido febrero de 2019.

[37] CryptoKitties. «CryptoKitties | Collect and Breed Digital Cats!» CryptoKitties, https://www.cryptokitties.co. Accedido febrero de 2019.

[38] «How EOS, Tron and Ethereum Have Impacted the Gambling Industry». CryptoSlate, 4 de diciembre de 2018, https://cryptoslate.com/blockchain-impacts-gambling-industry/.

[39] Governance — Dash latest documentation. https://docs.dash.org/en/latest/governance/index.html. Accedido febrero de 2019.

[40] « Cardano Blockchain's First Use Case: Proof of University Diplomas in Greece». Nasdaq News, enero de 2018, https://www.nasdaq.com/article/cardano-blockchains-first-use-case-proof-of-university-diplomas-in-greece-cm899265.

[41] Corda Case Study: «How Finastra is harnessing R3's Corda Enterprise blockchain to open up a new business line and transform transparency and efficiency in the syndicated loan market». R3, https://www.r3.com/wp-content/uploads/2018/07/US_11_Finastra_CS_JUN26_final.pdf. Accedido febrero de 2019.

[42] SouthEX | DappRadar. https://dappradar.com/eos/675/southex. Accedido febrero de 2019.

[43] NEM blockchain DNS. 2018. https://github.com/aenima86/NEM-DNS. Accedido febrero de 2019.

[44] GiveMatters. http://givematters.io/. Accedido febrero de 2019.

[45] CryptoKitties Cripple Ethereum Blockchain. 5 de diciembre de 2017. www.bbc.com, https://www.bbc.com/news/technology-42237162.

[46] Blockchain and distributed ledger technologies. ISO/TC 307, 2016, https://www.iso.org/committee/6266604.html.

[47] Blockchain and distributed ledger technologies. ISO/TC 307, 2016. Standards catalogue, https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0.

[48] «Blockchain Community Group». W3C Community & Business Groups, https://www.w3.org/community/blockchain/. Accedido febrero de 2019.

[49] «How China Wants to Lead the World in Blockchain Technology». The Telegraph, 1 de junio de 2018. www.telegraph.co.uk, https://www.telegraph.co.uk/news/world/china-watch/technology/blockchain-technology-in-china/.

[50] P2418.2 - Standard Data Format for Blockchain Systems. IEEE Standards Association, 2018, https://standards.ieee.org/project/2418_2.html. Accedido febrero de 2019.

[51] The Web Ledger Protocol 1.0 - A format and protocol for decentralized ledgers on the Web. W3C Blockchain Community Group, https://w3c.github.io/web-ledger/.

[52] Winter, Johnson, et al. «Roadmap for Blockchain Standards». Lexology, Standards Australia, 2017, https://www.lexology.com/library/detail.aspx?g=6312e29a-4362-4568-b68e-9b9990907682.

[53] P2418.1 - Standard for the Framework of Blockchain Use in Internet of Things (IoT). IEEE Standards Association, 2017, https://standards.ieee.org/project/2418_1.html.

[54] Anjum, Ashiq, et al. «Blockchain Standards for Compliance and Trust». IEEE Cloud Computing, vol. 4, n.o 4, julio de 2017, pp. 84-90. Crossref, doi:10.1109/MCC.2017.3791019.

[55] Acevedo, Federico, y Guillermo Coduri. TETI. 2018.

[56] Vega, Cristian y Bonhomme, Juan. TETI. 2018.

[57] NEM Blockchain Applied to Supply Chain. https://nemtech.github.io/nem2-workshop-nem-applied-to-supply-chain/. Accedido febrero de 2019.

[58] IBM Blockchain and SAP IoT Solution for the Pharmaceutical Cold Chain. YouTube, https://www.youtube.com/watch?time_continue=14&v=-3FuWI9hTgc. Accedido febrero de 2019.

[59] Novo, Oscar. «Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT». IEEE Internet of Things Journal, vol. 5, n.o 2, abril de 2018, pp. 1184-95. Crossref, doi:10.1109/JIOT.2018.2812239.

[60] Ekblaw, Ariel, et al. «A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data». MIT Media Lab, Beth Israel Deaconess Medical Center, 2016.

[61] DokChain PokitDok. https://pokitdok.com/dokchain/. Accedido febrero de 2019.

[62] Smith, W. Bryan. DOKCHAIN: INTELLIGENT AUTOMATION IN HEALTHCARE TRANSACTION PROCESSING. 2017, https://pokitdok.com/wp-content/themes/pokitdok2017/dokchain/static/data/DokChainWhitepaper20170926Draft.pdf.

[63] Alketbi, Ahmed, et al. «Blockchain for government services — Use cases, security benefits and challenges». 2018 15th Learning and Technology Conference (L&T), IEEE, 2018, pp. 112-19. Crossref, doi:10.1109/LT.2018.8368494.

[64] Viant. https://viant.io. Accedido febrero de 2019.

[65] «Blockchain’s Latest Breakthrough? Sustainable Fish». Fortune, 2018, http://fortune.com/2018/01/03/blockchain-cryptocurrency-sustainable-fish/.

[66] IBM. IBM Announces Major Blockchain Collaboration with Dole, Driscoll’s, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, Unilever and Walmart to Address Food Safety Worldwide. 2017, https://www.prnewswire.com/news-releases/ibm-announces-major-blockchain-collaboration-with-dole-driscolls-golden-state-foods-kroger-mccormick-and-company-mclane-company-nestle-tyson-foods-unilever-and-walmart-to-address-food-safety-worldwide-300507604.html.

[67] Insurwave, a New near-Real-Time, Blockchain-Enabled Platform to Secure and Streamline the Marine Insurance Process Is Now Live. https://webforms.ey.com/gl/en/industries/financial-services/insurance/ey-blockchain-marine. Accedido febrero de 2019.

[68] Farwell, Lee Ann. «World's first blockchain platform for marine insurance now in commercial use». Business Insider, 2018, https://markets.businessinsider.com/news/stocks/world-s-first-blockchain-platform-for-marine-insurance-now-in-commercial-use-1025259012.

[69] Better-working insurance: moving blockchain from concept to reality. https://webforms.ey.com/Publication/vwLUAssets/ey-better-working-insurance-moving-blockchain-from-concept-to-reality/$FILE/ey-better-working-insurance-moving-blockchain-from-concept-to-reality.pdf. Accedido febrero de 2019.

[70] «TrustChain». TrustChain, https://www.trustchainjewelry.com/. Accedido febrero de 2019.

[71] Kim, Henry M., y Marek Laskowski. «Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance». SSRN Electronic Journal, 2016. Crossref, doi:10.2139/ssrn.2828369.

[72] «Programming As Art: How Blockchain Can Help Artists (And Save Art)». Inc.com, 23 de mayo de 2018, https://www.inc.com/john-koetsier/programming-as-art-how-blockchain-can-help-artists-and-save-art.html.

[73] «This Startup Is Using Blockchain to Fight Art Forgers». Bloomberg, marzo de 2018, https://www.bloomberg.com/news/articles/2018-03-23/art-forgers-find-a-new-enemy-in-veris-art-s-blockchain-startup.

[74] Rossow, Andrew. «Why Does The Art Community Need Blockchain On Its Palette?» Forbes, https://www.forbes.com/sites/andrewrossow/2018/04/07/why-does-the-art-community-need-blockchain-on-its-palette/. Accedido febrero de 2019.

[75] «Why Should I Use It?» Verisart, http://verisart.zendesk.com/hc/en-us/articles/115002326493-Why-should-I-use-it-. Accedido febrero de 2019.

[76] Ujo Music. https://ujomusic.com. Accedido febrero de 2019.

[77] «Challenge Accepted: Your Chance to Make the World Better with Blockchain». Blockchain Pulse: IBM Blockchain Blog, 11 de mayo de 2018, https://www.ibm.com/blogs/blockchain/2018/05/challenge-accepted-chance-make-world-better-blockchain/.

[78] Identity Now - Building a Digital Identity Ecosystem on Blockchain with SecureKey in the Banking Industry. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=BKW03040USEN. Accedido febrero de 2019.

[79] ETHLend - Get a crypto loan without selling your cryptocurrencies. https://ethlend.io/es/. Accedido febrero de 2019.

[80] WeiFund - Decentralized Fundraising. http://weifund.io/. Accedido febrero de 2019.

[81] «Democracia líquida». Wikipedia, la enciclopedia libre. Wikipedia, https://es.wikipedia.org/w/index.php?title=Democracia_l%C3%ADquida&oldid=113800363. Accedido febrero de 2019.

[82] Entendiendo la governanza de Dash — documentación de Dash - latest. https://docs.dash.org/es/latest/governance/understanding.html. Accedido febrero de 2019.

[83] Zhang, Bingsheng, et al. «A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence». Lancaster University, UK, https://www.lancaster.ac.uk/staff/zhangb2/treasury.pdf. Accedido febrero de 2019.

[84] «Welcome to Corda !» R3 Corda 1.0 documentation, https://docs.corda.net/releases/release-V1.0/index.html. Accedido febrero de 2019.

[85] «Network Bootstrapper». R3 Corda V4.0 documentation, https://docs.corda.net/network-bootstrapper.html. Accedido febrero de 2019.

[86] «Building Your First Network». hyperledger-fabricdocs master documentation, diciembre de 2018, https://hyperledger-fabric.readthedocs.io/en/latest/build_network.html.

[87] Tasca, Paolo y Tessone, Claudio. «Taxonomy of Blockchain Technologies. Principles of Identification and Classification» SSRN Electronic Journal, 2018. Crossref, doi:10.2139/ssrn.2977811

[88] «Hyperledger Blockchain Performance Metrics». Hyperledger, https://www.hyperledger.org/wp-content/uploads/2018/10/HL_Whitepaper_Metrics_PDF_V1.01.pdf. Accedido febrero de 2019.

[89] Definición seguridad de la información. Curso «Administración y Seguridad de Sistemas Informáticos», https://eva.fing.edu.uy/course/view.php?id=785. Accedido febrero de 2019.

[90] Account — NEM Developer Center. https://nemtech.github.io/concepts/account.html. Accedido febrero de 2019.

[91] Arabaci, Okan. Blockchain consensus mechanisms - the case of natural disasters. Uppsala Universitet, 2018, https://pdfs.semanticscholar.org/0afd/a615470760dd1cd661fe4b5f7d3e9b39cdf3.pdf.

[92] Macdonald, M, et al. «The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin» 2018. 10.13140/RG.2.2.23274.52164.

[93] Mattila, Juri. The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures. University of California, Berkeley, 2016.

[94] Blockchain Beyond the Hype A Practical Framework for Business Leaders. World Economic Forum, http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf. Accedido febrero de 2019.

[95] The Founder’s Handbook, Your guide to getting started with blockchain. 2.0, IBM, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=28014128USEN&. Accedido febrero de 2019.

[96] Tapscott, Don, y Alex Tapscott. Realizing the Potential of Blockchain A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies. World Economic Forum, http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf.

[97] Xu, Xiwei, et al. «A Taxonomy of Blockchain-Based Systems for Architecture Design». 2017 IEEE International Conference on Software Architecture (ICSA), IEEE, 2017, pp. 243-52. Crossref, doi:10.1109/ICSA.2017.33.

[98] Smith, T. D. «The blockchain litmus test». 2017 IEEE International Conference on Big Data (Big Data), IEEE, 2017, pp. 2299-308. Crossref, doi:10.1109/BigData.2017.8258183.

[99] Brinckman, Adam, et al. «A Comparative Evaluation of Blockchain Systems for Application Sharing Using Containers». 2017 IEEE 13th International Conference on e-Science (e-Science), IEEE, 2017, pp. 490-97. Crossref, doi:10.1109/eScience.2017.80.

[100] Valenta, Martin, y Philipp Sandner. Comparison of Ethereum, Hyperledger Fabric and Corda. Frankfurt School Blockchain Center, 2017, http://explore-ip.com/2017_Comparison-of-Ethereum-Hyperledger-Corda.pdf.

[101] Assessing a Blockchain Platform: A Technical Primer. http://www.gartner.com/webinar/3805068.

[102] Eberhardt, Jacob, y Stefan Tai. «On or Off the Blockchain? Insights on Off-Chaining Computation and Data». Service-Oriented and Cloud Computing, editado por Flavio De Paoli et al., vol. 10465, Springer International Publishing, 2017, pp. 3-15. Crossref, doi:10.1007/978-3-319-67262-5_1.

[103] Corda | Home. https://www.corda.net/. Accedido marzo de 2019.

Anexo 1: Plataformas relevadas

Plataforma	Open Source		Popularidad	
	Licencia	Repositorio	Stars	Documentación
Ethereum	Si (LGPL-3.0)	https://github.com/ethereum	17091	http://www.ethdocs.org/en/latest/
Corda	Si (Apache-2.0)	https://github.com/corda/corda	1818	https://docs.corda.net/
EOS	Si, MIT License	https://github.com/EOSIO/eos	6871	https://github.com/EOSIO/Documentation
Hyperledger Fabric	Si (Apache-2.0)	https://github.com/hyperledger/fabric	5080	Hyperledger Fabric Wiki
Cardano	Si	https://github.com/input-output-hk/cardano-sl	2421	https://cardanodocs.com/
Nem	Si, MIT License	https://github.com/NemProject/nem.core	266	https://docs.nem.io/en
Stellar	Si, Apache License v2	https://github.com/stellar/stellar-core	1521	https://www.stellar.org/developers/
BigChainDB	Si, Apache 2.0	https://github.com/bigchaindb/bigchaindb	2499	
Neo	Si, MIT License	https://github.com/neo-project/neo	2317	http://docs.neo.org/en-us/index.html
Quorum	Si (LGPL-3.0)	https://github.com/jpmorganchase/quorum	2155	https://github.com/jpmorganchase/quorum/wiki
Hyperledger Sawtooth	Si (Apache-2.0)	https://github.com/hyperledger/sawtooth-core	6242	https://sawtooth.hyperledger.org/docs/
Tendermint	Si	https://github.com/tendermint/tendermint	1795	https://tendermint.readthedocs.io/en/master/
Hyperledger Composer	Si (Apache-2.0)	https://github.com/hyperledger/composer	1051	https://hyperledger.github.io/composer/latest/introduction/introduction.html
IOTA	Si (GPL-3.0)	https://github.com/iotaledger	937	
Hyperledger Iroha	Si (Apache-2.0)	https://github.com/hyperledger/iroha	764	http://iroha.readthedocs.io/en/latest/
Waves	Si, Apache 2.0	https://github.com/wavesplatform/Waves	666	https://docs.wavesplatform.com/
Elements	Si, Mit license	https://github.com/ElementsProject/elements	525	
RSK	Si, LGPL-3	https://github.com/rsksmart/rskj	412	
Hyperledger Burrow	Si (Apache-2.0)	https://github.com/hyperledger/burrow	385	https://wiki.hyperledger.org/projects/burrow
Multichain	Si (GPL-3.0)	https://github.com/MultiChain/multichain	372	https://www.multichain.com/developers/
OpenChain	Si (Apache-2.0)	https://github.com/openchain/openchain	370	https://docs.openchain.org/en/latest/
Ethereum classic	Si (LGPL-3.0)	https://github.com/ethereumproject/go-ethereum	311	http://ethereum-classic-guide.readthedocs.io/en/latest/
HydraChain	Si (MIT)	https://github.com/HydraChain/hydrachain	302	
Counterparty	Si, MIT License	https://github.com/CounterpartyXCP/counterparty-lib	238	https://counterparty.io/docs/protocol_specification/
Omni	Si, MIT license	https://github.com/OmniLayer/spec	0	https://github.com/OmniLayer/spec
Nxt	Si, Apache 2.0	https://bitbucket.org/Jelurida/nxt/src/master/	0	http://nxtwiki.org/wiki/Main_Page
Symbiont Assembly	Si	N\A	0	
GemOS	No	N\A	NA	
MasterCard Blockchain	No	N\A	NA	
Sequence	No		NA	https://dashboard.seq.com/docs
Factom	No		NA	https://www.factom.com/devs/docs
Domus tower	No		NA	
Constellation	No		NA	
Pokitdok/Dockchain	No		NA	https://platform.pokitdok.com/documentation/v4/
StreamCore	No		NA	
Onchain	No		NA	
AxCore	No		NA	
Coinstack	No		NA	https://docs.bigchaindb.com/en/latest/
Bubichain	No		NA	
Digital Asset Platform	No		NA	
Oracle Blockchain Cloud Service	No		NA	
Polkadot	No		NA	
Nexledger	No		NA	
OpenCSD	No		NA	
Swirlds	No		NA	
Stratis platform	No		NA	https://stratisplatform.com/academy/academy-resources/
IBM Blockchian Platform	No		NA	
Ripple	No		NA	
Coco framework	No		NA	
Bankchain	No		NA	
Ziliqa	No		NA	
Viant				

Plataforma	Support and Documentation Web Oficial	Whitepaper
Ethereum	https://www.ethereum.org/	https://github.com/ethereum/wiki/wiki/White-Paper
Corda	https://www.corda.net/	https://docs.corda.net/_static/corda-technical-whitepaper.pdf
EOS	https://eos.io/	https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md
Hyperledger Fabric	https://www.hyperledger.org/projects/fabric	https://arxiv.org/pdf/1801.10228.pdf
Cardano	https://www.cardano.org/	https://www.cardano.org/en/academic-papers/
Nem	https://nem.io	https://docs.nem.io/en/whitepapers
Stellar	https://www.stellar.org/	https://www.stellar.org/papers/stellar-consensus-protocol.pdf
BigChainDB	https://www.bigchaindb.com/	
Neo	https://neo.org/	http://docs.neo.org/en-us/index.html
Quorum	https://www.jpmorgan.com/quorum	https://www.blocksg.com/single-post/2017/12/27/Quorum-Whitepaper
Hyperledger Sawtooth	https://www.hyperledger.org/projects/sawtooth	https://www.hyperledger.org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_WhitePaper.pdf
Tendermint	https://tendermint.com/	https://cosmos.network/whitepaper
Hyperledger Composer	https://hyperledger.github.io/composer	
IOTA	https://www.iota.org/	https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvslqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf
Hyperledger Iroha	http://iroha.tech/	https://github.com/hyperledger/iroha/blob/master/docs/iroha_whitepaper.md
Waves	https://wavesplatform.com/	https://s3.ca-central-1.amazonaws.com/wavesdb.com/images/whitepaper_v0.pdf
Elements	https://elementsproject.org/	https://blockstream.com/bitcoin17-final41.pdf (Confidential assets)
RSK	https://www.rsk.co/	https://uploads.strikinglycdn.com/files/ec5278f8-218c-407a-af3c-ab71a910246d/RSK%20White%20Paper%20-%20Overview.pdf
Hyperledger Burrow	https://www.hyperledger.org/projects/hyperledger-burrow	https://www.hyperledger.org/wp-content/uploads/2017/06/HIP_Burrowv2.pdf
Multichain	https://www.multichain.com/	https://www.multichain.com/download/MultiChain-White-Paper.pdf
OpenChain	https://www.openchain.org/	
Ethereum classic	https://ethereumclassic.github.io/	https://ethereumclassic.github.io/assets/etc-thesis.pdf
HydraChain		
Counterparty	https://counterparty.io/	
Omni	http://www.omnilayer.org/	
Nxt	https://nxtplatform.org/	https://www.dropbox.com/s/cbuwrorf672c0yy/NxtWhitepaper_v122_rev4.pdf
Symbiont Assembly	https://symbiont.io/	
GemOS	https://gem.co/	
MasterCard Blockchain	https://developer.mastercard.com/product/mastercard-blockchain	
Sequence	h https://www.factom.com/	
Factom	https://www.factom.com/	https://www.factom.com/devs/docs/guide/factom-white-paper-1-0
Domus tower	http://domustower.com/	http://domustower.com/domus-tower-blockchain-latest.pdf
Constellation	https://constellationlabs.io/	https://github.com/Constellation-Labs/Whitepaper/blob/master/constellation_whitepaper_v0.1.pdf
Pokitdok/Dockchain	https://pokitdok.com/dokchain/?source=download/whitepaper/	https://pokitdok.com/wp-content/themes/pokitdok2017/dokchain/static/data/DokChainWhitepaper20170926Draft.pdf
StreamCore	https://www.alphapoint.com/trans-streamcore.html	
Onchain	http://www.onchain.com/	
AxCore	https://axoni.com/	
Coinstack	https://www.blocko.io/	
Bubichain	http://www.bubi.cn/	http://www.bubi.cn/whitePaper/index.jhtml
Digital Asset Platform	http://www.digitalasset.com/	
Oracle Blockchain Cloud Service	https://www.oracle.com/cloud/blockchain/index.html	
Polkadot	https://polkadot.network/	https://polkadot.network/Polkadot-lightpaper.pdf
Nexledger	https://www.samsungsds.com/global/en/solutions/off/nexledger/Nexledger.html	https://www.samsungsds.com/global/en/enterprise-asset/cello_WP12_en.html
OpenCSD	https://setl.io/	
Swirlds	https://www.swirlds.com/	
Stratis platform	https://stratisplatform.com/	https://stratisplatform.com/files/Stratis_Whitepaper.pdf
IBM Blockchian Platform	https://console.bluemix.net/docs/services/blockchain/index.html#ibm-blockchain-platform	
Ripple	https://ripple.com/	
Coco framework		https://github.com/Azure/coco-framework/blob/master/docs/Coco%20Framework%20whitepaper.pdf
Bankchain	https://www.paxos.com/bankchain	
Ziliqa	https://www.zilliqa.com/	
Viant	https://viant.io/	

Plataforma	Consenso		Permissioned	Smart Contracts	
	Mecanimismo	Nivel		Turing completo	Verificable
Ethereum	Proof of Work (soon PoS)	Ledger	No	Si	En desarrollo
Corda	"pluggable" consensus (se puede elegir según necesidad). Verification y Uniqueness	Transacción	Si	Si	
EOS	Delegated proof of stake		Role Based Permission Management	Si	
Hyperledger Fabric	pluggable consensus protocols	Transacción	Si	Si	
Cardano	Ouroboros Proof of Stake https://www.cardano.org/en/ouroboros/		No	Si	Si
Nem	Proof of Importance			No	
Stellar	Stellar consensus protocol (https://www.stellar.org/developers/guides/concepts/scp.html)			Si	
BigChainDB					
Neo	Delegated Byzantine Fault Tolerant			Si	
Quorum	QuorumChain (basado en votación)		Si	Si	
Hyperledger Sawtooth	Proof of Elapsed Time		Si	Si	
Tendermint	Byzantine-Fault Tolerant				
Hyperledger Composer	pluggable consensus protocols		Si	Si	
IOTA	Proof of work		No	No	
Hyperledger Iroha	YAC		Si		
Waves	Leased Proof of Stake			Si	
Elements					
RSK				Si	
Hyperledger Burrow	Tendermint		Si	Si	
Multichain	No necesita algoritmo de consenso ya que los miners son un conjunto de entidades identificadas			No	
OpenChain	Basado en confianza		Si		
Ethereum classic	Proof of Work		No	Si	
HydraChain					
Counterparty	Proof of Work		No	Si	
Omni				Si	
Nxt	Proof of Stake		No	No	
Symbiont Assembly					
GemOS					
MasterCard Blockchain			Si		
Sequence				No	
Factom					
Domus tower					
Constellation	Algoritmo propio. HyloChain			Si	
Pokitdok/Dockchain	Proof of Elapsed Time (PoET)		Si	Si	
StreamCore					
Onchain					
AxCore					
Coinstack					
Bubichain				Si	
Digital Asset Platform				Si	
Oracle Blockchain Cloud Service					
Polkadot					
Nexledger					
OpenCSD					
Swirlds					
Stratis platform			Si	Si porque soporta el desarrollo sobre Ethereum	
IBM Blockchian Platform					
Ripple					
Coco framework					
Bankchain					
Ziliqa					
Viant					

Plataforma	Lenguajes de programación	Interoperabilidad	Gobierno	Escalabilidad
Ethereum	GoLang, Solidity	Minima	Ethereum developers	Sharding y posible implementacion de Raiden Network
Corda	Kotlin, Java	Entre redes corda y en desarrollo con Hyperledger Fabric (https://www.r3.com/blog/interoperability-types/)	R3	
EOS	c++, web assambly			
Hyperledger Fabric	Go, Java, NodeJS		Linux Foundation	
Cardano	Haskell			
Nem	Python, Java, C#, Javascript, NodeJS, Ruby, PHP, Go			
Stellar	REST API, Java, Javascript, Go, Python, C#, Ruby			
BigChainDB				
Neo	Java, .NET, Kotlin, C#			
Quorum				
Hyperledger Sawtooth	Python, JavaScript, Go, C++, Java, Rust		Linux Foundation	
Tendermint				
Hyperledger Composer	Javascript		Linux Foundation	
IOTA	Java			
Hyperledger Iroha			Linux Foundation	
Waves				
Elements				
RSK				
Hyperledger Burrow			Linux Foundation	
Multichain				
OpenChain	C#			
Ethereum classic	GoLang			
HydraChain				
Counterparty				
Omni				
Nxt				
Symbiont Assembly				
GemOS				
MasterCard Blockchain				
Sequence	Java, Ruby, node			
Factom				
Domus tower				
Constellation				
Pokitdok/Dockchain	Python, Ruby, Java, C#			
StreamCore				
Onchain				
AxCore				
Coinstack				
Bubichain				
Digital Asset Platform				
Oracle Blockchain Cloud Service				
Polkadot				
Nexledger				
OpenCSD				
Swirlds				
Stratis platform	C#			
IBM Blockchian Platform				
Ripple				
Coco framework				
Bankchain				
Ziliqa				
Viant				

Plataforma	Criptomoneda	Pricing	First commit	Latest commit	Commits	Contributors	Forks
Ethereum	Ether	No	22/12/2013	Today	9562	259	5416
Corda	No	NA	1/11/2015	Today	5605	70	472
EOS			2/04/2017	Today	6099	108	1658
Hyperledger Fabric	No		22/05/2016	Today	5898	121	3017
Cardano	ADA		25/09/2016		13880	67	371
Nem			19/04/2015	24 days ago	671	4	88
Stellar			23/11/2014		4144	47	408
BigChainDB			7/02/2016	Today	4091	48	476
Neo			31/05/2015	2 days ago	385	20	715
Quorum			22/12/2013	Today	7942	113	446
Hyperledger Sawtooth	No		27/03/2016	Today	830	56	422
Tendermint			18/05/2014	Today	3677	49	362
Hyperledger Composer	No		13/11/2016	Today	4845	72	506
IOTA			23/10/2016	Today	1498	32	320
Hyperledger Iroha			4/09/2016	Today	5799	34	234
Waves			18/01/2015	Today	7572	30	178
Elements			30/08/2009	Today	13706	419	193
RSK			14/05/2017	Today	2323	19	94
Hyperledger Burrow			7/06/2015		1281	16	145
Multichain			25/12/2016	Jan 29, 2018	481	3	164
OpenChain			28/06/2015	Dec 6, 2016	600	1	152
Ethereum classic	Ether, Tokens via smart contracts	No	22/12/2013	Today	9205	102	124
HydraChain			30/08/2015	Dec 28, 2016	297	10	100
Counterparty			15/12/2015		2984	24	158
Omni			3/11/2013	N\A	N\A	N\A	N\A
Nxt			2013	2017-08-24			
Symbiont Assembly			0	N\A	N\A	N\A	N\A
GemOS			2013	Today	N\A	16	N\A
MasterCard Blockchain			0	N\A	N\A	N\A	
Sequence			0	N\A	N\A	N\A	
Factom	Si, Factom		0	N\A	N\A	N\A	N\A
Domus tower			0	N\A	N\A	5	N\A
Constellation			0	N\A		N\A	N\A
Pokitdok/Dockchain			0	N\A	N\A	N\A	N\A
StreamCore			0	N\A	N\A	N\A	N\A
Onchain			0	N\A	N\A	N\A	N\A
AxCore			0	Today	N\A		N\A
Coinstack			0		N\A		N\A
Bubichain			0	N\A	N\A		N\A
Digital Asset Platform			0	N\A	N\A	N\A	N\A
Oracle Blockchain Cloud Service			0	N\A	N\A	N\A	N\A
Polkadot			0	N\A	N\A	N\A	N\A
Nexledger			0	N\A	N\A	N\A	N\A
OpenCSD			0	N\A	N\A	N\A	N\A
Swirlds			0	N\A	N\A	N\A	N\A
Stratis platform			0	NA	NA	NA	NA
IBM Blockchian Platform			0				
Ripple			0				
Coco framework			0				
Bankchain			0				
Ziliqa			0				
Viant							

Plataforma	Desventajas conocidas	Ventajas conocidas	Aplicaciones
Ethereum			Proposito general
Corda			Insurewave
EOS			
Hyperledger Fabric		Modular, performante	
Cardano			
Nem			
Stellar			
BigChainDB			
Neo			
Quorum			
Hyperledger Sawtooth		Admite smart contracts de ethereum	
Tendermint			
Hyperledger Composer		Desarrollo rápido de aplicaciones	
IOTA	Actualmente no se permite correr una red privada	Muy escalable, bajo consumo de recursos, "Quantum Immune" (seguridad frente a computación cuántica)	
Hyperledger Iroha			
Waves		Soporta hasta 6.000 transacciones por minuto.	
Elements			
RSK			
Hyperledger Burrow		Admite smart contracts de ethereum	
Multichain			
OpenChain		transacciones se agregan en tiempo real	
Ethereum classic			
HydraChain			
Counterparty			
Omni			
Nxt		Blocktime de 1 minuto	
Symbiont Assembly			
GemOS			
MasterCard Blockchain			
Sequence			
Factom			
Domus tower			
Constellation		Horizontally Scalable, Fast Transactions, No Transaction Fees, Truly Decentralized, Mobile Compatible, Smart Contracts	
Pokitdok/Dockchain		Identity Management	
StreamCore			
Onchain			
AxCore			
Coinstack			
Bubichain			
Digital Asset Platform			
Oracle Blockchain Cloud Service			
Polkadot			
Nexledger		Distributed Ledger Platform for Enterprise	
OpenCSD			
Swirlds			
Stratis platform			
IBM Blockchian Platform			
Ripple			
Coco framework			
Bankchain			
Ziliqa			
Viant			

Plataforma	Notas
Ethereum	
Corda	
EOS	Aún en desarrollo
Hyperledger Fabric	
Cardano	
Nem	
Stellar	
BigChainDB	The blockchain database.
Neo	
Quorum	
Hyperledger Sawtooth	
Tendermint	Tendermint admite miles de transacciones por segundo.
Hyperledger Composer	
IOTA	No usa una cadena de bloques sino un grafo dirigido y acíclico de transacciones
Hyperledger Iroha	
Waves	"fastest blockchain in the world"
Elements	
RSK	
Hyperledger Burrow	
Multichain	
OpenChain	
Ethereum classic	
HydraChain	
Counterparty	Corre sobre la blockchain de Bitcoin
Omni	Built on top of the Bitcoin blockchain, Como es fork the bitcoin los forks y commits no dicen nada del proyecto
Nxt	
Symbiont Assembly	
GemOS	
MasterCard Blockchain	
Sequence	
Factom	
Domus tower	1 million transactions per second.
Constellation	Es del estilo de IOTA, no es una plataforma de blockchain estrictamente sino que es una red descentralizada
Pokitdok/Dockchain	Es blockchain as a service
StreamCore	
Onchain	
AxCore	THE FINTECH 250 The Fintech 250 identifies and recognizes the 250 most promising private fintech companies from around the world. DERIVATIVE INDUSTRY INITIATIVE OF THE YEAR The GlobalCapital awards honor the companies, platforms, services, and products that have grown, innovated, and strengthened the global derivatives market.
Coinstack	COINSTACK, LA SOLUCIÓN BLOCKCHAIN PARA EMPRESA.
Bubichain	
Digital Asset Platform	
Oracle Blockchain Cloud Service	
Polkadot	
Nexledger	Distributed Ledger Platform for Enterprise
OpenCSD	
Swirlds	
Stratis platform	
IBM Blockchian Platform	
Ripple	No es una blockchain, es una moneda digital para bancos
Coco framework	
Bankchain	
Ziliqa	
Viant	

Plataforma	Partners	Utilizado por	Topología	Fork of
Ethereum	Microsoft, JP.Morgan, Satander, BBVA, Intel (500)			Ethereum Classic
Corda	Son más de 60, entre ellos Microsoft, Intel, Oracle, AWS https://www.r3.com/ecosystem/			No aplica
EOS				
Hyperledger Fabric				
Cardano			https://cardanodocs.com/cardano/topology/	
Nem				
Stellar		Deloitte, Tempo, Parkway		
BigChainDB				
Neo				
Quorum				Ethereum
Hyperledger Sawtooth				
Tendermint				
Hyperledger Composer				
IOTA				
Hyperledger Iroha				
Waves	Deloitte			
Elements				
RSK				
Hyperledger Burrow				Ethereum
Multichain				
OpenChain				
Ethereum classic				No aplica
HydraChain				Ethereum
Counterparty				
Omni				Bitcoin
Nxt				
Symbiont Assembly				
GemOS				
MasterCard Blockchain				
Sequence	VISA, citi, Nasdaq, State Street			
Factom				
Domus tower				
Constellation	Batshit, Cryptodex, Connectcapital, TLDRCapital, Chainrock, CRYPTOBazar			
Pokitdok/Dockchain				
StreamCore				N\A
Onchain				
AxCore				
Coinstack				
Bubichain				
Digital Asset Platform	JP.Morga, citi, NEX, Santander, IBM			
Oracle Blockchain Cloud Service				
Polkadot				
Nexledger				
OpenCSD				
Swirlds				
Stratis platform				NA
IBM Blockchian Platform				
Ripple				
Coco framework				
Bankchain				
Ziliqa				
Viant				Ethereum

Anexo 2: Análisis y especificación de casos de uso

A continuación se mencionan escenarios, contextos y casos de uso particulares en donde la aplicación de la tecnología blockchain constituye una solución a problemas existentes.

Para desarrollar el conjunto de escenarios a presentar se analizan propuestas existentes respecto a cuándo aplica la utilización de una blockchain y cuando no. Estas propuestas se encuentran disponibles en [3] [4].

Los escenarios identificados se clasifican según el área al cual pertenecen:

Salud

Una de las posibles industrias o sistemas en los cuales puede incorporarse blockchain es en salud. Es conocido como uno de los sectores en los cuales la digitalización ha sido un proceso lento en comparación con adopciones en otras industrias, por varios motivos, uno de ellos debido a la sensibilidad de la información que en este ámbito se manipula. Además, la gestión de los servicios de salud y las partes involucradas pueden ser de suma complejidad dependiendo de las reglamentaciones de los diferentes países.

Existen actualmente algunas iniciativas que pretenden resolver algunos de los problemas en esta área utilizando blockchain:

- Pagos en el sistema de salud: No es el caso de Uruguay, pero en países como Estados Unidos donde los servicios de salud se contratan en modalidad de seguros, los pagos de los mismos involucran a muchas entidades y pueden resultar de gran complejidad. Un seguro de salud puede ser utilizado en diferentes instituciones prestadoras de servicios y con estos se accede a un conjunto de servicios dependiendo del tipo de seguro que se obtenga, los pagos pueden realizarse a través de bancos, préstamos, etc.

  IBM Blockchain propone la utilización de blockchain para resolver alguno de los problemas que el pago en los sistemas de salud implica (pagar a los proveedores y aseguradoras a tiempo, brindar servicios a pacientes cuando lo requieren, evitar un

"doble registro" y acceder desde un solo sitio a la información completa de los pacientes)

- MedRec: Esta iniciativa proponen una nueva forma de almacenar historias clínicas electrónicas (HCE) utilizando blockchain, con el objetivo de brindar a los pacientes un registro inmutable de fácil acceso a las mismas. La plataforma resuelve el problema de la autenticación, confidencialidad, contabilidad y la posibilidad de intercambiar datos entre los prestadores de salud. Utilizan prueba de trabajo como protocolo de consenso incentivando a investigadores y autoridades sanitarias a participar en la red como mineros recibiendo a cambio acceso a la información (anonimizada) para ser utilizada con diferentes propósitos [60].
- PokitDok/DocChain: DokChain es una red distribuida de nodos que procesan transacciones sobre datos clínicos e información financiera relativa a la industria de la salud. Tiene como objetivo aprovechar las ventajas que brinda la tecnología blockchain involucrando a las diferentes partes interesadas para construir una nueva economía en la cual los datos y servicios en salud sean cuantificables e intercambiables; garantizando además la seguridad y privacidad de la información [61] [62].

Gobierno

Una de las principales áreas en las cuales la tecnología blockchain promete contribuir es en el desarrollo de aplicaciones para gobiernos.

En [63] se presentan diferentes escenarios en los cuales al utilización de blockchain resulta de utilidad, entre ellos se encuentran:

- Manejo de identidad y almacenamiento de registros (Se menciona el caso de Estonia, en donde se encuentran realizando un proyecto para otorgar residencias electrónicas).
- Almacenamiento de documentos (por ejemplo partidas de nacimiento, certificados de votación, libretas de matrimonio, etc.).
- Sistemas de votación.
- Salud (almacenar las historias clínicas de modo que sean accesibles desde cualquier prestador en caso de así requerirse, así como también contribuir en tareas de investigación publicando en la blockchain registros anonimizados).

- Smart cities, IoT.

Cadenas de suministro

Existen hoy en día numerosas alianzas entre diferentes empresas y organizaciones con el objetivo de incorporar la tecnología blockchain a los procesos involucrados en las cadenas de suministro. Si bien las posibles aplicaciones entorno a estos procesos difieren, existen elementos que son comunes:

- La utilización de blockchain en estos casos tiene como objetivo brindar transparencia al proceso así como también agilizarlo. Se pretende además reducir la posibilidad de fraude u ocurrencia de errores, mejorar la administración de inventarios, minimizar los costos de traslados, identificar a los involucrados en el proceso, reducir demoras por papeleo.
- Respecto a la solución para registrar la trazabilidad de diferentes productos/objetos/activos involucrados, los proyectos propuestos proponen la utilización de sensores conectados a internet que permitan determinar en dónde y en manos de quién se encuentran los productos.
- Son proyectos pilotos, acuerdos entre organizaciones y el acceso a información académica o formal respecto a su implementación en particular es escasa.
- Se propone la utilización de contratos inteligentes para definir reglas de negocio.

A continuación se detallan algunos ejemplos de este tipo de caso de uso:

- Viant: Es una plataforma de blockchain, basada en Ethereum que en conjunto con Microsoft Azure, lanzaron en Diciembre un proyecto que tiene como objetivo, utilizando blockchain, proveer un mecanismo que permita verificar paso a paso el trayecto del pescado desde que es capturado en el océano hasta que llega al plato de los consumidores [64] [65].
- Blockchain Food Safety Alliance: IBM Blockchain Platform, Walmart, JD.com y la universidad de Tsinghua anunciaron en Diciembre de 2017 un proyecto en el cual se pretende mejorar el *tracking*, la trazabilidad y la seguridad de los alimentos en China. La blockchain pretende ser utilizada para brindar información acerca de la trazabilidad de los alimentos en tiempo real. El grupo pretende cumplir sus objetivos involucrando a proveedores, reguladores de la industria y la comunidad científica,

desarrollando protocolos y procesos que, utilizando blockchain, brinden mayor transparencia al proceso. Existen actualmente pilotos de este proyecto, para registrar la trazabilidad del cerdo y el mango en China y en Estados Unidos y Walmart afirma que, la utilización de blockchain para el proceso, ha reducido el tiempo necesario para rastrear mangos desde la granja hasta el supermercado (pasando de llevar días e incluso semanas a segundos).

Similar a esta propuesta IBM ha anunciado colaboraciones con otras empresas de la industria alimenticia como son: Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, Unilever and Walmart to Address Food Safety Worldwide [66].

- IBM Blockchain and SAP IoT Solution for the Pharmaceutical Cold Chain. Este proyecto pretende, utilizando blockchain y IoT brindar una solución a la cadena de frío que debe mantenerse en la industria farmacéutica para determinados fármacos. Se propone utilizar sensores, conectados a internet que brinden información de los fármacos (ubicación, temperatura) y que dicha información sea registrada en una blockchain en determinados eslabones de la cadena. Se propone la utilización de contratos inteligentes para establecer reglas de negocio. A modo de ejemplo, si el sensor de temperatura registra un valor superior a determinado umbral establecido el paquete debe ser inspeccionado y se asigna como responsable de las pérdidas al integrante de la cadena que registre temperaturas superiores al umbral [58].
- Insurwave: Es una plataforma, construida sobre Corda, puesta en producción por EY, Guardtime, A.P.Moller-Maersk, Microsoft, Willis Towers Watson, XL Catlin, MS Amlin, y ACORD. Pretende que todas las partes accedan en tiempo "casi" real a la ubicación, condiciones y seguridad de los activos [67] [68] [69].
- TrustChain: Es una colaboración que tiene el objetivo de utilizar la IBM Blockchain Platform para registrar la trazabilidad de las joyas desde que se extraen hasta que son transformadas en una pieza final y entregadas a un punto de venta [70]. Es por ahora una prueba de concepto pero se espera su puesta en producción para fines de 2018.

Artículos académicos al respecto:

"Towards an Ontology-Driven Blockchain Design for Supply Chain" [71]: propone una ontología para el diseño de este tipo de sistemas.

“Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT” [59]. Se estudia la utilización de blockchain e internet de las cosas y en especial, se propone un sistema de control de acceso para dispositivos de IoT que permita escalar en escenarios donde este tipo de dispositivos abundan, como es el caso mencionado en este punto.

Arte

En la industria del arte y el entretenimiento ha existido desde sus inicios problemáticas relacionadas con el derecho de autor y la autenticidad. La utilización de la tecnología blockchain en esta industria puede ser de especial utilidad para garantizar un intercambio de este tipo de bienes en dónde sus propietarios así como también quienes crearon las piezas de arte (esculturas, pinturas, música, etc.) reciban la remuneración correspondiente según los derechos de autor, pudiendo evitar también casos de falsificación o piratería sin la necesidad de contar con un intermediario.

A continuación se detallan algunos ejemplos de este tipo de casos de uso:

- Una de las propuestas es la utilización de la tecnología blockchain para llevar un registro de las transacciones de pinturas, esculturas, etc. de modo de conocer cuando estas están siendo exhibidas en exposiciones, a quién pertenecen, su origen, etc. [72] [73] [74].

  Como ejemplo de un proyecto en particular, se destaca Verisart [75]. Verisart utiliza la tecnología blockchain para generar certificados de autenticidad de las piezas de arte, verificar la proveniencia de las piezas, registrar a quién pertenecen y proteger la identidad de los propietarios, entre otros. Además, provee de una API para interactuar con la plataforma.
- Ujo: Este proyecto utiliza blockchain para crear una base de datos de derechos y propiedad intelectual en la industria de la música [76].

Filantropía

Otra de las posibles aplicaciones de la tecnología blockchain, que se encuentra relacionada de cierto modo con las aplicaciones respecto a cadenas de suministro, son las donaciones. Es un problema conocido que en muchos casos quienes realizan donaciones no reciben garantías ni retroalimentación respecto al destino y distribución de sus contribuciones. En muchos casos, en circunstancias en las cuales se realizan donaciones ocurren robos, pérdidas o los activos donados no tienen los destinos que deberían.

IBM en conjunto con Global Citizen, lanzaron en Mayo de 2018 el concurso “Challenge accepted” para construir una aplicación utilizando blockchain que permita llevar un registro de las donaciones. La propuesta particular es construir una red con tres nodos: un gobierno, AID.org y GlobalCitizen en la cual las transferencias de fondos las realiza el gobierno, se registran con las organizaciones AID y se validan por parte de GlobalCitizen [77].

Si bien esta propuesta pretende resolver una realidad acotada se espera que se desarrollen nuevos proyectos entorno a esta área.

Identidad

La validación de identidad es muy importante en el sector financiero. Identificar usuarios normalmente requiere el uso de canales físicos para demostrar ser quien dice ser, un usuario muestra algún tipo de documento de identidad, lo cual es ineficiente y propenso a errores.

Instituciones financieras de Canadá reconocieron este problema y se asociaron con SecureKey Technologies para lanzar el servicio SecureKey Concierge, el cual permite a los usuarios autenticarse utilizando por ejemplo sus credenciales bancarias [78]. Utilizando Hyperledger Fabric se construyó una herramienta donde los bancos y otras empresas son proveedores de datos relacionados a la identidad de las personas tales como su nombre, número de documento, edad o puntaje crediticio, y los usuarios eligen cuándo y a quién mostrar atributos específicos de su identidad.

Sector financiero

La tecnología blockchain adquirió popularidad tras la publicación del artículo de Nakamoto en el cual presenta Bitcoin.
Así como Bitcoin se han desarrollado diferentes sistemas de pago electrónico, sin embargo este tipo de aplicaciones no es el único en el sector financiero.
Existen, por ejemplo, aplicaciones para adquirir y realizar préstamos [79]; *crowd-funding* [80], aseguradoras, entre otros.

Gobierno

La democracia líquida o democracia delegativa revocable es una forma de democracia directa que incluye la posibilidad de delegación de voto revocable de forma instantánea, de ahí su liquidez [81]. Este tipo de sistemas puede ser implementado a través de un sistema de tesorería. Un sistema de tesorería es un mecanismo de toma de decisiones colaborativo descentralizado y controlado por la comunidad para el financiamiento sostenible del desarrollo y mantenimiento de blockchain. Durante cada período de tesorería, las propuestas de proyectos se envían, discuten y votan; los proyectos mejor calificados son financiado por el tesoro. El sistema de gobierno Dash [82] es un ejemplo del mundo real de ese tipo de sistemas [83].

De esta forma la blockchain brinda soporte para la utilización de democracia líquida a aplicaciones que se construyan encima de la misma.

Anexo 3: Conociendo plataformas

Para elaborar una taxonomía que resulte de utilidad a la hora de tomar decisiones en un proyecto donde se pretenda utilizar blockchain, es necesario primero conocer al menos algunas de las plataformas más relevantes. Por ello, se realiza un relevamiento y posterior análisis de plataformas existentes, identificando las características más importantes.

Luego de estudiar a nivel teórico las plataformas seleccionadas como más relevantes, se procede a implementar pruebas de concepto sobre algunas de ellas. Esto permite identificar posibles fortalezas y debilidades en las plataformas, adicionales a las características encontradas en el relevamiento inicial. Por ejemplo, una plataforma puede tener a primera vista muchos puntos a favor por ser flexible en muchos aspectos y ser en teoría aplicable para una gran variedad de escenarios de negocio distintos, pero por otro lado puede ser mucho más compleja de utilizar que otras plataformas más sencillas o con características más restringidas.

Otra ventaja de realizar pruebas de concepto es la posibilidad de validar la información relevada anteriormente. Es decir, comprobar en cierta medida las especificaciones de cada plataforma. Los desarrolladores de este tipo de tecnologías suelen promocionar su trabajo alegando muchas virtudes tales como facilidad de uso e instalación en múltiples plataformas, pero esta información es generalmente subjetiva.

Puntualmente las plataformas elegidas para realizar pruebas de concepto son tres: Corda, Hyperledger Fabric y NEM. Para la implementación de pruebas de concepto sobre las plataformas seleccionadas se utilizan guías o tutoriales provistos por los propios desarrolladores, en los cuales se especifica cómo instalar los componentes necesarios, y construir una red básica.

A continuación se describen las pruebas realizadas sobre cada plataforma.

Corda

Corda es una plataforma de blockchain privada de código abierto, según la clasificación especificada en la taxonomía. Sin embargo, si bien en la documentación de dicha plataforma se especifica que es una plataforma blockchain, se hace especial hincapié en que es una tecnología de libro mayor distribuido o DTL por sus siglas en inglés. Corda se diferencia de las plataformas tradicionales en que no todos los nodos de la red cuentan con

una copia de todas las transacciones efectuadas, sino que solo conocen y almacenan aquellas transacciones realizadas por dicho nodo o de las cuales son participantes.

El análisis de la plataforma implica, la comprensión de los conceptos característicos de las plataformas, estudio de la documentación disponible y cómo conceptos generales de las plataformas blockchain se implementan en Corda.

Para comprender en profundidad los conceptos e implementaciones particulares, se realiza el despliegue de un proyecto de ejemplo publicado en la documentación oficial de Corda [84]. La aplicación de ejemplo utiliza la blockchain para llevar un registro de deudas entre diferentes participantes de la red. La red desplegada se constituye de tres nodos: A y B que simulan participantes que pueden emitir deudas entre ellos y un nodo controlador que ejecuta el mapa de la red y cumple el rol de notario (concepto propio de Corda para referenciar a el/los nodo/s de la red encargados de garantizar el consenso así como también opcionalmente validar transacciones). La interacción del usuario de la aplicación con la red blockchain se realiza a través de una interfaz web en la cual se realizan las solicitudes de registro de deudas y consultas sobre el estado del libro mayor.

Con el objetivo de poder determinar la facilidad de extender el escenario utilizado así como también el esfuerzo de agregar nuevos nodos a la red e implementar validaciones específicas de otro escenario, se plantea un caso de uso a ser implementado utilizando la plataforma Corda. El escenario propuesto para extender la prueba de concepto realizada es utilizar la blockchain como un registro de auditoría respecto al acceso a las historias clínicas electrónicas (HCE) por parte de los diferentes actores del ecosistema en Uruguay.

Para ello, se modifican las características de los nodos A y B del escenario anterior y se agrega un nodo adicional de modo que:

- exista un nodo por prestador de servicios de salud
- un nodo representa al Ministerio de Salud
- un nodo representa al Sistema Nacional de Salud (SNS): entidad a la cual los distintos prestadores y el Ministerio de Salud solicitan acceso a las HCE

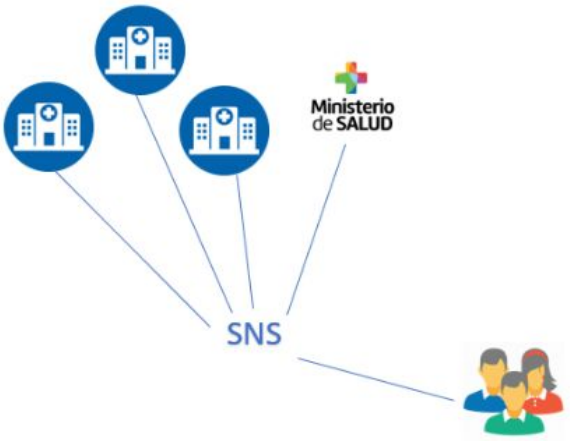


Imagen 35 - Escenario alternativo Corda

El objetivo de utilizar una blockchain en este escenario es brindar un mecanismo que garantice al usuario del ecosistema, es decir al paciente, el acceso autorizado a su história clínica. Para ello se propone que cada vez que un prestador o el Ministerio de Salud soliciten al SNS el acceso a una HCE, se invoque a un servicio que registre en la blockchain el acceso a la HCE (registrando la cédula de identidad del paciente y el identificador del acto médico del paciente que se solicita obtener de su historia clínica). Como fue mencionado, en Corda, el acceso al libro mayor se restringe a los participantes de una transacción, de este modo los prestadores de salud conocen únicamente sus solicitudes y no es posible que otros prestadores las conozcan (garantizando la privacidad de las mismas); pero siendo todas estas transacciones accesibles para el Sistema Nacional de Salud.

Se propone la implementación de una aplicación web para que los pacientes puedan verificar los accesos a sus HCE, lo cual se resuelve realizando una consulta sobre la blockchain, específicamente a la versión del libro mayor que tiene el nodo del SNS por la cédula del paciente.

Del escenario propuesto se implementa el hecho de agregar nodos adicionales identificando cierta dificultad en el proceso ya que es necesario ejecutar comandos específicos para actualizar una red ya existente y específicamente para una ambiente de prueba como el instalado [85]. Además, se modifica el contrato del escenario IOU (en Corda para que una transacción sea aceptada, entre otras cosas, se deben validar lo que se denomina contratos cuya ejecución es determinista) agregando al contrato: la verificación de la cédula de

identidad del paciente, la validación que el identificador del acto médico sea mayor que 0 y que uno de los participantes sea el Sistema Nacional de Salud.
Por último, se modifican la API utilizada por la aplicación web, de modo que el método invocado al querer ingresar una registro en la blockchain reciba los parámetros: identificador del acto médico y cédula del paciente, en lugar de los parámetros utilizados en el escenario de registro de deudas.

Con la prueba de concepto mencionada. se conocen los conceptos e implementación característica de Corda como plataforma blockchain así como también se realizan cambios al escenario de ejemplo provisto en la documentación para conocer el esfuerzo que implica agregar nuevos nodos a la red y crear condiciones específicas en contratos.

La información obtenida es de especial para el desarrollo de la taxonomía ya que contribuye a la especificación de la característica “Control de acceso al libro mayor” y al proceso de aplicación de la taxonomía.

Hyperledger Fabric

Se siguen los pasos indicados en la documentación de Hyperledger [86] para instalar todos los requisitos previos antes de crear una red. Si bien el despliegue de una red en esta plataforma solo requiere la instalación de determinada versión de Docker y Docker-Compose, en fines prácticos es necesario también la instalación de algunos extras tales como el lenguaje de programación Go, Node.js y otros específicos dependiendo del sistema operativo utilizado. De todas formas vale destacar la portabilidad de las soluciones implementadas en esta plataforma, ya que para correr nodos que participen de una red basta con configurar y encender instancias de docker que son compatibles con la mayoría de los sistemas operativos utilizados hoy en día.

Las herramientas brindadas por los desarrolladores permiten rápidamente tener una red de prueba en la que se tienen dos organizaciones, cada una con dos nodos, además de una organización independiente que brinda el servicio de ordenamiento de las transacciones.

El tutorial seguido explica cómo configurar diversos aspectos tales como mecanismos de encripción, políticas de validación de transacciones y creación de canales independientes. Se hace evidente un arma de doble filo de Fabric: su flexibilidad. Por un lado, se permite elegir cómo funcionan muchos aspectos de la red, como por ejemplo su mecanismo de consenso o sus políticas de validación, pero por otro lado, toda esta flexibilidad puede

resultar intimidante aún para usuarios técnicos. Es decir que se tiene un gran control, pero con ello viene también mucha complejidad y responsabilidad en manos del usuario que se encargue de la creación de la red.

Nem

NEM es una plataforma de blockchain de código abierto que se caracteriza por la usabilidad de su API que facilita su incorporación en los sistemas actuales. La plataforma puede utilizarse de forma nativa en su formato de red público o privado. Además esta plataforma carece de contratos inteligentes, y en su lugar utiliza *a*ctivos inteligentes, los cuales permiten realizar transacciones complejas.

Para realizar pruebas sobre una red de NEM se utilizó el tutorial oficial de la plataforma [57]. El mismo consiste en el caso de uso de una cadena de suministros, en la cual se realizan una sucesión de validaciones por parte de varios actores para asegurar que los productos de la cadena cumplan los requerimientos de calidad de la industria.

NEM destaca por su fácil configuración y rápida puesta en marcha. El sistema que se utilizó para la investigación de la plataforma utilizaba contenedores Docker para simular todos los nodos de la red y constituye el proyecto de base para la implementación utilizada como mecanismo de validación de la taxonomía.

Anexo 4: Características de la taxonomía y sus valores posibles

Características duras

Permisionada

Las plataformas de blockchain se pueden clasificar en dos grandes categorías: si son públicas o permisionadas/privadas.

Una blockchain es pública si no existen restricciones en el ingreso a la red, es decir, cualquier nodo que pretenda unirse a la red puede hacerlo. Por otra parte una blockchain es permisionada, o también denominada privada, si el ingreso a la red se encuentra restringido a un conjunto de participantes o se requiere de permisos especiales para formar parte de dicha red. Dichos permisos pueden, según la implementación, ser otorgados por nodos que cumplen un rol específico dentro de la red.

Valores posibles:

- Si: plataforma que permite implementar redes permisionadas/privadas
- No: plataforma que permite implementar redes públicas
- Ambas: plataforma que permite implementar redes públicas y permisionadas

Interoperabilidad

Otra de las características a tener en cuenta al evaluar una plataforma de blockchain es su capacidad de poder comunicarse con otros sistemas fuera de la red.

Según esta clasificación, la interoperabilidad puede ser implícita y/o explícita o no existir interoperabilidad.

Como se menciona en “Taxonomy of blockchain technologies. Principles of identification and classification” [87] la interoperabilidad implícita se encuentra dada por la capacidad de un contrato inteligente de interactuar con interfaces externas y APIs. Esto puede garantizarse si dichos contratos son implementados utilizando un lenguaje de scripting que sea Turing completo. Por ejemplo en Hyperledger Fabric, los contratos inteligentes pueden ser escritos en Node o en Go, lo cual permite interactuar con APIs externas.

Por otra parte, una blockchain tiene la característica de ser interoperable de manera explícita si implementa un mecanismo específico que permita comunicarse con otros sistemas fuera de la red. Por ejemplo en Corda, pese a ser una plataforma privada, existen mecanismos explícitos de comunicación con otras redes Corda, y se están desarrollando mecanismos de comunicación con blockchains de otras plataformas. En este caso la interoperabilidad es una decisión de diseño de la plataforma.

Valores posibles:

- **Implícita**
    - Si: la plataforma implementa mecanismos de interoperabilidad implícita
    - No: la plataforma no implementa mecanismos de interoperabilidad implícita
    - En desarrollo: el proveedor de la plataforma manifiesta dicha característica se encuentra en desarrollo
- **Explícita**
    - Si: la plataforma implementa mecanismos de interoperabilidad explícita
    - No: la plataforma no implementa mecanismos de interoperabilidad explícita
    - En desarrollo: el proveedor de la plataforma manifiesta dicha característica se encuentra en desarrollo

Desempeño

Como se menciona en el artículo “Hyperledger Blockchain Performance Metrics” [88] existen varias medidas que pueden contribuir a determinar el desempeño de una plataforma. En esta clasificación se definen dos: 1) el tiempo de confirmación de una transacción, es decir, el tiempo que transcurre entre que se realiza una propuesta de transacción hasta que luego de ser validada es almacenada en el libro mayor y 2) la cantidad de transacciones que se pueden ejecutar por segundo.

Valores posibles:

- **Tiempo de confirmación**: tiempo en segundos
- **Transacciones por segundo**: cantidad de transacciones por segundo

Tolerancia a fallas

La tolerancia a fallas refiere a la capacidad de continuar funcionando en caso de ocurrir eventos inesperados, garantizando en todo momento la confiabilidad, validez y seguridad de la información almacenada en el libro mayor.

En blockchain este concepto se encuentra fuertemente ligado al consenso y los mecanismos utilizados para ello. A modo de ejemplo, si el consenso no existiera y hubiera una autoridad central que decida qué transacciones agregar a la cadena y cuáles no, no se tendría tolerancia a fallas debido a que la caída de un único nodo (el de la autoridad central) afectaría por completo el funcionamiento de la aplicación. Por el contrario, si se utiliza un consenso como por ejemplo prueba de trabajo, se tendría tolerancia a fallas bizantinas.

La clasificación definida en cuanto a la tolerancia a fallas se realiza en función del mecanismo de consenso utilizado y provee una medida de la cantidad de nodos de la red que pueden estar no disponibles o ser maliciosos sin que esta falle.

Valores posibles:

- **Tolerancia a fallas**: Nombre del tipo de tolerancia a fallas alcanzado por la plataforma.

Contratos inteligentes

Uno de los componentes que ha adquirido gran popularidad en las plataformas blockchain son los contratos inteligentes

La clasificación propuesta se divide en tres subcategorías:

- **Turing completos**: implica que tiene un poder computacional equivalente a la máquina de Turing universal. Estos contratos inteligentes soportan la ejecución de ciclos.
- **Verificables**: la plataforma provee de algún mecanismo que permita detectar contratos que puedan comprometer el funcionamiento de la plataforma como pueden ser bucles infinitos y/o verificar la correctitud de los mismos. Los niveles de verificación varían ampliamente en las diferentes plataformas y es por estas razones que la propuesta en cuanto a este atributo de los contratos inteligentes es clasificarlos según si se provee algún mecanismo de verificación o no en términos generales y adjuntar un comentario que detalle dichos mecanismos.

Valores posibles:

- **Turing completos**
    - Si: si son Turing completos.

    - No: si no son Turing completos.
    - N/A: si la plataforma no soporta contratos inteligentes
- **Verificables:**
    - Si: si son verificables
    - No: si no son verificables
    - N/A: si la plataforma no soporta contratos inteligentes

Manejo de identidad

La clasificación según el manejo de identidad permite brindar conocimiento acerca de si existe o no mecanismos de acceso a la red y si es posible identificar a los participantes de la misma. Por estas razones, la clasificación se divide en dos sub-categorías

- Control de acceso: refiere al mecanismo de control de acceso a la red. Este punto aplica únicamente a redes permisionadas.
- Identidad: el manejo de identidad refiere a la capacidad de la plataforma de validar organizaciones, atributos o datos de un nodo que permitan identificarlo de cierta forma.

Valores posibles:

- **Control de acceso**:
    - N/A: la plataforma no implementa mecanismos de control de acceso a la red.
    - se indica el mecanismo utilizado
- **Identidad**:
    - Si: la plataforma provee de un mecanismo para validar organizaciones, atributos o datos de un nodo que permitan identificarlo.
    - No: la plataforma no provee ningún mecanismo para validar organizaciones, atributos ni datos de un nodo que permitan identificarlo.

Seguridad y privacidad

Según ISO/IEC 27002, la seguridad de la información es la preservación de la confidencialidad, integridad y la disponibilidad de la información [89].

La integridad es una característica intrínseca de la tecnología blockchain, por lo cual no aporta valor a la hora de decidir entre una plataforma u otra debido a que cualquier

plataforma debería asegurar dicha característica. Las plataformas de blockchain implementan diferentes mecanismos para garantizar la seguridad y para la clasificación propuesta se identifican dos de ellos:

- Mecanismo de encripción: refiere al mecanismo de encripción utilizado para la comunicación entre nodos. En versiones posteriores de la taxonomía podría descartarse la clasificación según este mecanismo ya que es altamente probable (en función de las plataformas analizadas) que todas las plataformas utilicen TLS.
- Control de acceso al libro mayor: refiere a si existe un mecanismo que permita restringir el acceso al libro mayor, es decir, que no todos los nodos de la red tengan acceso a todas las transacciones de la blockchain.

Valores posibles:

- Mecanismo de encripción: nombre del mecanismo utilizado
- Control de acceso al libro mayor:
    - Obligatorio: la plataforma implementa un mecanismo de control de acceso al libro mayor y no provee de un mecanismo para no utilizarlo.
    - Opcional: la plataforma implementa un mecanismo de control de acceso al libro mayor y la utilización de dicho mecanismo es opcional.
    - No: la plataforma no implementa un mecanismo de control de acceso al libro mayor.

Involucra criptomoneda:

Este atributo puede valer Sí en caso de involucrar una criptomoneda (tanto para el intercambio de bienes, como incentivo a los mineros o para ejecutar contratos inteligentes) o No en caso contrario.

Valores posibles:

- Si: en caso de involucrar una criptomoneda
- No: en caso de no involucrar una criptomoneda

Consenso

La clasificación definida en cuanto al consenso se define en función del mecanismo utilizado (es decir, el algoritmo) y si este es intercambiable*,* es decir si pueden utilizarse diferentes mecanismos en diferentes contextos dentro de la plataforma.

Valores posibles:

- Intercambiable:
    - Si: El mecanismo de consenso se puede sustituir por otro
    - No: El mecanismo de consenso es fijo
- Mecanismo:
    - Nombre del mecanismo de consenso utilizado por defecto

Protocolo de comunicación

Refiere al protocolo de comunicación utilizado entre los nodos de la red.

Valores posibles:
Se indica el nombre del protocolo de comunicación utilizado.

Incentivos

Particularmente en las plataformas de blockchain públicas existen diferentes mecanismos de incentivos a los nodos mineros para que validen las transacciones
Una posible clasificación de los incentivos es la siguiente:

- Por bloque añadido a la cadena (Caso bitcoin a los mineros)
- Cuotas por transacción (Caso bitcoin a los mineros)
- Al ejecutar contratos inteligentes (Caso Ethereum a los mineros)

Valores posibles:

- **Por bloque**
    - Si: la plataforma provee de un mecanismo de incentivo a mineros por añadir un bloque a la cadena
    - No: la plataforma no provee de un mecanismo de incentivo a mineros por añadir un bloque a la cadena
    - N/A: no aplica este concepto para la plataforma en estudio, esto es común en redes permisionadas dónde pueden no existir mecanismos de incentivos o nodos mineros.
- **Por transacción**
    - Si: la plataforma provee de un mecanismo de incentivo a mineros por cada transacción verificada
    - No: la plataforma no provee de un mecanismo de incentivo a mineros por cada transacción verificada

    - N/A: no aplica este concepto para la plataforma en estudio, esto es común en redes permisionadas dónde pueden no existir mecanismos de incentivos o nodos mineros.
- **Por ejecución de contrato inteligente**
    - Si: la plataforma provee de un mecanismo de incentivo a mineros por cada contrato inteligente ejecutado.
    - No: la plataforma no provee de un mecanismo de incentivo a mineros por cada contrato inteligente ejecutado.
    - N/A: no aplica este concepto para la plataforma en estudio, esto es común en redes permisionadas dónde pueden no existir mecanismos de incentivos o nodos mineros.

Despliegue

Al construir una red de blockchain las plataformas proveen diferentes mecanismos para realizar el despliegue de los nodos. Este punto de la clasificación permite brindar información acerca de las posibilidades y si los principales proveedores de infraestructura brindan entornos pre-configurados para trabajar con plataformas blockchain.

Las alternativas identificadas hasta el momento son: despliegue en la nube, es decir existen proveedores que brindan servidores pre-configurados con el software necesario; despliegue utilizando contenedores Docker u otros mecanismos, por ejemplo, como un servicio del sistema operativo.

Valores posibles:

- **Nube**
    - Si: existen proveedores que brindan servidores pre-configurados con el software necesario
    - No: no existen proveedores que brindan servidores pre-configurados con el software necesario
    - N/A: no es posible, para la plataforma en estudio, realizar el despliegue de nuevos nodos.
- **Docker**
    - Si: la plataforma provee de mecanismos para realizar el despliegue utilizando contenedores Docker

    - No: la plataforma no provee de mecanismos para realizar el despliegue utilizando contenedores Docker
    - N/A: no es posible, para la plataforma en estudio, realizar el despliegue de nuevos nodos.
- **Otro**:
    - N/A: la plataforma no provee de otra alternativa de despliegue.
    - se especifica la alternativa de despliegue.

Entorno de ejecución

Refiere al entorno de ejecución de los nodos. A modo de ejemplo, la plataforma Ethereum implementó su propia máquina virtual denominada Ethereum Virtual Machine (EVM), en Corda los nodos ejecutan en una JVM con restricciones particulares, entre otros.

Valores posibles: se especifica el/los entornos de ejecución.

Tipos de nodos

Según la plataforma considerada, los nodos de la red pueden adquirir diferentes roles y ejecutar diferentes acciones. Cada plataforma define nombres específicos para los diferentes tipos de nodos, es por esto, que se define una clasificación de nodos.

Tipo de nodos:

- **Oráculo**: Nodo que permite obtener información del “mundo exterior”, es decir, fuera de la red.
- **Verificador**: Nodo encargado de verificar las transacciones (que estén firmadas por los involucrados, que no ocurra doble gasto, que se cumplan las condiciones especificadas en contratos, etc.)
- **Portero**: Nodo encargado de controlar el acceso a una blockchain (verifica la identidad y asigna identificación a los nodos)
- **Ordenador**: Nodo encargado de determinar el orden de las transacciones
- **Pares comunes**: Nodos que se comunican con las aplicaciones y el resto de los nodos de la red.

Valores posibles:

- Si: existe un nodo que realice las acciones mencionadas.
- No: no existe un nodo que realice las acciones mencionadas.

Se indica además para cada plataforma el nombre específico que adquiere en la misma.

Costo

Algunas de las plataformas involucran algún tipo de costo, ya sea por su utilización (tanto la capacidad de poder construir una red utilizando la plataforma en cuestión o el acceso a una API que permite implementar aplicaciones sobre blockchains ya operativas) o por ejecutar transacciones.

Valores posibles:

- No: no existe un costo asociado a la participación en la red
- Costo asociado: cuál es el costo y a que aplica el mismo

Características blandas

Usabilidad

La usabilidad es uno de los atributos cuya definición resulta compleja de precisar de modo que resulte medible y comprobable en la industria de software en general. En el caso de las plataformas blockchain, se identifican dos características de las mismas que contribuyen a determinar la usabilidad.

Estas características son:

- Tipo de API: Refiere al lenguaje de programación y/o protocolo de comunicación utilizado de la API provista.
- Existencia de GUI: Una blockchain tiene esta característica si provee de una interfaz de usuario gráfica que permita al dueño del nodo interactuar con el mismo.

Valores posibles:

- **Tipo API**: no se especifica un conjunto de valores posibles, depende de la plataforma. Ejemplos de estos valores son: REST y RPC.
- **GUI**:
    - Si: La plataforma provee de una interfaz gráfica para interactuar con los nodos

- No: La plataforma no provee de una interfaz gráfica para interactuar con los nodos

Áreas de investigación/Proyectos

Como fue mencionado, la tecnología blockchain se encuentra actualmente en desarrollo y las organizaciones se encuentran evaluando cuales pueden ser potenciales escenarios de uso de esta tecnología. Poder contar con una referencia de qué proyectos o áreas de investigación son abordados utilizando qué plataforma contribuye a la tarea antes mencionada y es por esta razón que se incluye en la taxonomía.

Soporte y Documentación

Se decide cuantificar el nivel de soporte y documentación provisto por la plataforma en función de si la plataforma es código abierto o no, si existe documentación técnica accesible en internet, si existe un *whitepaper* asociado y si se cuenta con una comunidad. Respecto a la comunidad, se considera que una plataforma cuenta con ella si existe un conjunto de personas que se encuentra utilizando la tecnología y mantienen una plataforma de intercambio accesible como puede ser Twitter, Slack, GitHub, entre otros.

Valores posibles:

- **Código abierto**:
  - Si: la plataforma es de código abierto
  - No: la plataforma no es de código abierto
- **Documentación técnica**:
  - Si: la plataforma provee documentación técnica
  - No: la plataforma no provee documentación técnica
- **Papel blanco**:
  - Si: en caso de contar con este tipo de documento
  - No: en caso de no contar con este tipo de documento
- **Comunidad**:
  - Si: existe comunidad, se listan los canales utilizados
  - No: no existe una comunidad

Madurez

Al igual que el punto anterior, la madurez es otro de los atributos que resulta complejo precisar de modo que este resulte medible y comparable. Por estas razones, según la clasificación definida se identifican los atributos: Primer *commit* y Último *commit* que permiten conocer el tiempo en el cual la plataforma se ha encontrado en desarrollo y qué tan frecuente es la actualización de la misma.

Valores posibles:

- Primer *commit*: fecha del primer *commit*
- Último *commit*: fecha del último *commit*
- N/A: la plataforma no es de código abierto o no se provee las fechas de los *commits*

Bifurcación de

Al estudiar las plataformas blockchain es posible identificar que muchas de ellas se construyen a partir de implementaciones existentes de esta tecnología. Para clasificar a las plataformas resulta de especial interés conocer si estas surgen como una bifurcación de alguna de las existentes.

Valores posibles:

- N/A: La plataforma no es una bifurcación de otra plataforma ya existente.
- Nombre de la plataforma de la cual es una bifurcación.

Proveedor

Refiere a la entidad u organización que provee la plataforma.

Valores posibles: Se indica el nombre la entidad u organización que provee la plataforma.

Gobernanza abierta

Refiere a si la plataforma es gobernada de forma abierta o si es gobernada por una entidad u organización.

Valores posibles:

- Si: la plataforma es gobernada de forma abierta
- No: la plataforma es gobernada por una entidad u organización

Anexo 5: Taxonomía

Plataforma	Permisionada	Interoperabilidad		Desempeño		Tolerancia a fallas	Contratos inteligentes	
		Implícita	Explícita	Tiempo de confirmación	Transacciones por segundo		Turing completos	Verificables
Ethereum 3	×	×	✓	3 minutos	15	Tolerante a fallas bizantinas	✓	✓
EOS	×	×	×	1 segundo	3000+	Tolerante a fallas bizantinas	×	×
Hyperledger Fabric 1.1.0	✓	✓	✓	< 1 segundo	3500+	Tolerante a fallas bizantinas o tolerante a crashes	✓	×
Cardano 1.3	×	×	En desarrollo	?	?	Tolerante a fallas bizantinas	✓	✓
Corda 2.0	✓	✓	✓	?	1000-1800	Tolerante a fallas bizantinas	✓	×
Stellar 9.2	×	×	✓	3-5 segundos	1000-10000	Tolerante a fallas bizantinas	×	×
Nem 2	Ambas	×	×	20 segundos	3000	Tolerante a fallas bizantinas	N/A	N/A

Plataforma	Manejo de identidad		Seguridad y Privacidad		Involucra Criptomoneda	Consenso	
	Control de acceso a la red	Identidad	Encripción	Control de acceso al libro mayor		Intercambiable	Mecanismo
Ethereum 3	✗	✗	TLS	Opcional	✓	✗	Prueba de trabajo
EOS	✗	Si (para los 21 nodos que validan los bloques)	?	✗	✓	✗	Prueba de participación delegada
Hyperledger Fabric 1.1.0	Intercambiable: LDAP, Open Id	✓	TLS	Opcional	✗	✓	Kafka
Cardano 1.3	N/A	✗	TLS	Opcional	✓	✗	Prueba de participación Ouroboros
Corda 2.0	LDAP, Active directory	✓	TLS	Obligatorio	✗	✓	Validez y Unicidad
Stellar 9.2	N/A	✗	?	✗	✓	✗	Acuerdo bizantino federado
Nem 2	N/A	✓	TLS	✗	✓	✗	Prueba de importancia

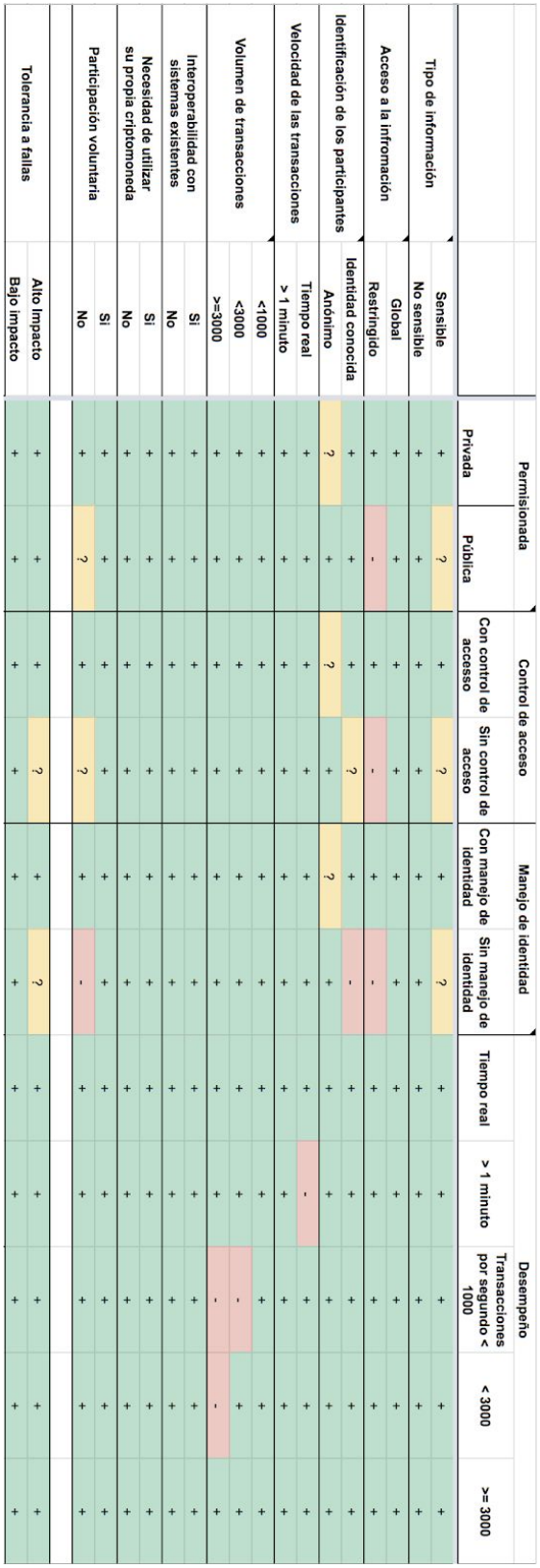
Plataforma	Protocolo de comunicación	Incentivos			Despliegue			Entorno de ejecución	Tipo de nodos				
		Por bloque	Por transacción	Por ejecución de contratos inteligentes	Nube	Docker	Otro		Oráculo	Verificador	Portero	Ordenador	Pares comunes
Ethereum 3	DEVP2P/RLP	✓	✓	✓	✓	✓	✓	EVM	✓	✗	✗	✗	✓
EOS	?	✓	No	✓	✗	✓	✓	Intercambiable	✗	✓	✗	✗	✓
Hyperledger Fabric 1.1.0	Google RPC/HTTP2	N/A	N/A	N/A	✓	✓	✗	Docker	✗	✓	✗	✓	✓
Cardano 1.3	Kademlia DHT protocol	✓	✓	✓	N/A	N/A	N/A	IELE	✓	✗	✗	✗	✓
Corda 2.0	AMQP sobre TLS	N/A	N/A	N/A	✓	✗	✓	JVM	✓	✓	✓	✓	✓
Stellar 9.2	?	✗	✓	✗	✗	✓	✓	N/A	✗	✓	✗	✗	✓
Nem 2	HTTP	✗	✓	N/A	✓	✓	✗	Docker	✗	✓	✗	✗	✓

Plataforma	Costo	Usabilidad		Áreas de investigación/Proyectos
		Tipo API	Interfaz gráfica	
Ethereum 3	×	REST	✓	Crowdfunding, Redes sociales, Búsqueda de empleo, Salud, Juegos, Arte
EOS	×	REST	✓	Salud, búsqueda de empleo/trabajadores
Hyperledger Fabric 1.1.0	×	gRPC	✓	Identidad
Cardano 1.3	×	REST	✓	Criptomoneda
Corda 2.0	×	RPC: Kotlin y Java	✓	Seguros, Financiero, Salud, KYC
Stellar 9.2	×	REST	✓	Pagos, transacciones interbancarias
Nem 2	×	REST	✓	Finanzas, Administración de Empresas, Registros Seguros, Organizaciones Descentralizadas

Plataforma	Soporte y documentación			
	Código abierto	Documentación técnica	Papel blanco	Comunidad
Ethereum 3	✓	✓	✓	Blog, GitHub, YouTube, Reddit, Gitter,Twitter, Stack Exchange, Facebook, Meetups
EOS	✓	✓	✓	Github, Telegram, Twitter, Facebook, Medium
Hyperledger Fabric 1.1.0	✓	✓	✓	Github, Stack Overflow, Youtube, Twitter, Facebook, Linkedin, Chat platform
Cardano 1.3	✓	✓	✓	Github, Youtube
Corda 2.0	✓	✓	✓	Twitter, Stack Overflow, Slack, Office hours, GitHub, Global Meetups
Stellar 9.2	✓	✓	✓	Twitter, Facebook, Github, Linkedin, Blog, Slack, Reddit
Nem 2	✓	✓	✓	Twitter, Facebook, Github, Reddit, Telegram, Linkedin, Blog

Plataforma	Madurez		Bifurcación de	Proveedor	Gobernanza abierta
	Primer commit	Ultimo Commit			
Ethereum 3	22/12/2013	Hoy	N/A	Ethereum Fundation	✕
EOS	2/04/2017	Hoy	N/A	Block.one	✓
Hyperledger Fabric 1.1.0	22/05/2016	Hoy	N/A	Linux Foundation	✓
Cardano 1.3	25/09/2016	Hoy	N/A	IOHK	✕
Corda 2.0	1/11/2015	Hoy	N/A	R3	✕
Stellar 9.2	23/11/2014	Hoy	N/A	Stellar Development Foundation	✕
Nem 2	19/4/2015	Hoy	N/A	NEM	✕

Anexo 6: Tabla de decisión de plataforma dado un escenario



		Permisionada		Control de acceso		Manejo de identidad		Desempeño			
		Privada	Pública	Con control de acceso	Sin control de acceso	Con manejo de identidad	Sin manejo de identidad	Tiempo real	> 1 minuto	Transacciones por segundo < 1000	< 3000	>= 3000
Tipo de información	Sensible	+	?	+	?	+	?	+	+	+	+	+
	No sensible	+	+	+	+	+	+	+	+	+	+	+
Acceso a la infromación	Global	+	+	+	+	+	+	+	+	+	+	+
	Restringido	+	-	+	-	+	-	+	+	+	+	+
Identificación de los participantes	Identidad conocida	+	+	+	?	+	?	+	+	+	+	+
	Anónimo	?	+	?	+	?	+	+	+	+	+	+
Velocidad de las transacciones	Tiempo real	+	+	+	+	+	+	+	-	+	+	+
	> 1 minuto	+	+	+	+	+	+	+	+	+	+	+
Volumen de transacciones	<1000	+	+	+	+	+	+	+	+	+	+	+
	<3000	+	+	+	+	+	+	+	+	-	+	+
	>=3000	+	+	+	+	+	+	+	+	-	-	+
Interoperabilidad con sistemas existentes	Si	+	+	+	+	+	+	+	+	+	+	+
	No	+	+	+	+	+	+	+	+	+	+	+
Necesidad de utilizar su propia criptomoneda	Si	+	+	+	+	+	+	+	+	+	+	+
	No	+	+	+	+	+	+	+	+	+	+	+
Participación voluntaria	Si	+	+	+	+	+	+	+	+	+	+	+
	No	+	?	+	?	+	-	+	+	+	+	+
Tolerancia a fallas	Alto Impacto	+	+	+	?	+	?	+	+	+	+	+
	Bajo Impacto	+	+	+	+	+	+	+	+	+	+	+

		Interoperabilidad		Canales privados		Incentivos		Gobierno		Involucra Criptomoneda	
		Si	No	Si	No	Si	No	Abierto	Otro	Si	No
Tipo de información	Sensible	+	+	+	?	+	+	+	?	+	+
	No sensible	+	+	+	+	+	+	+	+	+	+
Acceso a la infromación	Global	+	+	?	+	+	+	+	+	+	+
	Restringido	+	+	+	-	+	+	+	+	+	+
Identificación de los participantes	Identidad conocida	+	+	+	?	+	+	+	+	+	+
	Anónimo	+	+	+	+	+	+	+	+	+	+
Velocidad de las transacciones	Tiempo real	+	+	+	+	+	?	+	+	+	+
	> 1 minuto	+	+	+	+	+	+	+	+	+	+
Volumen de transacciones	<1000	+	+	+	+	+	+	+	+	+	+
	<3000	+	+	+	+	+	?	+	+	+	+
	>=3000	+	+	+	+	+	?	+	+	+	+
Interoperabilidad con sistemas existentes	Si	+	-	+	+	+	+	+	+	+	+
	No	+	+	+	+	+	+	+	+	+	+
Necesidad de utilizar su propia criptomoneda	Si	+	+	+	+	+	?	+	+	+	-
	No	+	+	+	+	+	+	+	+	?	+
Participación voluntaria	Si	+	+	+	+	+	?	+	+	+	+
	No	+	+	+	+	+	+	+	+	+	+
Tolerancia a fallas	Alto Impacto	+	+	+	+	+	+	+	?	+	+
	Bajo impacto	+	+	+	+	+	+	+	+	+	+

Anexo 7: Ejemplos de uso del proceso de selección de plataformas

En este anexo se presentan ejemplos de aplicación del procedimiento de selección de plataformas descripto en la sección 3.3.

Como se menciona en dicha sección, el primer paso de proceso consiste en seleccionar el escenario o caso de uso a implementar. En la práctica, los pasos siguientes a esta etapa pueden solaparse entre sí, y puede no ser necesario realizarlos por completo debido a que algunas características del escenario pueden imponer fuertes restricciones que marquen la decisión de qué plataforma utilizar. Esto se puede ver en el siguiente ejemplo:

Caso 1:

Suponiendo que ya se tiene elegido el caso de uso o escenario de negocio, se procede a especificar las características relevantes. Si el acceso a la información no puede ser global e igual para todos los participantes (debe ser restringido), entonces esta característica impone las siguientes restricciones sobre la plataforma a elegir:

- Debe ser privada, porque si fuera pública todos los participantes tendrían el mismo acceso y la información almacenada en el libro mayor puede ser accesible para cualquier participante de la red.
- Debe tener control de acceso al libro mayor para que algunos participantes puedan ver información que otros no.
- Debe tener algún tipo de manejo de identidad para poder definir qué participantes tienen cuáles permisos de acceso.
- Debe manejar canales privados o algún mecanismo equivalente para que ciertos participantes tengan su información privada en un lugar independiente del resto.

En este caso, con una única característica definida para el escenario hasta el momento ya se imponen los valores que debe tener una potencial plataforma en cuatro diferentes características. De las plataformas estudiadas en la taxonomía solo hay tres que cumplen el requisito de ser privadas: Hyperledger Fabric, Corda y NEM. Esta última debe descartarse por no manejar control de acceso al libro mayor ni canales privados, por lo que quedan Hyperledger Fabric y Corda, que sí cuentan con estas características y además tienen manejo de identidad.

Si el escenario requiere la creación de más de tres mil transacciones por segundo, esto implica que la plataforma a elegir debe soportar este volúmen, y de las dos plataformas restantes solo Hyperledger Fabric soporta tal cantidad.
En este caso, solapando los pasos del proceso, con tan solo evaluar dos características del escenario en cuestión, se llega a una única plataforma posible. Este no siempre es el caso. Si el escenario impone menos restricciones puede que se precisen evaluar todas sus características y aún así llegar a un conjunto de plataformas entre las cuales se debería elegir basándose en las características blandas.

Caso 2:

Por otra parte, si el escenario en cuestión exige la utilización de criptomonedas, esto impone una restricción sobre las plataformas, con lo cual se descartan las que no tengan criptomoneda propia. De las plataformas estudiadas en la taxonomía, las que cumplen este requisito son: Ethereum, EOS, Cardano, Stellar y NEM. Si además se requiere la creación de más de tres mil transacciones por segundo, la plataforma elegida debe soportar este volúmen, y de las plataformas restantes solo Stellar y NEM soportan dicha cantidad de transacciones. En caso de que el escenario no precise interoperabilidad con otros sistemas existentes, las dos plataformas restantes serían igual de válidas según las características duras debido a que tienen valores muy similares para dichas características. En este caso se debe tomar la decisión basándose en características blandas. Si se busca la mayor simplicidad posible en la implementación y despliegue, se debería priorizar la plataforma que cuente con soporte para ser desplegada en la nube por ejemplo de AWS o Azure, y esta característica hace que la balanza se incline hacia NEM por encima de Stellar que no cuenta con soporte para deployment en la nube.

Anexo 8: Aplicación del procedimiento de selección de plataformas sobre escenarios existentes

Escenario	Plataforma	Enlace	Permisionada	Manejo de identidad	Control de acceso al ledger	Velocidad de las transacciones	Volumen de transacciones	Interoperabilidad	Necesidad de utilizar su propia criptomoneda	Participacion voluntaria	Tolerancia a fallas	Plataformas sugeridas
Validación de identidad	Fabric	https://securekeyconcierge.com/	+	+	+	> 1 minuto	> 3000	No necesariamente	No	Si	Bajo impacto	Fabric, NEM
Transferencias internacionales	Stellar	https://tempo.eu.com/en	?	?	+	> 1 minuto	> 3000	No necesariamente	Si	Si	Alto impacto	Stellar, NEM
Micropagos	Stellar	https://www.stellar.org/blog/deloitte-launch/	?	?	+	Tiempo real	> 3000	No necesariamente	Si	Si	Alto impacto	Stellar, NEM
CryptoKitties (juego)	Ethereum	https://www.cryptokitties.co	?	?	+	Tiempo real	> 3000	No necesariamente	Si	Si	Bajo impacto	EOS
Apuestas	EOS	https://cryptoslate.com/blockchain-impacts-gambling-industry	-	-	+	> 1 minuto	>1000	No necesariamente	Si	Si	Alto impacto	EOS, Stellar
Sistema de votos	Dash	https://docs.dash.org/en/latest/governance/index.html	?	?	+	> 1 minuto	> 3000	No necesariamente	No	Si	Alto impacto	EOS, NEM, Cardano
Validación de diplomas universitarios	Cardano	https://www.nasdaq.com/article/cardano-blockchains-first-use-case-proof-of-university-diplomas-in-greece-cm899265	?	+	+	> 1 minuto	< 1000	No necesariamente	No	Si	Bajo impacto	Ethereum, EOS, Fabric, Cardano, Corda, Stellar, NEM
Royal payments / Pago de regalías	Corda	https://guild1.co/https://aws.amazon.com/partners/apn-journal/all/guildone/	?	+	+	> 1 minuto	< 1000	No necesariamente	No, pero una alternativa podria haber sido manejar los pagos en la plataforma utilizando criptomonedas	No	Alto impacto	EOS, Fabric, Corda, NEM
Syndicated loan market	Corda	https://www.r3.com/wp-content/uploads/2018/07/US_11_Finastra_CS_JUN26_final.pdf	?	+	+	> 1 minuto	< 1000	No necesariamente	No, pero una alternativa podria haber sido manejar los pagos en la plataforma utilizando criptomonedas	No	Alto impacto	EOS, Fabric, Corda, NEM
Cambios de monedas	EOS	https://southtex.com/	-	+	+	> 1 minuto	>3000	Si	Si	Si	Alto impacto	EOS, NEM, Cardano
DNS	NEM	https://github.com/aenima86/NEM-DNS	-	-	-	Tiempo real	>3000		Si	Si	Alto impacto	EOS, NEM
Donaciones	NEM	http://givematters.io/	?	?	?	> 1 minuto	< 1000	No	Si	Si	Alto impacto	Corda, Fabric, NEM, Ethereum

Anexo 9: Implementación

Este anexo se presenta información complementaria a lo mencionado en el capítulo 5 respecto a la etapa de implementación. Se describen las tecnologías utilizadas, se especifican diagramas de flujo de las principales funcionalidades, los requerimientos del proyecto y los pasos a seguir para su ejecución.

Tecnología

En esta sección se describen las tecnologías utilizadas según los componentes mencionados en la sección 5.4.3.

Servidor

Encargado de *cachear* los datos que se obtienen de la cadena y almacenar claves privadas. En la tabla 14 se listan las principales tecnologías utilizados para su implementación.

Tecnología	Nombre	Versión
Lenguaje	Typescript	v3.0.1
Base de datos	SQLite	v3
Framework	Express	v4.16.4
Librería	nem2-sdk	v0.10.1

Tabla 14 - Tecnologías utilizadas en la implementación del servidor

Aplicación (Tablero)

Utilizado por los operadores para crear productos y enviar los sellos de calidad. Muestra el estado actual de cada producto. En la tabla 15 se listan las principales tecnologías utilizados para su implementación.

Componente	Nombre	Versión
Lenguaje	Typescript	v3.0.1
Framework	Angular	2
Librería	nem2-sdk	v0.10.1

Tabla 15 - Tecnologías utilizadas en la implementación del tablero

Red blockchain

Para la implementación de la red, se utiliza como base el repositorio 'catapult-service-bootstrap' de NEM, el cual despliega localmente cantidades arbitrarias de nodos para el desarrollo de aplicaciones.

En la tabla 16 se detallan los servicios necesarios para el correcto funcionamiento de la red NEM.

Servicio	**Funcionalidad**
Base de datos MongoDB	Es donde los nodos almacenan la cadena de bloques
Par	Nodo que participa en la cosecha de XEM validando transacciones
Puerta de acceso	Encargado de recibir las solicitudes del exterior y de redirigirlas hacia los nodos API
API	Implementa los servicios de la red NEM y procesa las solicitudes que recibe desde la puerta de enlace.

Tabla 16 - Servicios utilizados

Funcionalidades - Diagramas de flujo

En esta sección, para cada una de las funcionalidades descriptas en la sección 5.5, se especifican las interacciones entre la aplicación y la blockchain mediante diagramas de flujo.

Como fue mencionado, las principales funcionalidades del sistema son:

- Crear productos
- Asignar sellos de seguridad a los productos
- Analizar el estado del producto en la cadena de suministro (visualizar los sellos de seguridad otorgados y el conjunto de transacciones almacenadas en la blockchain)

Creación de productos

En la imagen 36 se presenta un resumen de las invocaciones entre los diferentes componentes de la arquitectura para la creación de un producto.

Cuando un operador selecciona la opción “Crear nuevo Producto” desde el portal web se realiza un POST HTTP al servidor web.
Al recibir la solicitud, el servidor realiza un post al nodo API de la red de blockchain realizando así la solicitud para registrar el nuevo producto en la blockchain y almacena el producto en la base de datos SQLIte.

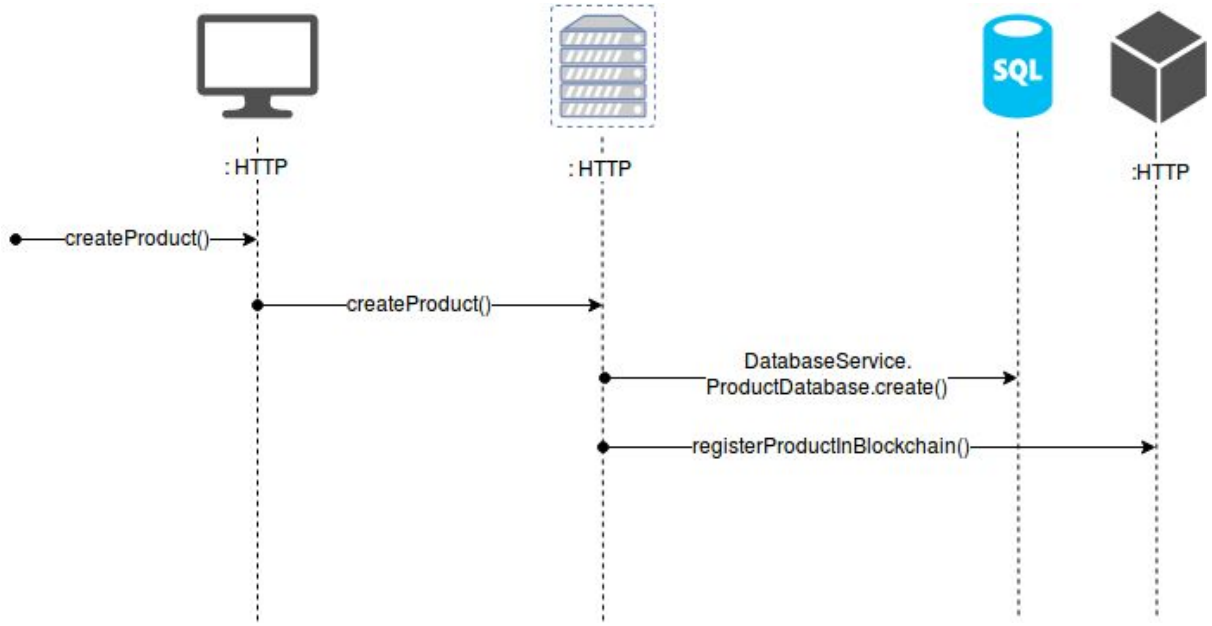


Imagen 36 - Creación de productos en el proyecto

Los productos creados, como fue mencionado, son activos, los cuales pertenecen a una cuenta. Todos los productos en este escenario al crearse pertenecen a la cuenta asociada a la empresa “Fábrica”

Asignar sellos de seguridad a los productos

Cuando los operadores ingresan el producto a asignar un sello de seguridad, junto la empresa a la que pertenecen y la clave privada, se realizan consultas a la blockchain solicitando la cuenta del operador cuyas claves fueron ingresadas, la clave pública del producto a otorgar el sello de seguridad y la dirección de la cuenta de dicho producto.

Una vez obtenidas, se realiza una solicitud de transacción para realizar la transferencia de un mosaico al producto (representando el sello de seguridad).

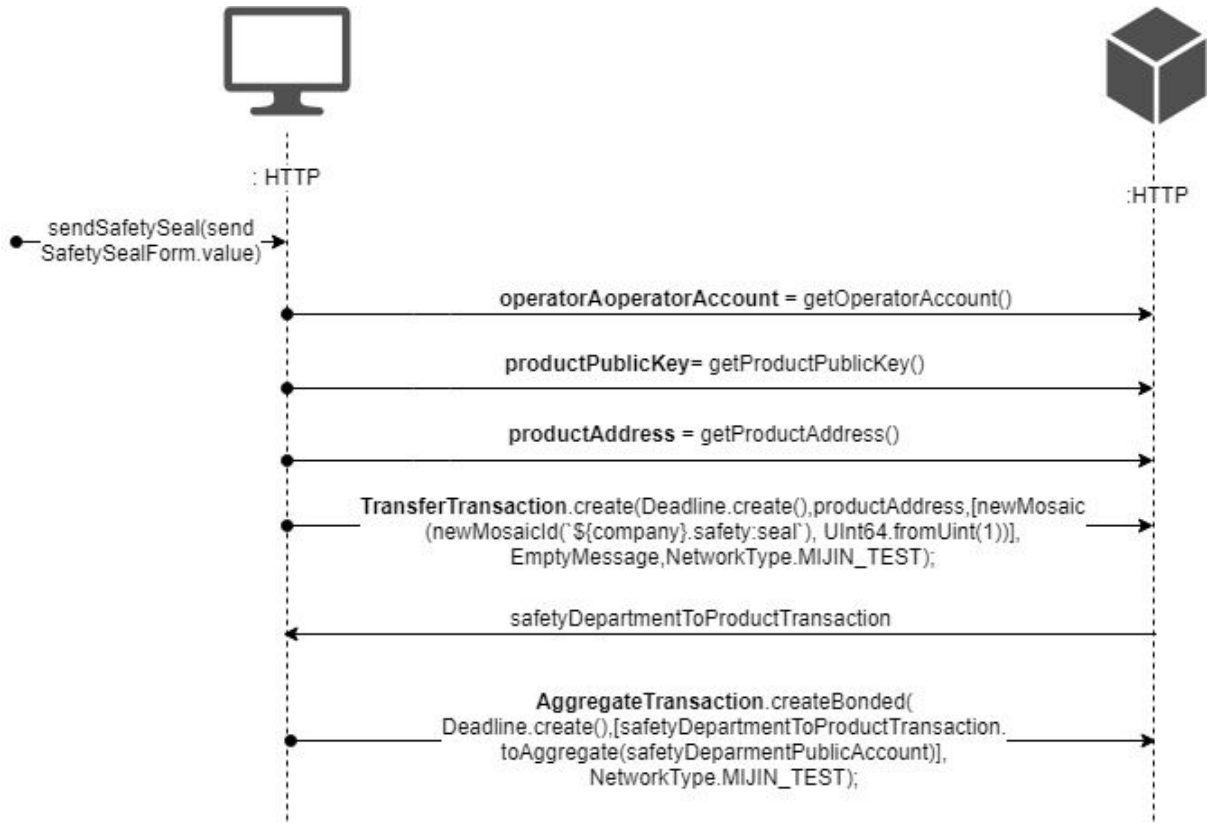


Imagen 37 - Envío de sello de seguridad

Como se requiere que para otorgar el sello de seguridad el sensor certifique la calidad del producto además de la certificación del operador, se crea una transacción agregada. El sensor se encuentra suscripto a ese tipo de transacciones y cuando las recibe, se simula su validación y en caso de ser la calidad correcta se firma la transacción agregada. Este proceso se ilustra en la imagen 38.

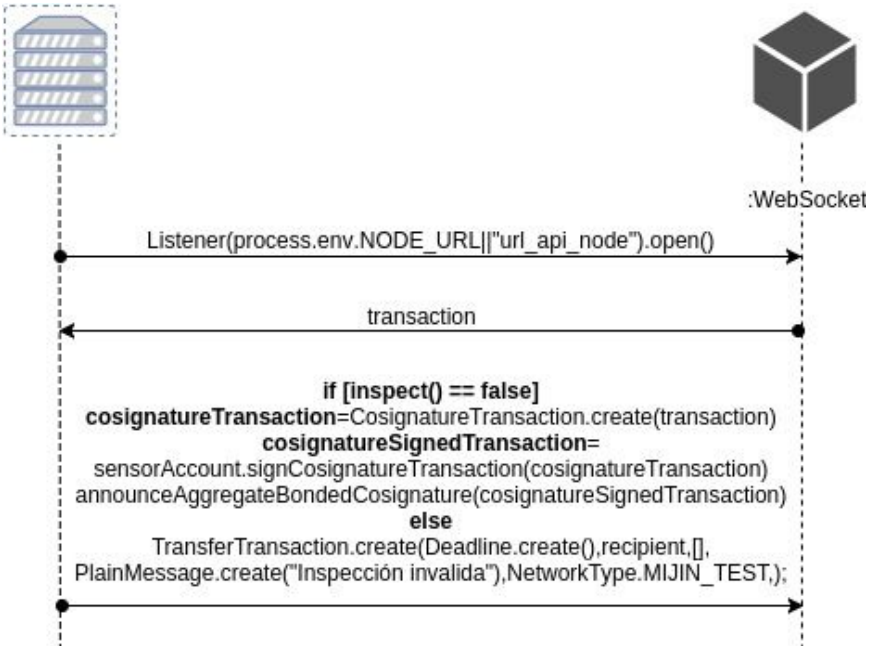


Imagen 38 - Validación del sensor

Analizar el estado del producto en la cadena de suministro

Para obtener los datos del producto se consulta a través del nodo API a la blockchain por la cuenta asociada al producto y una vez obtenida, se tiene la información de la cuenta, las transacciones asociadas a la misma y los mosaicos que le han sido otorgados en este caso por los operadores.

En la imagen 39 es posible observar las interacciones de la aplicación con la blockchain para obtener los datos asociados al producto y poder así trazarlo.

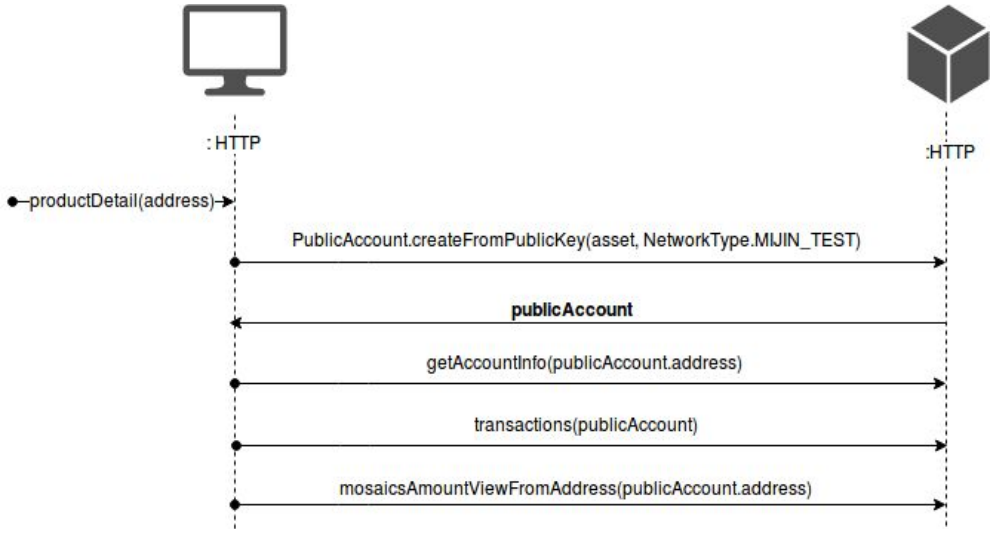


Imagen 39 - Obtener información del producto

Requerimientos y ejecución del proyecto

Requerimientos

A continuación se menciona el conjunto de requerimientos necesarios para la ejecución del proyecto, además de contar con docker y python3 instalado:

```
sudo apt install yarn
export PATH="$(yarn global bin):$PATH"
yarn global add nem2-cli
yarn global add typescript
pip3 install PyYAML
pip3 install ipdb
```

Para la correcta ejecución del proyecto utilizado para la implementación [57] resulta necesario en algunos ambientes actualizar la librería rxjs:

MAC OS:

```
yarn upgrade rxjs@6.3.3
```

En los directorios: `nem2-workshop-nem-applied-to-supply-chain/project/dashboard` y `nem2-workshop-nem-applied-to-supply-chain/project/server`

Ubuntu 16.04:

Además de actualizar en el `/server` y `/dashboard` resulta necesario ejecutar

`yarn upgrade rxjs@6.3.3` en el directorio `nem2-workshop-nem-applied-to-supply-chain/project/dashboard/node_modules/nem2-sdk/node_modules`

Ejecución del proyecto

A continuación se mencionan los pasos a realizar para ejecutar el proyecto.

1. En NEM/catapult-service-bootstrap:
`docker-compose -f docker-compose-with-explorer.yml up`

2. En NEM:
La ejecución del programa main.py permite crear todas las estructuras necesarias en la blockchain para el escenario descripto.

```
ipython main.py
```

El programa requiere interacción por parte del usuario, ingresar n + c + enter cada vez que se solicite.

3. En nem2-workshop-nem-applied-to-supply-chain/project/server y nem2-workshop-nem-applied-to-supply-chain/project/dashboard iniciar el servidor:

```
yarn install
yarn start
```

El panel web para los operadores se encuentra accesible en: localhost:4200.

Automatización de la creación de estructuras - Ejemplo de archivo YAML

El archivo YAML utilizado en el proyecto:

```
tambo:
  operadores: 2
  sensor: true

transporte_tambo_fabrica:
  operadores: 1
  termómetro: true

fábrica:
  operadores: 2
  sensor: true

transporte_fabrica_tienda:
  operadores: 1
  termómetro: true

tienda:
  operadores: 2
  sensor: true
```