

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA – INSA LYON
DEPARTEMENT INFORMATIQUE
VALPARAISO – CHILE
LYON – FRANCE



“EL USO DE TECNOLOGÍAS DE BLOCKCHAIN PARA LA TRAZABILIDAD DE MEDICAMENTOS”

JOACHIM DOREL

**MEMORIA DE TITULACION PARA OPTAR AL TITULO DE
INGENIERO CIVIL INFORMATICA**

Profesor Guía: Xavier Bonnaire (xavier.bonnaire@inf.utfsm.cl)
Profesor Correferente: Erika Rosas (erika.rosas@inf.utfsm.cl)

Septiembre 2019

DEDICATORIA

*Gracias a mis padres por su apoyo durante mis largos años de estudio,
Gracias a la INSA de Lyon y a la Federico Santa María por la oportunidad que me han brindado estas escuelas para lograr este doble título,
Gracias a Xavier Bonnaire, José Contreras, Florent De Dinechin y Omar Hasan por enmarcar esta memoria.*

Resumen

Resumen — Esta tesis explora el uso de tecnologías relacionadas con la blockchain para mejorar el proceso de trazabilidad de medicamentos. Esta exploración tiene dos objetivos principales: llevar a cabo un análisis teórico del uso de Blockchain y realizar la implementación de una versión de demostración. La implementación de la solución demuestra que la trazabilidad de los medicamentos a través de una cadena de bloques es mucho más efectiva para rastrear los medicamentos y no falsificarlos. La presente investigación, también presenta un análisis de la cadena de suministro de la industria farmacéutica, y un modelo de esta para adaptarla a las necesidades de trazabilidad.

Palabras Claves — Blockchain, Trazabilidad, Seguridad, Supply Chain, Industria farmacéutica

Abstract

Abstract—This thesis will explore the use of technologies associated with the Blockchain in order to improve the current process of drugs traceability. This exploration will have two main goals: analyze the theoretical use of the Blockchain for our problem and developed an implementation of a solution. The implementation of the solution will allow to prove that drugs traceability is possible through a blockchain, and that this traceability is more efficient in order to follow the drugs and to keep them safe from corruption. This memoir also presents an analysis of the pharmaceutical industry's supply chain, and a modelization of that supply chain in order to adapt the traceability to the supply chain.

Keywords— Blockchain, Traceability, Security, Supply Chain, Pharmaceutical Industry

Índice de Contenidos

Índice de Figuras	7
Introducción.....	8
Capítulo 1: Definición del problema	10
1.1. Mercado de medicamentos y falsificaciones	10
1.1.1. Un mercado mundial.....	10
1.1.2. Consecuencias económicas de la falsificación.....	10
1.1.3. El atractivo mercado falsificado	11
1.1.4. Medidas implementadas para combatir la falsificación	11
1.2. Objetivos de esta memoria	12
Capítulo 2: Marco conceptual	13
2.1. La Cadena de Suministro Industria Farmacéutica	13
2.1.1. ¿Qué es un medicamento?.....	13
2.1.2. La creación de un medicamento	14
2.1.2.1. El descubrimiento de un nuevo medicamento	14
2.1.2.2. El desarrollo preclínico	15
2.1.2.3. El desarrollo clínico	15
2.1.3. La cadena de suministro	16
2.1.3.1. La cadena de suministro para Novartis.....	16
2.1.3.1.1. Las operaciones químicas.....	17
2.1.3.1.2. Las operaciones farmacéuticas	17
2.1.3.1.3. Las oficinas farmacéuticas nacionales.....	18
2.1.3.2. Un modelo teórico de la cadena de suministro	19
2.2. El estado actual de la trazabilidad en la industria farmacéutica.....	20
2.2.1. Análisis de datamatrix.....	21
2.2.2. Análisis de la RFID	23
2.3. Las blockchains	25
2.3.1. Cadenas, bloques y datos	25
2.3.1.1. Los datos	25
2.3.1.2. Los bloques	25
2.3.1.3. Las cadenas	27
2.3.2. El sistema distribuido.....	28
2.3.2.1. Las propiedades de un sistema distribuido.....	28
2.3.2.2. El problema de generales bizantinos	30
2.3.2.3. Los mecanismos de consenso	31
2.3.2.3.1. Paxos	31
2.3.2.3.2. Raft	32
2.3.2.3.3. Practical Byzantine Fault Tolerance (PBFT)	32
2.3.2.3.4. Consenso de Nakamoto	33
2.3.2.4. El derecho a voto	34
2.3.2.4.1. Prueba de trabajo (<i>Proof-of-Work</i>)	34
2.3.2.4.2. Prueba de estacas (<i>Proof-of-Stake</i>).....	34
2.3.2.4.3. Prueba de Actividad (<i>Proof-of-Activity</i>).....	34
2.3.2.4.4. Prueba de ardor (<i>Proof-of-Burn</i>)	35
2.3.2.4.5. Prueba de espacio (<i>Proof-of-Space</i>).....	35
2.3.2.4.6. Prueba de capacidad (<i>Proof-of-Capacity</i>).....	35
2.3.2.4.7. Prueba de tiempo transcurrido (<i>Proof-of-Elapsed-Time</i>).....	35
2.3.2.4.8. Prueba de autoridad (<i>Proof-of-Authority</i>)	35
Capítulo 3: Propuesta de solución	36

3.1. Adaptación de trazabilidad	36
3.1.1. Datamatrix contra etiquetas RFID.....	36
3.1.2. El uso de datamatrix	37
3.2. La retención de datos	39
3.2.1. Datos de la transacción.....	39
3.2.1.1. Los actores no identificados.....	40
3.2.1.2. Los actores identificados.....	40
3.2.1.3. Los fabricantes de medicamentos	41
3.2.2. Los datos de los bloques.....	41
3.2.3. Los datos de los medicamentos.....	42
3.3. La blockchain y su funcionamiento	44
3.4. Historias de usuarios de la solución	45
Capítulo 4: Validación de la Solución.....	47
4.1. La gestión de los datos.....	47
4.1.1. La gestión de la base de datos	47
4.1.2. La gestión de la blockchain	48
4.2. Interacción con la base de datos	49
4.3. Validación de historias de usuarios	50
4.3.1. Historias de usuarios de actores no identificados	50
4.3.2. Récits d'utilisateurs des acteurs identifiés.....	52
4.3.3. Récits des fabricants de médicaments.....	55
4.4. Ejemplos de intentos de sobornar a la cadena de bloques	56
4.4.1. Adición de medicamentos externos por un transportista	56
4.4.2. Cambiar la cantidad de un lote	57
Capítulo 5: Conclusión.....	58
5.1. Conclusiones generales.....	58
5.2. Logro de los objetivos	58
5.3. Trabajos futuros	59
Bibliografía.....	60
Anexos.....	63
1. Ejemplo de blockchain	63
2. Código de un block	64
3. Código de la blockchain.....	64

Índice de Figuras

FIGURA 2: UN MODELO GENÉRICO DE CADENA DE SUMINISTRO	20
FIGURA 3: EJEMPLO DE DATAMATRIX Y DATOS ASOCIADOS - FUENTE: HTTPS://EC.EUROPA.EU/ [36]	22
FIGURA 4 : EJEMPLO DE UN CHIP RFID - FUENTE: WIKIMEDIA	23
FIGURA 5: ESQUEMA DE UNA TRANSACCIÓN.	25
FIGURA 6: EJEMPLO DE HASH CON SHA-256	26
FIGURA 7: COMPOSICIÓN DEL HASH DE UN BLOQUE EN FORMA DE ÁRBOL DE MERKLE.....	26
FIGURE 8: COMPOSICIÓN DE UN BLOCK	27
FIGURE 9 : SCHÉMA D'UNE BLOCKCHAIN	28
FIGURA 10: REPRESENTACIÓN DEL TEOREMA CAP - FUENTE: TOWARDSDATASCIENCE.COM [26].....	29
FIGURA 11: PROBLEMA DE LOS GENERALES BIZANTINOS - FUENTE: EDX.ORG	30
FIGURA 12 : DIAGRAMA DE CÓMO FUNCIONA BPFT - FUENTE: EDX.ORG	33
FIGURA 13 : FLUJO DE NÚMERO DE LOTE	38
FIGURA 14: DIAGRAMA DE LA BASE DE DATOS.....	43
FIGURA 15: ARQUITECTURA DE LA SOLUCIÓN.....	45
FIGURA 16: PAGINA DEL ÍNDIX	50
FIGURA 17: PÁGINA DE UN LOTE DE MEDICAMENTOS, CON LAS TRANSACCIONES DE ESE LOTE.	50
FIGURA 18: INFORMACIÓN SOBRE LOS SUCESIVOS PROPIETARIOS DE UN MEDICAMENTO.....	51
FIGURA 19: ACEPTACIÓN O RECHAZO DE UN LOTE.....	52
FIGURA 20: PAGINA DE IDENTIFICACIÓN	52
FIGURA 21: PÁGINA DE REGISTRO	53
FIGURA 22: BOTÓN DE DESCONEXIÓN	53
FIGURA 23: PERFIL DE UN USUARIO	53
FIGURA 24: VER EL INVENTARIO DE UN USUARIO	54
FIGURE 25: ENVIAR LOTE 8 DE TAMAÑO 10 AL ACTOR CON NÚMERO DE IDENTIFICACIÓN 2.....	54
FIGURA 26: FILTRANDO LOS MEDICAMENTOS	54
FIGURA 27: BOTÓN DE SOLICITUD DE SINCRONIZACIÓN DE BLOCKCHAIN	55
FIGURA 28: DIVISIÓN DE UN LOTE EN DOS, Y ENVÍA UNO DE LOS SUB LOTES.....	55
FIGURA 29: VISUALIZACIÓN DEL DATAMATRIX DE UN LOTE	55
FIGURA 30: AGREGAR UN NUEVO MEDICAMENTO A LA BASE DE DATOS	56
FIGURA 31: AGREGAR UN NUEVO LOTE DE MEDICAMENTO	56

Introducción

Miles de personas usan los medicamentos todos los días. Su uso tiene varios contextos, pero lo más importante es sanar. Para curar, un medicamento debe adaptarse a la enfermedad que tiene un paciente. Originalmente, los medicamentos eran principalmente productos naturales (plantas, raíces y otros). Pero con la llegada de la química en el siglo XX, la creación de medicamentos sintéticos aumentó drásticamente, y el uso de medicamentos por parte de los humanos aumentó en paralelo.

El aumento en el tamaño del mercado de medicamentos ha llevado al desarrollo de un mercado paralelo de falsificaciones: los medicamentos que se encuentran en este mercado son más baratos, pero la calidad y efectividad de estos son inciertas o incluso peligrosas.

Identificación del problema

Los medicamentos falsificados representan un riesgo para los consumidores, un riesgo potencialmente mortal. Consumir un medicamento inadecuado o ineficaz no ayuda a curar, un paciente debe poder verificar el origen del medicamento sin importar de dónde lo consiga. Al confirmar esto, el paciente puede estar seguro de no poner en riesgo su salud.

Para confirmar el origen de un medicamento, un paciente debe poder identificar el medicamento y conocer los diferentes manipuladores del medicamento y su ubicación. Todos los manipuladores de medicamentos, que forman parte de la cadena de suministro de medicamentos, son las claves para garantizar que el medicamento consumido no fuera, en algún momento, reemplazado por un medicamento alternativo.

La falsificación de medicamentos es hoy uno de los principales problemas de la industria farmacéutica, y este resumen pretende presentar una solución a este problema.

Objetivos

Objetivo General

Crear y desarrollar una solución para rastrear medicamentos a través de una cadena de bloques.

Objetivos específicos

- Comprender y saber qué es una cadena de bloques, cómo funciona y la utilidad futura de la tecnología.
- Analizar la cadena de suministro de la industria farmacéutica.
- Desarrollar un programa para mejorar el seguimiento de medicamentos con una cadena de bloques

Plan de la memoria

Esta tesis presenta en una primera parte la problemática del monitoreo de medicamentos por parte de la industria farmacéutica, y los problemas actuales que la industria encuentra en la lucha contra las medicinas falsificadas. Por otra parte, presenta un análisis de los temas centrales de la disertación: medicamentos, blockchains y la cadena de suministro de la industria farmacéutica. La definición de los temas centrales permitirá conocer y dominar las principales opciones posibles para resolver el problema de la memoria. Luego, a esta parte de las definiciones le sigue una propuesta de solución basada en lo que se ha estudiado previamente. Esta última parte explora las posibilidades que actualmente ofrece la industria farmacéutica para el monitoreo de medicamentos y la adaptación de este seguimiento para usar una cadena de bloques. En una cuarta parte se estudiará la validación de esta solución, si la solución responde bien a los problemas de la memoria y si esta permite evitar la

corrupción de la cadena de suministro de los medicamentos. Finalmente, una conclusión cerrará la presentación y mostrará el trabajo futuro para la solución propuesta.

Las memorias tienen la siguiente estructura:

Capítulo 1 - Definición del problema: introducción al tema de los medicamentos falsificados.

Capítulo 2 - Marco conceptual: presentación de las diferentes herramientas y técnicas de memoria, como la industria farmacéutica, el funcionamiento actual de la trazabilidad y el funcionamiento de una cadena de bloques.

Capítulo 3 - Propuesta de solución: La construcción de una solución para resolver el problema del rastreo de medicamentos a través de una cadena de bloques.

Capítulo 4 - Validación de la solución: Verificación de que el recurso tiene una solución al problema inicial, y que la solución evita la corrupción de la cadena de suministro de medicamentos.

Capítulo 5 - Conclusión: Las conclusiones generales de la disertación, así como las perspectivas creadas gracias a la realización de la disertación.

Capítulo 1: Definición del problema

1.1. Mercado de medicamentos y falsificaciones

1.1.1. Un mercado mundial

La falsificación de medicamentos es uno de los mercados ilegales más grandes y lucrativos del mundo: casi doscientos mil millones de dólares en 2017 [3] según la OMS, la Organización Mundial de la Salud. Los medicamentos de este mercado se dividen en tres categorías:

- Los medicamentos de calidad inferior son medicamentos autorizados que no cumplen con los estándares o especificaciones de calidad, o ambos.
- Los medicamentos no registrados o sin licencia son productos médicos que no han sido evaluados o aprobados por la autoridad nacional o regional de un mercado en el que se distribuyen.
- Los medicamentos falsificados son productos médicos que se presentan deliberadamente con información falsa que puede afectar su identidad, composición o fuente.

Las siguientes cifras ayudan a profundizar y comprender mejor este problema [34]:

- El 10% de las ventas en el mercado mundial de medicamentos son para medicamentos falsificados, desglosados de la siguiente manera:
 - o 1% en países desarrollados
 - o 5 a 30% en países emergentes
 - o Casi el 70% en algunos países asiáticos y africanos

Además de estos números, también debe tenerse en cuenta que el 50% [7] de los medicamentos comprados en línea están falsificados. Estos medicamentos tienen consecuencias directas para los consumidores. Cada año, casi 1,000,000 de personas mueren por el consumo de estos medicamentos. Además, la ingesta de estos fármacos que no es adecuado para los pacientes provoca una sobredosis o una dosis insuficiente al momento de su consumo, el uso de una molécula diferente o principio activo, excipientes peligrosos, la presencia en el medicamento de otras moléculas, el riesgo de interacciones farmacológicas. Esta droga falsificada con otros medicamentos o moléculas, o una droga que no tiene ningún efecto para mejorar la salud del paciente, lo que provoca serias consecuencias para el consumidor, lo que puede empeorar su estado.

1.1.2. Consecuencias económicas de la falsificación.

La falsificación de medicamentos también tiene importantes consecuencias económicas [18]. Las compañías farmacéuticas están invirtiendo grandes sumas en el objetivo de desarrollar nuevos medicamentos, y la falsificación de estos reduce el retorno de la inversión de los laboratorios.

Si una empresa tiene que invertir millones en el desarrollo de un medicamento, una vez que se desarrolle y esté listo para ser comercializado, será rentable en términos de costos de investigación, producción y comercialización. Por lo tanto, los laboratorios y las compañías farmacéuticas concentrarán la búsqueda de nuevos medicamentos en fármacos "públicos en general", que posiblemente tengan muchos consumidores, reduciendo así el riesgo de falta de rentabilidad y abandonando enfermedades más raras cuyo tratamiento sería menos rentable.

1.1.3. El atractivo mercado falsificado

Para las empresas y las personas que producen o comercializan medicamentos falsificados, existen múltiples motivaciones. El tráfico de medicamentos falsificados es de 10 a 25 veces más rentable que el tráfico de estupefacientes (por ejemplo, cannabis) en comparación con el costo de inversión inicial [31]. Además, el aumento de las compras en tiendas en línea (como Amazon o EBay) y el crecimiento del comercio electrónico desde los años 90, muchas personas están acostumbradas a comprar en línea. Casi el 50% de los medicamentos comprados en línea son falsificados. Finalmente, las desigualdades en el acceso a los medicamentos: la presencia o ausencia de subsidios, en forma de seguro o seguridad social, afectarán directamente la proporción de compras de medicamentos en mercados paralelos.

Para los compradores y consumidores de medicamentos, hay muchas razones para comprar fármacos que son potencialmente cuestionables y difíciles de rastrear. En los países desarrollados, las razones principales son:

- El medicamento se considera tabú: por ejemplo, medicamentos para bajar de peso o impotencia sexual.
- El medicamento es costoso, y pasar por circuitos alternativos para comprar un medicamento que parece ser el mismo puede adquirirlo o pensar en adquirirlo a un precio más bajo.
- El medicamento solo está disponible con receta médica, como medicamentos para combatir el insomnio.
- El medicamento mejora su rendimiento, pero su venta legal no tiene este objetivo, y se prescribe principalmente para otros trastornos: encontramos en esta categoría anabólicos, hormonas y medicamentos para aumentar su rendimiento y concentración.
- La droga no es legal en algunos países, pero sí en otros. Por ejemplo, los medicamentos para el aborto (misoprostol y mifepristona) son legales en muchos países, pero bastante ilegales en otros.
- El medicamento no tiene valor científico, como algunas pastillas para la garganta que se encuentran en los mercados de Chile.

Además de todas estas razones globales, existen otras justificaciones en los países en desarrollo que explican el fenómeno:

- Los medicamentos básicos están falsificados, como antibióticos, medicamentos contra la malaria o antiparasitarios.
- Las agencias de control son ineficaces y, por lo tanto, tienen muy poco control sobre los medicamentos para ayudar a garantizar que los medicamentos vendidos en un territorio sean las correctas.
- Los sistemas de salud no son efectivos, por lo que la única forma de comprar algunos medicamentos es a través de mercados paralelos.
- La escasez de algunos medicamentos, incluidos medicamentos básicos, es regular [34]
- La pobreza de algunas personas los empuja a buscar medicamentos cada vez más baratos.
- La corrupción de algunas élites impide un lugar de circuito de distribución de calidad y empuja a los consumidores a pasar por un circuito de distribución paralelo.

El tamaño y la importancia del mercado de medicamentos falsificados se debe a razones económicas, pero también a razones de suministro, gestión o la estabilidad de ciertos países.

1.1.4. Medidas implementadas para combatir la falsificación

Para combatir los problemas de falsificación de medicamentos, existen tecnologías y métodos para compensar algunos de estos problemas:

- Establecimiento de una trazabilidad del medicamento, para dar a conocer todo el proceso de producción y distribución al consumidor final. En Europa, el uso de datamatrix es obligatorio desde el 9 de febrero de 2019 [36]. Estos han fortalecido la trazabilidad de los medicamentos, pero aún son perfectibles. Más adelante en esta memoria habrá un análisis de estos.

- Pruebas de laboratorio de ciertos lotes para asegurar que el medicamento vendido coincida con el fármaco en la caja. Este método, aunque extremadamente efectivo, es imposible de implementar a gran escala, debido a su costo y velocidad.

En términos más generales, la lucha contra la falsificación de medicamentos implica que los países establecen una vigilancia más importante de lo que regresa o sale del país, y eso con la acción de las aduanas principalmente. También está el *International Medical Products Anti-Counterfeiting Taskforce* (IMPACT), un equipo internacional formado por la OMS para luchar contra la falsificación de medicamentos, y que está trabajando con la Aduana en muchos países y otras asociaciones internacionales para expandirse. El impacto de su lucha. Los miembros de IMPACT trabajan, entre otras cosas, para ayudar a los países a fortalecer sus sistemas de aplicación de la ley y ayudar a la industria farmacéutica a desarrollar medidas internacionales para combatir los medicamentos falsificados [15]. Prueba de la importancia del tema, desde 2013, la Universidad Panthéon-Assas en París ofrece un "diploma universitario de delitos farmacéuticos", para conocer las leyes y procedimientos para luchar contra estos delitos.

En el sector médico ahora hay más y más productos a seguir, ya sean medicamentos genéricos vendidos en farmacias o la prótesis de cadera utilizada en la sala quirúrgica de un hospital. Todas las cadenas de suministro en la industria deben asegurarse utilizando un máximo de herramientas. Las tecnologías actuales deberían mejorar en gran medida la trazabilidad de estos productos. Esta tesis se basa en tecnología reciente (blockchain) y propone una solución a los problemas de trazabilidad de medicamentos.

1.2. Objetivos de esta memoria

Por lo tanto, la industria farmacéutica necesita, por un lado, su estabilidad económica a largo plazo y, por otro lado, garantizar la confianza del consumidor en la industria en su conjunto, actualizar sus estándares y prácticas para combatir la falsificación de medicamentos en todo el mundo. La lucha contra la falsificación también puede permitir a las empresas del sector compensar los problemas o la introducción de medicamentos fraudulentos en sus cadenas de suministro. Esta tesis es principalmente para medicamentos, pero todas las herramientas del sector médico deben rastrearse de una mejor manera a nivel mundial, desde el medicamento hasta el corazón protésico, esta trazabilidad permite al consumidor tener una mejor visión general y, por lo tanto, un mejor conocimiento de lo que pondrá en su cuerpo. Brindar a los consumidores la oportunidad de conocer el origen de los medicamentos que compran y consumen podría dar a las farmacias en línea una verdadera legitimidad, gracias a una garantía para los consumidores sobre lo que compran.

Esta memoria tiene dos objetivos principales, tanto en torno a una cadena de bloques como a la implementación de esta. El primer objetivo, que es un objetivo intermedio, es explorar las posibilidades que ofrecen las blockchains para mejorar la trazabilidad de los medicamentos y, en términos más generales, las posibilidades de blockchains dentro de la cadena de suministro. Un segundo objetivo es desarrollar una prueba de concepto para demostrar una solución, con el interés potencial de esta satisfacción para la industria farmacéutica, y los límites de la solución. Estos dos objetivos globales se dividen en varias partes para comprender mejor las opciones técnicas propuestas en este documento.

Capítulo 2: Marco conceptual

Como parte del desarrollo de una nueva solución para garantizar una mejor trazabilidad de los medicamentos, es necesario saber un poco más sobre la trazabilidad actual de los medicamentos, la cadena de suministro de la industria farmacéutica y las cadenas de bloques. Explorar cómo se encuentran estas diferentes partes proporcionará una solución conceptual en la siguiente parte.

Estos tres temas distintos de trazabilidad de medicamentos, la cadena de suministro de la industria farmacéutica y las cadenas de bloques forman las tres ramas principales de esta sección. La trazabilidad de los medicamentos se debe a que necesitamos aprender más sobre el sistema actualmente en funcionamiento para descubrir sus diversas debilidades y, por lo tanto, destacar algunas áreas para mejorar. El estudio de las cadenas de suministro debe permitir comprender los diferentes flujos para producir y distribuir medicamentos, y saber más sobre qué es un medicamento. Finalmente, el estudio de blockchains y las diferentes posibilidades asociadas con ellos ayudarán a aclarar sus usos potenciales y a abrir una propuesta conceptual del uso de estos.

2.1. La Cadena de Suministro Industria Farmacéutica

Todos los flujos de medicamentos en la industria farmacéutica pasan por una cadena de suministro. Como parte de la búsqueda de la mejora de este, analizar y comprender esta cadena de suministro es primordial, ya que este tiene un vínculo directo con la trazabilidad de los medicamentos. Es el análisis de la cadena de suministro de Novartis lo que permitirá identificar a los actores y los flujos clave. La identificación de sus actores y flujos permitirá entonces construir y desarrollar un modelo de cadena de suministro genérica. Un segundo objetivo de este análisis es identificar los momentos clave durante los cuales se establece la trazabilidad de los medicamentos y, por lo tanto, la solución presentada deberá intervenir en la cadena de suministro. Estos momentos clave permitirán comprender cuándo se pueden implementar nuevos procesos de seguridad que dependen de una cadena de bloques.

2.1.1. ¿Qué es un medicamento?

Para comprender mejor el corazón de esta memoria, es importante definir los fundamentos de qué es un medicamento y comprender cómo se fabrican y de qué están hechos. Además del pellet, el jarabe o la crema comprados en las tiendas, los consumidores saben muy poco acerca de los medicamentos. Simplemente, y en una ecuación simple, un medicamento es [9]:

$$\text{Droga} = \text{Principio activo} + \text{Excipientes}$$

El ingrediente activo corresponde a la molécula que permite apoyar la actividad farmacológica (la "molécula activa"), y los excipientes corresponden a los diversos productos que permiten moldear el medicamento (un jarabe, un gel, una pastilla, etc.) para dosificar. El principio activo, para ayudar a la digestión del ingrediente activo, para facilitar la producción del medicamento, para proteger el ingrediente activo del ambiente externo (una cápsula, por ejemplo, que contiene un polvo en el interior), o para ayudar a los pacientes a "aceptar" el medicamento más fácilmente (agregando un sabor, un color, una textura) También debe tenerse en cuenta que el ingrediente activo y los excipientes están compuestos de un conjunto de materia prima. Las materias primas pueden ser orgánicas o químicas.

Las materias primas orgánicas, aunque a menudo modeladas químicamente, tienen su origen en las plantas medicinales. Y cuando la fragilidad del ecosistema de una planta medicinal no puede garantizar la necesidad y el volumen de producción de un medicamento, los químicos deben desarrollar alternativas: este es, por ejemplo, el caso del Tejo occidental o del Pacífico (*Taxus*

brevifolia), un árbol conífero utilizado en medicina porque contiene paclitaxel, una sustancia que puede tratar el cáncer de pulmón, ovario y seno. Cuando se descubrió esta sustancia en la década de 1960, la sobreexplotación de los tejos causó una disminución de la población y la protesta pública. El método utilizado en ese momento para obtener paclitaxel dejó los árboles muertos, y los químicos tuvieron que desarrollar una alternativa. Hoy, el paclitaxel se desarrolla en el laboratorio utilizando resina presente en las ramas y agujas de los tejos europeos, y la resina se modifica y se cultiva a través de la fermentación celular. Este proceso de fabricación es sostenible y permite no dejar árboles muertos [39].

Desde un punto de vista más legislativo, los medicamentos también están enmarcadas por un conjunto de leyes y normas. En Francia, el artículo L5111-1 es responsable de definir qué es un medicamento [23]:

"Medicamento" significa cualquier sustancia o composición presentada como poseedor de propiedades curativas o preventivas con respecto a enfermedades humanas o animales, así como cualquier sustancia o composición que se pueda usar en el hombre o en animales o que se les pueda administrar, establecer un diagnóstico médico o restaurar, corregir o modificar sus funciones fisiológicas ejerciendo una acción farmacológica, inmunológica o metabólica.

Esta definición de lo que permite un medicamento, además de resaltar el hecho de que los medicamentos y sus usos, están y permanecen enmarcados. Su comercialización, distribución y consumo son, por lo tanto, elementos clave de los sistemas de salud actuales.

2.1.2. La creación de un medicamento

Algunos medicamentos fueron descubiertos por accidente, como la penicilina por Alexander Fleming en 1928 (este descubrimiento le valió el Premio Nobel de Medicina en 1945 con Howard Walter Florey y Ernst Boris Chain) [28]. Pero en general, y aún más hoy en día con los gigantes farmacéuticos que dominan la industria, se necesitan millones, en algunos casos miles de millones de dólares para desarrollar un medicamento con una autorización de comercialización y propiedades. medicamentos específicos

2.1.2.1. El descubrimiento de un nuevo medicamento

El primer paso para crear un medicamento [1] es buscarlo. La duración de este período es aleatoria, un laboratorio puede encontrarse muy rápidamente con un conjunto de moléculas efectivas, o pasar años para realizar simulaciones para obtener un alto rendimiento con una molécula objetivo. Esta investigación a menudo es inhibida por la investigación de mercado. Estos estudios de mercado están destinados a identificar las diferentes enfermedades que necesitan medicamentos, para verificar la viabilidad de la comercialización y el rendimiento. Hay dos formas distintas de descubrir un nuevo medicamento:

- El cribado de alto rendimiento consiste en probar una gran cantidad de moléculas diferentes con un sustrato dado, lo que permite identificar las moléculas más eficientes con bastante rapidez, y a medida que se realizan las pruebas (pruebas en animales o células cultivadas), para aislar ciertas moléculas que ofrecen reacciones a las pruebas.
- El enfoque racional es desarrollar moléculas específicas para un sustrato modelando las pruebas con una computadora y luego realizar pruebas para corroborar los modelos creados.

Estos dos métodos, aunque tienen enfoques distintos, permiten la identificación de aproximadamente 250 moléculas potenciales diferentes que luego se deben filtrar y volver a probar durante el desarrollo preclínico.

2.1.2.2. El desarrollo preclínico

Esta fase de desarrollo, que dura entre 2 y 4 años para llegar a su conclusión, tiene como objetivo determinar la mejor manera de garantizar el diseño del medicamento para su uso final. Permite analizar cómo el cuerpo recibe el medicamento, la reacción del cuerpo, cómo el cuerpo elimina el medicamento y reduce a unas pocas moléculas candidatas en las que se basará el medicamento comercial futuro. Estos desarrollos corresponden a baterías de prueba de la droga, principalmente para una mejor orientación de una patología específica.

Esta fase también determina la forma comercial del medicamento: en forma de crema, píldora, inyección o aerosol. La forma del medicamento no es insignificante, ya que tiene un impacto directo en la efectividad del medicamento, pero también en la aceptación potencial del medicamento por parte de los consumidores (los supositorios, por ejemplo, son más ampliamente aceptados en los países América).

La finalización del desarrollo preclínico corresponde a la aprobación (o no) del medicamento por parte de las agencias de salud de los diferentes países en los que la compañía desea probar su producto. Si las agencias de salud validan la utilidad del medicamento, esa comienza su siguiente fase, la del desarrollo clínico.

2.1.2.3. El desarrollo clínico

Este paso corresponde a ensayos clínicos en voluntarios para aprender más sobre el medicamento, incluida su efectividad y seguridad. El desarrollo clínico de un medicamento consta de 5 fases: 0 (efecto sobre el cuerpo), I (seguridad para el hombre), II (eficiencia para tratar la enfermedad objetivo), III (seguridad y efectividad del medicamento a gran escala) y IV (monitoreo continuo de los efectos de los medicamentos en los pacientes). Las primeras cuatro fases (de 0 a III) tardan entre tres y seis años en llegar a su fin.

Aproximadamente cinco moléculas alcanzan el desarrollo clínico, y de estas cinco moléculas una o dos van a la autorización de comercialización. Una vez que se permite que un medicamento ingrese al mercado, la compañía que lo desarrolló tiene una exclusividad sobre el medicamento, lo que le permite recuperar los costos de desarrollo. Es después de un cierto período de comercialización que un competidor puede desarrollar un genérico del medicamento, los genéricos tienen la particularidad general de tener un precio más bajo. Esta duración varía según los países y las zonas económicas: entre 5 y 12 años en los Estados Unidos de América según el tipo de droga, 6 años en Japón, 8 años (con 2 años adicionales de exclusividad de mercado, y un año adicional si el medicamento es innovador) en Europa [40], y 20 años en Chile. Incluso después de la validación por parte de las agencias de salud, la compañía debe continuar probando y monitoreando los comentarios de los usuarios para garantizar la seguridad y efectividad del medicamento.

La autorización de comercialización de un medicamento depende de las agencias nacionales de salud. En Francia, la agencia nacional para la seguridad de los medicamentos y productos de salud es responsable de autorizar la comercialización de medicamentos, mientras que en Chile es el ministerio de salud [11]. Una vez que se ha obtenido la autorización, el medicamento se puede vender en todos los puntos de venta autorizados.

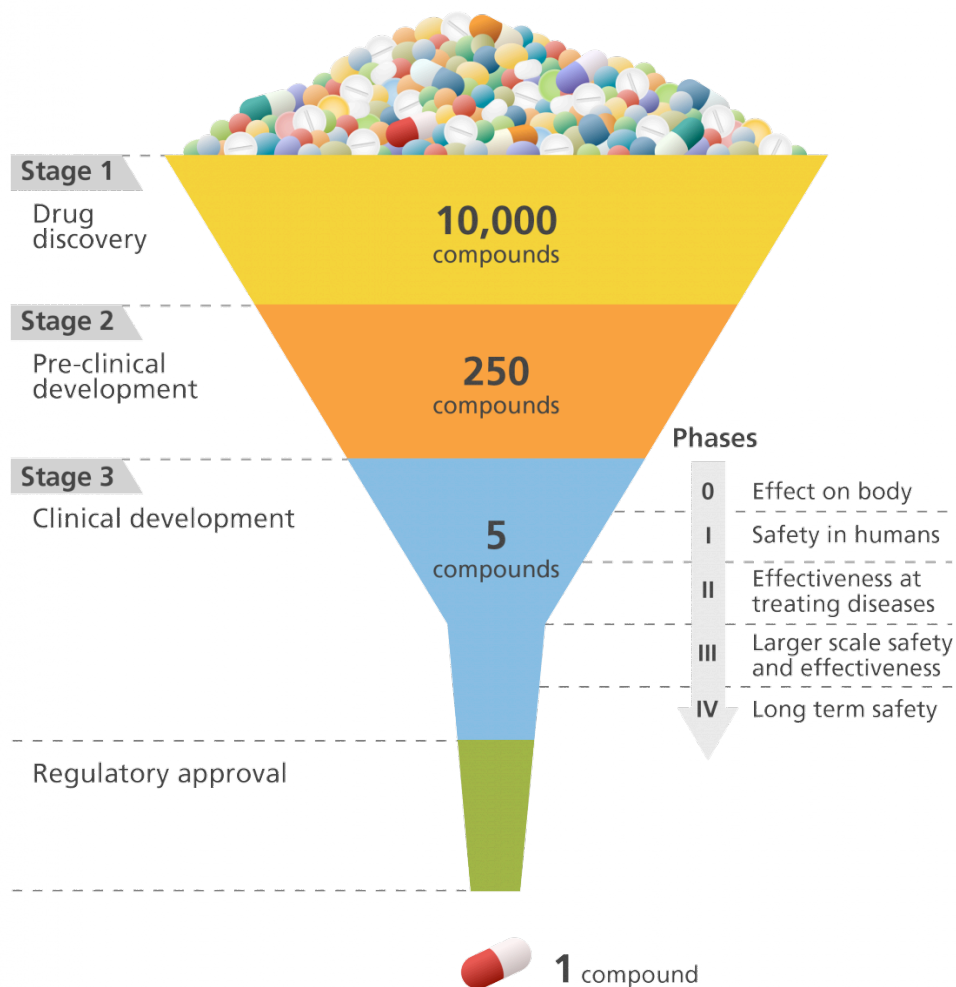


Figura 1: Las fases del diseño del medicamento - Fuente: Genome Research Limited

2.1.3. La cadena de suministro

La cadena de suministro de medicamentos consta de cuatro etapas sucesivas. Estas etapas tienen lugar en centros a miles de kilómetros de distancia entre sí, por lo tanto, el funcionamiento adecuado de la cadena es esencial: un retraso en la entrega de uno de los centros puede causar un retraso en toda la línea de producción. El objetivo del análisis de la cadena de suministro es identificar los pasos clave que podrían afectar a los consumidores y, por lo tanto, aquellos para los que es importante una mejor trazabilidad.

Debido a la importancia en los resultados finales del buen funcionamiento de las cadenas de suministro, la mayoría de las empresas del sector farmacéutico intentan mantenerlo en secreto, a fin de preservar las especificidades y ventajas propias de cada una de ellas. Por otro lado, es posible teorizar y crear un modelo cercano a todos los modelos existentes, basándose en datos públicos. Para desarrollar este modelo, se utilizará la cadena de suministro de Novartis [35]. Novartis es un grupo farmacéutico suizo, el cuarto grupo farmacéutico más grande en términos de ingresos en 2018 [24].

2.1.3.1. La cadena de suministro para Novartis

Para gestionar su proceso de fabricación y cadena de suministro, Novartis divide sus operaciones en 3 divisiones: Operaciones Químicas, Operaciones Farmacéuticas y Oficinas Farmacéuticas Nacionales. Estas tres divisiones tienen objetivos independientes en la producción de

medicamentos, con vínculos físicos entre los conductores de entrega, miembros de Novartis o no. Cada una de estas subdivisiones está presente en varios países, además de Suiza, donde Novartis tiene su sede.

2.1.3.1.1. Las operaciones químicas

Las operaciones químicas, llamadas ChemOps internamente (por *Chemical Operations* en inglés), son responsables de transformar materiales iniciales puros en sustancias farmacológicas. Novartis tiene 4 centros en todo el mundo:

- Ringaskiddy, Irlanda
- Grimsby, Gran Bretaña
- Basilea, Suiza
- Resende, en Brasil

Cada centro ChemOps es responsable de su propia red de suministro de materia prima para crear sustancias farmacológicas. Una vez que se producen dichas sustancias, se conservan en almacenes. Desde estos almacenes, las sustancias se envían a centros de operaciones farmacéuticas en todo el mundo. La mayoría del transporte de carga entre los diversos centros de Novartis es por vía aérea, por dos razones principales; La distancia entre la mayoría de los centros es importante, y el transporte aéreo permite garantizar la conservación de las sustancias medicinales en un estado excelente (la cadena de frío se conserva, las sustancias farmacológicas no conocen ningún cambio de temperaturas importantes ni de choques ...).

2.1.3.1.2. Las operaciones farmacéuticas

Las operaciones farmacéuticas, llamadas PharmOps internamente (para Operaciones Farmacéuticas en inglés) son responsables de recuperar las sustancias farmacológicas producidas por los cuatro centros de producción para convertirlas en medicamentos finales (en forma de cápsulas, jarabes, líquidos inyectables ...), luego administrar el empaque de los medicamentos en forma de producto terminado y luego distribuir los medicamentos listos para ser comercializados en las distintas oficinas farmacéuticas nacionales. En todo el mundo, Novartis tiene 15 centros PharmOps:

- Stein, Suiza
- Wehr, en Alemania
- Huninge, Francia
- Horsham, en Gran Bretaña
- Barberà del Vallés, España
- Torre Annunziata, Italia
- Kurtköy, Turquía
- Tabao de Serra, Brasil
- Tlaplan, México
- Suffern, Estados Unidos
- Sasayama, Japón
- Beijing, China
- Rabat, Marruecos
- Yakarta, Indonesia
- El Cairo, Egipto

Además de 15 centros internos de PharmOps en Novartis, la compañía también trabaja con proveedores externos. El trabajo de estos proveedores externos es fabricar medicamentos Novartis, ya sea bajo diferentes marcas o medicamentos genéricos. Estas compañías son completamente independientes, pero pasan por las oficinas farmacéuticas nacionales para comercializar sus productos. Estos proveedores externos son las siguientes ocho empresas:

- Noven Pharmaceuticals, con sede en Miami, Estados Unidos.
- Patheon, con sede en Durham, Estados Unidos
- Famar, con sede en París, Francia.
- Jamshoro, con sede en la ciudad de Jamshoro, Pakistán
- Mipharm, con sede en Milán, Italia.
- Orion, con sede en Espoo, Finlandia.
- Akorn, con sede en Hettlingen, Suiza.
- Zárate, con sede en Zárate, Argentina.

Todos estos centros y empresas están agrupados por Novartis en grupos geográficos para gestionar la coordinación con las oficinas farmacéuticas nacionales. Estas agrupaciones son las siguientes:

- El grupo Europa (compuesto por centros PharmOps en Gran Bretaña, Alemania, Francia, España, Italia, Turquía y Suiza, y proveedores externos de Famar en París, Francia, Mipharm en Milán, Italia), Orion a Espoo en Finlandia y Akorn a Hettlingen en Suiza)
- El grupo de América del Norte (compuesto por el Centro de Farmacia de los EE. UU. Y terceros Noven Pharmaceuticals en Miami y Patheon en Durham, ambos en los EE. UU.)
- El grupo latinoamericano (compuesto por los centros PharmOps de Brasil y México, y el proveedor externo Zarate, en Zarate, Argentina)
- Agrupación de otros países, que operan a nivel nacional (que consta de centros PharmOps en Marruecos, Egipto, Indonesia, China y Japón, y el proveedor externo Jamshoro con sede en Pakistán). Cada uno de estos centros es independiente y es responsable de un país o área geográfica.

2.1.3.1.3. Las oficinas farmacéuticas nacionales

Las oficinas farmacéuticas nacionales, llamadas Oficina Farmacéutica del País interna, o CPO, son responsables de la venta y distribución de productos Novartis en una región geográfica específica (un país o un conjunto de países). Estos son administrados por Novartis o administrados por terceros. En general, Novartis prefiere administrar sus centros y todo su proceso de producción, con el fin de aumentar su valor para sus accionistas, pero en algunos países, las leyes o regulaciones locales requieren que utilicen PO de terceros. Las oficinas farmacéuticas nacionales se distribuyen según las siguientes regiones:

- La región de Asia / Pacífico, que obtiene sus medicamentos del grupo de Europa.
- La región de Europa, que obtiene sus medicamentos del grupo de Europa.
- La región de América del Norte, que obtiene sus medicamentos del grupo norteamericano.
- La región de América Latina, que obtiene sus medicamentos del grupo latinoamericano.
- Y, finalmente, las oficinas nacionales en los países, que obtienen sus medicamentos del grupo de otros países (por ejemplo, Japón, que obtiene sus productos del centro PharmOps de Sasayama)

Una vez que los medicamentos se distribuyen en sus respectivos OAC, Novartis vende los medicamentos directamente a sus clientes, sin pasar por terceros. Los clientes pueden ser hospitales, cadenas de farmacias, mayoristas, agentes nacionales y, en casos específicos (en el caso de una enfermedad rara con un número limitado de pacientes en todo el mundo), directamente a los pacientes.

Además de este conjunto de centros en todo el mundo, también debe tenerse en cuenta que Novartis también gestiona laboratorios de investigación y desarrollo y oficinas más tradicionales (que se ocupan del marketing, las relaciones con los clientes y todas operaciones que no afectan la fabricación y la cadena de suministro de medicamentos). Aunque estos centros no entran en el proceso de la cadena de suministro, citarlos proporciona una visión más integral de todo el negocio.

2.1.3.2. Un modelo teórico de la cadena de suministro.

A partir del modelo de la cadena de suministro de Novartis, es posible generalizar la forma en que opera la industria farmacéutica y crear un modelo de la cadena de suministro teórica. El objetivo, mediante el modelado, es analizar el papel de cada uno y los vínculos existentes entre los diferentes actores. Este análisis será útil para la solución propuesta.

Este modelo de cadena de suministro se basará en gran medida en el de Novartis, al tiempo que pretende generalizar varios elementos y varios actores. Será imperfecto y tendrá un aspecto más teórico (operación global, vínculos entre las diferentes partes) que práctico (en correspondencia clara con la cadena de suministro de una determinada empresa). La idea aquí es generalizar la lógica de las cadenas de suministro de varias compañías farmacéuticas (Novartis, Pfizer, Sanofi, Johnson & Johnson ...), y no analizar la cadena de suministro de cada compañía conocida. Este análisis tiene la ventaja, durante la fase de implementación de la solución de trazabilidad, de ser lo suficientemente genérico como para poder parecerse al modelo de la empresa A, B o C, con cada empresa con una cadena de suministro diferente. Por ejemplo, donde Novartis tiene quince PharmOps, un modelo tendrá entre cero y n PharmOps, y n podrá ir al infinito. Este modelo también supone que todas las cadenas de suministro en el sector farmacéutico tienen equivalentes a PharmOps y CPO.

Los ChemOps no se utilizan en este modelo, porque la trazabilidad de un medicamento es importante en el caso del medicamento final, y porque las compañías farmacéuticas tienen el objetivo de ofrecer productos terminados, no ingredientes activos, para los consumidores.

Al generalizar los actores en la cadena de suministro de Novartis, se identifican los siguientes actores:

- Fabricantes de sustancias medicinales (FSM), que están presentes en la cadena de suministro en las diversas plantas de fabricación de medicamentos. Estos transforman los diferentes productos y moléculas básicas en sustancias medicinales. Los FSM corresponden a Novartis PharmOps.
- Oficinas farmacéuticas nacionales (BPN), que son responsables de recuperar los medicamentos para un área geográfica determinada y de venderlos a los clientes en un área geográfica designada. A diferencia del modelo Novartis, este modelo no formará un grupo geográfico de fabricantes de medicamentos (FSM). Cada BPN puede comprar a cualquier fabricante (y, por lo tanto, un BPN puede recibir un medicamento de diferentes FSM). Aquí se tiene en cuenta que el futuro usuario del modelo será exigente e irá a buscar suministros a un centro ubicado en su área geográfica (el suministro a un centro ubicado en su área geográfica tiene el objetivo de reducir los costos el transporte global y el suministro a un centro ubicado fuera de su área geográfica solo aumentará los costos).
- Clientes finales (CF), que pueden ser farmacias, hospitales, mayoristas, pacientes. Como parte de este modelo, los clientes finales pueden comprar a otros clientes finales de acuerdo con una lógica. Por ejemplo, un mayorista que compra medicamentos no está destinado a

consumirlos, sino a venderlos, mientras que un paciente final no debe vender los medicamentos que posee. El modelo es lo suficientemente extensible como para aceptar que un cliente final vende medicamentos y, por lo tanto, se convierte en un intermediario.

Hay tres jugadores principales en una cadena de suministro farmacéutica. El objetivo de la trazabilidad es permitir que el paciente sepa si el medicamento que va a consumir es el que compró, y no un medicamento potencialmente falsificado.

Además de los tres jugadores principales, hay diferentes operadores. Las interacciones entre los actores se realizan a través de ellos (el químico que diseña los medicamentos perdería su tiempo y su energía para transportar un medicamento a una oficina farmacéutica nacional). Estos transportistas son importantes en la cadena de suministro porque también pueden ser un defecto (por ejemplo, un transportista puede "hincharse" mucho con medicamentos similares, pero no tiene el mismo ingrediente activo). La lucha contra la falsificación debe permitir identificar a los actores que traen productos falsificados a una cadena de suministro segura y tomar medidas contra estos actores en caso de duda.

La siguiente figura muestra los diferentes actores del modelo de cadena de suministro, con las diferentes interacciones entre estos actores:



Figura 1: Un modelo genérico de cadena de suministro

En este esquema, FSM corresponde al fabricante del medicamento, las dos Ts a los transportistas (que pueden o no ser dos transportistas diferentes), BPN a una oficina farmacéutica nacional y CF a un cliente final. Este diagrama presenta la cadena de suministro más simple y directa. Hay muchas variaciones posibles de esta cadena, con, por ejemplo, una serie de medicamentos para la venta de CF a otros clientes finales (en el contexto de los mayoristas).

2.2. El estado actual de la trazabilidad en la industria farmacéutica

Dada la importancia de la trazabilidad de los medicamentos para la salud pública y económica de muchos países, ahora hay muchas herramientas implementadas para garantizar esto. Es una de las pocas herramientas que permiten al cliente asegurarse de que el medicamento que está comprando coincide con el medicamento que quiere comprar. Sin embargo, esta herramienta no es perfecta, a diferencia de las pruebas de laboratorio de un medicamento en un lote. No todos pueden probar cada lote de medicamentos en el hogar, la trazabilidad utilizando datos en el empaque ahora es la herramienta configurada para escalar los medicamentos. Durante la producción de medicamentos, estos se producen por lotes (o por lotes en inglés). Es este número de lote el que se rastrea, lo que permite a los productores de medicamentos saber, en el caso de un medicamento defectuoso, recordar todo un lote del medicamento en cuestión y, por lo tanto, prevenir posibles peligros. lo que podría ser perjudicial para la salud del consumidor (así como para mantener la confianza del consumidor en los medicamentos de este productor). Este número de lote se encuentra necesariamente en una matriz de datos, así como en el empaque del medicamento.

2.2.1. Análisis de datamatrix

Las datamatrix son hoy las herramientas más modernas utilizadas por la industria farmacéutica. Estos son muy similares a los códigos QR (QR significa respuesta rápida), muy populares hoy en día, pero existen varias diferencias entre los códigos QR y la matriz de datos. En paralelo con estos dos sistemas de codificación, los códigos de barras tradicionales, también conocidos como códigos de barras lineales, también se encuentran comúnmente en la mayoría de las empresas. Estos tres sistemas representan los sistemas más comunes, pero hay docenas de otros tipos de códigos: código azteca, código de barras de color de alta capacidad, ShotCode y muchos otros [5]. Entre los códigos QR, la matriz de datos y los códigos de barras, existen diferencias, representadas en la tabla anterior [29]:

QR Codes	Datamatrix	Código de barras lineal
		
• Código en 2D • Desarrollado en 1994 • 4296 caracteres • Entre el 7% y el 30% de corrección de posibles errores en la lectura	• Código en 2D • Desarrollado en 1989 • 2335 caracteres • 30% posible corrección de errores	• Código en 1D • Desarrollado en 1951 • 80 caracteres¹ • 0% de error, pero un número de clave de control para identificar errores en la lectura

En uso, los códigos unidimensionales pueden codificar mucha menos información que un código en varias dimensiones. Además, solo se pueden leer alineando correctamente el lector con el código. En contraste, los códigos bidimensionales son mucho más convenientes de manipular porque se pueden leer en cualquier dirección. Esto se debe a la antigüedad de los códigos de barras: estos se desarrollaron en los años 50 (y en realidad se usaron a partir de los 70, con el primer uso en un paquete de chicle de la Wrigley Company en junio de 1974 [13]), y los lectores en ese momento no eran tan accesibles como lo son hoy. Los códigos QR y datamatrix, más nuevos, se pueden jugar en cualquier teléfono hoy.

Sin embargo, los códigos QR tienen una debilidad significativa, que se puede utilizar con fines maliciosos. Estos se redirigen automáticamente a las páginas web si eso es lo que se escanea, y estas páginas pueden descargar virus cuando se abren, contienen contenido ilegal y, en general, contienen contenido peligroso. Además, los códigos QR están en muchos lugares, una etiqueta que contiene otro código QR se puede colocar encima de un código QR en un póster oficial (por ejemplo, un banco), el código QR "pirata" se refiere a un sitio que es muy similar al sitio web del banco y en el que se le puede solicitar que ingrese datos personales (número de tarjeta de crédito, nombre y dirección de la persona ...). Por lo tanto, los códigos QR se pueden usar para usuarios de phishing que no conocen los riesgos que presentan.

¹ Existen diferentes tipos de códigos de barras lineales, aquí se ha elegido comparar con el Código 128, utilizado principalmente para envíos (y, por lo tanto, la cadena de suministro de elementos).

Por lo tanto, la industria farmacéutica ha recurrido a datamatrix, más segura y que permite registrarse en un espacio más pequeño que los códigos QR. Este problema del espacio utilizado es importante para los medicamentos, porque el espacio disponible en las cajas y el empaque de los medicamentos es muy débil. Algunos países y gobiernos, como los países de la Unión Europea, se han visto obligados a utilizar datamatrix desde el 9 de febrero de 2019 para el envasado de medicamentos. Pero de manera más general, GS1 (Global Standards 1) regula y desarrolla la estandarización de los métodos de codificación utilizados en las cadenas de suministro. Francia y Chile son parte de esta organización. Aunque este organismo ofrece cierta libertad con respecto a los estándares de trazabilidad de medicamentos (el uso de datamatrix no es obligatorio en todos los territorios), datamatrix se ha establecido globalmente en todo el mundo (Chile, Argentina, Estados Unidos de América). Estados Unidos, miembros de la UE, entre otros) [12].

En Europa, el uso de datamatrix permite tener mucha información sobre un medicamento determinado. Esta información está estandarizada de acuerdo con ISO / IEC 16022: 2006 [17], que define los requisitos para el uso de datamatrix. Los datos codificados por datamatrix en los paquetes de medicamentos son los siguientes:

ASCII23201034009300001201715081010234X22ASCII299123587

El desglose de estos datos se realiza de acuerdo con el siguiente modelo:

- En rojo es una baliza de computadora (generalmente no transcrita por el lector) que permite conocer el formato de codificación. En este ejemplo, es ASCII 232, un formato de codificación de caracteres
- En verde son marcadores para ayudar al lector a reconocer lo que está leyendo.
- En azul, este es el número GTIN (Número de artículo comercial global) impuesto por el GS1. Este número contiene 14 caracteres, y el primer carácter indica si es un medicamento para venta directa (si comienza con un 0), otro tipo de venta (1-8) o un medicamento específico (9). El número GTIN permite adaptarse a una codificación nacional (en Francia, por ejemplo). Esta codificación nacional corresponde al número NTIN (Número de artículo comercial nacional). Estos 14 caracteres identifican el medicamento y su marca (por ejemplo, dos medicamentos genéricos vendidos por la misma marca tendrán el mismo número GTIN).
- En morado está la fecha de vencimiento del medicamento, con el formato JJMMAA (DD corresponde al día, MM al mes y AA al año).
- En naranja es el número de lote del medicamento.
- En marrón, estos son números gratuitos que permiten a la compañía que produce el medicamento agregar la información que desea.



Figura 2: Ejemplo de Datamatrix y datos asociados - Fuente: <https://ec.europa.eu/> [36]

En este ejemplo, los datos corresponden a los codificados por la matriz de datos, pero además legibles: PC (código de producto, código de producto), SN (número de serie, número de serie), NN (número nacional, número nacional para identificar el producto en un país determinado y permitiendo el reembolso de este), Lote (el número de lote) y Vencimiento (la fecha de vencimiento).

Toda esta información identifica claramente un lote defectuoso para la compañía que vende el medicamento, pero brinda muy poca información al consumidor sobre el origen de su medicamento y qué pasos de producción ha seguido. Además, toda la información codificada también se encuentra en el envase del medicamento, y simplemente se codifica de nuevo en la matriz de datos. Pero no hay información adicional en esta matriz de datos, y como se ha visto anteriormente, se puede codificar mucha más información (2335 caracteres) dentro de una matriz de datos. Esta nueva información se puede codificar dentro de números libres, usando nuevas etiquetas.

Además, cualquiera puede generar esta matriz de datos de código solo, y hacer una casilla "pirata" para pasar medicamentos falsificados por medicamentos legítimos. Aunque las diversas personas capacitadas para identificar y leer una matriz de datos podrían estar al tanto de la falsificación, para la mayoría de las personas esta información parecería legítima. La falta de protección de datamatrix y la facilidad de falsificación hacen que sea una evolución importante en la trazabilidad de los medicamentos, pero que sigue siendo imperfecta.

2.2.2. Análisis de la RFID

Otra tecnología actualmente disponible es el chip de identificación por radio, más comúnmente llamado así por la abreviatura RFID (abreviatura de identificación por radiofrecuencia). El uso del acrónimo RFID, aunque de origen inglés, se acepta en francés. La tecnología RFID se basa en la radiofrecuencia, que es la frecuencia de una onda magnética entre 30 Hz y 3000 GHz. La identificación de un elemento de radiofrecuencia es una técnica que permite identificar objetos utilizando un dispositivo electrónico capaz de transmitir información a un lector especializado. Hoy, el uso de RFID es diario para la mayoría de las personas, sin que se den cuenta. Por ejemplo, esta tecnología se puede encontrar en tarjetas sin contacto, en bibliotecas para seguir libros, en tiendas para combatir el robo...

La tecnología RFID utiliza radiación electromagnética para identificar o rastrear objetos o personas con una etiqueta cuando pasa cerca de un lector. A diferencia de los códigos de barras lineales, el lector no requiere alineación en la etiqueta. La lectura de una etiqueta es automática y puede realizarse a distancias entre 10 metros y casi 200 metros. Una etiqueta RFID puede almacenar hasta 64000 caracteres [14], mucho más que los 4296 caracteres ofrecidos por los códigos QR (y 2335 caracteres de datamatrix). Además, RFID no requiere escaneos, permite leer de forma secuencial pero muy rápida, y sin intervención humana, una gran cantidad de etiquetas. Esta lectura secuencial está adaptada a la industria, para escanear a la vez un conjunto de productos que llegan del mismo proveedor.

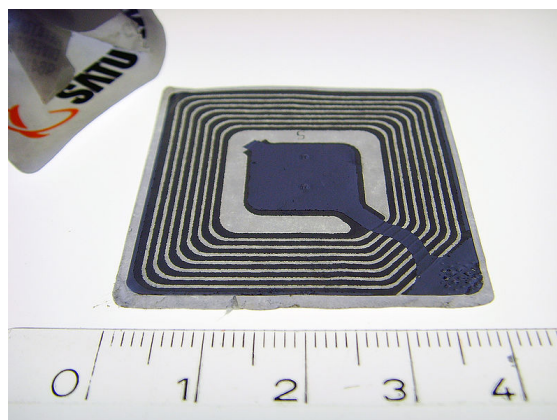


Figura 3 : Ejemplo de un chip RFID - Fuente: Wikimedia

Una etiqueta (que también se puede llamar etiqueta o etiqueta de radio) consta de al menos un microchip. Es en este chip electrónico donde se ubica la información. Hay tres tipos diferentes de etiquetas. Esta distinción se realiza independientemente del medio, la forma y el tamaño de la

etiqueta, pudiéndose variar y combinar estos parámetros hasta el infinito. Los tres tipos de etiquetas son:

- Pasivo; Este tipo de etiqueta es la más extendida, y está presente hoy en la compra de muchos productos (ropa, videojuegos, libros ...). Esta etiqueta, como su nombre indica, es puramente pasiva. La etiqueta contiene datos congelados leídos por el interrogador RFID cuando está cerca.
- Semi-pasivo; Este tipo de etiqueta se utiliza para aplicaciones específicas (registro de temperatura, flujo de personas ...). Incluye una fuente de alimentación para actualizar los datos contenidos en ella con la ayuda de sensores, pero esta fuente de alimentación no transmite datos: su lectura es pasiva, utiliza la onda del interrogador RFID para alimentar el chip electrónico incorporado, y así transmitir la información contenida en su memoria [14].
- Activo; Este tipo de etiqueta incorpora una batería y un transmisor de radiofrecuencia. La batería, a diferencia de una etiqueta semi-pasiva, alimenta el transmisor y, por lo tanto, permite interactuar de forma autónoma con el entorno, por ejemplo, cuadrando una zona y comunicándose con otras etiquetas activas en Cambios en la zona. Esta etiqueta registra datos en un área utilizando un conjunto de sensores.

Como parte del monitoreo de medicamentos, la etiqueta utilizada es una etiqueta pasiva: contiene información sobre el medicamento (los mismos que están en la matriz de datos). Esta información permite que un escáner lea todas las cajas de medicamentos que llegan a un almacén o farmacia [16].

Pero un sistema RFID, además de las etiquetas que pueden ser únicas o en grandes cantidades, consiste en una base de datos que contiene información sobre los datos presentes en las etiquetas, una interfaz para vincular esta base de datos. datos con el lector RFID y uno o más lectores RFID. Estos lectores son responsables de leer y transmitir la información contenida en una etiqueta [30]. En el mercado, hay una gran cantidad de antenas y lectores dependiendo de la frecuencia y el uso deseado. Se pueden usar varias frecuencias RFID en el mismo lugar sin que las ondas compitan (si están en diferentes bandas).

Sin embargo, como cualquier sistema electrónico, las etiquetas RFID tienen varias vulnerabilidades de seguridad. Estas fallas, que permiten leer la información contenida en la etiqueta (lectura por un sistema externo, análisis de poder), cambiar esta (retroingeniería, clonación de la etiqueta), o más ampliamente para extinguir el conjunto sistema (virus, denegaciones de servicio en la base de datos), que el uso de RFID tiene ciertas limitaciones. Estas fallas pueden compensarse mediante un mejor cifrado de la información en el chip, los métodos de filtrado de los lectores y los métodos de identificación [33]. El uso del estándar GS1 más reciente, el G2V2 (para la Generación 2 versión 2), mejora la seguridad de las etiquetas RFID pasivas, con la incorporación de nuevas características: medidas contra la falsificación, seguridad mejorada, derechos acceso, trazabilidad mejorada y posibilidad de etiquetar un artículo (por ejemplo, con "vendido", "en el estante" o "robado" [4]).

Como parte del sector farmacéutico, la FDA (*Food and Drug Administration*), la agencia estadounidense responsable de regular los medicamentos, comenzó a trabajar con la tecnología RFID a principios de la década de 2000 ante la aparición de medicamentos falsificados en el territorio. Estadounidense [8]. Es la miniaturización de las etiquetas RFID en los últimos años lo que sugiere una mayor adopción de tecnología dentro del sector médico. En 2008 se fundó la organización RFID in *Healthcare Consortium* (RHCC) [2], cuyo objetivo es promover el uso de la tecnología RFID dentro del sector médico y la optimización de su integración teniendo en cuenta varios problemas. (confidencialidad, riesgo de interferencia o seguridad, por ejemplo). Esto hace posible saber que el uso de RFID en el sector médico es reciente, pero tiene un gran potencial en el futuro.

El uso de RFID podría, además de ayudar con la trazabilidad de los medicamentos, ayudar a saber cuándo un paciente está tomando y siguiendo su tratamiento [16], que es uno de los otros

desafíos de la industria farmacéutica en la actualidad. Sin embargo, el costo de una etiqueta RFID es de aproximadamente 10 centavos para una etiqueta pasiva (una etiqueta activa, que cuesta casi 40 dólares, tiene poco interés en la industria farmacéutica para medicamentos consumidos y distribuidos ampliamente), mientras se imprime una matriz de datos en una caja de medicamentos a un costo sustancialmente menor (en milésimas de centavo). Para medicamentos que valen entre 1 y 2 euros, este es un aumento de precio del 5 al 10%, apenas justificable para el consumidor. Hoy, el costo de los sistemas RFID es una de las limitaciones clave para su adopción general por parte de la industria farmacéutica. Pero a la larga, esta tecnología debería reemplazar en gran medida la matriz de datos en las cajas de medicamentos. Sin embargo, debe enfatizarse que la información, ya sea contenida en una matriz de datos o una etiqueta RFID, sigue siendo la misma.

2.3. Las blockchains

En una frase, una cadena de bloques es un registro de transacciones digitalizado, transparente y descentralizado. Blockchains registra una lista cada vez mayor de registros, llamados bloques, que están vinculados y protegidos por criptografía. Las cadenas de bloques resuelven un problema fundamental: varias computadoras, que no se conocen y no confían entre sí, intentan ponerse de acuerdo en algo. El objetivo de una aplicación que utiliza una cadena de bloques es implementar una red en la que los usuarios de diferentes partes del mundo puedan interactuar entre sí con confianza. Para lograr este objetivo, es necesario utilizar un sistema distribuido capaz de acordar una única verdad por consenso, sin confiar en ninguno de los usuarios. Un consenso puede crear un sistema confiable a partir de entidades potencialmente no confiables.

2.3.1. Cadenas, bloques y datos

Una cadena de bloques, antes de distribuirse entre varias máquinas, es una estructura de datos. La ausencia de distribución elimina el principio mismo de la cadena de bloques, que es tener una verdad única distribuida entre varios usuarios, pero eliminar la distribución permite comprender la estructura de datos y los componentes internos de una cadena de bloques.

2.3.1.1. Los datos

Un blockchain es, desde un punto de vista externo, una base de datos. Permite seguir un conjunto de transacciones entre diferentes actores. Este conjunto de transacciones, representadas en forma de registro, permite saber qué datos pertenecen a qué actores. Por ejemplo, en el contexto de una criptomoneda, los datos rastreados son la cantidad de dinero que posee cada actor, mientras que las transacciones rastreadas son las transferencias de esa moneda entre los actores. Una blockchain es, por lo tanto, una base de datos de transacciones.

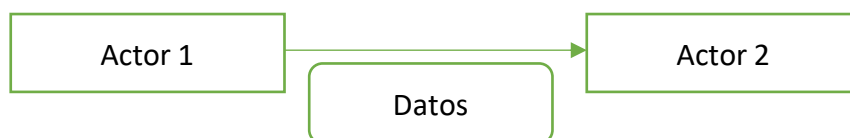


Figura 4: Esquema de una transacción.

2.3.1.2. Los bloques

En forma de un registro de transacciones, la cantidad de transacciones contenidas en la cadena de bloques aumenta rápidamente. No debe olvidarse que las cadenas de bloques son sistemas distribuidos y, en consecuencia, existe la posibilidad de que ocurran varias transacciones al mismo

tiempo entre varios actores. Para evitar la sincronización entre los diferentes actores de la cadena de bloques para cada transacción, las transacciones se agrupan en bloques.

La formación de bloques pasa por varias etapas. En un primer paso, los actores crearán transacciones entre ellos, que se agregarán dentro de un grupo de transacciones. Esta reserva consiste en transacciones, pero la peculiaridad de estas es que aún no están validadas por todos los actores. De hecho, un actor podría declarar poseer datos al resto de la red, mientras que él no lo es. Es para este propósito que existe el grupo de transacciones. En la mayoría de las implementaciones de blockchain, este grupo no es único, sino que consiste en un conjunto de grupos más pequeños.

Los actores específicos, llamados menores, irán a estas reservas y verificarán las transacciones. Si son correctos (los propietarios correctos envían los datos correctos, no hay duplicados), pueden agregar las transacciones a un bloque. Varios menores pueden seleccionar las mismas transacciones para agregar a sus bloques, la única condición para agregar una transacción a un bloque es su validez.

Además de las transacciones, un bloque debe contener un conjunto adicional de datos [38]. Estos datos adicionales se usan para validar o no la adición de un bloque a la cadena de bloques. Uno de los datos más importantes que debe tener un bloque es un hash (huella digital francesa). Este hash digital se calcula utilizando una función hash, que toma una entrada de texto y la asocia con una huella digital e identifica los bloques entre sí. Se necesitan pocos recursos para generar un hash.



Figura 5: Ejemplo de hash con SHA-256

Cada cadena tiene su propio hash, y una ligera modificación de una cadena cambia por completo el hash asociado con la cadena, ya que las funciones hash son funciones deterministas. Otra ventaja de los hashes es que es imposible determinar el texto codificado a partir de ellos. En una cadena de bloques, para calcular un hash, la función de hash del bloque tendrá en cuenta el hash de la cadena de bloques anterior y el hash asociado con el bloque actual. Por ejemplo, el hash del número de bloque 32 se generará a partir del hash del bloque 31 y el hash de texto del bloque 32. Cada bloque que contiene una multitud de transacciones, el hash del bloque se compone del conjunto de hashes de transacciones del bloque, usando un árbol Merkle, también conocido como un árbol hash.

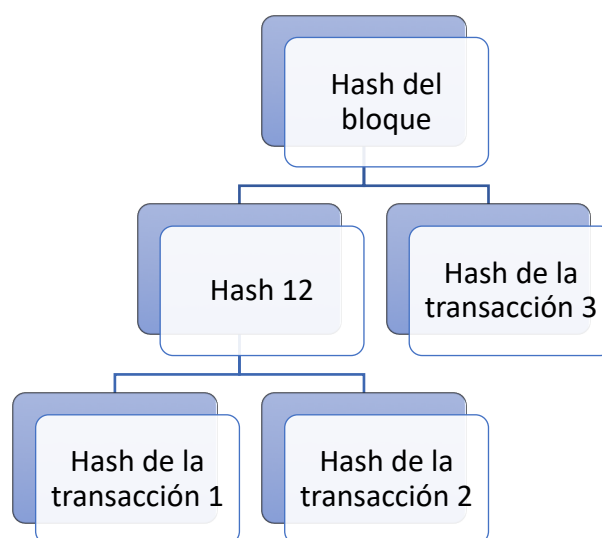


Figura 6: Composición del hash de un bloque en forma de árbol de Merkle.

El primer hash, el del bloque llamado "génesis", se genera sin tener en cuenta el hash del bloque anterior. Este hash solo se genera utilizando las transacciones contenidas en este primer bloque.

Otro dato incluido en un bloque es el nuncio. Es un número arbitrario que está destinado a usarse una vez y que permite crear una dificultad para el menor. Este nuncio se genera utilizando el hash del bloque. Por ejemplo, si se determina que el nuncio es "00", cada hash debe comenzar con ese nuncio para que sea válido. Esto permite crear, para el minero del bloque actual, una dificultad adicional al calcular el hash, mientras que los mineros que verificarán la validez del bloque pueden calcular rápidamente si un bloque es válido (si el hash es correcto y si comienza bien con "00"). El objetivo de este nonce, de esta dificultad, es evitar la adición permanente de bloques a la cadena de bloques por parte de menores que buscan corromperla.

Finalmente, cada bloque está marcado con una marca de tiempo. Esta marca de tiempo es un valor generado teniendo en cuenta la fecha y hora actuales. Esta marca de tiempo es una capa adicional de protección de blockchain, que evita la corrupción, ya que todas las transacciones deben tener marcas de tiempo crecientes (las transacciones más recientes en blockchain son transacciones con las últimas marcas de tiempo).

Para resumir, un bloque consta de transacciones, un hash, un nuncio y una marca de tiempo:

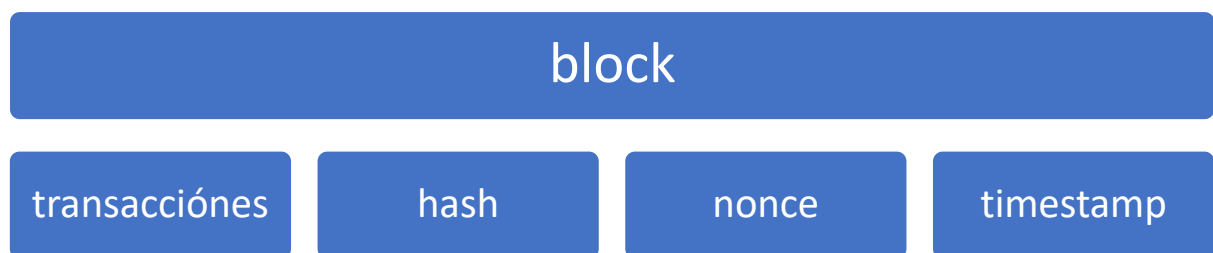


Figure 7: Composición de un block

2.3.1.3. Las cadenas

Como se indicó anteriormente, los bloques contienen hashes. Estos hashes se generan usando hashes de funciones anteriores. Estos permiten vincular las transacciones entre ellos y, por lo tanto, crear la cadena. En consecuencia, cualquier transacción depende de todas las transacciones anteriores para generar su hash. Es esta dependencia la que crea la inmutabilidad de una cadena de bloques: cada transacción depende de las anteriores, la modificación de una de las transacciones anteriores

cambia por completo las siguientes transacciones y, por lo tanto, modifica (o corrompe) la cadena de bloques.

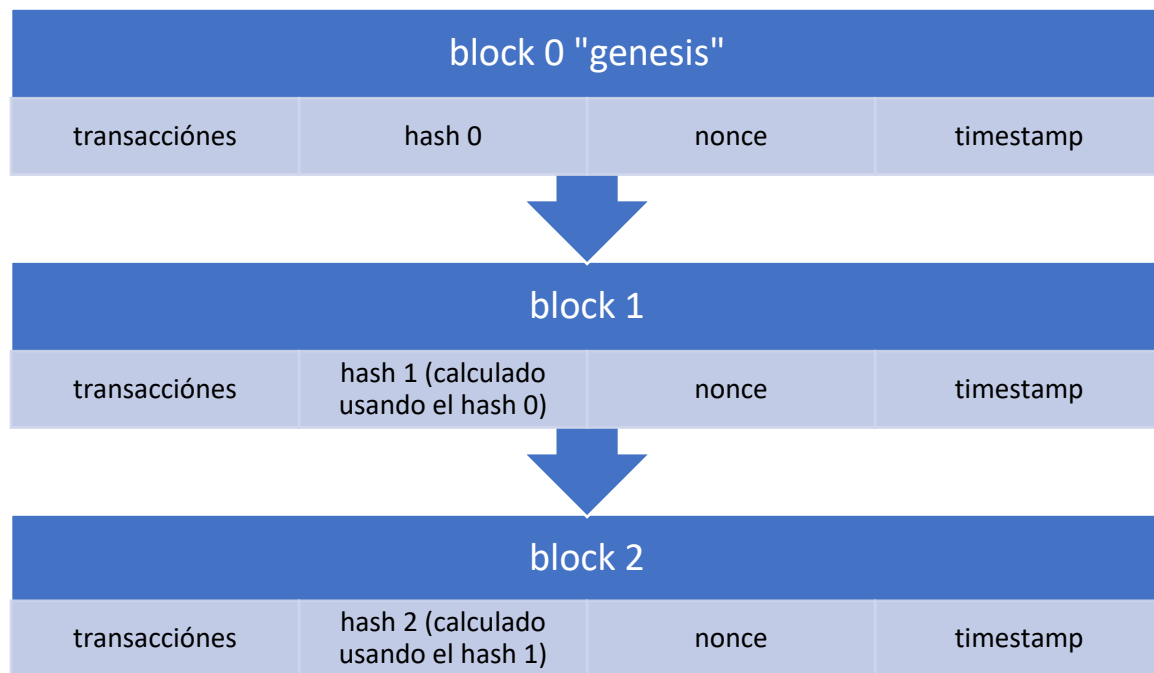


Figura 8 : Diagrama de una cadena de bloques

2.3.2. El sistema distribuido

2.3.2.1. Las propiedades de un sistema distribuido

Una cadena de bloques se distribuye entre varios mineros o nodos. Un sistema distribuido consta de nodos independientes que representan diferentes procesos y canales de mensajes que permiten que los nodos se intercambien entre sí. El objetivo de todos los nodos, y por lo tanto del sistema distribuido, es lograr una tarea global. Como parte de una cadena de bloques, la tarea es garantizar la validez de la cadena de bloques. Los nodos pueden realizar cuatro acciones: enviar, recibir, guardar y hacer cálculos sobre los datos que tienen. Un sistema distribuido tiene varias ventajas sobre un sistema centralizado: mientras que un sistema centralizado puede dejar de funcionar, cometer errores, perder datos o estar dañado, un sistema distribuido debe ser capaz de garantizar la persistencia de los datos entre diferentes nodos, y para evitar errores por parte del sistema. Es por eso por lo que los sistemas distribuidos son adecuados para almacenar información confidencial (como datos bancarios). Un sistema distribuido tiene varias propiedades:

- Los nodos compiten entre sí para gestionar la información.
- No hay un reloj global entre los nodos, cada nodo es responsable de su propio tiempo, pero todos los nodos intentan mantenerse sincronizados entre sí.
- Existe la posibilidad de que uno o más de los nodos experimenten fallas (pérdida de un mensaje de sincronización, un proceso que no se ejecuta correctamente ...). En el caso de fallas, los protocolos de intercambio (por ejemplo, el algoritmo Chandy-Lamport [10]) entre los nodos deben administrarlo, para que todo el sistema realice su trabajo correctamente.

Para garantizar la precisión de un sistema distribuido, es decir que cumple su propósito correctamente, utiliza algoritmos de consenso. Un algoritmo de consenso correcto debe satisfacer 3 propiedades.

- La validez de la solución final, es decir que el valor sobre el cual el algoritmo estará de acuerdo debe ser propuesto por uno de los procesos.
- Un acuerdo sobre el valor final entre los diferentes procesos (acuerdo), es decir, todos los procesos que no han conocido ningún fallo están conforme con el mismo valor final.
- Una conclusión, el algoritmo necesariamente debe devolver un valor final: no puede buscar un valor indefinidamente.

Estas 3 propiedades se dividen en dos categorías: las propiedades de seguridad, que aseguran que el resultado final sea correcto, la validez y el acuerdo, y la vida, que garantiza que se devolverá un valor, y esa es la conclusión. La definición de estas propiedades y categorías es el trabajo de Leslie Lamport.

Pero los sistemas distribuidos también tienen limitaciones. El teorema de Brewer (o teorema CAP) define estos límites. Según este teorema, es imposible para un sistema informático de computación distribuida garantizar al mismo tiempo:

- Consistencia: todos los nodos en el sistema ven exactamente los mismos datos al mismo tiempo.
- Disponibilidad (disponibilidad): se garantiza que todas las solicitudes recibirán una respuesta.
- Tolerancia a la partición (tolerancia de partición): ninguna falla menos importante que un corte total de la red debe evitar que el sistema responda correctamente (y, por lo tanto, una falla de los nodos no debe evitar que el sistema responda correctamente).

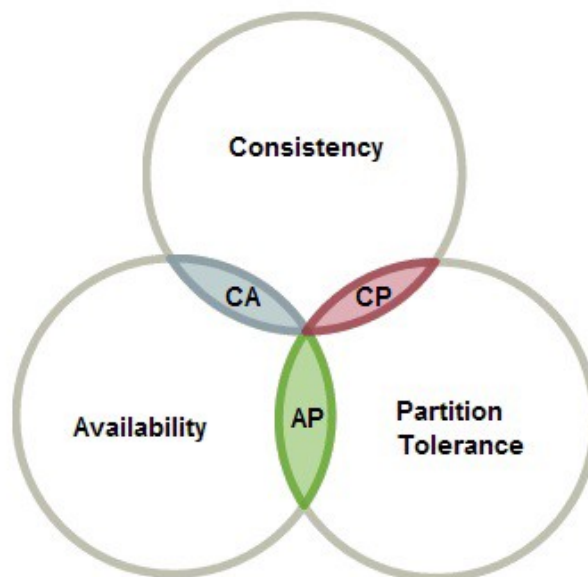


Figura 9: Representación del teorema CAP - Fuente: towardsdatascience.com [26]

Según este teorema, un sistema distribuido puede garantizar en un momento T solo dos de estas tres restricciones, pero no las tres. Por lo tanto, el sistema debe comprometer la consistencia, la disponibilidad y la tolerancia de partición.

En un sistema distribuido, este se divide entre diferentes máquinas. Por lo tanto, la tolerancia a la partición siempre debe tenerse en cuenta. Por lo tanto, la elección es elegir entre la coherencia del sistema y, por lo tanto, devolver un valor potencialmente falso y disponibilidad, y por lo tanto no devolver nada. Pero el teorema no es binario, responde más a un espectro de posibilidades. Por ejemplo, la disponibilidad puede no ser inmediata (la latencia es aceptable) para cumplir con el requisito de disponibilidad. El teorema de CAP permite comprender los límites de los sistemas distribuidos. Por lo tanto, los sistemas distribuidos pueden no generar un resultado. Un ejemplo de

falla del sistema distribuido es el de los generales bizantinos, en sí mismo una generalización del problema de los dos generales.

2.3.2.2. El problema de generales bizantinos

Este problema es uno de los problemas clásicos de los sistemas distribuidos. Su declaración es la siguiente:

"Los generales bizantinos rodean una ciudad que desean tomar. Para comunicarse entre sí, solo pueden usar mensajeros, y no han decidido qué harán: atacar la ciudad o abandonar el ataque y regresar a casa. Para conquistar la ciudad, todos los generales deben atacar al mismo tiempo. Pero el problema es que algunos generales han sido corrompidos a cambio de una suma de dinero y, por lo tanto, enviarán un mensaje incorrecto para derrotar el asalto y evitar así un consenso entre los generales. Además de los traidores, algunos mensajeros pueden perderse o corromper su mensaje ellos mismos. El objetivo es lograr un consenso entre los generales para atacar la ciudad, al tiempo que se garantiza que las comunicaciones entre ellos no se corrompan (pierdan o cambien). Permitidos los generales, hay un comandante y tenientes. Todo puede ser corrompido. Los generales corruptos son nudos bizantinos. "

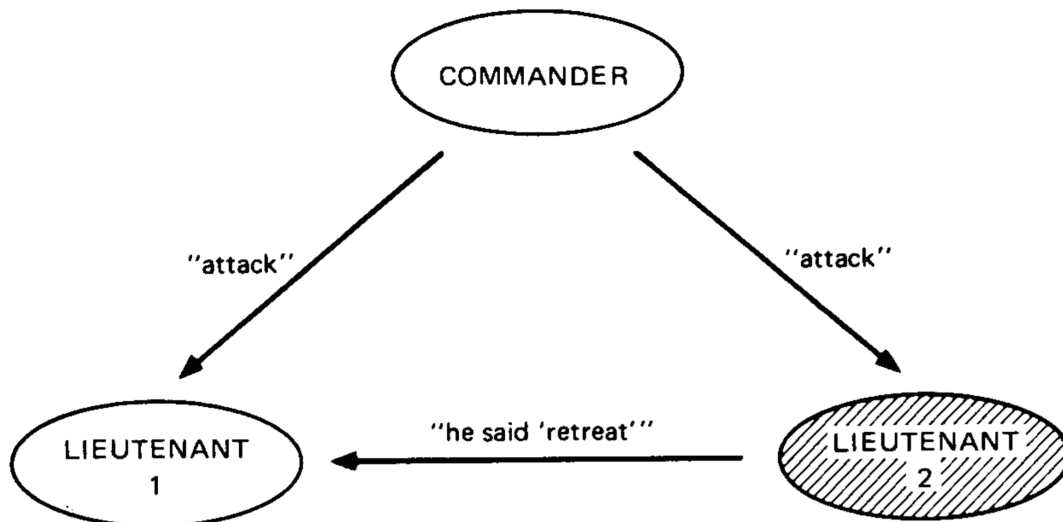


Figura 10: Problema de los generales bizantinos - Fuente: edx.org

En el ejemplo anterior, el comandante envía la orden de ataque, pero el teniente 2 está corrupto y modifica el mensaje que le envía al teniente 1. El teniente 1 recibe dos mensajes en sentido contrario: uno de ellos ataque, el otro para retirarse. Pero el teniente 1 no puede saber quién es el traidor. El comandante también puede haber enviado los mensajes de "ataque" al teniente 1 y "retirarse" al teniente 2. Por lo tanto, el teniente no sabe qué hacer, ni sabe quién es el traidor entre el comandante y el teniente 2. Este problema no tiene solución si más de un tercio de los nodos son traidores.

Este problema hace posible identificar los dos tipos de errores que pueden ocurrir en un sistema distribuido, errores de detención de fallas y errores de tipo bizantino. Un error de detención de falla es el bloqueo de un nodo o la ausencia de un valor devuelto. Este primer problema es el más fácil de identificar para los otros nodos del sistema, porque son conscientes de la ausencia de una respuesta de un nodo. Un error bizantino está inspirado en el problema de los generales bizantinos: los nodos pueden no funcionar, pueden no devolver valor, pero también pueden responder a información o corruptos o falsos. Los errores de tipo bizantino son una generalización de los errores de detención de fallas. Una blockchain pública debe evitar a toda costa un error bizantino, porque los

participantes de una blockchain son anónimos e impredecibles. La presencia de un error bizantino en una cadena de bloques lo corrompe.

El problema de los generales bizantinos se puede comparar con una cadena de bloques. Es el mismo concepto con dos nombres diferentes:

Distancia geográfica	Red distribuida
Generales	Nodos
Generales traicioneros	Nodos defectuosos o maliciosos
Mensajeros poco confiables	Mensajes entre nodos perdidos o dañados
Atacar o retirarse	Consenso sobre transacciones

El problema de los generales bizantinos es típico en el caso de las cadenas de bloques. Para resolverlo, debemos usar algoritmos de consenso, lo que permite que diferentes nodos acuerden un valor para devolver.

2.3.2.3. Los mecanismos de consenso

Los mecanismos de consenso son la columna vertebral de los sistemas distribuidos. Estos mecanismos funcionan principalmente en un principio de votación durante las actualizaciones del sistema distribuido. Este sistema de votación se basa en una lógica matemática.

2.3.2.3.1. Paxos

Paxos es una isla frente a las costas de Grecia. También es una familia de algoritmos de consenso para sistemas distribuidos, creada por Leslie Lamport [20], el mismo Lamport del algoritmo Chandy-Lamport. El nombre Paxos proviene del sistema político establecido en la isla de Paxos durante la antigua Grecia. Para aprobar decretos, el parlamento de Paxos, apodado "el parlamento a tiempo parcial", tenía un funcionamiento adecuado. Los parlamentarios solían dejarlo esporádicamente para asistir a banquetes y otras actividades. Como todos los parlamentarios nunca estuvieron en el parlamento al mismo tiempo, cada uno tenía un diario que contenía todo lo que estaba sucediendo. Todos los periódicos tenían que ser iguales. Los parlamentarios se dividieron en tres grupos: los proponentes, los aceptantes y los alumnos. Los defensores defendieron las peticiones e ideas de los ciudadanos, los aceptantes votaron las peticiones y las leyes, y los estudiantes recordaron las peticiones y las pasaron a los ciudadanos.

Las peticiones y leyes se decidieron por consenso. Para llegar a un consenso, la mayoría de los aceptantes tenían que estar en el parlamento: esta mayoría de los aceptantes correspondía a un quórum. Para llegar a un quórum (y, por lo tanto, la mayoría de los aceptantes están de acuerdo con una ley), tomó muchos turnos para llegar a un consenso entre los aceptantes. Cada turno se realizó en dos partes: preparar y aceptar.

Primero, los ciudadanos de la isla podrían hablar y hablar con los proponentes. Una vez que un defensor está listo para defender una causa, lo propone en forma de decreto en el parlamento. Cada decreto tiene un número y un valor (por ejemplo: "45. Está prohibido escribir en los templos"). Los números relacionados con los decretos deben necesariamente aumentar. Luego, una vez que el decreto propuesto en el parlamento, los aceptantes discuten y votan. Si en algún momento hay un quórum de aceptantes que votan en mayoría por el decreto, se ha aprobado y está escrito en los periódicos de cada parlamentario. Una vez que se llega a un consenso, los alumnos aprenden el resultado y lo transmiten a la gente de la isla.

El parlamento de Paxos funcionaba exactamente como un consenso distribuido. Los miembros del parlamento corresponden a los nodos de un sistema distribuido, los ciudadanos corresponden a los clientes y la ley actual al estado en el que los nodos deben estar de acuerdo. Sin embargo, el

parlamento de Paxos hace algunas suposiciones: los alumnos siempre transmiten el mensaje correcto a los ciudadanos y no intentan corromperlo. En otras palabras, el parlamento trabaja solo para un error de falla, es decir, la ausencia de nodos (y por lo tanto la ausencia de quórum), que luego corresponde a un parlamento vacío. No responde al problema de los generales bizantinos. La ausencia de uno de los miembros del parlamento no hace que este sea cerrado, y el funcionamiento de Paxos hace posible garantizar la velocidad de las leyes, y hace posible producir un conjunto importante de datos (aquí leyes y decretos), y para reproducir estos datos [21]. Solo Paxos siempre ha sido difícil de entender, y Lamport ha tratado de aclararlo publicando un nuevo artículo, "*Paxos made simple*" [22]. En 2014, se propuso una alternativa más comprensible a Paxos, Raft.

2.3.2.3.2. Raft

El algoritmo alternativo, apodado Raft, fue propuesto en un artículo llamado "*In Search of an Understandable Consensus Algorithm*" de 2014, escrito por Diego Ongaro y John Ousterhout [27]. En este artículo, el objetivo es escapar usando un bote ("*raft*" en inglés) de la isla de Paxos. Este algoritmo está formulado para tener un líder, que es elegido en cada turno, y seguidores, que son todos los demás nodos. El líder es el único que se comunica con el cliente, y es responsable de organizar y organizar el envío de mensajes del cliente a los diferentes nodos, mientras mantiene un registro de todo lo que se transmite. Cuando el líder recibe una solicitud de un cliente, verifica que todos los demás nodos hayan recibido la solicitud y que todos hayan escrito la solicitud en su propio registro. El líder lidera el consenso, hasta que se detiene o comete errores (stop-stop). Y en el caso de una falla, se elige un nuevo líder.

El líder es responsable de enviar consultas regularmente a otros nodos, anunciando que todavía está presente y vivo. Si los otros nodos no reciben más solicitudes, suponen que el líder está "muerto" y eligen un nuevo líder. Cada nodo tiene un reloj interno, que comienza cuando ya no recibe una solicitud del líder. Después de un cierto tiempo determinado por este reloj interno, cada nodo puede postularse para ser el nuevo líder. El nuevo líder es aquel cuyo reloj interno es el valor más grande (cada nodo comunica su valor a otro nodo, y el nodo con el valor más pequeño se convierte en un soporte del otro, esto hasta que solo hay un nodo, el líder elegido). Cabe señalar, sin embargo, que el algoritmo Raft no puede compensar los errores bizantinos.

2.3.2.3.3. Practical Byzantine Fault Tolerance (PBFT)

El algoritmo alternativo, apodado Raft, fue propuesto en un artículo llamado "En busca de un algoritmo de consenso comprensible" de 2014, escrito por Diego Ongaro y John Ousterhout [27]. En este artículo, el objetivo es escapar usando un bote ("*balsa*" en inglés) de la isla de Paxos. Este algoritmo está formulado para tener un líder, que es elegido en cada turno, y seguidores, que son todos los demás nodos. El líder es el único que se comunica con el cliente, y es responsable de organizar y organizar el envío de mensajes del cliente a los diferentes nodos, mientras mantiene un registro de todo lo que se transmite. Cuando el líder recibe una solicitud de un cliente, verifica que todos los demás nodos hayan recibido la solicitud y que todos la hayan escrito en su propio registro. El líder lidera el consenso, hasta que se detiene o comete errores (stop-stop). Y en el caso de una falla, se elige un nuevo líder.

Publicado por Miguel Castro y Barbara Liskov en 1999 [6], este algoritmo de consenso aborda el problema de los generales bizantinos. Si bien Paxos y Raft son algoritmos de detención de fallas, el PBFT puede admitir errores bizantinos (y así resolver un problema de tipo general bizantino). El algoritmo PBFT puede manejar f errores bizantinos cuando el número de nodos es igual a $3f + 1$ (por lo tanto, puede resolver el algoritmo por menos de $1/3$ de los nodos "traicioneros"). Es un algoritmo que consta de 3 partes: preparación previa, preparación y realización. PBFT comienza cuando el cliente envía una solicitud a uno de los nodos, cuyo nodo se hace responsable de reenviar la solicitud (en Paxos, los proponentes cumplen esta función).

Luego viene la fase de preparación previa, durante la cual el nodo responsable del mensaje lo envía a toda la red. Cada nodo acepta el mensaje solo si es válido (los mensajes deben contener un número secuencial, como en el caso de Paxos, y otros datos para determinar la validez de estos). Si un nodo acepta un mensaje preparado previamente, se envía un mensaje de disponibilidad entre sí en la red (que solo es aceptado por otros nodos si es válido). Un nodo se considera preparado si ha recibido el mensaje original y si ha recibido $2f$ mensajes leídos (y al hacerlo, el nodo sabe que hay $2f + 1$ nodo preparado).

Una vez que los nodos están preparados, deben enviar un mensaje de realización. Si un nodo recibe mensajes de preparación de $f + 1$, ejecuta la solicitud del cliente y la envía al cliente. El cliente considera que ha recibido una respuesta aceptable si recibe $f + 1$ respuestas idénticas. La siguiente figura explica la cadena de mensajes, teniendo en cuenta que el nodo 3 está fallando.

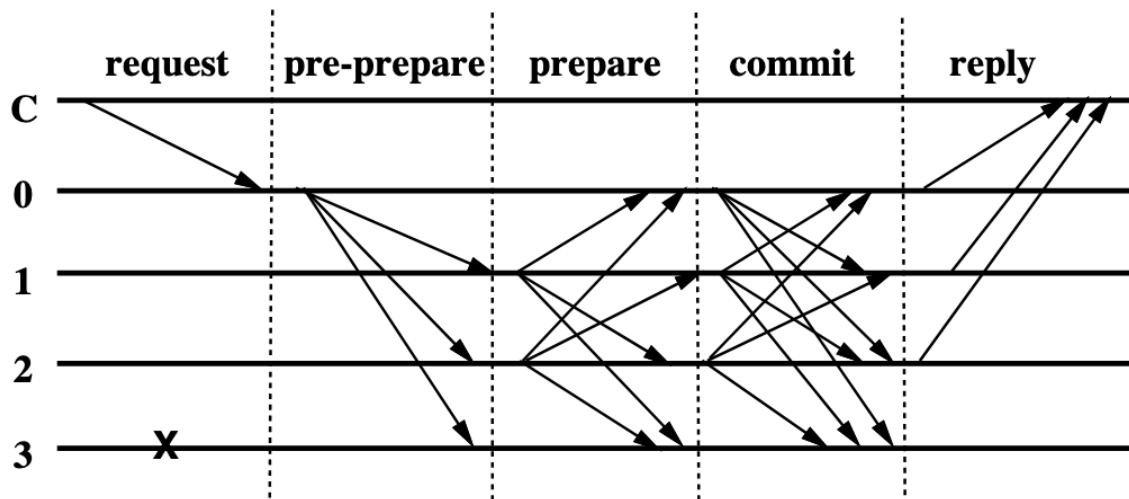


Figura 11 : Diagrama de cómo funciona BPFT - Fuente: edx.org

2.3.2.3.4. Consenso de Nakamoto

En 2008, Satoshi Nakamoto (supuesto nombre del préstamo) presentó en un artículo llamado *"Bitcoin whitepaper A peer-to-peer electronic cash system"* [25]. Este documento ha revolucionado ambas transacciones financieras, pero también ha introducido una nueva clase de consenso: los mecanismos de consenso de Nakamoto. Estos son diferentes del consenso basado en los votos sobre cómo se realizan las actualizaciones de datos distribuidos. El consenso basado en la votación requiere votos explícitos de cada uno de los nodos en la red, mientras que los mecanismos de consenso de Nakamoto hacen que los usuarios voten implícitamente. Estos votos implícitos se basan en un sistema de lotería aleatorio, donde los usuarios compiten entre sí para actualizar el sistema. Es el ganador de esta lotería quien obtiene el derecho de actualizar el sistema.

El consenso de Nakamoto tiene varias propiedades especiales, que los distinguen del consenso tradicional, el consenso basado en el voto. Primero, esta familia de consenso puede permitir que usuarios conocidos o poco confiables actualicen el sistema. En Bitcoin, un dinero electrónico y su implementación, cualquiera puede unirse a la red y cualquiera puede enviar mensajes erróneos o corruptos a otros nodos de la red. Además, cualquier usuario puede utilizar tantas identidades virtuales (una clave pública y una clave privada) como desee. Para evitar la corrupción de la red (por ejemplo, por un usuario con múltiples identidades), el privilegio de votación debe ser poco frecuente y, por lo tanto, debe estar vinculado a un recurso escaso.

2.3.2.4. El derecho a voto

En las blockchains, el derecho de voto permite determinar quién tiene el derecho de agregar un bloque o no a la cadena, y si la adición de este bloque es coherente. Existen diferentes mecanismos para determinar quién tiene este derecho a votar.

2.3.2.4.1. Prueba de trabajo (*Proof-of-Work*)

Para bitcoin, la solución fue vincular el derecho de voto a la potencia informática de los participantes (es el sistema de validación por prueba de trabajo o *proof-of-work*). Esta es una de las posibles soluciones para alcanzar un consenso de Nakamoto. La prueba de trabajo apareció en el mismo artículo que en bitcoin, en 2008 [25]. Debido a esta forma implícita de votar, los líderes son elegidos a través de una lotería aleatoria, donde las posibilidades de ganar esta lotería están relacionadas con el poder de cómputo de los participantes. El ganador de la lotería tiene derecho a realizar la próxima actualización de los datos.

Pero es posible que el líder electo quiera corromper los datos. En este caso, los otros participantes en la red votan eligiendo si actualizan o no sus versiones locales de la red. Para el bitcoin, cada nodo puede elegir los bloques que agrega en su cadena de bloques, y esta adición es válida solo si el resto de la red está de acuerdo con la presencia de este bloque en la cadena de bloques. Por lo tanto, el Consenso de Nakamoto debe definir un conjunto de reglas para elegir y decidir sobre el estado de la red. Una de estas reglas puede ser mantener la cadena de red más larga (en el caso de Bitcoin). El consenso de Nakamoto es, por lo tanto, un consenso basado en una cadena.

En el caso de Bitcoin, el primer menor (un menor, en este caso, y un participante de la red) que resuelve un bloqueo lo envía a toda la red. La red luego vota implícitamente en este bloque, con cada nodo de la red que agrega o no la copia del bloque a encadenar. En las validaciones por prueba de trabajo, el recurso utilizado es la potencia informática de cada uno de los nodos del sistema. Cuanto antes calcule un minero, más probabilidades tendrá de resolver el siguiente bloque y enviarlo al resto de la red, y así actualizarlo (y en el proceso ganar una recompensa por su trabajo).

2.3.2.4.2. Prueba de estacas (*Proof-of-Stake*)

Otro ejemplo del consenso de Nakamoto es la prueba de participación (*proof-of-stake*), presentada por Sunny King (nombre falso) en 2012 [19]. Al igual que los menores en el caso de trabajo, los validadores en la prueba de participación deben actualizar y ayudar a la red. En lugar de utilizar la potencia informática para determinar quién puede actualizar la red, este algoritmo utiliza un sistema de tokens. Cuanto más un validador tenga tokens de la red en cuestión (por ejemplo, ether para Ethereum, otra criptomoneda introducida por Vitalik Buterin), es más probable que sea elegido para proponer una nueva actualización de la red.

2.3.2.4.3. Prueba de Actividad (*Proof-of-Activity*)

Otro consenso de Nakamoto es la prueba de actividad (*proof-of-activity*). Este consenso es un híbrido entre la evidencia de participación y la prueba de trabajo. Al principio, en el modelo de prueba de trabajo, los menores resuelven y envían bloques a la red. En un segundo paso, y esta vez en el modelo de la prueba de participación, el bloque tiene en sus metadatos una lista de validadores que pueden confirmarlo. Esta lista de validadores se genera aleatoriamente, pero cuanto más un validador tenga tokens de dinero, más probable es que esté en estos metadatos (y, por lo tanto, validar o no el bloque). Una vez que el bloque ha sido validado por los validadores, los otros miembros de la red pueden agregarlo a sus copias locales.

2.3.2.4.4. Prueba de ardor (Proof-of-Burn)

El consenso por prueba de ardor (*proof-of-burn*) es una alternativa a la evidencia de estaca. En este consenso, cuantos más chips acepte enviar un validador a una dirección de grabación (esta dirección no es accesible y, como resultado, se perderán los tokens enviados a esta dirección), es más probable que sea elegido para proponer el próximo bloque.

2.3.2.4.5. Prueba de espacio (Proof-of-Space)

Este otro tipo de consenso de Nakamoto, la prueba de espacio (*proof-of-space*), utiliza el espacio de almacenamiento como recurso para obtener el derecho al voto. Este tipo de consenso se considera más ecológico y menos costoso porque el espacio de almacenamiento es menos costoso que la capacidad informática de una computadora y consume menos energía. Este tipo de consenso se usa más para el almacenamiento de datos que como un método de votación en sí mismo (por ejemplo, con el filecoin).

2.3.2.4.6. Prueba de capacidad (Proof-of-Capacity)

Una alternativa a la prueba de espacio, la prueba de capacidad (*proof-of-capacity*) se basa en la prueba del uso de una cierta cantidad de almacenamiento para la resolución de este, lo que permite proponer el siguiente bloque o la próxima actualización del sistema.

2.3.2.4.7. Prueba de tiempo transcurrido (Proof-of-Elapsed-Time)

Otro tipo de consenso, la prueba del tiempo transcurrido (*proof-of-elapsed-time*) es un algoritmo que se basa en el tiempo de cálculo de cada nodo. Cada nodo selecciona un tiempo de espera aleatorio y espera esa duración. El nodo con el tiempo de espera más largo es el siguiente en enviar un bloque. Para evitar que este tipo de algoritmo sea manipulado por los otros participantes de la red, es necesario contar con la presencia de entornos de ejecución aprobados (*trusted execution environment*, por ejemplo, aquellos que permiten desbloquear los teléfonos con la ayuda de una impresión específica). Estos entornos, que son literalmente parte de algunos procesadores, solo responden a ciertas condiciones de ejecución asegurando que el tiempo transcurrido sea el tiempo que tuvo que esperar, y así evitar la corrupción del sistema.

2.3.2.4.8. Prueba de autoridad (Proof-of-Authority)

La prueba de autoridad (*proof-of-authority*) no es un tipo de consenso del propio Nakamoto, sino una alternativa a ellos. Este tipo de evidencia se basa en un conjunto de nodos de confianza que tienen derecho a actualizar la red. El recurso para utilizar en este tipo de prueba es la identidad: un nodo tiene derecho a actualizar la red de acuerdo con su identidad.

Capítulo 3: Propuesta de solución

El objetivo de esta tesis es fortalecer la seguridad de la trazabilidad de los medicamentos de acuerdo con los estándares actuales establecidos por el GS1. Para lograr este objetivo, el uso de los estándares actuales es una prioridad, para evitar un cambio profundo en la organización de la cadena de suministro de la industria farmacéutica. Para la mayoría de las grandes empresas del sector, establecer su cadena de suministro y hacerlo funcionar fueron pasos clave para reducir los costos de los medicamentos (y/o aumentar las ganancias).

3.1. Adaptación de trazabilidad

Por lo tanto, la solución presentada en este memo debe ser retro compatible con los estándares actuales encontrados para la trazabilidad de medicamentos. Por lo tanto, es necesario adaptar el antiguo modelo de trazabilidad al nuevo.

3.1.1. Datamatrix contra etiquetas RFID

El modelo actual de configuración de trazabilidad es utilizar datamatrix para garantizar la trazabilidad. Una alternativa a la matriz de datos presentada anteriormente es el uso de etiquetas RFID. La clara ventaja de las etiquetas RFID es que se puede escanear un conjunto de medicamentos al mismo tiempo (con lectores que leen lotes), lo que facilita el seguimiento y reduce los costos de manipulación. Sin embargo, el precio de las etiquetas RFID es prohibitivo: en algunos casos es para medicamentos comunes (por ejemplo, paracetamol) casi el 10% del precio de venta. Sin embargo, estos medicamentos tienen el mayor volumen de ventas, y aumentar su precio en un 10% solo empujará a los consumidores a los medicamentos o canales de distribución "alternativos" (potencialmente peligrosos). Dado que el objetivo principal de la disertación es evitar que los consumidores tengan que pasar por canales de distribución no oficiales para comprar medicamentos a precios competitivos pero falsificados, la solución del uso de etiquetas RFID, a pesar de su potencial, es No es adecuado para la trazabilidad en la actualidad.

Por el contrario, el precio de datamatrix es bajo (en milésimas de dólar). Teniendo en cuenta que el modelo actual de trazabilidad se basa en la matriz de datos, el costo es casi cero: es suficiente adaptar la matriz de datos a una trazabilidad más eficiente. Por otro lado, la obligación de escanear cada caja de medicamento para conocer su contenido gracias a datamatrix representa un costo significativo. Pero debemos poner datamatrix en su contexto actual: hoy dos medicamentos (de la misma marca, que tienen la misma molécula activa y comparten el mismo lote) tienen la misma matriz de datos. Esta matriz de datos permite a los productores del medicamento, en el caso de que uno de los medicamentos por lotes presente problemas, identifique y recupere rápidamente el lote en cuestión, pero desde el punto de vista del consumidor, el número de lote solo da poca información.

Hacer que este número de lote sea más informativo para el consumidor le permitiría saber más información sobre los medicamentos que consume: ¿de dónde viene, quién lo produjo, de dónde fue, a qué es el medicamento oficial... Estas cuestiones, centrales para el consumidor, se descuidan hoy en el principio de que todos compran sus medicamentos en farmacia, lo cual no es necesariamente cierto. La explosión de las compras en línea indica que los consumidores tienden a preferir comprar en línea. Asegurar este sector, mientras se minimizan los costos de esta seguridad, es por lo tanto una clave para el sector farmacéutico. Datamatrix cumple completamente esta función de seguridad, respetando las limitaciones económicas del sector farmacéutico, en comparación con las alternativas (incluidas las etiquetas RFID).

3.1.2. El uso de datamatrix

Como se vio anteriormente, la trazabilidad usando datamatrix se realiza a través de una serie de figuras. Estos números permiten rastrear varias informaciones sobre el medicamento. Esta información es la siguiente:

- Un número GTIN (*Global Trade Item Number*) impuesto por el GS1). Estos 14 caracteres permiten identificar el medicamento y su marca (como recordatorio, dos medicamentos genéricos vendidos por el mismo laboratorio, potencialmente bajo diferentes marcas, tendrán el mismo número GTIN).
- La fecha de vencimiento del medicamento, con el formato DDMMYY (DD corresponde al día, MM al mes y AA al año).
- El número de lote del medicamento.
- Y números gratuitos que permiten a la agencia nacional o al productor del medicamento agregar información sobre el medicamento en cuestión.

Como se indicó anteriormente, esta información es más útil para el productor del medicamento que para el consumidor de este. Sin embargo, nada impide el uso de la información de este medicamento para permitir que el consumidor final tenga información al respecto. Los números libres presentes en la matriz de datos se pueden usar para agregar información. Otra solución sería cambiar el número de lote cada vez que se corta este lote. Esta segunda solución ofrece varias ventajas, con la principal ventaja de utilizar un sistema que ya existe.

La actualización del número de lote cada vez que se transfiere un medicamento, al tiempo que se mantiene el historial del número de lote de este medicamento, permite muy poca modificación del sistema actual y limita las inversiones de las compañías farmacéuticas. De hecho, las tecnologías actuales para imprimir en cajas de medicamentos y crear una matriz de datos relacionada con los medicamentos ya están en marcha en las fábricas de los productores. Por lo tanto, el costo de actualizar el sistema de trazabilidad sería mínimo para los productores actuales.

Pero actualizar un sistema siempre tiene costos adicionales para algunos actores en la cadena de suministro. Estos actores deben equiparse con máquinas para imprimir datamatrix. Como parte de la solución propuesta, la impresión de una nueva matriz de datos solo se realizaría en el caso de que se dividan muchos medicamentos. Por ejemplo, si un mayorista que busca revender medicamentos después de comprarlos quiere dividir mucho en dos, debe generar dos nuevas matrices de datos (una para el primer lote, la segunda para el segundo lote) para vincularlas. Dos lotes nuevos en el lote inicial. Este enlace será a través de una nueva trazabilidad basada en software, explicada más adelante en esta memoria.

La idea principal aquí es que los estándares actuales siguen vigentes. Mantener los estándares actuales permite a los productores de medicamentos la libertad de actualizar sus sistemas de trazabilidad o no, y mantener la compatibilidad con versiones anteriores entre sistemas. Esta libertad es esencial porque permite a los productores seguir respetando la legislación vigente mientras adapta su sistema a estándares más modernos. El número de lote actual de medicamentos está destinado a ayudar a los productores a identificar medicamentos defectuosos. Gracias a la generación de nuevos números de lote en cada división de un lote, números de lote vinculados al lote inicial, los productores aún podrán identificar lotes defectuosos. Para el consumidor, estos nuevos números de lote tienen la ventaja de conocer el circuito seguido por el medicamento y, por lo tanto, asegura la trazabilidad de este.

Para comprender mejor esta solución, nada mejor que un ejemplo. El circuito completo de un medicamento consiste en una serie de transferencias entre diferentes propietarios. Estos propietarios, ya sea el propietario original (por lo tanto, el productor), un propietario intermedio o el propietario final, deben declarar la propiedad del medicamento en un momento dado. Para pasar la propiedad de este medicamento a otro propietario, necesita dos cosas:

- La primera es que el propietario envía el medicamento al siguiente propietario.
- El segundo en que el nuevo propietario acepta recibir el medicamento.

La mayoría de las veces, los medicamentos no se envían individualmente, sino que se envían por lotes. Estos lotes, de tamaño variable, circulan entre los propietarios. El único momento en que un medicamento se individualiza de un lote es cuando el consumidor final lo compra. La trazabilidad de un medicamento se detiene en ese momento, porque el siguiente paso es el consumo de este medicamento.

En el caso de que el futuro propietario rechace el lote de medicamentos, lo devuelve al propietario anterior. En caso de que acepte el lote, se convierte en el propietario del lote de medicamentos. En este punto, puede enviar el lote nuevamente, ya sea completo o particionado. Si envía el lote completo, simplemente cambie el propietario del lote, sin actualizar el número de este. Por el contrario, si decide dividir su lote, se encuentra con dos lotes (o más si se producen otras particiones). Ninguno de estos lotes nuevos tiene la misma cantidad de medicamento que el lote original. Por lo tanto, se deben generar nuevos números de lote para cada lote creado a partir de este lote inicial. En este momento, el propietario debe actualizar el paquete del medicamento para que la matriz de datos del paquete sea correcta.

A continuación, se muestra un diagrama para visualizar el funcionamiento de este sistema:

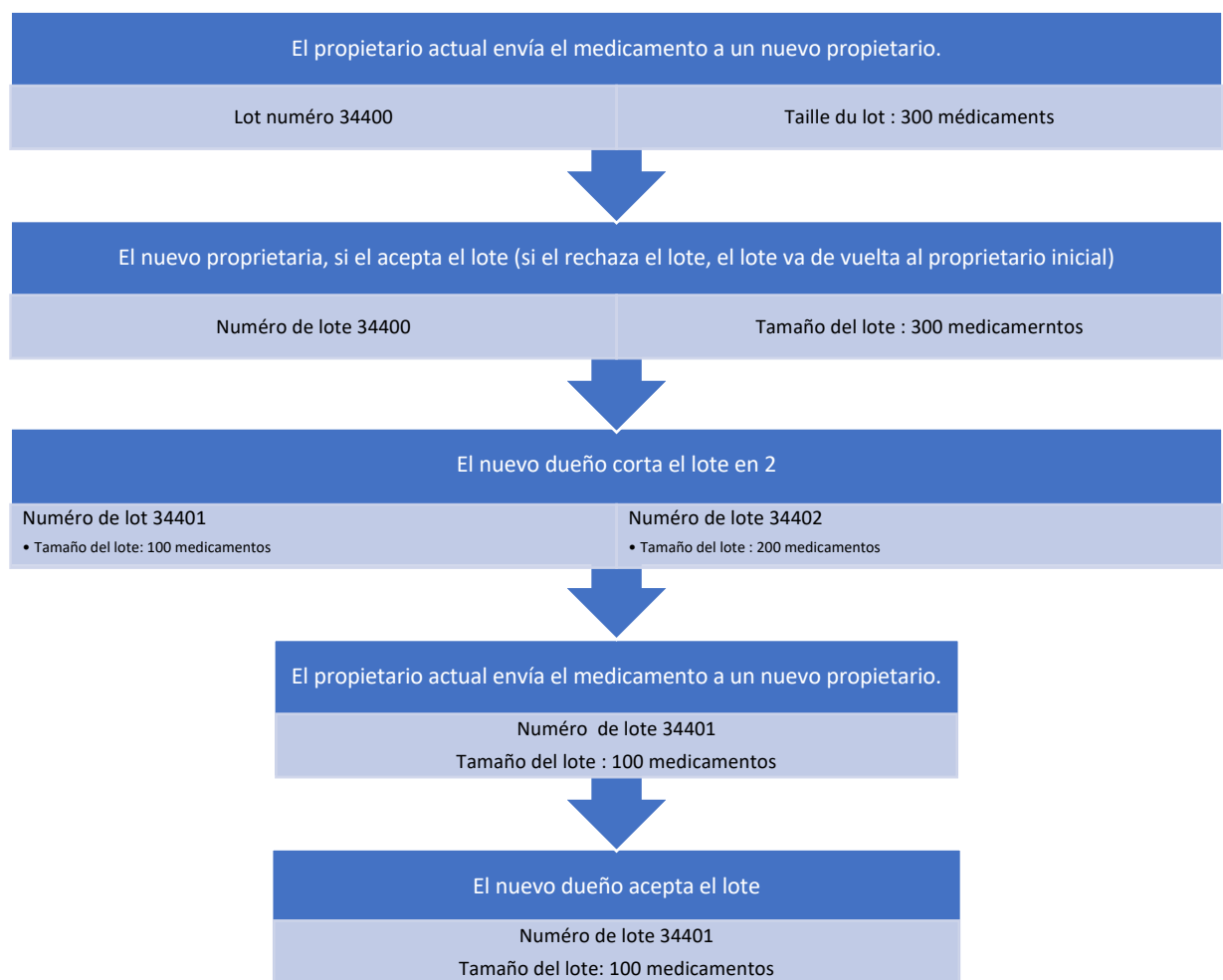


Figura 12 : Flujo de número de lote

Volviendo a través de este sistema los diferentes propietarios de un lote, podemos reconstruir el origen del lote y su número original, así como la lista completa de propietarios. El primer propietario del lote en este sistema es el productor del lote, que es una compañía farmacéutica. Gracias a esta nueva trazabilidad, las modificaciones realizadas en el sistema existente son mínimas: la única novedad es la actualización periódica de la matriz de datos de cada paquete de medicamentos para cada lote.

Esto puede parecer una tarea desalentadora, pero la automatización de las cadenas de recepción y envío es una solución directa para actualizar la matriz de datos de cada medicamento. En un mundo que tiende cada vez más a la automatización, este sistema también brinda una velocidad de ejecución. Por otro lado, en la automatización, existe una barrera económica comparable al uso de etiquetas RFID. Sin embargo, a diferencia de las RFID, la implementación de la automatización se realiza una vez, mientras que un paso a través de RFID requeriría que toda la cadena a la vez pase por la automatización de las lecturas para cada enlace en la cadena, y además de instalar etiquetas RFID en cada caja de medicamentos. Pero la clara ventaja de las etiquetas RFID y la velocidad de las actualizaciones del número de lote (simplemente pase un sub-lote frente a un lector y vuelva a escribir el número de lote para cada etiqueta). A largo plazo, el uso de etiquetas RFID parece, en el caso en que el precio de las etiquetas disminuye, una solución ideal. Una solución que utiliza etiquetas RFID sería compatible con la solución presentada aquí, por lo que podría ser un paso futuro para mejorar la trazabilidad de los medicamentos.

3.2. La retención de datos

Al establecer una trazabilidad con la matriz de datos, es necesario almacenar los datos de los medicamentos para que cualquier participante pueda interactuar con los datos de estos. Esta interacción ocurre en dos partes. Estas dos partes se cruzan entre sí, pero son disociables en varios puntos. La diferencia más importante entre estas partes es cómo se almacenan los datos: como una base de datos SQL o como una cadena de bloques. Como se explicó anteriormente, una cadena de bloques permite almacenar datos de forma permanente e intangible. Cada pieza de datos almacenados en una cadena de bloques ya no se puede eliminar: y este es el corazón de la cadena de bloques, que es crear un registro de datos inmutables. Otra peculiaridad de una cadena de bloques es que se distribuye: hay varias máquinas con control de esta, y estas máquinas trabajan juntas para producir un resultado. Estos dos formatos de almacenamiento de datos están presentes dentro de la solución presentada porque se complementan entre sí: donde la cadena de bloques permite la trazabilidad, la base de datos de soporte enriquecerá los datos de la cadena de bloques.

3.2.1. Datos de la transacción

Una cadena de bloques se usa para almacenar datos. Estos datos son permanentes. Esta permanencia es una herramienta concreta para garantizar la inviolabilidad de una cadena de bloques y los datos que están escritos en ella. Una vez que un dato se escribe en una cadena de bloques, y es validado por los participantes de esta cadena de bloques, es permanente. Por lo tanto, las cadenas de suministro tienen una herramienta para registrar todos los intercambios y transacciones. Los datos son formas escritas de transacciones, y las transacciones se almacenan en bloques. Por lo tanto, es necesario determinar qué datos están contenidos en los bloques y qué datos están contenidos en las transacciones.

El objetivo de la cadena de bloques de la cadena de suministro es seguir las transacciones entre dos actores, es posible deducir dos de los datos contenidos en las transacciones: dos identificadores para identificar al remitente del medicamento y al receptor de este. Estos identificadores, presentes en forma de un identificador numérico único, están vinculados a la base de datos. En la base de datos, estos identificadores corresponden a los datos de los actores.

Estas credenciales permiten dos cosas:

- El primero, identificar a un actor cuando quiere hacer una transacción en la cadena de bloques. De hecho, no todos los actores tienen los mismos derechos.
- En segundo lugar, estos datos enriquecen la información relativa a los actores: su dirección, su correo electrónico ... El enriquecimiento de estos datos hace posible evitar tener transacciones que contengan docenas y docenas de datos. El tamaño de los datos en la cadena de bloques de trazabilidad debe mantenerse al mínimo, mientras se conserva la mayor cantidad de información posible, a fin de garantizar una velocidad de ejecución de la cadena de bloques.

3.2.1.1. Los actores no identificados

Los actores no identificados, que no tienen un número de identificación, solo pueden consultar la cadena de bloques. No pueden interactuar con él mediante la adición de una transacción, o conectarse con identificadores. Transpuestos a un caso de uso, estos actores no identificados corresponden a los consumidores finales de los medicamentos. Una vez que se ha comprado un medicamento, y si el nuevo propietario quiere información sobre su medicamento, puede escanear la matriz de datos en el paquete del medicamento y usar una plataforma basada en blockchain para obtener información sobre el medicamento. droga que acaba de comprar (que han sido los propietarios sucesivos, su lugar de fabricación ...).

3.2.1.2. Los actores identificados

Un segundo tipo de actor debe interactuar con la cadena de bloques. Estos actores tienen todos los derechos de los actores no identificados, más otros derechos. Pueden recibir transacciones y aceptarlas. Para esto, estos actores deben registrarse en la plataforma para obtener un número de identificación. Estos actores corresponden a todos los actores de la cadena de suministro de la industria farmacéutica: transportistas, mayoristas, farmacias, oficinas nacionales ... Este número de identificación les permitirá interactuar con la cadena de bloques al vincular las transacciones con las suyas. número de identificación. El vínculo entre la transacción y el actor se realiza si el actor es receptor o remitente de un medicamento. Estos actores son gestionados por las autoridades locales responsables de autorizar la comercialización de medicamentos.

Esto permite identificar otro dato contenido en las transacciones. Cuando un actor recibe un lote de medicamentos, puede aceptarlo, pero también puede rechazarlo (por ejemplo, si el lote no está completo, si el receptor encuentra problemas en el lote ...). Por lo tanto, es necesario definir un estado para todas las transacciones. Este estado puede tomar 3 valores:

- *accepted*: si el receptor acepta el lote que se le envió. En este caso, el receptor del lote se convierte en el propietario.
- *refused*: si el receptor rechaza el lote enviado a él. En este caso, el propietario del lote es el remitente. El lote regresa a su dueño original.
- *waiting*: si el envío ha sido enviado por el remitente, pero el receptor aún no ha tomado la decisión de aceptarlo o rechazarlo. El receptor debe tomar la decisión de cambiar el estado del lote a «*accepted*» o «*refused*».

Un lote también se puede dividir en 2 lotes más pequeños: por ejemplo, si un mayorista tiene 100 unidades de un medicamento X y tiene un pedido de 20 unidades de ese medicamento, dividirá el lote en un lote de 20 y otro de 80. Además de generar dos lotes con su número de identificación respectivo, también es necesario indicar en la cadena de bloques la actualización del lote original dividido. Por lo tanto, necesita un valor para el estado además de:

- *split*: el propietario de un lote ha tomado la decisión de compartir este lote en dos. El lote original se elimina y se reemplaza por dos lotes nuevos. Sin embargo, el estado dividido no está registrado en la cadena de bloques. Cuando un lote se divide en dos, se crean dos lotes

nuevos. Entonces, hay dos nuevas transacciones para agregar en la cadena de bloques, y estas dos transacciones son transacciones creativas.

La capacidad de dividir un lote en lotes más pequeños introduce nuevos datos para las transacciones: cada transacción tendrá información sobre el tamaño del lote. Este tamaño permitirá dividir un lote en dos lotes más pequeños.

El uso de informes le permite tener acceso rápido al tipo de operación que cada lote puede realizar: ser transferido, aceptado, rechazado o dividido. Estas son las cuatro operaciones que muchos pueden sufrir.

3.2.1.3. Los fabricantes de medicamentos

En el proceso de seguimiento de un lote, también debe crear el lote en un momento dado. Crear un lote es una acción especial porque implica un parámetro importante: el creador del lote solo puede ser un fabricante de medicamentos. Para que un nuevo lote ingrese al mercado, los productores de medicamentos deben vender el lote en cuestión. Todo lo que sucede antes para el lote no existe, desde el punto de vista de la cadena de bloques, antes de que se grabe el lote. El registro de un lote es el momento en que se agrega a las existencias del productor del medicamento, lo que resulta en el registro del lote en la cadena de bloques. Esta grabación agrega un nuevo tipo de actor, el fabricante de medicamentos. Estos actores tienen todos los derechos de los actores no identificados y los actores identificados, además del derecho de agregar lotes a la cadena de bloques.

Al agregar un lote a la cadena de bloques, este lote tiene una marca de tiempo. La marca de tiempo es otro dato incluido en una transacción. Certifica cuándo agregar un bloque a la cadena de bloques. Es una herramienta para clasificar las transacciones presentes en la cadena de bloques. Todas las transacciones se agregan a los bloques.

3.2.2. Los datos de los bloques

Como se indicó en la primera parte, en cualquier blockchain, las transacciones se agrupan dentro del bloque. Los bloques contienen datos que enriquecen la información que contienen. Estos datos se utilizan para las diversas operaciones que deben sufrir los bloques, operaciones que se detallarán en la siguiente parte. Las transacciones se organizan en una lista, con todos los datos detallados anteriormente para cada transacción (número de lote, cantidad, ID del receptor, ID del remitente, estado de la transacción y la marca de tiempo de esta).

Además de los datos de transacción, un bloque tiene sus propios datos. Los primeros datos, que certifican el momento en que el bloque fue validado y agregado a la cadena de bloques, es la marca de tiempo de este. En cuanto a las transacciones, la marca de tiempo de los bloques proporcionará información sobre cuándo se agregó el bloque a la cadena de bloques (y, por lo tanto, el momento en que se validó). Sin embargo, la marca de tiempo no es útil para clasificar las transacciones.

Para la clasificación de transacciones entre sí, cada bloque tiene un índice. Este índice está aumentando estrictamente (desde el índice cero del bloque "génesis").

Además del índice y la marca de tiempo, cada bloque tiene datos criptográficos útiles para soportar la cadena de bloques. Estos datos criptográficos son un hash, un nuncio y el hash del bloque anterior. El hash del bloque certifica este y se calcula utilizando el hash del bloque anterior.

La presencia del hash del bloque anterior no es importante para calcular el hash del bloque actual. Su utilidad viene al agregar un bloque en la cadena de bloques: si el hash del bloque anterior en la cadena de bloques no corresponde al hash del bloque anterior presente en el bloque que debe agregarse, permite comprender que el bloque que se agrega no está en el lugar correcto, tampoco está corrupto. El hash actual se usa para identificar un bloque en relación con otros bloques en la cadena de bloques.

Finalmente, cada bloque contiene un nuncio, para permitir que toda la red verifique que se haya calculado el bloque agregado, y que tomó un trabajo por parte del bloque menor para agregarlo a la cadena de bloques. Con el hash del bloque y el hash del bloque anterior, estas son tres herramientas para verificar la validez de un bloque y la validez general de la cadena de bloques.

3.2.3. Los datos de los medicamentos

Además de contener los identificadores de los actores del sistema de trazabilidad, las transacciones deben contener información sobre los lotes de medicamentos transferidos entre los actores. La identificación de lotes de medicamentos ya sea en la cadena de bloques o en la base de datos SQL, se realiza mediante identificadores numéricos únicos. Estos identificadores permiten vincular los lotes de medicamentos con datos adicionales: el nombre de los medicamentos, el identificador del fabricante o incluso la fecha de vencimiento de estos. Para habilitar esto, cada lote y la información relacionada con él se escriben en la base de datos y blockchain. La diferencia entre los dos es la ubicación de los datos en el sistema de información.

Para identificar lotes, ya sea en la cadena de bloques o en la base de datos, cada lote tiene un identificador único. En la cadena de bloques, este identificador del lote permite seguir las transacciones que este experimenta. En la base de datos, el identificador de lote permitirá vincular un lote a todos los datos vinculados a él. También en la base de datos se encuentra información sobre un lote:

- Un identificador único, para vincular un lote de la base de datos a la cadena de bloques.
- Una fecha de vencimiento, que indica hasta cuándo una gran cantidad de medicamentos es consumible.
- Una cantidad que corresponde al tamaño del lote.
- El identificador de la droga en el lote. Este identificador es una clave externa que permite vincular la información de los lotes y la información de los medicamentos.
- Si un lote se divide de otro lote, el identificador de la base de datos para el lote "padre" se encuentra en los datos del lote "hijo". Este identificador permite hacer un enlace entre todos los hijos de un padre.

Gracias al identificador del medicamento que comprende un lote, es posible recuperar la información de un medicamento. Esta información es la siguiente:

- Un identificador único para identificar el medicamento en comparación con otros (por ejemplo, si dos medicamentos tienen el mismo nombre).
- El nombre del medicamento, que permite al consumidor establecer una conexión entre la caja del medicamento que acaba de comprar y su receta.
- El número GTIN (*Global Trade Item Number*), que luego identifica el medicamento y su marca.
- El identificador del fabricante del medicamento. Este identificador, que funciona como una clave externa, proporciona acceso a información adicional sobre el medicamento. Esta información es del fabricante del medicamento.

Los fabricantes de medicamentos son actores. Como se mencionó anteriormente, hay tres tipos de actores que interactuarán con la cadena de bloques:

- Los actores no identificados.
- Los actores identificados.
- Los fabricantes de medicamentos.

La interacción entre los actores y la cadena de bloques se realiza a través de una plataforma web. Los actores no identificados no necesitan mantener información en la base de datos. Para los actores identificados y los fabricantes de medicamentos, la base de datos solo hace una ligera distinción entre

los dos, una distinción contenida en la base de datos. Los datos de los actores y fabricantes de medicamentos identificados son los mismos y son:

- Un identificador único para distinguir dos actores entre ellos.
- Un nombre, que puede ser el nombre comercial de un actor o su nombre en la cámara de comercio local. La importancia aquí no es el nombre en sí, y dos actores pueden tener el mismo nombre (por ejemplo, si todos los centros Novartis desean ser llamados "Novartis", eso es muy posible).
- Un correo electrónico, identificador único, que permite a un actor conectarse y comunicarse con los clientes si tienen preguntas sobre un medicamento.
- Una contraseña, codificada para mayor seguridad, que permite que un actor se identifique en la plataforma.
- Un número de teléfono, para que un consumidor pueda contactar a un actor.
- Un binario, para distinguir a los fabricantes de medicamentos de los actores normales. Este binario, verdadero si el actor es fabricante, incorrecto si el actor no lo es. Solo el binario "verdadero" permite obtener para un actor el derecho de agregar medicamentos a la plataforma.

Finalmente, las direcciones de los actores se almacenan en la base de datos. Estas direcciones contienen los siguientes datos:

- Un identificador único para cada dirección, que actúa como la clave principal.
- La calle, que contiene el número y el nombre de la calle.
- La ciudad.
- El estado o región.
- Código postal vinculado a la dirección.
- El país.
- Una clave externa para vincular una dirección a un actor.

Todos estos datos están en la base de datos de la plataforma. Estos son datos adicionales que permiten obtener información sobre las transacciones y los actores de estas transacciones, lo que le permite interactuar con la cadena de bloques.

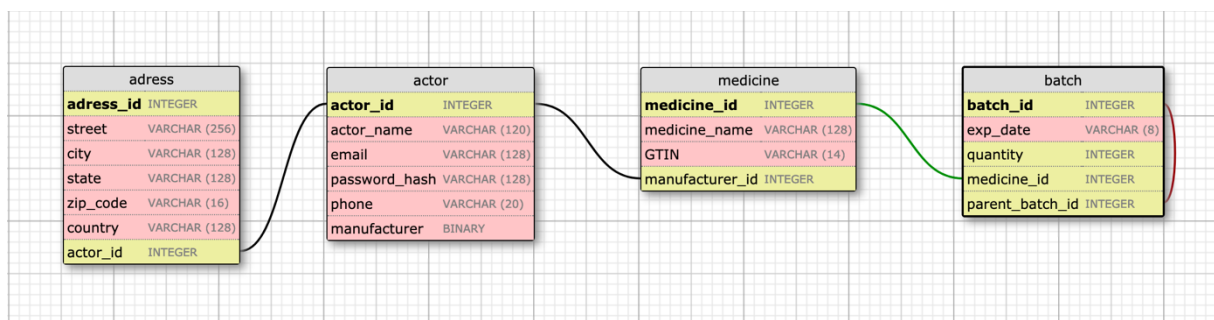


Figura 13: Diagrama de la base de datos

Estos datos, que sirven como datos de soporte, no son fundamentales para el funcionamiento de la cadena de bloques. Pero son útiles para automatizar esta (por ejemplo, agregar una transacción en la cadena de bloques es más fácil de realizar con botones de activación de acción que ingresando manualmente cada transacción).

3.3. La blockchain y su funcionamiento

Todos los bloques y transacciones están vinculados entre sí en una cadena de bloques. Esta cadena de bloques tiene datos y un conjunto de interfaces que permiten interacciones con ella. Los datos contenidos en la cadena de bloques son el conjunto de transacciones contenidas en los bloques extraídos por los participantes. Uno de los datos de los nodos de la cadena de bloques es la dirección de cada nodo, lo que permite la descentralización de este. En la industria farmacéutica, estos nodos corresponden a las agencias nacionales que autorizan la comercialización de medicamentos. Por lo tanto, para la solución propuesta, el papel y la gestión de los nodos de blockchain serían responsabilidad de los organismos que autorizan la comercialización de medicamentos. Por lo tanto, esta cadena de bloques sería semipública: cualquier actor (de los tres tipos de actores previamente identificados) puede leerla, pero su escritura es un derecho reservado para los nodos y, por lo tanto, para las agencias nacionales.

Cada organismo nacional administraría un nodo que acceda a la cadena de bloques. Toda empresa farmacéutica que desee vender en el territorio de la organización debe registrarse en la base de datos. Como la base de datos es global entre los actores, todos los actores tienen acceso a todos los datos relacionados con los actores, los medicamentos y los lotes (así como las direcciones secundarias). Hacer que la base de datos sea completa evita las colisiones entre dos actores, dos lotes o dos medicamentos con los mismos números de identificación. Además, esto permite que muchos medicamentos crucen fronteras: los números de identificación son únicos, muchos pueden pasar fácilmente de un cliente a otro sin deber tener en cuenta los límites geográficos o de mercado. Dejar a los nodos responsables ante las agencias nacionales les permite filtrar a los actores (por ejemplo, una empresa pierde su autorización para comercializar un medicamento).

La implementación de esta arquitectura crea varias consecuencias para la implementación. La primera es que cada actor solo puede registrarse en una agencia nacional. Esta grabación hará que todas las solicitudes que un actor tenga para la cadena de bloques pasarán por la agencia nacional con la que este actor se ha registrado. Una segunda consecuencia se refiere a la base de datos: debe ser accesible para todos los actores, sin ningún vínculo con los nodos gestionados por las agencias nacionales. Finalmente, las agencias nacionales deben registrarse entre ellas para sincronizar la cadena de bloques es establecer un consenso, para evitar tener dos cadenas de bloques completamente diferentes entre dos nodos.

Por consenso, varios algoritmos son posibles. Los principales algoritmos de consenso se han mencionado anteriormente, y algunos se pueden eliminar. Se puede eliminar cierto consenso porque no cumplen con las especificaciones: por ejemplo, el consenso por prueba de participación presenta como defecto que no hay token para transmitir entre los nodos en esta cadena de bloques, y el uso de los tokens permitirían a los principales productores de medicamentos controlarlo. En una industria en la que los jugadores más grandes son acusados regularmente de comprensión, la cadena de bloques estaría bajo el riesgo de un ataque.

Anteriormente, la identificación de los nodos de blockchain como los organismos nacionales responsables de las autorizaciones de comercialización de medicamentos ha permitido destacar que un pequeño grupo tiene el monopolio de actualizar blockchain y el acceso a este. Esta operación de acceso a blockchain por un grupo restringido hace posible deducir que el tipo de consenso asociado con esta blockchain es un consenso por prueba de autoridad. La prueba de autoridad valida la idea de que solo las organizaciones que permiten la comercialización de medicamentos deben interactuar con la cadena de bloques. Es por prueba de autoridad que los nodos de la cadena de bloques le agregarán transacciones.

En caso de conflicto entre dos organizaciones, una solución simple sería tomar la cadena de bloques más larga desde la génesis de bloque entre los dos nodos en conflicto y enviar este cambio a todos los actores. El nodo con la cadena de bloques más corta ve su cadena de bloques reemplazada por la más larga. Esta solución simple crea un nivel inicial de requisitos. Cualquier sistema de resolución de conflictos que sea menos eficiente que esta solución debe ser eliminado. Todos los nodos tienen los

mismos derechos en la cadena de bloques, ninguno puede afirmar que es más importante que los demás y, por lo tanto, en caso de conflicto, imponga su cadena de bloques a los demás.

Resumir en un diagrama ayuda a comprender mejor la arquitectura de la solución. Para crear este esquema simplificado, se utilizan dos agencias nacionales y cuatro actores (dos para cada agencia), y la arquitectura de la solución se vería en la siguiente figura:

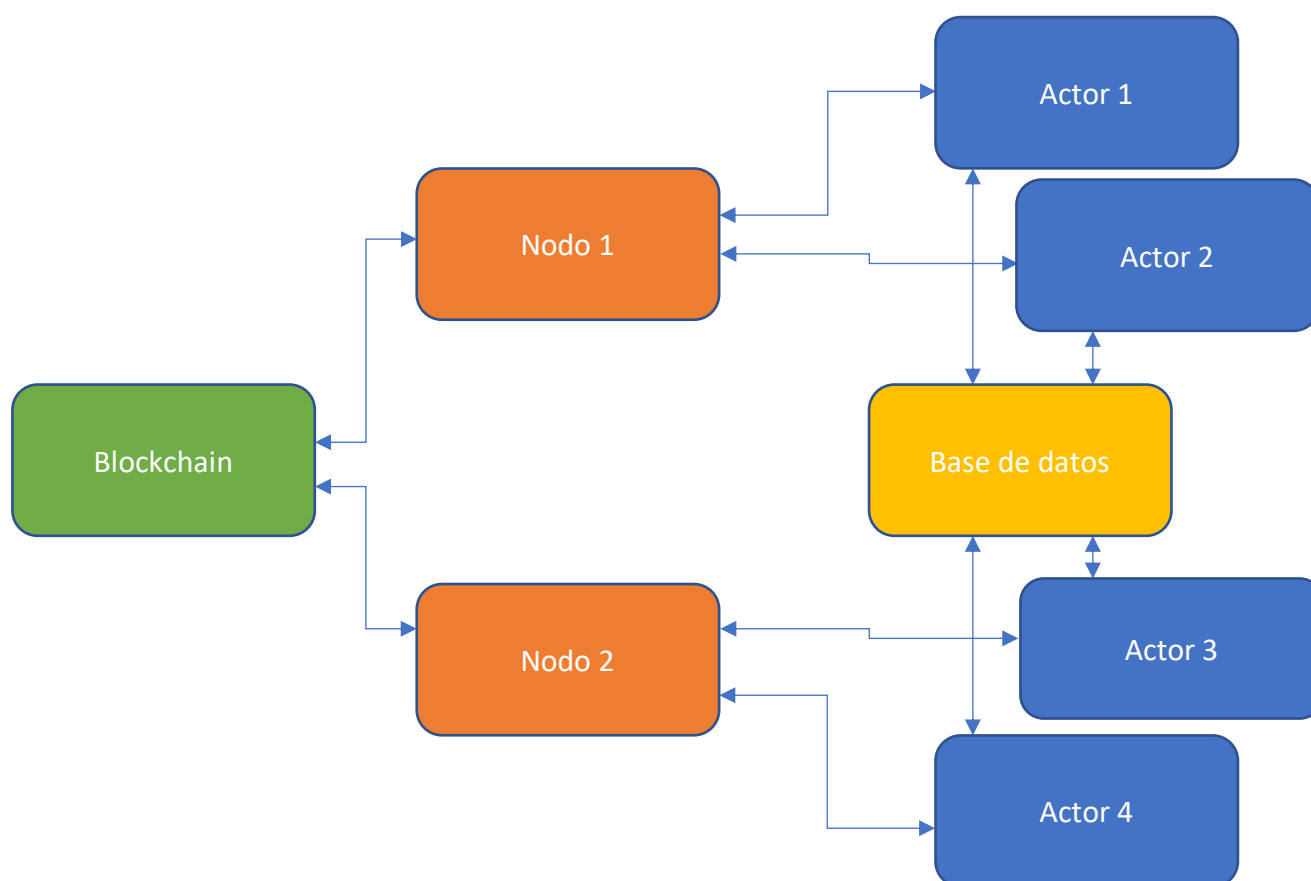


Figura 14: Arquitectura de la solución

3.4. Historias de usuarios de la solución

La arquitectura de la solución propuesta, ahora debemos definir las diferentes acciones de los actores. Para definir, las historias de usuarios son una herramienta adecuada. Gracias a esto, la determinación de las acciones de los diferentes actores permitirá sentar las bases de la validación de la solución.

Al identificar actores, se identificaron tres actores con acceso a la plataforma: actores no identificados, actores identificados y fabricantes de medicamentos. Además de estos tres jugadores, existe un cuarto: estos son los organismos de autorización de comercialización de medicamentos. Estas organizaciones tendrán el control de los nodos y deben cumplir con las especificaciones para realizar acciones de manera inteligente en la cadena de bloques.

Los actores no identificados corresponden a los consumidores que desean información sobre los medicamentos que compran: para esta categoría de actores, las historias de los usuarios son las siguientes:

- *Como consumidor, quiero leer una matriz de datos para obtener información sobre el medicamento que acabo de comprar (1).*
- *Como consumidor, quiero enumerar los diferentes propietarios de un medicamento para asegurarme del origen y el origen del medicamento (2).*
- *Como consumidor, quiero ver la cadena de bloques para tener información sobre los diversos actores en la cadena de suministro de la industria farmacéutica (3).*

Los actores identificados corresponden a los diferentes intermediarios entre los productores de medicamentos y los consumidores. Estos intermediarios pueden ser mayoristas, transportistas, hospitales ... Algunas de las historias de usuarios de estos son las mismas que para los actores no identificados, con varias adiciones:

- *Como intermediario, quiero poder recibir lotes de medicamentos para agregarlos a mi stock (4).*
- *Como intermediario, quiero poder aceptar o rechazar muchos medicamentos para administrar mis recibos de medicamentos y detectar lotes defectuosos (5).*
- *Como intermediario, quiero poder registrarme, iniciar sesión y cerrar sesión en mi cuenta para ser el único capaz de administrar mis transacciones (6).*
- *Como intermediario, quiero consultar mi perfil para modificar informaciones (7).*
- *Como intermediario, quiero poder enumerar los lotes de medicamentos en mi poder para obtener un inventario de mis existencias actuales (8).*
- *Como intermediario, quiero poder enviar un lote de medicamentos para venderlos (9).*
- *Como intermediario, quiero filtrar los lotes de medicamentos para visualizar los medicamentos para los cuales se debe llevar a cabo una acción de mi parte (10).*
- *Como intermediario, quiero poder solicitar a los nodos a los que estoy conectado que actualicen la cadena de bloques para confirmar mis transacciones y agregarlas a la cadena de bloques (11).*
- *Como intermediario, quiero dividir un lote de medicamentos para satisfacer la solicitud de un cliente (12).*
- *Como intermediario, quiero generar una matriz de datos para actualizar las cajas de medicamentos que pasan por mí (13).*

El tercer tipo de actor, un fabricante de medicamentos reúne todas las historias de usuarios de actores no identificados y actores identificados, junto con otras historias de usuarios:

- *Como fabricante de medicamentos, quiero poder agregar medicamentos con su número GTIN vinculado para crear muchos de ellos en la cadena de bloques (14).*
- *Como fabricante de medicamentos, quiero crear lotes de medicamentos con la fecha de vencimiento y la cantidad vinculada a ellos para comenzar su trazabilidad (15).*

Durante la validación de la solución propuesta, las historias de usuario validarán la solución y la vincularán a restricciones. Del conjunto de especificaciones definidas, con el funcionamiento de la cadena de bloques, la arquitectura de la solución y las historias de los usuarios, ahora debemos validar la solución después de desarrollarla.

Capítulo 4: Validación de la Solución

Para validar la solución, primero es necesario implementarla. Por elección técnica, la implementación de la solución es en python, con el uso del marco Flask. Es un marco orientado a aplicaciones web, con un motor de plantillas (Jinja2) para generar las páginas web. Este marco tiene la ventaja de ser ligero: inicialmente viene con muy pocos paquetes. Este marco contiene un servidor de desarrollo, así como un depurador y la gestión de cookies de sesión. A diferencia de otros frameworks (Django en particular), inicialmente se instalan pocos paquetes y esto permite que Flask se adapte rápidamente a necesidades específicas. La comunidad que apoya el marco es importante, y desarrolla regularmente extensiones adaptadas a él.

4.1. La gestión de los datos

Como se mencionó anteriormente, los datos se almacenan en dos espacios diferentes: una base de datos y una cadena de bloques.

4.1.1. La gestión de la base de datos

Para administrar la base de datos, Flask tiene una extensión llamada Flask-SQLAlchemy, una extensión de SQLAlchemy. SQLAlchemy es una herramienta que contiene un mapa relacional de objetos, que le permite convertir consultas escritas a python en SQL. El objeto central de esta memoria es la cadena de bloques, la presentación de la base de datos vinculada será mínima. SQLite es adecuado para esto: al mantener la base de datos en un archivo local, evita tener que usar una configuración más pesada con un servidor (por ejemplo, usando PostgreSQL). Para evitar conflictos y simplificar el desarrollo, es necesario poder migrar fácilmente la base de datos entre dos versiones: otra extensión de Flask que permite hacer esto es Flask-Migrate.

En el momento de la programación, el mapa Flask-SQLAlchemy se usa para vincular un modelo codificado en python a la tabla de base de datos vinculada. Por ejemplo, para los actores, el código del modelo en python será el siguiente:

```
class Actor(UserMixin, db.Model):
    id = db.Column(db.Integer, primary_key=True)
    actor_name = db.Column(db.String(120), index=True, unique=True)
    email = db.Column(db.String(120), index=True, unique=True)
    password_hash = db.Column(db.String(128))
    phone = db.Column(db.String(20))
    manufacturer = db.Column(db.Boolean, unique=False)
```

Debe enfatizarse que el código escrito en las memorias (y no el de los apéndices) está adaptado para ser legible. Ciertas funciones y propiedades que no contribuyen a la comprensión no están escritas. A partir de este código, Flask-SQLAlchemy es responsable de generar la tabla de datos. Flask-SQLAlchemy, porque es un mapeador relacional de objetos, le permite insertar datos en la base de datos sin tener que escribir código. Por ejemplo, para agregar un nuevo actor a la base de datos:

```
actor = Actor(actor_name=form.actor_name.data, email=form.email.data, phone=form.phone.data,
manufacturer=form.manufacturer.data)
```

El conjunto de tablas en la base de datos se basa en el mismo modelo. La abstracción de la interacción con la base de datos obtenida gracias a Flask-SQLAlchemy permite una gestión rápida y fácil de la base de datos.

4.1.2. La gestión de la blockchain

La cadena de bloques se almacena como una estructura de datos por los diferentes nodos. Cuando se indica que todos los nodos tienen acceso a la misma cadena de bloques, todos los nodos almacenan su propia cadena de bloques, pero con la intención de tener los mismos datos. En caso de desincronización, los nodos deben buscar un consenso para tener los mismos datos. Las interacciones con blockchain se realizan a través de una API Rest. El uso de una API brinda la oportunidad a algunas compañías farmacéuticas de desarrollar su propia capa de software para la interfaz. También permitiría a estas mismas compañías integrar el seguimiento de medicamentos blockchain en su propio programa de monitoreo de la cadena de suministro existente. Para esto, estas empresas solo deben registrarse con un nodo de blockchain y con la base de datos.

El primer paso es conectar los nodos entre sí. Si hay dos nodos que funcionan en las direcciones `http://localhost:8000/` y `http://localhost:8001/`, tienes que conectar los nodos de la siguiente forma:

- Desde el nodo en el puerto 8000, debe realizar una operación POST en la ruta `http://localhost:8000/register_with` con el objeto JSON:

```
{
  "node_address": "http://localhost:8001"
}
```

Este objeto JSON contiene la dirección del nodo al que este nodo quiere conectarse.

- Desde el nodo en el puerto 8001, debe realizar una operación POST en la ruta `http://localhost:8001/register_with` con el objeto JSON:

```
{
  "node_address": "http://localhost:8000"
}
```

Este objeto JSON contiene la dirección del nodo al que este nodo quiere conectarse. Para la gestión de los nodos, todo se hace gracias a las carreteras que ejecutan funciones internas del nodo. Estos nodos son los siguientes:

- `/register_node`: guarda los nuevos nodos pasados como parámetros (en forma de JSON) en el nodo actual.
- `/register_with`: guarda el nodo actual en otros nodos pasados como parámetros (como un JSON)
- `/add_block`: agrega un nuevo bloque al nodo actual. Para agregar un bloque, esta ruta requiere recibir la información del bloque. Esta información es el índice del bloque (*index*), las transacciones contenidas en el bloque (*transactions*), la marca de tiempo de la hora en que se agregó el bloque (*timestamp*), el hash del bloque anterior al agregado actualmente (*previous hash*), y el nuncio del bloque (*nonce*)

Una vez que dos nodos están conectados entre sí, la interacción con los nodos se realiza a través de las siguientes rutas:

- `/new_transaction`: le permite registrar una nueva transacción en blockchain. Esta ruta debe recibir el número de lote único que se reenviará (*batch_id*), el número único del remitente (*sender_id*), el número único del receptor (*recipient_id*) y el tamaño del lote a enviar (*quantity*).
- `/response_transaction`: permite registrar la respuesta de una transacción (aceptación o rechazo de la misma) cuando un actor desea transmitir un lote a otro actor. Esta ruta debe recibir el número único del lote que se transmitirá (*batch_id*), el número único del remitente (*sender_id*), el número único del receptor (*recipient_id*), el tamaño del lote a enviar (*quantity*) y El estado actual de la transacción a realizar (*status*).

- */register_batch*: permite que un fabricante de medicamentos agregue un nuevo lote de un medicamento. Esta ruta debe recibir el número único del lote que se registrará en blockchain (*batch_id*), el número único del remitente (*sender_id*) y el tamaño del lote a enviar (*quantity*).
- */chain*: permite preguntar a un nodo la cadena de bloques completa que almacena.
- */mine*: permite que un nodo "extraiga" transacciones no confirmadas ahora y las agregue a la cadena de bloques.
- */unconfirmed_transactions* : enumerar todas las transacciones no confirmadas para un nodo.

4.2. Interacción con la base de datos

La interacción con la base de datos se realiza desde el cliente. Pero estas rutas también permiten a los actores llamar a las rutas de los nodos a los que están conectados. La mayoría de las transacciones en la cadena de bloques necesitan soporte de la base de datos (para recuperar identificadores de lotes, por ejemplo) y, por lo tanto, al interactuar con la base de datos a través de estas rutas, los actores pasan por la base de datos para construir consultas que aborden la cadena de bloques.

- */*: ruta de índice que muestra la cadena de bloques. Esta ruta es pública, cualquier tipo de actor puede acceder a ella. Esta ruta usa la ruta del nodo */chain*.
- */update_connected_node_address/<address>*: ruta tomando en parámetros una dirección de nodo a la cual el cliente se conectará.
- */actor/<actor_name>*: ruta tomando en parámetro el nombre de un actor y que devuelve su perfil. Esta ruta es accesible para cualquier tipo de actor, ya que permitirá que un actor no identificado obtenga información sobre los diversos actores por los cuales el medicamento que acaba de comprar, que ha manejado el medicamento.
- */actorID/<actor_id>*: ruta tomando en parámetro el número de identificación único de un actor y que devuelve el perfil del actor en cuestión. Esta ruta, como la anterior, le permite al consumidor tener información sobre quién es el propietario del medicamento que acaba de comprar.
- */batch/<batch_id>*: ruta de acceso a la página de un lote pasando su número único como parámetro, con toda la información del lote enumerada en la página en cuestión (el nombre del medicamento del lote, el tamaño del lote y las transacciones del lote).
- */user_medicine*: lista de todos los medicamentos relacionados con un fabricante. Esta ruta le permite al fabricante llegar a una página desde la cual puede agregar medicamentos a la base de datos y crear nuevos lotes.
- */request_min* : ruta que permite a un actor consultar en el nodo al que está conectado para socavar un nuevo bloque.
- */fetch_medicine_for_user_id*: ruta para recuperar todos los medicamentos relacionadas con un usuario, gracias a su número único.
- */new_medicine*: ruta para crear un nuevo medicamento y agregarlo a una base de datos para un fabricante. Esta ruta necesita saber el nombre del medicamento a agregar y el número GTIN del mismo.
- */new_batch*: ruta para que un fabricante cree un nuevo lote de medicamentos con una fecha de vencimiento y cantidad asociada y lo agregue a la cadena de bloques.
- */send_batch*: ruta que permite que un actor identificado o un fabricante envíe un lote a otro actor con el número único. El remitente debe especificar el tamaño del lote a enviar. La fecha de vencimiento del lote enviado sigue siendo la misma que la del lote inicial.
- */user_transactions*: ruta listando todas las transacciones "activas" (es decir, para las cuales un actor puede tomar la decisión de aceptar un lote, rechazar un lote y enviar un lote) relacionadas con un actor.

- */submit_accept_transaction*: ruta que permite a un actor aceptar o rechazar mucho cuando lo envía otro actor.
- */decode_datamatrix*: ruta tomando en entrada una matriz de datos, conectando esta matriz de datos a un lote y mostrando la página del lote en cuestión. Si el lote no existe, se informa al usuario de su error.
- */login*: ruta que permite que un actor se conecte.
- */logout*: ruta que permite que un actor se desconecte.
- */register*: ruta que permite a un actor registrarse.

4.3. Validación de historias de usuarios

Usar las historias de los usuarios como referencias ayudará a confirmar el correcto funcionamiento del programa y el logro de los objetivos de la disertación. Como recordatorio, las historias de usuarios se dividieron en tres categorías: las de los actores no identificados, las de los actores identificados y las de los fabricantes de medicamentos.

4.3.1. Historias de usuarios de actores no identificados

- Como consumidor, *quiero* leer una matriz de datos *para* obtener información sobre el medicamento que acabo de comprar

Para validar la cuenta de este usuario, debe poder leer una matriz de datos y vincularla a la página de lote vinculada a esta matriz de datos. Esta página debe incluir toda la información del lote.

Figura 15: Pagina del índice

En la Figura 16, encontramos la página de índice con el área de importación de una matriz de datos. Una vez que se importa una matriz de datos, y si los datos de la matriz de datos corresponden a un lote de medicamento, el usuario es redirigido al lote de medicamento en cuestión.

Figura 16: Página de un lote de medicamentos, con las transacciones de ese lote.

La figura 17 enumera la información de un medicamento en la parte superior. La parte inferior enumera las diferentes transacciones y los diferentes propietarios de un medicamento.

- Como consumidor, quiero enumerar los diferentes propietarios de un medicamento para asegurarme del origen y el origen del medicamento.

Home

Login

Synchronise Blockchain



Batch 8

Medicine: Nouvel [ID number: 2]

Quantity: 10

Sender ID	Recipient ID	Batch ID	Quantity	Status	Date
2	1	8	10	accepted	26/08/2019 - 15:08:47
2	1	8	10	waiting	26/08/2019 - 15:08:31
2	2	8	10	accepted	26/08/2019 - 15:08:21

Figura 17: Información sobre los sucesivos propietarios de un medicamento.

Después de la importación de una matriz de datos, un consumidor puede enumerar los diferentes propietarios de un lote, el estado del lote después de cada transacción y las fechas de las transacciones. El consumidor puede seleccionar los identificadores del remitente y el receptor para obtener información sobre la ubicación de estos.

- Como consumidor, quiero ver la cadena de bloques para tener información sobre los diversos actores en la cadena de suministro de la industria farmacéutica.

Para enumerar la cadena de bloques, un consumidor debe ir a la página de índice y ver las diferentes transacciones de medicamentos. También puede filtrar transacciones a través de múltiples filtros: nombre del medicamento, número de lote, número de remitente, número de receptor y estado del lote.

Home

Login

Synchronise Blockchain

Browse...

No file selected.

Search with Datamatrix

Filter by Medicine Name

Filter by Batch ID

Filter by Sender ID

Filter by Recipient ID

All Transactions

Show

10

entries

Medicine ID	Medicine Name	Batch ID	Quantity	Sender ID	Recipient ID	Status	Date
2	Nouvel	8	10	2	1	accepted	26/08/2019 - 15:08:47
2	Nouvel	8	10	2	1	waiting	26/08/2019 - 15:08:31
2	Nouvel	8	10	Batch created	2	accepted	26/08/2019 - 15:08:21
2	Nouvel	7	30	Batch created	2	accepted	26/08/2019 - 15:08:19
1	Prode	6	40	Batch created	1	accepted	26/08/2019 - 13:31:44
1	Prode	5	20	Batch created	1	accepted	26/08/2019 - 13:31:42

Previous

1

Next

4.3.2. Historias de usuarios de actores identificados

- Como intermediario, quiero poder recibir lotes de medicamentos para agregarlos a mi stock.

El corazón de blockchain es poder gestionar transacciones entre diferentes actores. Los principales actores en estas transacciones son los intermediarios. Para recibir un lote de medicamentos, un intermediario debe registrarse para obtener un número de identificación. Este número de identificación servirá como una dirección cuando otro usuario desee enviarle mucho.

- Como intermediario, quiero poder aceptar o rechazar muchos medicamentos para administrar mis recibos de medicamentos y detectar lotes defectuosos.

Cuando un intermediario se encuentra en la página de administración de transacciones, puede elegir aceptar o rechazar un lote. Luego debe confirmar su elección.

Medicine ID	Medicine Name	Batch ID	Quantity	Sender ID	Status	Date	Confirm
1	Prode	11	5	1	✓ Accept Refuse	26/08/2019 - 16:48:47	Confirm

Figura 18: Aceptación o rechazo de un lote

- Como intermediario, quiero poder registrarme, iniciar sesión y cerrar sesión en mi cuenta para ser el único capaz de administrar mis transacciones.

Para acceder a su cuenta, los actores identificados tienen acceso a una página de identificación. En esta página de inicio de sesión, el usuario puede iniciar sesión si tiene una cuenta o registrarse.

[Home](#)

LoginSynchronise Blockchain



blockchain

Sign in

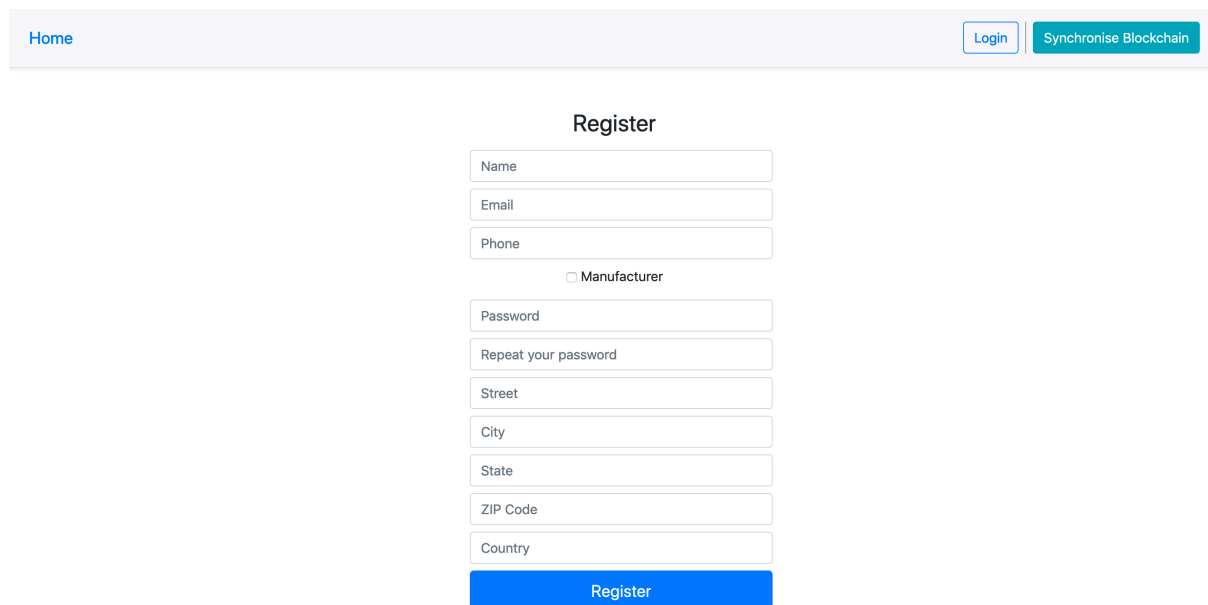
☐ Remember Me

Sign in

[Create an account](#)

Figura 19: Pagina de identificación

Si el usuario desea registrarse, puede acceder a la página de registro que le permite ingresar información útil de su perfil. Tenga en cuenta la presencia de un botón de verificación "fabricante" para especificar si el perfil utilizado es un perfil del fabricante del medicamento o no.



Home Login Synchronise Blockchain

Register

Name

Email

Phone

☐ Manufacturer

Password

Repeat your password

Street

City

State

ZIP Code

Country

Register

Figura 20: Página de registro

Una vez conectado, un usuario puede desconectarse con la ayuda de un botón «Logout».

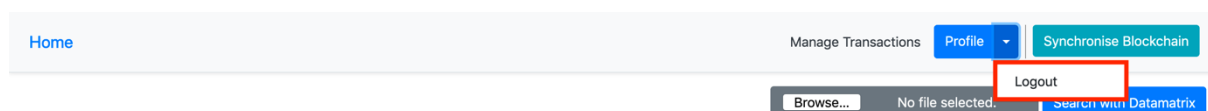
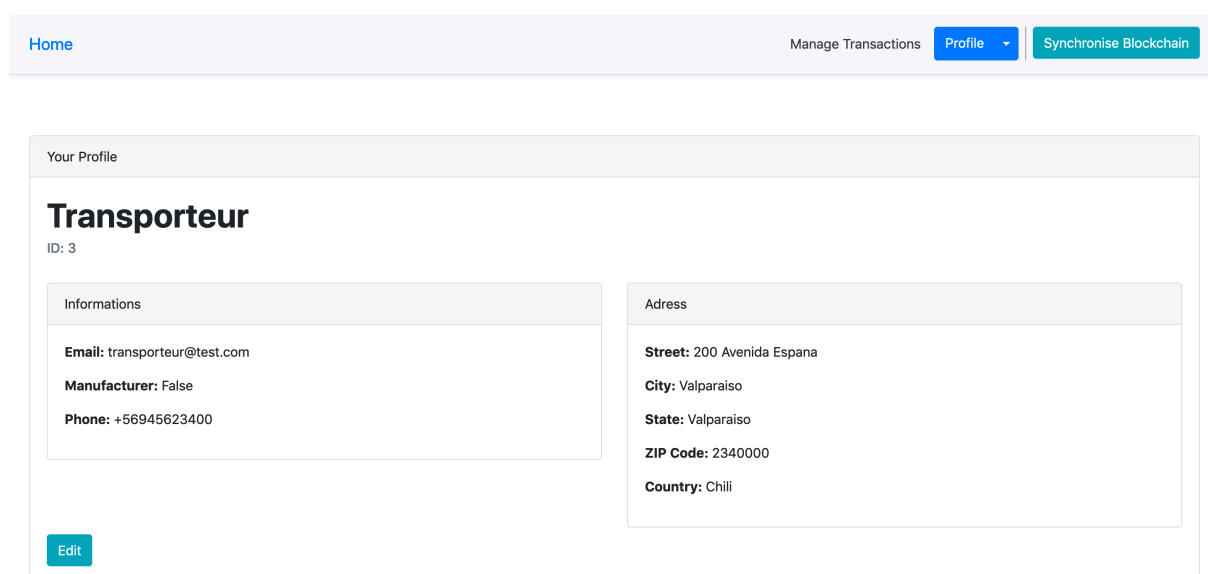


Figura 21: Botón de desconexión

- Como intermediario, quiero consultar mi perfil para modificar informaciones.

En la página de perfil de un usuario, el usuario puede ver su información y hacer clic en el botón de edición de perfil para modificar la información sobre él.



Home Manage Transactions Profile Synchronise Blockchain

Your Profile

Transporteur

ID: 3

Informations

Email: transporteur@test.com

Manufacturer: False

Phone: +56945623400

Address

Street: 200 Avenida Espana

City: Valparaiso

State: Valparaiso

ZIP Code: 2340000

Country: Chili

Edit

Figura 22: Perfil de un usuario

- Como intermediario, quiero poder enumerar los lotes de medicamentos en mi poder para obtener un inventario de mi stock actual.

Un usuario puede ver su inventario actual de medicamentos a través de la pestaña «Manage Transactions».

Medicine ID	Medicine Name	Batch ID	Quantity	Sender ID	Status	Date	Confirm
2	Nouvel	8	10	1	accepted	26/08/2019 - 16:21:20	
1	Prode	9	10	1	Accept	26/08/2019 - 16:21:03	Confirm

Figura 23: Ver el inventario de un usuario

- Como intermediario, quiero poder enviar un lote de medicamentos para venderlos.

El envío de un lote de medicamentos se realiza desde la página de administración de transacciones.

Figure 24: Enviar lote 8 de tamaño 10 al actor con número de identificación 2

- Como intermediario, quiero filtrar los lotes de medicamentos para visualizar los medicamentos para los cuales se debe llevar a cabo una acción de mi parte.

Los lotes en los que un actor debe realizar una acción son aquellos con el estado de "waiting". Cuando un lote tiene este estado, el actor puede aceptar o rechazar la transacción. Para filtrar lotes con este estado, hay un botón "Filter the Waiting Batch" en la página de administración de transacciones de un usuario que enumera solo los lotes con el estado "waiting".

Medicine ID	Medicine Name	Batch ID	Quantity	Sender ID	Status	Date	Confirm
1	Prode	9	10	1	Accept	26/08/2019 - 16:21:03	Confirm

Figura 25: Filtrando los medicamentos

- Como intermediario, quiero poder solicitar a los nodos a los que estoy conectado que actualicen la cadena de bloques para confirmar mis transacciones y agregarlas a la cadena de bloques.

Para solicitar la actualización de blockchain, un usuario puede hacer clic en el botón "sincronizar blockchain".

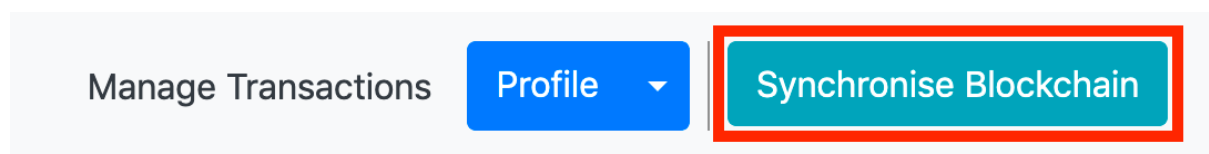


Figura 26: Botón de solicitud de sincronización de blockchain

- Como intermediario, quiero dividir un lote de medicamentos para satisfacer la solicitud de un cliente.

Cuando un actor envía un lote mucho más pequeño que el tamaño del lote original, el lote se divide en dos sublotes y uno de los sublotes se envía al destinatario del lote.

Medicine ID	Medicine Name	Batch ID	Quantity	Sender ID	Recipient ID	Status	Date
1	Prode	12	5	1	2	waiting	26/08/2019 - 16:42:31
1	Prode	12	5	Batch created	1	accepted	26/08/2019 - 16:42:31
1	Prode	11	5	Batch created	1	accepted	26/08/2019 - 16:42:31
1	Prode	10	10	Batch created	1	accepted	26/08/2019 - 16:39:22

Figura 27: División de un lote en dos, y envía uno de los sub lotes

- Como intermediario, quiero generar una matriz de datos para actualizar las cajas de medicamentos que pasan por mí.

Al ver un lote de medicamentos, la matriz de datos relacionada con el lote está disponible en la página del lote.

 Batch 12 Medicine: Prode [ID number: 1] Quantity: 5					
Sender ID	Recipient ID	Batch ID	Quantity	Status	Date
1	2	12	5	waiting	26/08/2019 - 16:42:31
1	1	12	5	accepted	26/08/2019 - 16:42:31
1	1	10	10	split	26/08/2019 - 16:39:22

Figura 28: Visualización del datamatrix de un lote

4.3.3. Historias de fabricantes de medicamentos.

Los fabricantes de medicamentos tienen acceso a una pestaña específica desde la cual pueden administrar medicamentos. Esta pestaña se llama «Manage Medicine».

- Como fabricante de medicamentos, quiero poder agregar medicamentos con su número GTIN vinculado para crear muchos de ellos en la cadena de bloques.

Home Manage Medicine Manage Transactions Profile Synchronise Blockchain

Medicine Name GTIN Number Add New Medicine

#	Medicine Name	GTIN	Expiration Date	Quantity
1	Prode	3450	01/01/2020	

Add New Batch

Figura 29: Agregar un nuevo medicamento a la base de datos

Desde la pestaña Administración de medicamentos, un fabricante puede agregar un nuevo medicamento con el nombre del medicamento y el GTIN del medicamento.

- Como fabricante de medicamentos, quiero crear lotes de medicamentos con la fecha de vencimiento y la cantidad vinculada a ellos para comenzar su trazabilidad.

Home Manage Medicine Manage Transactions Profile Synchronise Blockchain

Medicine Name GTIN Number Add New Medicine

#	Medicine Name	GTIN	Expiration Date	Quantity
1	Prode	3450	01/01/2020	

Add New Batch

Figura 30: Agregar un nuevo lote de medicamento

Una vez que se agrega un medicamento a la base de datos, un fabricante puede crear lotes cuando lo desee y agregar esos lotes en la cadena de bloques y la base de datos.

4.4. Ejemplos de intentos de sobornar a la cadena de bloques

Un segundo paso en la validación de la solución es la verificación de que la solución puede evitar la corrupción de la cadena de suministro por parte de un tercero. Para esto, se presentarán dos casos de ejemplos concretos: el caso en que un transportista desea agregar medicamentos externos y el caso en el que se infla un lote de medicamentos para cambiar la cantidad del lote.

4.4.1. Adición de medicamentos externos por un transportista

Un primer ejemplo de un intento de sobornar a la cadena de suministro sería un intento de un transportista de agregar medicamentos externos a la cadena de bloques. La adición de un medicamento externo y su seguimiento en la cadena de bloques solo puede hacerlo un fabricante de medicamentos (para obtener un identificador único para el lote de medicamentos). Por lo tanto, un transportista no puede agregar un medicamento externo. Pero tiene la opción de reemplazar un lote de medicamentos con otro lote de medicamentos (y dos medicamentos diferentes). Reemplazar un lote con otro, sin embargo, presenta un problema. Cuando el transportista en cuestión intenta transferir el lote a otro propietario, se dará cuenta de que el medicamento que quiere obtener no es el que recibe. Esta distinción hará que rechace el lote transferido, y el transportista retiene el lote en consecuencia. Para el transportista, su única solución es reintroducir el medicamento inicial para rastrearlo.

4.4.2. Cambiar la cantidad de un lote

Otro ejemplo de intento de seguimiento de la corrupción es el aumento en la cantidad de medicación contenida en un lote. Por ejemplo, un actor puede intentar duplicar el tamaño de un lote agregando copias del medicamento original al lote. Sin embargo, este intento ocurriría cuando se transfiere un lote (la única vez que un actor que no es un fabricante puede cambiar el tamaño de un lote). Solo existen salvaguardas: la cantidad de medicamentos por lote está presente en la cadena de bloques, e intentar transferir un lote más grande causará la negativa de la transferencia por parte de la cadena de bloques. De esta manera, es imposible para un actor cambiar el tamaño de un lote: solo puede enviar un sub-lote a otro actor, o al lote completo.

Capítulo 5: Conclusión

5.1. Conclusiones generales

Para concluir, el uso de una cadena de bloques, y la mejora de la trazabilidad relacionada con este uso, permite tener una trazabilidad clara de un medicamento, desde el fabricante hasta el vendedor final. Esta trazabilidad hace que sea imposible para los agentes externos incorporar medicamentos no autorizados a la cadena de suministro de la industria farmacéutica. La cadena de bloques también le permite crear un árbol de lotes, en el que los lotes se dividen en sub-lotes.

Para lograr esta trazabilidad, la solución hace posible seguir un medicamento con la ayuda de un número de lote único y actualizar este número de lote en caso de un cambio en el tamaño del lote. La actualización de este número de lote implica actualizar la matriz de datos presente en la caja del medicamento: hoy, esta solución es la más adecuada por una razón económica, pero en el futuro, el uso de chips RFID presenta un gran potencial, en comparación con el uso de datamatrix.

Sin embargo, establecer una trazabilidad precisa de los medicamentos tiene el límite de no ser tan favorable para las empresas del sector farmacéutico. Al mejorar la trazabilidad de los medicamentos, las compañías farmacéuticas se vuelven completamente transparentes para los consumidores, quienes pueden saber si un medicamento comprado proviene de su país de origen o es importado de otro país. Para las compañías farmacéuticas, esto puede evitar que puedan reducir los costos al fabricar un medicamento en un país donde los costos de producción son bajos y, por lo tanto, aumentar su margen. Este déficit puede ser una de las razones que justifican las traiciones actuales de la industria farmacéutica para la trazabilidad.

El diseño y desarrollo de una cadena de bloques ha demostrado que esta tecnología es adecuada para el seguimiento de lotes y, en general, el seguimiento de cualquier objeto con un identificador único, y esto con costos de implementación. Lugar mínimo en vista de las apuestas.

5.2. Logro de los objetivos

En la introducción de esta memoria, se ha especificado una serie de objetivos. Estos objetivos están destinados a demostrar que esta memoria cumple su función. A continuación, se presentan nuevamente estos objetivos, con el enfoque de esperarlos.:

- **Comprender y saber qué es una cadena de bloques, cómo funciona y la utilidad futura de la tecnología.**

En la parte del estado del arte se presentó lo que es una blockchain. El funcionamiento de esta tecnología y su uso para las cadenas de suministro se realizó ampliamente durante esta memoria (especialmente durante la construcción de la solución). También se presentaron algoritmos específicos de blockchain, principalmente aquellos relacionados con la resolución de conflictos. En general, se presentó y analizó toda la composición y operación de una cadena de bloques durante el desarrollo de esta memoria.

- **Analizar la cadena de suministro de la industria farmacéutica.**
Durante el análisis del marco conceptual de esta memoria se presentó la cadena de suministro de Novartis, con la especificidad específica de esta cadena. A partir del análisis de esta cadena de suministro, se creó una generalización para todas las cadenas de la industria farmacéutica. Es esta generalización la que hizo posible la creación de la solución de la memoria, con la identificación de los diferentes actores de la cadena.
- **Desarrollar un programa para mejorar el seguimiento de medicamentos con una cadena de bloques.**

El objetivo central de esta tesis era proponer una solución a los problemas de los medicamentos falsificados. El programa desarrollado con Flask ayuda a cumplir este objetivo, con el uso de una cadena de bloques para mejorar este monitoreo.

5.3. Trabajos futuros

Esta tesis presenta una base para mejorar la trazabilidad del sector farmacéutico. Potencialmente, la mejora de esta trazabilidad puede, en el mismo principio del uso de una cadena de bloques, extenderse a otros productos médicos, para ver sectores completamente distantes (por ejemplo, el monitoreo de la composición de los alimentos para el gran consumo). Con más granularidad, esta memoria podría seguir la composición anterior (de dónde provienen los excipientes, de dónde provienen las moléculas ...). La solución propuesta actualmente sigue solo al medicamento terminado.

Otro paso podría ser convertir la solución en una Planificación de Recursos Empresariales (ERP) completa para compañías farmacéuticas. La gestión actual ya garantiza la gestión del inventario, por lo que el programa ofrece una base ERP. Transformar la solución en ERP tendría muchos beneficios. Por ejemplo, los transportistas (considerados como actores en la solución actual) podrían administrar sus existencias en un flujo justo a tiempo y distribuir los medicamentos que transportan tal como están (según el modelo de la industria automotriz). En el caso de que uno de los clientes del transportista se niegue mucho, podría ofrecer este lote a todos los demás clientes en el camino, y así optimizar el transporte.

Finalmente, la estandarización de una cadena de bloques para realizar la trazabilidad de los medicamentos en la industria farmacéutica puede, a través de interfaces, permitir que diferentes empresas del sector adapten su ERP interno para acceder a esta cadena de bloques. Esto dejaría a las administraciones nacionales la tarea de gestionar rutas de interfaz y gestionar permisos para interactuar con la cadena de bloques (definir fabricantes y actores). Esta solución permitiría a las compañías farmacéuticas solo adaptar su sistema actual a esta nueva trazabilidad.

Bibliografía

- [1] (n.d.). Retrieved from http://archive.wikiwix.com/cache/?url=http://www.leem.org/htm/themes/article.asp?id_sous_rubrique=95&id_article=490
- [2] (n.d.). Retrieved from <http://rfidinhealthcare.org/>
- [3] Agnew, H. (2017, December 3). Sanofi leads charge against counterfeit drugs. Retrieved from <https://www.ft.com/content/7027df4e-d67a-11e7-8c9a-d9c0a5c8d5c9>
- [4] Armstrong, S., & ArmstrongShain, S. (2018, March 29). Gen2 V2: The Next Step In The Evolution of RFID. Retrieved from <https://blog.atlasrfidstore.com/g2v2>
- [5] (2019, August 13). Barcode. Retrieved from https://en.wikipedia.org/wiki/Barcode#Types_of_barcodes
- [6] Castro, M., & Liskov, B. (1999, February). Practical Byzantine Fault Tolerance. Retrieved from <http://pmg.csail.mit.edu/papers/osdi99.pdf>
- [7] Clark, F. (n.d.). Rise in online pharmacies sees counterfeit drugs go global ... Retrieved from [https://www.thelancet.com/journals/lancet/article/PIIS0140-6736\(15\)00394-3/fulltext](https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(15)00394-3/fulltext)
- [8] (n.d.). COMBATING COUNTERFEIT DRUGS A Report of the Food and Drug ... Retrieved from <https://www.fda.gov/media/77086/download>
- [9] (n.d.). Composition du médicament/Généralités. Retrieved from https://fr.wikiversity.org/wiki/Composition_du_m%C3%A9dicament/G%C3%A9n%C3%A9ralit%C3%A9s
- [10] (n.d.). Détermination d'un état global - dpt-info.di.unistra.fr. Retrieved from https://dpt-info.di.unistra.fr/~stella/enseignement/algos_distr/chapitre6_12_13.pdf
- [11] (n.d.). El Mercado de Medicamentos en Chile - economia.gob.cl. Retrieved from <https://www.economia.gob.cl/wp-content/uploads/2013/04/Boletin-Mercado-de-Medicamentos.pdf>
- [12] (n.d.). EXISTING TECHNOLOGIES AND “TRACK AND TRACE” MODELS IN USE ... Retrieved from https://www.who.int/medicines/regulation/ssffc/mechanism/country-experience-table_updated-nov2017.pdf
- [13] Fox, M. (2011, June 16). Alan Haberman, Who Ushered In the Bar Code, Dies at 81. Retrieved from https://www.nytimes.com/2011/06/16/business/16haberman.html?_r=1&hp
- [14] (2014, December 5). Guide pratique: choisir un tag RFID. Retrieved from <http://www.nexess-solutions.com/fr/choisir-un-tag-rfid-pour-des-applications-industrielles/>
- [15] (2011). IMPACT International Medical Products Anti-counterfeiting ... Retrieved from <http://apps.who.int/medicinedocs/en/d/Js20967en/>
- [16] (n.d.). Implementation of RFID in the Pharmaceutical Industry. Retrieved from <https://www.iopp.org/files/public/CAPolytechJDHoward.pdf>

- [17] (2014, October 24). ISO/IEC 16022:2006. Retrieved from <https://www.iso.org/standard/44230.html>
- [18] Kenney, J. T. (2014, June 25). The Health and Economic Effects of Counterfeit Drugs. Retrieved from <http://www.ahdbonline.com/issues/2014/june-2014-vol-7-no-4/1756-the-health-and-economic-effects-of-counterfeit-drugs>
- [19] King, S., & Nadal, S. (2012, August 19). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Retrieved from <https://decred.org/research/king2012.pdf>
- [20] Lamport, L. (n.d.). Time, Clocks, and the Ordering of Events in a Distributed ... Retrieved from <https://lamport.azurewebsites.net/pubs/time-clocks.pdf>
- [21] Lamport, L. (n.d.). The Part-Time Parliament - Leslie Lamports Home Page. Retrieved from <http://lamport.azurewebsites.net/pubs/lamport-paxos.pdf>
- [22] Lamport, L. (2001, November 1). Paxos Made Simple - Leslie Lamports Home Page. Retrieved from <https://lamport.azurewebsites.net/pubs/paxos-simple.pdf>
- [23] (n.d.). Legifrance - Le service public de l'accès au droit. Retrieved from <https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006072665&idArticle=LEGIARTI000006689867>
- [24] (2019, July 5). List of largest pharmaceutical companies by revenue. Retrieved from https://en.wikipedia.org/wiki/List_of_largest_pharmaceutical_companies_by_revenue
- [25] Nakamoto, S. (n.d.). A Peer-to-Peer Electronic Cash System. Retrieved from <https://bitcoin.org/en/bitcoin-paper>
- [26] Nazrul, S. S. (2018, November 5). CAP Theorem and Distributed Database Management Systems. Retrieved from <https://towardsdatascience.com/cap-theorem-and-distributed-database-management-systems-5c2be977950e>
- [27] Ongaro, D., & Ousterhout, J. (n.d.). In Search of an Understandable Consensus Algorithm ... Retrieved from <https://raft.github.io/raft.pdf>
- [28] (2019, April 26). Pénicilline. Retrieved from <https://fr.wikipedia.org/wiki/Pénicilline#Historique>
- [29] (n.d.). QR Code vs. Data Matrix vs. Linear. Retrieved from <https://nationalband.com/qr-code-vs-data-matrix-vs-barcode/>
- [30] (n.d.). Lecteur RFID : comment cela marche ? - rfid nfc iot ido rtls ble - Internet des Objets Connectés. Retrieved from <http://www.filrfid.org/article-3373163.html>
- [31] Sanofi. (n.d.). Fighting counterfeit drugs starts with knowing it exists: Sanofi. Retrieved from <https://mediaroom.sanofi.com/en/articles/2017/fighting-counterfeit-drugs-starts-with-knowing-it-exists/>
- [32] (n.d.). SANTÉ 2030 : analyse prospective pour relever les défis de la santé de demain. Retrieved from http://www.leem.org/htm/themes/article.asp?id_sous_rubrique=95&id_article=490

- [33] Smiley, S., & SmileySuzanne, S. (2018, March 27). 7 Types of Security Attacks on RFID Systems. Retrieved from <https://blog.atlasrfidstore.com/7-types-security-attacks-rfid-systems>
- [34] (n.d.). Substandard and falsified medical products. Retrieved from <https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products>
- [35] (n.d.). Supply Chain Excellence in the Pharmaceutical Industry ... Retrieved from [https://ctl.mit.edu/sites/ctl.mit.edu/files/SC2020 Thesis Novartis.pdf](https://ctl.mit.edu/sites/ctl.mit.edu/files/SC2020%20Thesis%20Novartis.pdf)
- [36] Tosetti, P. (2016, February 26). Medicines verification in Europe: What to expect in 2019. Retrieved from https://ec.europa.eu/health/sites/health/files/files/falsified_medicines/201602_stakeholders_workshop_final.pdf
- [37] (2019, February 10). Trading in Venezuela's pain: Border vendors do brisk business in meds. Retrieved from <https://www.france24.com/en/20190210-trading-venezuelas-pain-border-vendors-do-brisk-business-meds>
- [38] (n.d.). What is Hashing? » Learn about Blockchain: Lisk Academy. Retrieved from <https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/what-is-hashing>
- [39] Wu, J. (2015, May 22). Where does medicine come from? Retrieved from <http://sitn.hms.harvard.edu/flash/2011/where-does-medicine-come-from/>
- [40] (n.d.). ¿Cuándo se puede comercializar un medicamento genérico? Retrieved from <https://www.engenerico.com/cuando-se-puede-comercializar-un-medicamento-generico/>

Anexos

1. Ejemplo de blockchain

```
{
  "chain": [
    {
      "hash": "db22ee422d9cc3aefc571e093eb37bb89a8be980045f48b35ad11bac1ef6aa9e",
      "index": 0,
      "nonce": 0,
      "previous_hash": "00",
      "timestamp": 1566750163.615837,
      "transactions": []
    },
    {
      "hash": "006c5640b00aec6c5cbfdcf55d82224563ef7f08f7765a8b01a06dd6d90d7751",
      "index": 1,
      "nonce": 976,
      "previous_hash": "db22ee422d9cc3aefc571e093eb37bb89a8be980045f48b35ad11bac1ef6aa9e",
      "timestamp": 1566750262.134371,
      "transactions": [
        {
          "batch_id": 3,
          "quantity": 10,
          "recipient_id": 2,
          "sender_id": 2,
          "status": "accepted",
          "timestamp": 1566750257.638112
        },
        {
          "batch_id": 4,
          "quantity": 20,
          "recipient_id": 2,
          "sender_id": 2,
          "status": "accepted",
          "timestamp": 1566750259.762617
        }
      ]
    }
  ],
  {
    "hash": "0052d92fac470238f3d4678e08097913e1688a3d9e8f0c8a07390a8c63b8b81f",
    "index": 2,
    "nonce": 816,
    "previous_hash": "006c5640b00aec6c5cbfdcf55d82224563ef7f08f7765a8b01a06dd6d90d7751",
    "timestamp": 1566750272.456348,
```

```

    "transactions": [
        {
            "batch_id": 3,
            "quantity": 10,
            "recipient_id": 1,
            "sender_id": 2,
            "status": "waiting",
            "timestamp": 1566750271.120368
        }
    ]
}
],
"length": 3,
"peers": [
    "http://localhost:8000/",
    "http://localhost:8001/"
]
}

```

2. Código de un block

```

class Block:
    def __init__(self, index, transactions, timestamp, previous_hash,
nonce=0):
        self.index = index
        self.transactions = transactions
        self.timestamp = timestamp
        self.previous_hash = previous_hash
        self.nonce = nonce

```

3. Código de la blockchain

```

class Blockchain:

    #Difficulty of the proof of work
    difficulty = 2

    def __init__(self):
        self.unconfirmed_transactions = []
        self.chain = []

    def create_genesis_block(self):
        """
        Function to generate the first block and the first hash
        """
        genesis_block = Block(0, [], time.time(), "00")
        genesis_block.hash = genesis_block.compute_hash()
        self.chain.append(genesis_block)

```

```

@property
def last_block(self):
    return self.chain[-1]

def proof_of_work(self, block):
    """
    Proof of work's function that verify that the start of our hash is
a    number of zeros.
    """
    block.nonce = 0
    computed_hash = block.compute_hash()
    while computed_hash.startswith('0' * self.difficulty) is False:
        block.nonce += 1
        computed_hash = block.compute_hash()

    return computed_hash

def add_block(self, block, proof):
    """
    Function to add a block to the chain
    """
    previous_hash = self.last_block.hash

    if previous_hash != block.previous_hash:
        return False

    if not Blockchain.is_valid_proof(block, proof):
        return False

    block.hash = proof
    self.chain.append(block)
    return True

@classmethod
def is_valid_proof(cls, block, block_hash):
    """
    Check if block_hash is valid hash of block and comply
    with the difficulty
    """
    return (block_hash.startswith('0' * Blockchain.difficulty) and
            block_hash == block.compute_hash())

def add_new_transaction(self, transaction):
    self.unconfirmed_transactions.append(transaction)

@classmethod
def check_chain_validity(cls, chain):

```

```

"""
Check is the hash is correct or no
"""
result = True
previous_hash = "0"

for block in chain:
    block_hash = block.hash
    delattr(block, "hash")

    if not cls.is_valid_proof(block, block.hash) or previous_hash
!= block.previous_hash:
        result = False
        break

    block.hash, previous_hash = block_hash, block_hash

return result

def mine(self):
    """
    Function who add all the unconfirmed transactions to a block and
    getting then the proof of work
    """
    #if there is no transaction
    if not self.unconfirmed_transactions:
        return False

    last_block = self.last_block

    new_block = Block(index=last_block.index + 1,
                      transactions=self.unconfirmed_transactions,
                      timestamp=time.time(),
                      previous_hash=last_block.hash)

    proof = self.proof_of_work(new_block)
    self.add_block(new_block, proof)

    self.unconfirmed_transactions = []
    announce_new_block(new_block)
    return new_block.index

```