VICERRECTORÍA ACADÉMICA

OFICINA COORDINADORA DE CURSO MONOGRÁFICO

Modelo de sistema de trazabilidad de la cadena de suministro de alimentos utilizando Blockchain para el Supermercado Nuevo Amanecer, en Santo Domingo Este, RD, año 2018.

Sustentada por:

Br. Raymond Amado Coplin Cáceres	2013-2200
Br. María del Pilar Mireles Mateo	2013-2006
Br. Pamir Matos Mancebo	2012-0089

Asesor:
Ing. Santo Navarro

Monografía para optar por el título de:
Ingeniero en Sistemas de Computación,
Ingeniero de Software

Distrito Nacional, República Dominicana

Mayo - Agosto 2018

Los conceptos expuestos en esta investigación son de la exclusiva responsabilidad de su(s) autor(es).

Modelo de Sistema de Trazabilidad de la Cadena de Suministro de alimentos utilizando Blockchain para el Supermercado Nuevo Amanecer, en Santo Domingo Este, RD, año 2018.

ÍNDICE DE CONTENIDO

AGRADECIMIENTOS ..... **X**
DEDICATORIA ..... **XIII**
INTRODUCCION ..... **XIV**

1. ANTECENDETES Y ASPECTOS GENERALES 18
1.1. SITUACIÓN ACTUAL DEL LA CADENA DE SUMINISTRO DE LOS SUPERMERCADOS DE LA REPÚBLICA DOMINICANA 19
1.2. LEY GENERAL DE SALUD 42-01 23
1.2.1. Reglamento general para control de riesgos en alimentos y bebida en la república dominicana 24
1.3. LAS CADENAS DE SUMINISTROS INTELIGENTES 32
1.4. BLOCKCHAIN COMO TECNOLOGÍA DISRUPTIVA 44

2. ASPECTOS TECNICOS Y CONCEPTOS REFERENTES A LA SOLUCION 50
2.1. CADENA DE SUMINISTRO 50
2.1.1. Origen de la cadena de suministro 50
2.1.2. Características de la cadena de suministro 51
2.1.3. Procesos macro y funciones de la cadena de suministro en el Interior de una empresa 53
2.1.4. Los niveles de decisiones en una cadena de suministro 54
2.1.5. Visiones de una cadena de suministro 57
2.1.6. Una cadena de suministro más eficiente y productiva 58
2.1.7. Trazabilidad y visibilidad total 59
2.2. BLOCKCHAIN 62
2.2.1. Origen 63
2.2.2. Características de la Blockchain 65
2.2.3. La Blockchain para el negocio 68
2.2.3.1.Conceptos claves de la Blockchain para el negocio 70
2.2.4. Aplicaciones de la cadena de bloques 76
2.2.5. Aspectos Técnicos 78
2.2.5.1.Red Peer-To-Peer (P2p) 81
2.2.5.2.Sistema de intercambio Peer-To-Peer 83
2.2.5.3.Mecanismos de consenso de grupo 91
2.2.5.3.1. Diferentes mecanismos de consenso de grupo 96
2.2.5.4. Redes de validación distribuidas públicas y privadas 103
2.2.5.5.Contratos Inteligentes (Smart Contracts) 107
2.2.5.6.Lenguajes de programación orientados a contratos 113

2.3. SENSORES 115
2.3.1. Sensor de geolocalización 115
2.3.2. Sensor de temperatura 117
2.4. SEGURIDAD DE LA INFORMACIÓN 119
2.5. HARDWARE 124
2.5.1. Dispositivo 124
2.5.1.1. Composición del dispositivo 126
2.5.1.2. Costo de los dispositivos 127

3. ANALISIS Y DISEÑO DE LA SOLUCION PROPUESTA 129
3.1. ALCANCE Y ARQUITECTURA GENERAL DE LA PLATAFORMA 129
3.1.1. Alcance de la plataforma 129
3.1.2. Arquitectura General 130
3.2. DISEÑO Y ELEMENTOS DE LA ARQUITECTURA 133
3.2.1. Hyperledger Sawtooth 133
3.2.2. Arduino Y Sensores 142
3.2.3. Portal De Gestión Scm 145
3.2.4. Adapa Decision Engine 147
3.2.5. Amazon Web Services (Aws): Computación En La Nube 148
3.3. METODOLOGÍAS DE TRABAJO 155
3.3.1. Metodología Ágil Scrum 155
3.3.2. Actores E Historias De Usuarios 162
3.4. TECNOLOGÍAS Y HERRAMIENTAS 168
3.4.1. Repositorio de código y control de versiones 168
3.4.2. Lenguajes de programación 169
3.4.3. Entornos de Desarrollo Integrados (IDE) 170
3.4.4. Base de Datos 171
3.4.5. Frameworks y Librerías 171
3.5. REQUISITOS FUNCIONALES 173
3.6. REQUISITOS NO FUNCIONALES 180
3.7. ESTRUCTURA DE BASE DE DATOS 183
3.8. ANÁLISIS FINANCIERO 185
3.9. GASTOS OPERATIVOS 187

ÍNDICE DE FIGURAS

Figura 1. Organigrama del Supermercado 18

Figura 2. Presentación de los principales desafíos de la cadena de suministro, cadena de suministro inteligente y cadena de suministro del futuro 34

Figura 3. Gráfica de la prioridad del responsable de la cadena de suministro 32

Figura 4. Representación de en donde se centra la cadena de suministro 33

Figura 5. Cinco retos de la cadena de suministro 34

Figura 6. Grado de Implantación de las "Mejores Prácticas" de Integración Líderes vs. Seguidores 35

Figura 7. Gestión del Riesgo 36

Figura 8. Visión de Futuro de Gestión de Riesgo 38

Figura 9. Cadenas de suministro más inteligentes "escuchan al cliente" 39

Figura 10. Cadenas de suministro más inteligentes "escuchan al cliente" visión de futuro 40

Figura 11. Prácticas "verdes" o de sostenibilidad del medio ambiente 41

Figura 12. Representación gráfica del concepto trazabilidad 59

Figura 13. Un Ejemplo de Blockchain con Contratos Inteligentes 60

Figura 14. Conceptos claves de la cadena de bloques para el negocio 69

Figura 15. Representación gráfica de centralizada a sistema distribuido 85

Figura 16. Protocolo Blockchain de Bitcoin 89

Figura 17. Generación de un hash de encabezado de bloque "timestamped" SHA256 92

Figura 18. Representación de un proceso de Smart Contract 106

Figura 19. Acciones sucesivas en el establecimiento y ejecución de un contrato inteligente 110

Figura 20. Sensor Sim 7000A 114

Figura 21. Sensor MCP9808 116

Figura 22. Arduino 123

Figura 23. SIM 7000 LTE CAT-M1/NB-IoT + GPS Shield Kit 126

Figura 24. Shield Armado + Arduino + Antena 127

Figura 25. Vista General de la Cadena de Suministros 131

Figura 26. Representación de una simple con solo dos validadores y dos procesadores de transacciones 135

Figura 27. Comunicación entre elementos a traves de protocolo HTTP 142

Figura 28. Arduino UNO WiFi (ESP8266) 143

Figura 29. Dispositivos Arduinos conectados a Hyperledger Sawtooth vía Protocolo HTTP 144

Figura 30. Arquitectura General de Amazon Web Services para la plataforma 152

Figura 31. Flujo del marco de trabajo de Scrum para un Sprint 158

Figura 32. Entorno de Desarrollo Integrado (IDE) IntelliJ IDEA 172

Figura 33. Diagrama de Caso de Uso para la Configuración de la Plataforma…….....172

Figura. 34, Diagrama de Caso de Uso para la Configuración de la Plataforma……173

Figura. 35, Diagrama de Caso de Uso para la Gestión del Almacén……174

Figura. 36, Diagrama de Caso de Uso para la Gestión de Inventario…….....175

Figura. 37, Diagrama de Caso de Uso para la Gestión de Fresco (Vegetales, Carnes)……..176

Figura. 38, Diagrama de Caso de Uso para la Gestión operativa del Supermercado…….177

Figura. 39, Diagrama de Caso de Uso para la Gestión operativo de proveedores…….178

Figura 40, Estructura de la Base de Datos de la Plataforma SCM.....181

ÍNDICE DE TABLAS

Tabla 1. Hyperledger Sawtooh, REST API HTTP Status Codes 138

Tabla 2. Presupuesto De Recursos necesarios Pos-Proyecto de servicios Plan 148

Tabla 3. Nomina General 188

Tabla 4. Nómina de empleados 190

Tabla 5. Nómina de empleados, desglosada mensualmente 196

AGRADECIMIENTOS

Agradezco en primer lugar a Dios, porque me ha dado fuerza de voluntad, enfoque y discernimiento para lograr todas las metas establecidas durante este trayecto.

En segundo lugar, a mi madre Ana Cáceres Liriano, porque ha sido ese motor de vida y soporte para superar todos los obstáculos y limitaciones de la vida. Le agradezco por orientarme a ser una persona exitosa y por educar e inculcarme valores humanos y cristianos, los cuales me han ayudado bastante para definir el camino que debo seguir.

A mi hermana Anneris Coplin y el resto de la familia, por siempre confiar en mí y ver en mí una persona Responsable, Apasionado y Dedicado a mi profesión.

Agradezco a mis amigos Brenda Ruiz, Saul Espino, Pilar Mireles y Amalie Serrano por siempre estar a mi lado, aconsejarme y apoyarme en todas mis decisiones y logros. Por último, agradezco a todas esas personas quienes directamente o indirectamente han influenciado en mi vida para ser en día quien soy.

Por último, agradezco al Prof. Santo Navarro por su gran aporte y a todos los profesores de la institución quienes de una forma u otra estuvieron incentivándonos hasta el final de nuestra meta.

- **Raymond Amado Coplin Cáceres**

En Primer Lugar, a Dios, quien me ha guiado en este largo camino y por darme todo lo que tengo, ya que sus planes siempre han sido mejores que los míos. Como también, por ayudarme a alcanzar una de mis metas de vida más importantes.

A mis padres Eddy Mireles y Yolanda Mateo, por haber inculcado en mí la fe en Dios, valores y deseo de superación, dándome su apoyo desde el comienzo hasta ahora. Quienes me enseñaron a valorar las cosas y a nunca pisotear a otros para subir, sino a ayudar a mi prójimo sin importar el cómo han sido conmigo y a aprender a desprenderme de mi orgullo para ser una mejor persona.

A mis 11 Hermanos, Misael Mireles, Richard Mireles, Sebastian Mireles, Irene Mireles, David Mireles, Patricia Mireles, Mariam Mireles, Miguel Mireles, Carlos Mireles, Alejandro Mireles y Yolanda Edith Mireles (Yoyi), por haberme dado ese apoyo incondicional, estando ahí en las buenas y en las malas, soportando mis cambios de humores, pero enseñándome siempre a ser mejor persona y ayudarme a cumplir esta meta.

A mi pareja Kenji Mukai, quien estuvo conmigo la mitad de este transcurso de carrera y que pude conocerlo gracias a la universidad, quien desde que lo conocí me motivó a ser mejor y quien hizo que me dé cuenta de mi potencial, cuando ni yo misma sabía que lo tenía, como también, fue una de las personas más influyente en mi vida, quien me inspiró a que siga luchando y él ha sido un ejemplo para mí.

A mi asesor de monografía el profesor Santo Navarro , quien tuvo la disposición y buena actitud de orientarnos en el desarrollo de este trabajo de investigación y en todo el ciclo de la carrera.

Finalmente, a mis compañeros Raymond Coplin y Pamir matos por ayudarme a concluir está etapa, ya que sin ellos no sería posible la realización de esta investigación,a mi Familia, a mis amigos y a todas aquellas personas que me apoyaron durante este trayecto, en especial a mi equipo de Bonanza y Negored, quienes me dieron la motivación de seguir creciendo en esta área tan demandante, cuando ser mujer en esta área era tan difícil de ver, pero estas personas creyeron en mi potencial.

- **María Del Pilar Mireles Mateo.**

A Dios, pues, aunque le conozco no hace mucho, su disciplina ha sabido encaminar mi vida por la gracia. A mi madre, roble fuerte que no ha dejado flaquear.

- **Pamir Matos.**

DEDICATORIA

Dedico este monográfico con mucho amor a mi madre Ana Altagracia Cáceres Liriano, quien es la persona más importante e influyente en mi vida. Le dedico este esfuerzo por su amor incondicional y por su sacrificio para verme lograr unas de las metas más importante de mi vida.

- **Raymond Amado Coplin Cáceres.**

Le dedico este monográfico a mi familia por apoyarme incondicionalmente desde que inicié este trayecto, a mi pareja, Kenji Mukai, a la familia de mi pareja, los muchos Mukai, a mis grandes amigos, Keisy Perez, Marielle Arzeno y Raymond Coplin, quienes me han acompañado desde el principio hasta ahora que culminó esta importante etapa.

- **María Del Pilar Mireles Mateo.**

Dedico este esfuerzo a todo aquel que ha servido y servirá como un firme adoquín en mi camino.

- **Pamir Matos.**

INTRODUCCIÓN

La administración de las cadenas de suministros (todo lo que tiene que ver con el entramado desde la creación hasta la distribución de bienes) es extremadamente compleja. Dependiendo del producto, una cadena de suministro puede abarcar cientos de etapas, múltiples ubicaciones geográficas, una multitud de facturas y pagos, tener varias personas y entidades involucradas, y pudiéndose extender por una gran cantidad de meses.

Las cadenas de suministro actuales se están deteriorando. Hace más de cien años, las cadenas de suministro eran relativamente simples porque el comercio estaba basado en un solo punto geográfico, pero ya se han vuelto increíblemente complejas. A lo largo de la historia de las cadenas de suministro han producido innovaciones tales como el cambio para transportar mercancías a través de camiones en lugar de ferrocarriles o la aparición de computadoras personales en la década de 1980 que condujeron a cambios drásticos en la gestión de la cadena de suministro. Dado que la fabricación se ha globalizado, las cadenas de suministro son pesadas con su propia complejidad.

Es increíblemente difícil para los clientes o compradores conocer realmente el valor de los productos porque hay una falta significativa de transparencia en el sistema actual. De manera similar, es extremadamente difícil investigar las cadenas de suministro cuando existe la sospecha de prácticas ilegales o poco éticas. También pueden ser muy ineficientes a medida que los compradores y proveedores intentan interconectar los puntos sobre quién necesita qué, cuándo y cómo.

Debido a la complejidad y falta de transparencia de las cadenas de suministro actuales, en este se utilizará la tecnología Blockchain para solventar los obstáculos. La Blockchain puede aumentar la eficiencia y la transparencia de las cadenas de suministro y tener un impacto positivo en todo, desde el almacenamiento hasta la entrega y el pago.

El presente trabajo de investigación tiene como fin la presentación de un modelo práctico para la implementación de Blockchain dentro de una cadena de suministro de un supermercado.

En cada capítulo de este documento se estará contemplando los siguientes temas:

Capítulo I - En este primer capítulo se detallan los antecedentes y situación actual de las cadenas de suministros en la República Dominicana, específicamente el área de manejo de alimentos de los supermercados, mostrando una visión a grandes rasgos donde se muestran cuáles son los procesos, funciones, normas, leyes y regulaciones.

Capítulo II - En este segundo capítulo se definen y desarrollan los conceptos utilizados para el desarrollo del modelo. Se detallan granularmente los aspectos técnicos que son requeridos para el entendimiento de la propuesta y la implementación del modelo, así como las características de los periféricos que serán utilizados.

Capítulo III - En este capítulo final se explicará la solución propuesta, haciendo hincapié en las tecnologías utilizadas para su correcto desarrollo, como será la arquitectura necesaria junto a sus requerimientos, diagramas, metodologías y así como también, el análisis financiero.

CAPÍTULO I
ANTECEDENTES Y ASPECTOS GENERALES

1. ANTECENDETES Y ASPECTOS GENERALES

Una cadena de suministro es la red de todos los individuos, organizaciones, recursos, actividades y tecnología involucrados en la creación y venta de un producto, desde la entrega de materiales de origen del proveedor al fabricante, hasta su entrega final al usuario final.

"La Gestión de la Cadena de Suministro (SCM) se refiere a la coordinación de la producción, inventario, ubicación y transporte entre los participantes en una cadena de suministro para lograr la mejor combinación de capacidad de respuesta y eficiencia para el mercado que se atiende". (Hugos, 2003)

Se puede definir una Cadena de Suministros como el flujo de materias primas transformadas en productos terminados hasta que un consumidor final las adquiere. La administración de la cadena de suministro(SCM) es quien determina todo el proceso llevando la cantidad correcta al lugar correcto en el momento adecuado.

1.1. SITUACIÓN ACTUAL DEL LA CADENA DE SUMINISTRO DE LOS SUPERMERCADOS DE LA REPÚBLICA DOMINICANA

A lo largo del siglo XX las cadenas de suministros han evolucionado para enfrentarse a los grandes desafíos del mercado globalizado. En la actualidad, en la República Dominicana todavía las empresas conviven con muchas problemáticas debidas a la falta de interacción y comunicación con sus socios y proveedores.

En una entrevista con un gerente de distribución de las unas de las principales cadenas de supermercados del país, indicó que, las cadenas de supermercados no cuentan con un Sistema de Gestión de Cadena de Suministros de Alimentos trazable sino más bien se llevan a cabo un conjunto de procesos y prácticas manuales con la cuales se logra el abastecimiento.

Debido a la informalidad en el que se desarrolla el mercado en la República Dominicana los supermercados no cuentan con una visibilidad completa de todo el proceso por lo que es difícil cubrir el cien por ciento, mientras que si se tiene un control de todo lo que se almacena como importaciones en los centros de almacenes y eso es más o menos el 50% del abastecimiento. Los proveedores más dificultosos de darle seguimiento son los que proveen productos frescos, vegetales y frutos.

En los centros de distribución hay todo un proceso de filtro de calidades, sobre todo personal experimentado que han recibido diversas capacitaciones en los niveles de calidad, hay departamentos de calidad que

se ocupa de que los estándares se cumplan al recibir la mercancía, ya sea lotes, fechas de caducidad y sin son productos perecederos la calidad de frescura y demás.

Hay diversos puntos de mejora, lo primero es que los proveedores deben de mejorar sus data y debe ser más formales en cuanto a saber su disponibilidad, muchas veces la empresa le piden mercancía y son muy incumplidores con sus servicios y eso repercuta en abastecimiento de los supermercados, como también en el trato de la mercancía en cómo debe llegar para cuando esta sea recibida pueda ser transportada a los supermercados de manera ágil, pero esta suele ser muy inusual y muy informal, bravo creó un manual de entrega a los proveedores y eso es a cada momento devolviendo camiones, porque se tiene la costumbre de que la mercancía llegue en un camión de tres gente y la mercancía esté puesta en el piso y cuando vienen con la mercancía arman todo en el momento mientras que el bravo solo te permite traer la mercancía paquetizada, con el chofer y con factura, eso ayuda un poco a recibir productos con calidad.

En los supermercados existen estándares establecidos con proveedores de acuerdo con la línea de productos, por ejemplo: los vegetales se manejan con una temperatura muy diferente en lo que se maneja un lácteo o un helado, hay proveedores que van más allá, que se ocupan desde la transportación hasta el almacenamiento y hasta el producto recibido, porque tienen que cuidar su marca, que es la que está exponiendo en el supermercado pero la marca sigue siendo de ellos y tienen que valorarla.

Se hizo un encuesta a 108 personas, con la cual se pudo determinar que todos prefieren el supermercados bravo por la calidad, que los otros supermercados planteado en la encuesta y hoy en día en república dominicana no existe un supermercado que este implementando tecnología blockchain y esto se debe por la falta de conocimiento, porque hoy en día se conoce de esta tecnología utilizada en estados unidos en la empresa Walmart, Nestlé, Unilever, Tyson Foods, Kroger y Dole Food Company por el momento.

“La tecnología Blockchain permite una nueva era de transparencia de extremo a extremo en el sistema alimentario mundial, equivalente a iluminar a los participantes del ecosistema alimentario, que promoverá más acciones y comportamientos responsables”, dijo Frank Yiannas, vicepresidente de seguridad alimentaria de Walmart, en un comunicado de prensa.

En la siguiente figura se encuentra el organigrama actual del supermercado Nuevo Amanecer, de la gestión de la cadena de suministro:

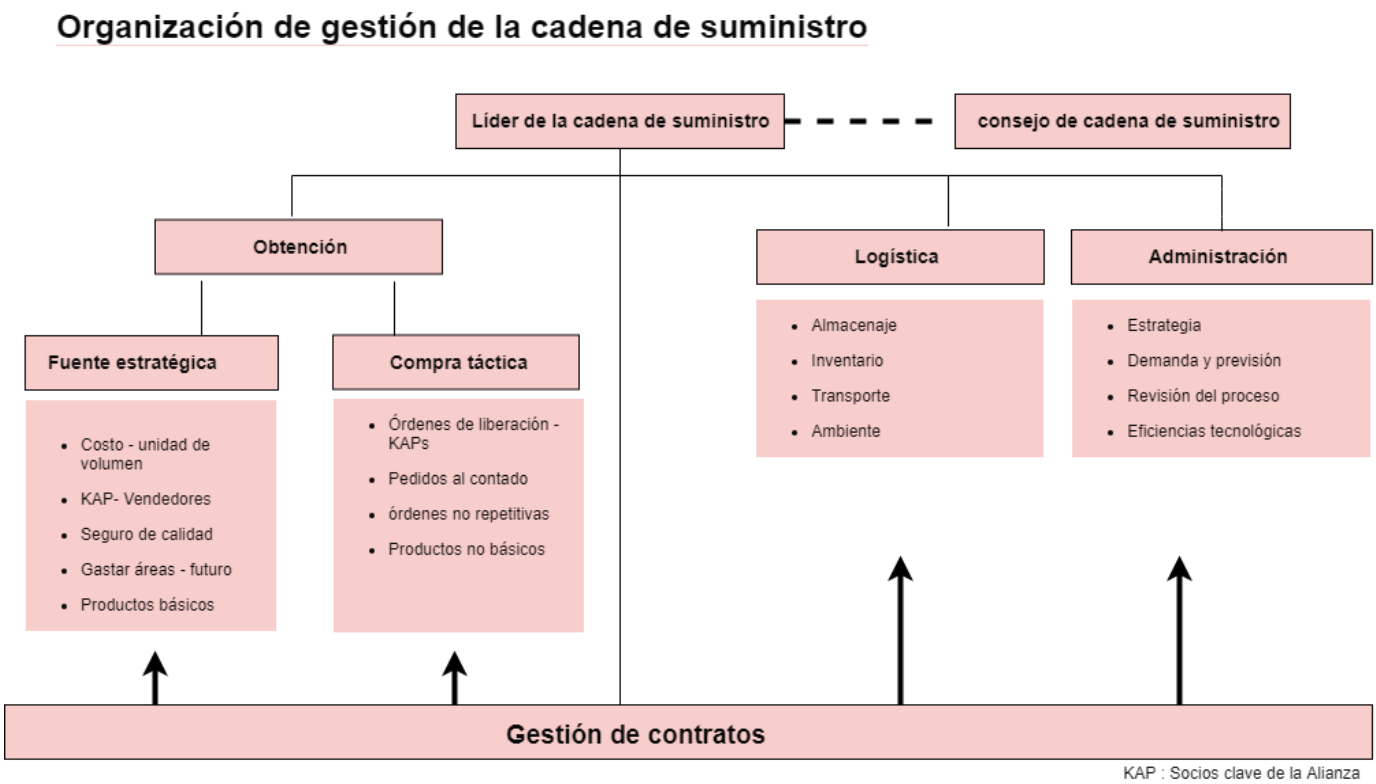


Fig. 1, Organigrama del Supermercado.
Fuente: Propia

En la fig. #1 se puede visualizar el organigrama del supermercado Nuevo Amanecer, donde es definido cada puesto de los responsables de que la cadena de suministro, como también las tareas correspondiente a cada uno.

1.2. LEY GENERAL DE SALUD 42-01

Disposiciones de la Ley de Salud 42-01, que son relevantes para el desarrollo de esta investigación:

Del capítulo III:

Art. 127.- La producción, la elaboración, el almacenamiento, la fabricación, la importación, el comercio en todas sus formas, el transporte, la manipulación, el suministro a cualquier título, y el expendio de productos alimentarios quedan sujetos a las disposiciones de esta ley, de sus reglamentos y de las resoluciones emanadas de la SESPAS. Estas disposiciones deberán establecer criterios y definiciones oficiales a fin de garantizar que estos alimentos sean sanos, aptos para el consumo humano, con calidad nutritiva y provengan de establecimientos autorizados por SESPAS.

Art. 130.- Todo alimento o bebida que no se ajuste a las condiciones señaladas en esta ley o sus reglamentaciones, será retirado de la circulación, destruido o desnaturalizado, por la Secretaría de Estado de Salud Pública, sin desmedro de las atribuciones de otras instituciones competentes, a fin de impedir su consumo; sin más requisito que la sola comprobación de su, mala calidad, levantándose acta de su decomiso o destrucción.

Art. 155.- Constituyen delitos y se castigarán con pena de tres (3) meses a dos (2) años de prisión correccional o con multas que oscilarán entre quince y veinticinco veces el salario mínimo nacional,

establecido por la autoridad legalmente competente para ello o por la ley; o ambas penas a la vez, las siguientes infracciones:

13.- Fabricar, manipular, transportar, almacenar, importar, exportar, alquilar, distribuir, comercializar o suministrar, en cualquiera de sus formas, medicamentos, alimentos y bebidas no aptos para el consumo por no responder a los requerimientos o condiciones fijadas en los reglamentos de la presente ley y normas vigentes sobre la materia. Además, por su comercialización sin cumplir con los requisitos previstos por esta ley para la etiquetación de los citados productos.

1.2.1. REGLAMENTO GENERAL PARA CONTROL DE RIESGOS EN ALIMENTOS Y BEBIDA EN LA REPÚBLICA DOMINICANA

Título 1: Disposiciones Generales y Denominaciones,

Capítulo 1: Los Objetivos del Reglamento

Art. 1.- Los objetivos del presente Reglamento son los siguientes:

a) Establecer y hacer cumplir las disposiciones sanitarias en el proceso de producción y comercialización de alimentos y bebidas para consumo humano.
b) Controlar los riesgos para la salud generados por el inadecuado uso de aditivos contaminantes o toxinas, así como por la presencia de organismos causantes de enfermedades.

Art. 2.- Las disposiciones del Reglamento tienen alcance nacional y son de aplicación obligatoria en todos los establecimientos que producen y comercializan alimentos y/o bebidas, así como para toda persona física o jurídica que se dedique a la importación y comercialización de productos alimentarios.

Art 18.- Se entenderá por "ALIMENTO CONTAMINADO" gérmenes patógenos, sustancias químicas o radioactivas, toxinas o parásitos capaces de producir o transmitir enfermedades al hombre.

Título VI: De Las Especificaciones, Capitulo: XVIII: De los Pescados y Mariscos Frescos

Artículo 198.- Los Pescados y Mariscos son las especies comestibles, marinas o fluviales, destinadas a la alimentación humana.

Artículo 199.- El Pescado Fresco deberá expenderse con el nombre que le es propio y en adecuadas condiciones de conservación, cumpliendo con los siguientes requisitos: los ojos deben conservar su claridad y transparencia; la piel y la escama serán brillantes y firmes; las agallas son de color rojo y la carne será consistente y elástica, debiendo desaparecer rápidamente de ella la huella que se deja al comprimirla con el dedo.

Artículo 200.- Los Pescados y Mariscos que se expendan en estado fresco, además de las condiciones de los alimentos en general, deberán cumplir las siguientes condiciones específicas:

a) No deberán tener sustancias conservadoras, salvo aquella autorizada por la SESPAS a través de su unidad técnica;
b) No deberán contener sustancias colorantes, nitritos ni nitratos;
c) No deberá presentar signos de enfermedades ni contener parásitos;
d) No deberán estar en mal estado de conservación;
e) No deberán estar mutilados, traumatizados o deformado en cuanto al aspecto, olor y sabor repugnantes.

Artículo 201.- El almacenamiento y expendio de los pescados y mariscos, sólo deberá efectuarse en locales que reúnan las condiciones señaladas en el presente Reglamento.

Artículo 202.- En los puertos y demás lugares de la costa en que se realicen labores de pesca, se permitirá el comercio ambulatorio de pescado y mariscos, siempre que su distribución y expendio al público esté autorizado por la SESPAS.

Artículo 203.- Los pescados podrán transportarse solamente en envases adecuados debidamente acondicionados con hielo troceado o molido. La proporción de hielo no será inferior a 0.5 kilogramo por cada kilogramo de pescado.

Artículo 204.- Se considera pescado refrigerado el pescado fresco previamente limpio y eviscerado que ha sido sometido a conservación por el frío a temperatura comprendida entre 0 y 5º C durante 48 horas como máximo.

Artículo 205.- Se considera pescado congelado el pescado fresco previamente limpio y eviscerado que ha sido sometido a conservación por el frío a temperatura inferior a 2° C durante un plazo que permita su congelación a fondo.

Título VI: De las Conservas, Capítulo: III: De las Conservas de Origen Animal

Párrafo I- De las Conservas de Pescados y Mariscos. Para la elaboración de ellas debe emplearse pescado fresco, sano y en buen estado de conservación.

PÁRRAFO II.- Se prohíbe el empleo de mariscos muertos, o previamente desvaluados, en la elaboración de tales conservas.

Título IV: De la Protección y Manipulación de los Alimentos, Capítulo I: De la Protección

Artículo 429.- Los alimentos y bebidas serán guardados, exhibidos y manipulados de tal modo que estén siempre protegidos de contaminación y daños por roedores o insectos.

Artículo 430.- Los alimentos perecederos deberán conservarse y mantenerse por medio del frío o de cualquier otro método de preservación autorizado por la SESPAS a través de su unidad técnica.

Artículo 431.- El fraccionamiento de los alimentos deberá realizarse por medio de equipos adecuados y por procedimientos que aseguren su protección.

Título IV: De la Protección y Manipulación de los Alimentos, Capítulo II: De los Manipuladores

Artículo 432.- Entiéndase por "MANIPULADOR DE ALIMENTOS" toda persona que trabaje, a cualquier título y aunque sea ocasionalmente, en un local o establecimiento, o en el comercio ambulante, donde se produzcan, almacenen, distribuyan o expendan alimentos.

Artículo 433.- Los manipuladores de alimentos estarán sujetos a las siguientes obligaciones:

a) Poseer la autorización vigente de la SESPAS a través de su unidad técnica y exhibirla cuando ésta le sea solicitada.
b) Estar libres de enfermedades infectocontagiosas.
c) Mantener un perfecto aseo corporal y en especial de las manos. No se permitirá mantener las uñas largas ni cubiertas de barniz.
d) Usar uniforme completo de color claro, incluido el gorro, en perfectas condiciones de conservación y aseo, y guantes, cuando el caso lo requiera.
e) Dentro del recinto de trabajo no se permitirá fumar ni escupir.
f) Se prohíbe al manipulador atender los pagos del público, recibiendo o entregando dinero.

Título IV: De la Protección y Manipulación de los Alimentos, Capítulo II: De los Vehículos de Transporte de Alimentos

Artículo 453.- Los furgones, camiones y otros compartimentos de los vehículos destinados a transporte de alimentos deberán cumplir, al menos, con los siguientes requisitos:

a) Estar convenientemente cerrados para evitar las contaminaciones;
b) Estar forrados interiormente con material inoxidable e inatacable;
c) Contar con adecuada ventilación e iluminación;
d) Ser fácilmente lavable en su interior y contar con desnivel para el drenaje del agua;
e) Ser mantenido permanentemente en buen estado de aseo y conservación.

PÁRRAFO I.- No se incluyen en esta disposición los vehículos destinados a transporte de productos agropecuarios en su estado natural.

Artículo 454.- El transporte de la leche y los productos lácteos, las carnes, el pescado, los mariscos y el hielo sólo podrá hacerse en vehículos exclusivamente destinados a dicho objeto.

Artículo 455.- Los vehículos interprovinciales de transporte de leche, carne, pescado y mariscos deberán contar con un sistema adecuado de refrigeración.

Cada uno de estos capítulos y artículos hacen entender que existen un régimen de consecuencias/medidas que difícilmente pueden llevarse a cabo por la falta de transparencia en los procesos actuales.

Con un buen sistema de trazabilidad como el planteado en este modelo estas medidas pueden en forzar y así, garantizar que la población pueda consumir bienes nutricionales que aporten al desarrollo de cada individuo.

1.3. LAS CADENAS DE SUMINISTROS INTELIGENTES

Hoy en día se dice que las cadenas de suministro serán más complejas, pero a la vez más global.

David Soto, vicepresidente de IBM Global Business Services (2009) dice que los principales desafíos de la cadena de suministro son:

Actual:

El 55% se basa en la contención de los costes donde los principales responsables de la cadena de suministro de la empresa consideran la contención de costes como su responsabilidad número uno y luego se encuentra la visibilidad de la cadena de suministro con 70% donde la mayoría de las empresas no tienen una visibilidad completa de su cadenas de suministro, también está la parte de la gestión de riesgo con un 60% donde esté nos deja ver claramente de que este empieza siendo el más preocupante, sin embargo no está formado parte de la mitigación del día a día. Entre otras cosas podemos notar que se debe de esperar un cliente más exigente en lo cual gráficamente este tiene un 56% que nos indica que la mayoría de las empresas no toman en cuenta a sus clientes y por último tenemos la globalización con un 43% el cual nos indica **David Soto, vicepresidente de IBM Global Business Services (2009)** que la crisis y la globalización empujan a las empresas a comprar y relocalizar más en países de bajo coste.

En la siguiente figura se encuentra la representación de los principales desafíos de la cadena de suministro, como esta estará preparada de acuerdo con la época en que se está viviendo junto a la tecnología y con una mira al futuro de lo que será la cadena de suministro y como esta será una cadena más inteligente :

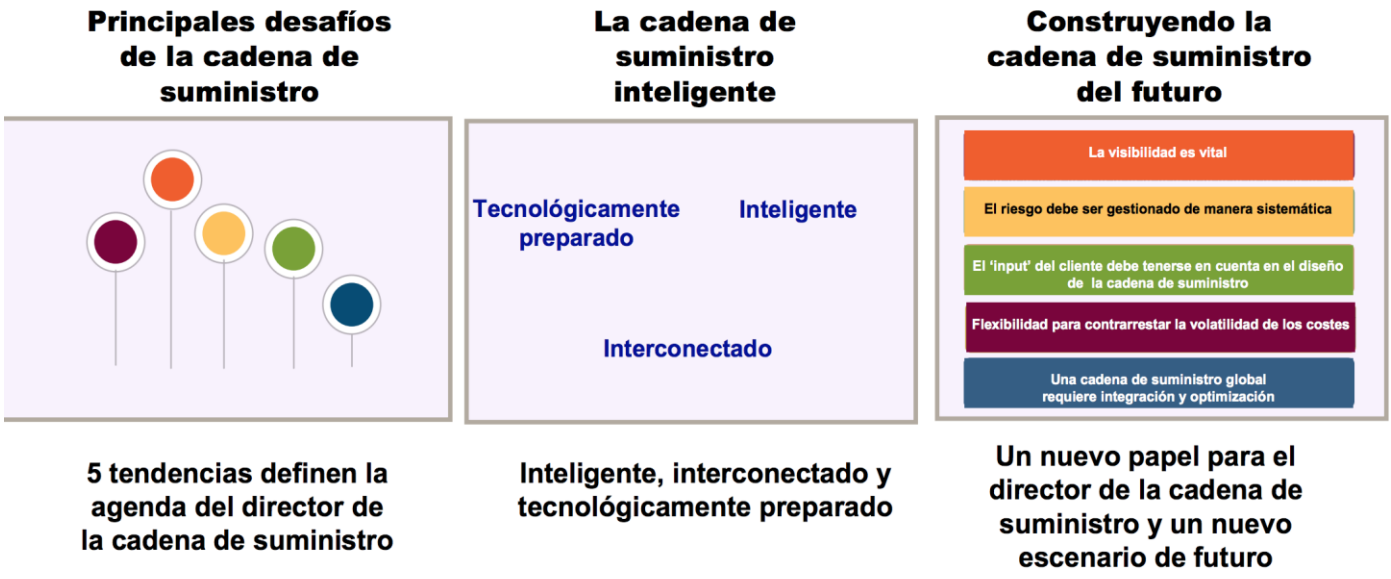


Fig. 2 Presentación de los principales desafíos de la cadena de suministro, cadena de suministro inteligente y cadena de suministro del futuro
Fuente: (Soto and Rovira, 2009)

En la figura #2 se encuentra lo que en el mañana se espera de la cadena de suministro, como lo que en épocas atrás era importante, hoy ya no es tan relevante, en esta nueva alternativa de mejora, se podrá notar la participación de cada una de las personas que intervienen en la cadena de suministro y cómo mejorar la visibilidad de un 70%, a un 100% de visibilidad de esa trazabilidad.

LA CADENA DE SUMINISTRO INTELIGENTE DEL FUTURO:

Juan Miguel Rovira, director de soluciones para la cadena de suministro de IBM (2009) dice que la contención de costes será, aún más, la prioridad del responsable de la cadena de suministro.

En la figura #3 se encuentra la representación de prioridad del responsable de la cadena de suministro:

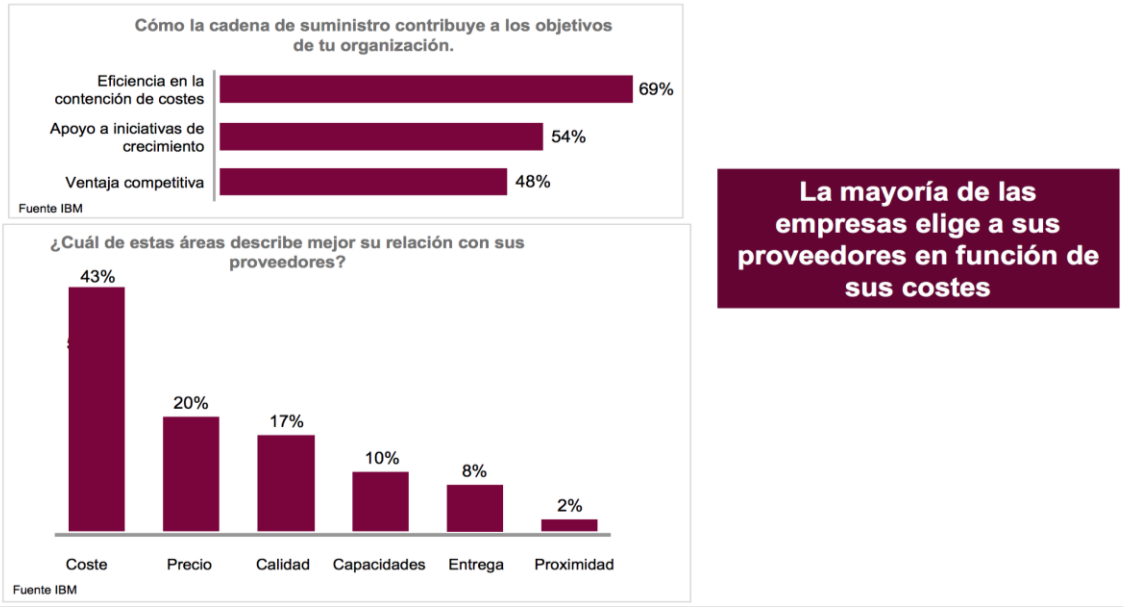


Fig. 3, Gráfica de la prioridad del responsable de la cadena de suministro
Fuente: (Soto and Rovira, 2009)

Desde que una persona decide abrir lo que es un negocio, su principal elección a la hora de elegir un proveedor es el coste del producto, porque con esto pueden determinar la ganancias que pueden sacarle a dicho producto, ya que este es el valor monetario de una compra que va destinada a una actividad económica de producción de un bien, como también de un servicio o una actividad, entonces con esta nueva propuesta se puede eficientizar la elección de proveedores no solo en

su coste, sino también en precio, calidad, capacidades, entrega y proximidad.

Las cadenas de suministro más inteligentes se centran en:

- ➢ Flexibilidad (con estructuras de costes variables) .
- ➢ Agilidad (para responder rápidamente a los cambios del mercado).

Entonces, teniendo en cuenta lo que se mencionó anteriormente en la Fig. 4, se encuentra la Representación de en donde se centra la cadena de suministro:

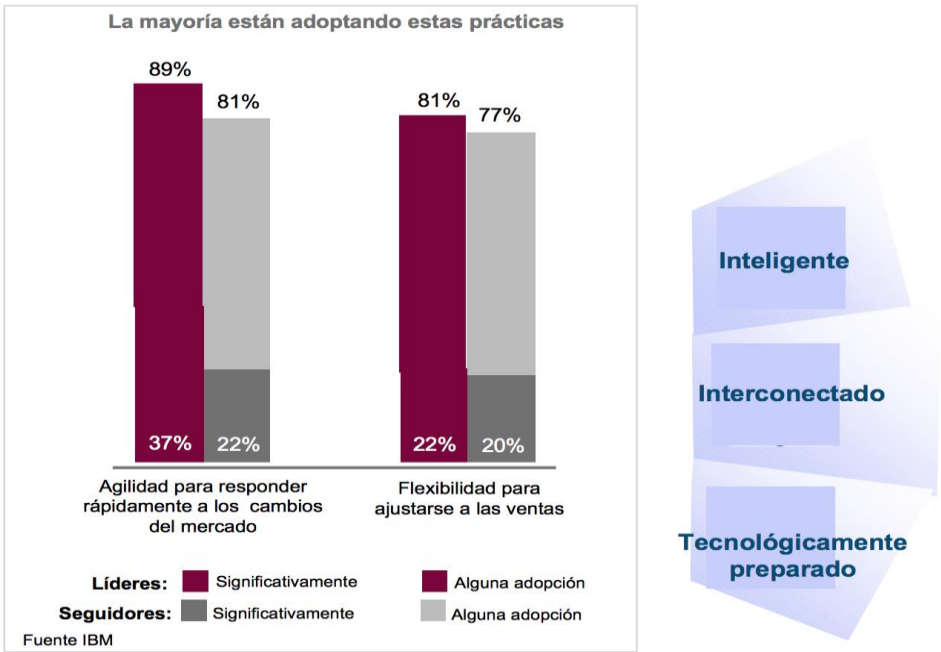


Fig. 4, Representación de en donde se centra la cadena de suministro Fuente (Soto and Rovira, 2009)

Hay que tener en cuenta que existen algunas razones por las cuales las empresas no tienen visibilidad de su cadena de suministro,

pero es mayormente porque existen barreras organizativas y falta de incentivos para colaborar, como también el compartir información.

Es por eso que en la siguiente gráfica se puede ver los Cincos retos de la cadena de suministro:

Fig. 5, Cincos retos de la cadena de suministro
Fuente: (Soto and Rovira, 2009)

En la figura #5 se tome cuenta lo que dice el autor de este artículo, en cual le crea cuestionantes a la persona que lee esto y que a la vez lo pone a pensar, si esa es la razón por la cual está ocurriendo ese problema, porque no se empieza a compartir estas informaciones, porque aún no se han roto esas barreras, es por eso que en el siguiente párrafo se puede leer lo que se espera de esta cadena de suministro del futuro.

Visión de futuro:

La cadena de suministro inteligente requerirá una mayor conectividad, colaboración e integración de procesos entre la red de "partners" para mejorar la visibilidad. Juan **Miguel Rovira, director de soluciones para la cadena de suministro de IBM (2009)**.

La siguiente gráfica representa lo que es el Grado de Implantación de las "Mejores Prácticas" de Integración Líderes vs. Seguidores:

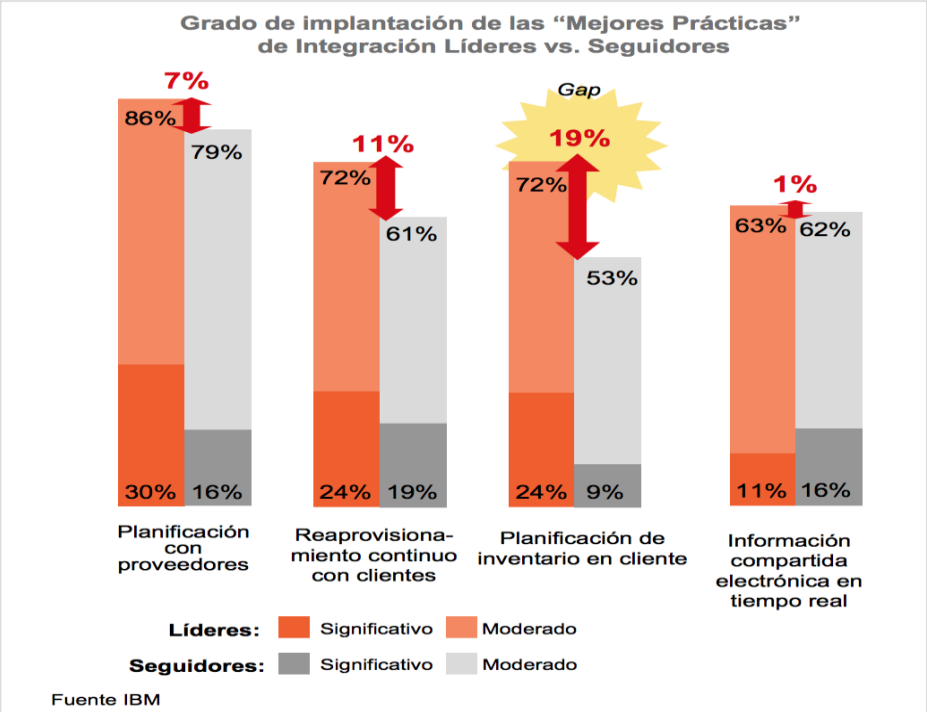


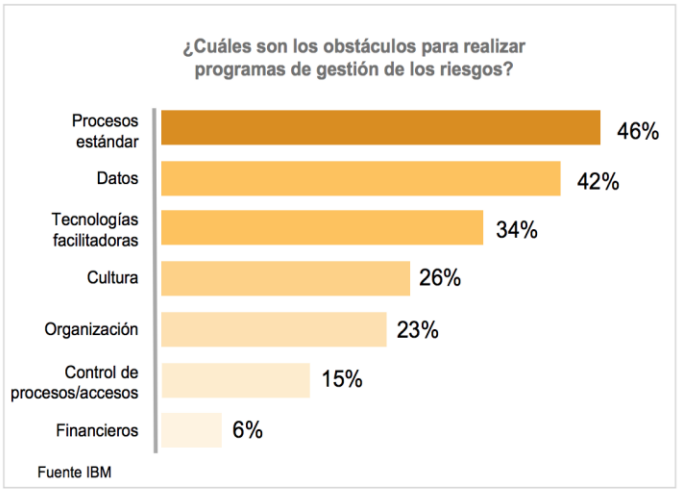
Fig. 6, Grado de Implantación de las "Mejores Prácticas" de Integración Líderes vs. Seguidores
Fuente: (Soto and Rovira, 2009)

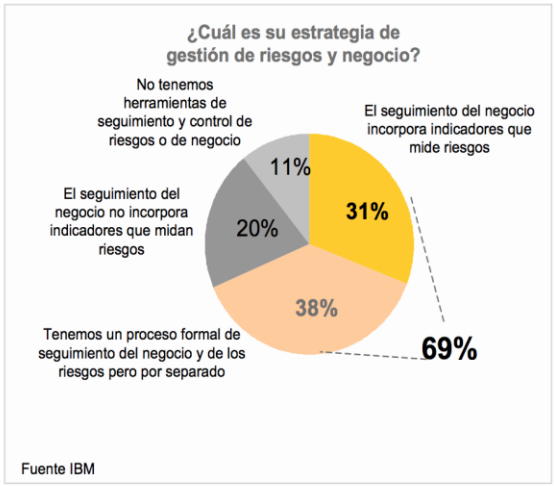
En la figura #6 se ve como se ha estado tratando de implementar las mejores prácticas y cómo dependiendo de los actores que están presentando esta, cada uno le ponen más importancia a la cual ellos creen que es la verdadera prioridad.

Gestión de Riesgo:

Es un planteamiento estructurado para tener un buen manejo frente a la inseguridad que aparece referente a una amenaza, a través de un orden de actividades humanas que implican una exhaustiva evaluación de riesgo, estrategias de preparación para manejarlo y por último una mitigación del riesgo utilizando herramientas para está, junto a recursos gerenciales.

En la siguiente figura se puede visualizar una gráfica de la gestión de riesgo de la cadena de suministro:





El 69% gestiona el riesgo de alguna manera

Fig. 7, Gestión del Riesgo
Fuente: (Soto and Rovira, 2009)

El 69% de las empresas gestionan el riesgo de alguna manera según las necesidades que esté presente. La mayoría tienen un proceso formal de seguimiento del negocio y de los riegos por

separado, otros prefieren darle seguimiento a el negocio, pero dejando afuera un indicador que mida el riesgo, sino que esperan a que suceda, existen otros que tampoco cuenta con una herramienta, lo cual con la solución propuesta se va a erradicar ese tipo de situación.

Visión de futuro:

Las empresas líderes planifican la cadena de suministro teniendo en cuenta los riesgos a priori, gracias a tecnologías que los monitorizan continuamente. **Juan Miguel Rovira, director de soluciones para la cadena de suministro de IBM (2009)**. En la siguiente figura se puede visualizar una gráfica de la Visión de Futuro de la Gestión de Riesgo:

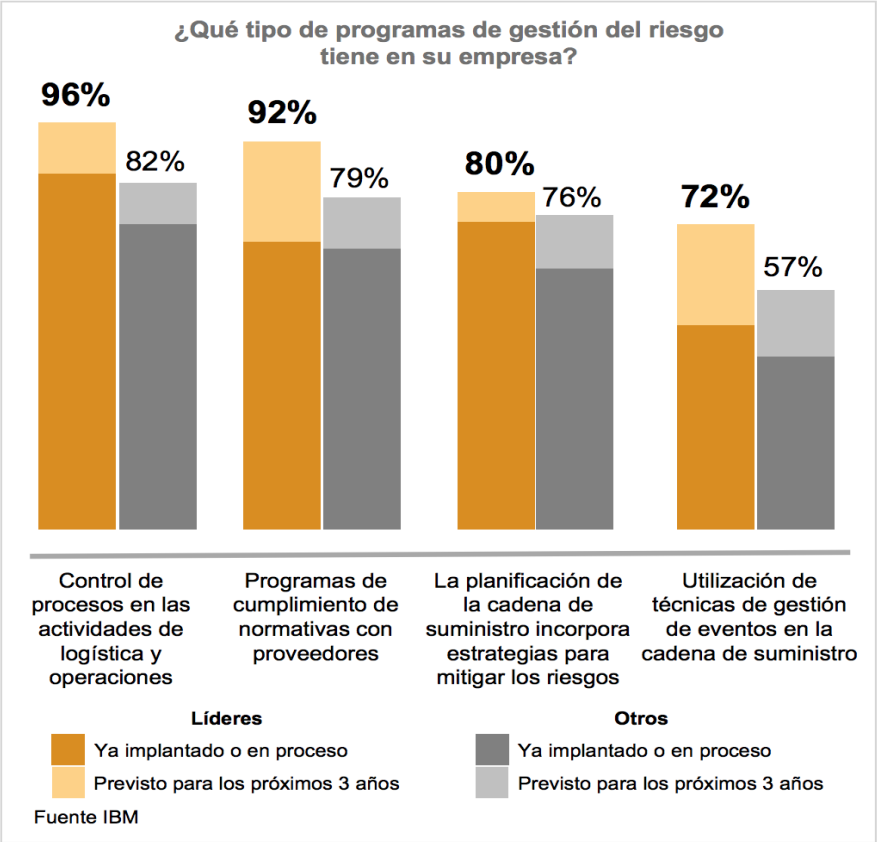


Fig. 8, Visión de Futuro de Gestión de Riesgo
Fuente: (Soto and Rovira, 2009)

Las empresas hoy en día tienden a centrarse más en sus proveedores que en sus clientes, entonces no escuchan la demanda de sus clientes.

En la siguiente figura se puede visualizar una gráfica de una cadena de suministro más inteligentes, en la cual se esfuerza por escuchar más al cliente y la cual se espera cambiar la cadena de suministro de hoy en día, en donde se tiene de mentalidad el centrarse más en sus proveedores y no en sus cliente, en la visión del futuro de esta se espera que sea el cliente el escuchado, una cadena de suministro donde "escuchan al cliente":

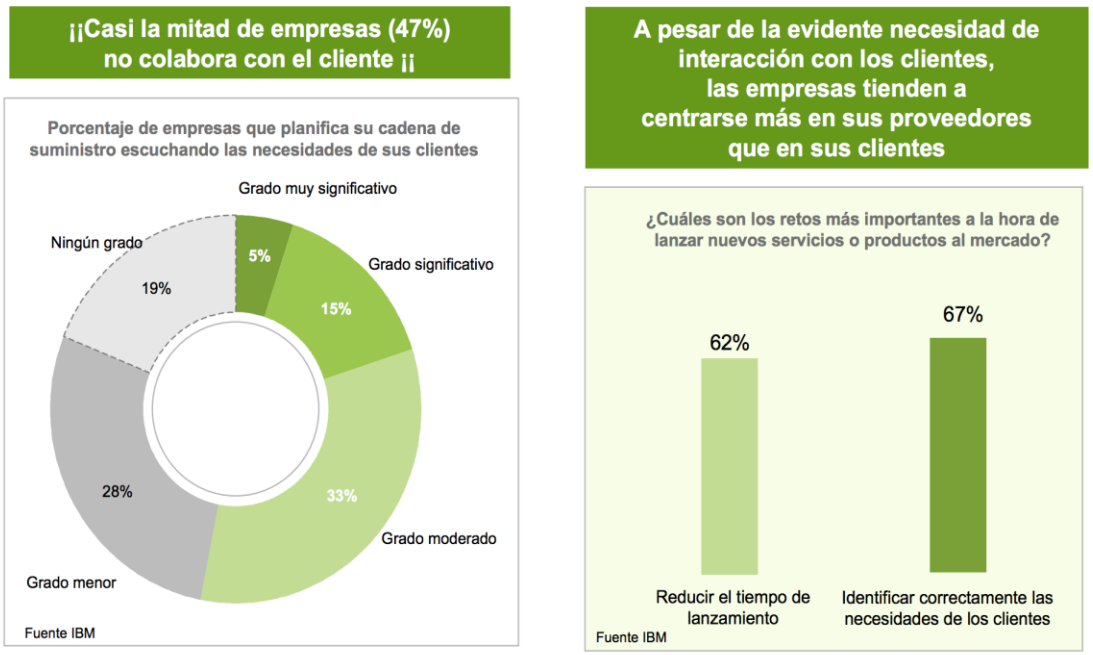


Fig. 9, Cadenas de suministro más inteligentes "escuchan al cliente"
Fuente: (Soto and Rovira, 2009)

Visión de futuro:

Las cadenas de suministro más inteligentes “escuchan al cliente” durante todo el ciclo de vida del producto: desde su concepción hasta su entrega al cliente.

En la siguiente figura se puede visualizar una gráfica de la Cadenas de suministro más inteligentes “escuchan al cliente” visión de futuro:

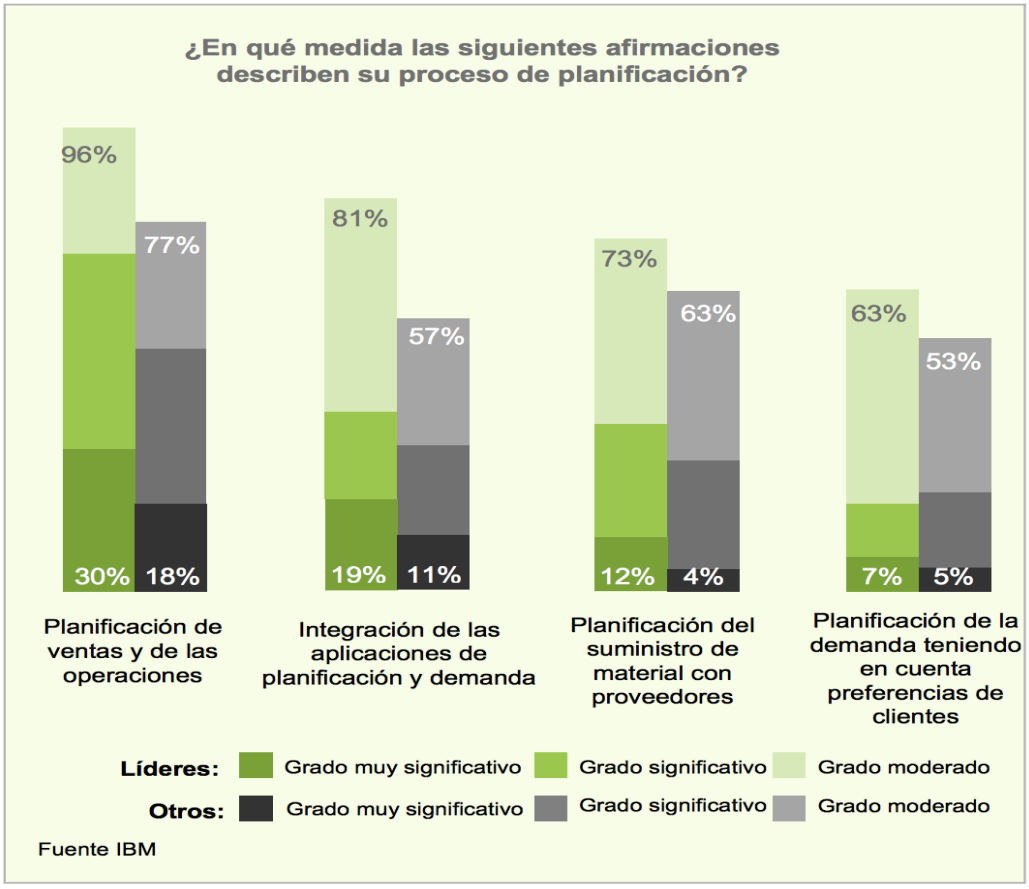


Fig. 10, Cadenas de suministro más inteligentes “escuchan al cliente” visión de futuro. Fuente: (Soto and Rovira, 2009)

Visión de futuro: Las redes de suministro inteligentes necesitarán ser más eficientes ya que actualmente no han conseguido su objetivo de reducción de costes con la globalización. La globalización ha permitido a las empresas mejorar sus márgenes, pero no sus costes en el nivel previsto, con fallos como la falta de calidad o incumplimiento de los compromisos. **Juan Miguel Rovira, director de soluciones para la cadena de suministro de IBM (2009)**.

El impacto en el medio ambiente: A pesar de que no serán viables las cadenas de suministro que no tengan en cuenta el medio ambiente, sólo un 37% de los directivos lo considera actualmente un desafío.

En la siguiente figura se puede visualizar una gráfica de la Prácticas “verdes” o de sostenibilidad del medio ambiente:

Fig. 11, Prácticas “verdes” o de sostenibilidad del medio ambiente. Fuente: (Soto and Rovira, 2009)

El responsable de la cadena de suministro debe asumir un nuevo papel en la orquestación de todos los recursos de la cadena de suministro y debe conectar con otros líderes y grupos.

La necesidad de una nueva organización: El reto es construir el rol de un director global, que tenga la visión completa y que gobierne todas las áreas que componen la cadena de suministro y en cada geografía.

El director de la cadena de suministro del futuro:

- Un papel crítico y crucial para continuamente buscar el equilibrio, optimizar y “orquestar” recursos mundiales.
- Es el optimizador de la organización.
- Requiere habilidades de negociación, capacidad de gestión con stakeholders, conocedor de la estrategia de la cadena de suministro y su ejecución y conocimiento del mercado.
- Incluye las funciones del anterior director de compras y director de operaciones, junto con funciones de ventas y marketing, finanzas alineado con el aprovisionamiento, operaciones y logística.

1.4. BLOCKCHAIN COMO TECNOLOGÍA DISRUPTIVA

Blockchain es un libro de contabilidad electrónico público o privado que puede ser compartido abiertamente entre usuarios dispares y que crea un registro inalterable de sus transacciones, cada una de ellas sellada en el tiempo y vinculada a la anterior. Cada registro o transacción digital en el hilo se llama un bloque (de ahí el nombre), y permite que un conjunto abierto o controlado de usuarios participe en el libro de contabilidad electrónico. Cada bloque está vinculado a un participante específico.

La cadena de bloques sólo puede actualizarse por consenso entre los participantes en el sistema y, cuando se introducen nuevos datos, nunca pueden borrarse. La cadena de bloques contiene un registro verdadero y verificable de todas y cada una de las transacciones realizadas en el sistema.

Como una red peer-to-peer, combinada con un servidor distribuido de estampación de tiempo, los libros de bloque pueden ser administrados autónomamente para intercambiar información entre partes dispares. No hay necesidad de un administrador. En efecto, los usuarios de Blockchain son los administradores.

Además, las redes de cadenas de bloques pueden utilizarse para "contratos inteligentes" o scripts que se ejecutan automáticamente cuando se cumplen ciertas condiciones. Por ejemplo, los usuarios del intercambio Ethereum Ether deben cumplir con

condiciones predeterminadas que prueban que alguien es dueño de la “cryptocurrency” y tiene autoridad para enviar el dinero que dicen poseer. Además, los usuarios de múltiples cadenas de bloques pueden crear contratos que requieren más de un conjunto de entradas para desencadenar una transacción.

Si bien ningún sistema es "imposible de piratear", la simple topología de la cadena de bloques es la más segura hoy en día, según Alex Tapscott, CEO y fundador de Northwest Passage Ventures, una firma de capital de riesgo que invierte en compañías de tecnología de cadenas de bloques.

"Para poder mover cualquier cosa de valor sobre cualquier tipo de cadena de bloqueo, la red [de nodos] debe primero estar de acuerdo en que esa transacción es válida, lo que significa que ninguna entidad por sí sola puede entrar y decir de una forma u otra si ocurrió o no una transacción", dijo Tapscott. "Para hackearlo, no tendrías que hackear un sistema como en un banco, tendrías que hackear todos y cada uno de los ordenadores de esa red, que está luchando contra eso."

Los recursos informáticos de la mayoría de las cadenas de bloques son tremendos, apuntó Tapscott, porque no se trata de una sola computadora, sino de muchas. Por ejemplo, la cadena de bloques Bitcoin aprovecha entre 10 y 100 veces más potencia informática que todas las granjas de Google juntas.

Envíos, Fintech, Salud, Energía. Las cadenas de bloques están siendo utilizadas para una amplia variedad de usos en varias industrias. (Más recientemente ha sido promocionado como una forma de intercambiar créditos de carbono.)

En el transporte marítimo, por ejemplo, un conocimiento de embarque para envíos de carga ha sido tradicionalmente basado en papel, lo que requiere múltiples aprobaciones por parte de inspectores y receptores antes de que las mercancías puedan ser entregadas. Incluso cuando el sistema es electrónico, todavía requiere que múltiples partes firmen los embarques de carga, lo que crea un largo proceso administrativo.

Para tratar de agilizar ese engorroso proceso, el mayor operador de transporte de contenedores del mundo, Maersk, anunció en marzo de 2017 que está utilizando un libro de contabilidad basado en una cadena de bloques para gestionar y rastrear el rastro en papel de decenas de millones de contenedores de transporte mediante la digitalización de la cadena de suministro. Y Maersk ahora se ha asociado con IBM en una nueva plataforma de envío electrónico basada en una cadena de bloques. Se espera que esté en funcionamiento más adelante en 2018.

Cada participante en la cadena de suministro de envío puede ver el progreso de las mercancías a través del libro mayor de la cadena de bloques, entendiendo dónde está en tránsito un contenedor. También pueden ver el estado de los documentos

aduaneros, o ver los conocimientos de embarque y otros datos en tiempo real. Y, debido a que crea un registro inmutable, ninguna de las partes puede modificar, borrar o incluso agregar cualquiera de los bloques sin el consenso de los demás en la red.

Blockchain está para quedarse, ya que este sustituye los procesos antiguos de transacciones, como también “Es una revolución en el mundo de la contabilidad, de las finanzas y de los negocios”, concluyó Gili el 21 de abril de 2017 en el Campus Pocitos de la Universidad ORT Uruguay.

Blockchain es una de estas tecnologías, que viene a cambiar todo un proceso de verificación de productos que eran utilizados por la sociedad. Se trata de una base de datos distribuida que realiza una operación única para todas las partes. Elimina intermediarios y la necesidad de conciliar. En los “contratos inteligentes” se vuelven casi instantáneas la seguridad, la asimetría de información, y los costos (de información y transaccionales). Gili el 21 de abril de 2017 en el Campus Pocitos de la Universidad ORT Uruguay.

La corporación multinacional de tiendas Walmart en China, uno de los principales clientes de IBM, tuvo problemas de contaminación alimenticia con la carne de cerdo en ese país. Walmart pidió a IBM una solución y se optó por implementar un registro de trazabilidad de alimentos basado en Blockchain. Entonces a través de las diferentes experiencias, se está tomando como opción es el utilizar un sistema de trazabilidad que nos ayude con el cumplimiento de estándar de calidad

que debe tener un producto. Gili el 21 de abril de 2017 en el Campus Pocitos de la Universidad ORT Uruguay.

CAPÍTULO II

ASPECTOS TÉCNICOS Y CONCEPTOS REFERENTES A LA SOLUCIÓN

2. ASPECTOS TECNICOS Y CONCEPTOS REFERENTES A LA SOLUCION

2.1. CADENA DE SUMINISTRO

"La cadena de suministro es el nombre que se le otorga a todos los pasos involucrados en la preparación y distribución de un elemento para su venta, es decir, es el proceso que se encarga de la planificación o coordinación de las tareas a cumplir, para poder realizar la búsqueda, obtención y transformación de distintos elementos, de esta forma poder comercializar un producto para que el mismo sea de fácil acceso al público." (Definista, 2018)

La cadena de suministro está compuesta de todos aquellas etapas o procesos involucrados en satisfacer una necesidad. En esta intervienen los proveedores, los almacenes y los canales de distribución.

2.1.1. ORIGEN DE LA CADENA DE SUMINISTRO

La palabra Cadena de suministro se deriva de la palabra latina cadena de abasto, que significa que es una red de empresas de suministro que es tomado desde el proveedor de la materia prima que requiere un producto hasta el producto final.

La definición de Wikipedia para cadena de suministro es que este es el proceso de acciones tomadas que recorren un ciclo completo de un producto o un servicio, desde que se idea hasta que este es consumido.

2.1.2. CARACTERÍSTICAS DE LA CADENA DE SUMINISTRO

Existen algunas características que hay que tomar en cuenta a la hora de hablar de cadena de suministro:

- ➢ Es un método dinámico que conlleva un flujo de manera constante de comunicación, artículos y fondos entre las diferentes etapas.

- ➢ Algo más importante que el cliente no hay, el cliente es la parte elemental del proceso, ya que todo gira entorno a la satisfacción de las necesidades de ellos.

- ➢ Una de las características mencionadas por Wikipedia es sobre Una cadena de suministro típica puede abarcar varias etapas que incluyen: clientes, detallistas, mayoristas/distribuidores, fabricantes, proveedores de componentes y materias primas.

- ➢ Cada etapa por la que debe de pasar una típica cadena de suministro es conectándose a través de un movimiento de productos, informaciones y fondos.

- ➢ Debe tenerse en cuenta que es necesario y que no es necesario, porque no es muy necesario que cada una de las etapas se encuentre presente en la cadena de suministro.

- Para diseñar una buena cadena de suministro debe tenerse en cuenta es que todo dependerá de la necesidad del cliente, como de las funciones que desempeñan las etapas que abarca.

2.1.3. PROCESOS MACRO Y FUNCIONES DE LA CADENA DE SUMINISTRO EN EL INTERIOR DE UNA EMPRESA

En los procesos macro y funciones de una cadena se debe tomar en cuenta una serie de grandes procesos principales que se encontraran dentro de un negocio u organización, este está dividido en:

- Administrar cada una de las interacciones con los proveedores, lo cual se divide en pequeñas funciones, las cuales dice que son:
    - Se selecciona y evalúa cada uno de los proveedores.
    - Convenio de contratos.
    - Desarrollo de proveedores.
    - Compras.
    - Asistencia en el diseño.
    - Asistencia en el suministro.

- Se debe de dar seguimiento y armar un plan para las cadenas de suministro que se encuentra de manera interna en la empresa a la cual se está dirigiendo:

    - Planificación estratégica.
    - Planificación de la demanda.
    - Planificación del abasto.

- Verificar el correcto funcionamiento en el procesamiento de órdenes.
- Cumplimiento en el servicio

➢ Se debe de llevar un seguimiento, creando las relaciones con los clientes:

- Marketing
- Fijación de precios
- Ventas
- Atención al cliente
- Administración de órdenes

2.1.4. LOS NIVELES DE DECISIONES EN UNA CADENA DE SUMINISTRO

Las decisiones que se deben de tomar en una cadena de suministro se dividen en tres categorías muy importante las cuales son:

➢ **Estrategias o diseños de la cadena de suministro**

- La compañía es quien decide cómo estará la estructura de su cadena de suministro.
- Se deben de tomar decisiones sobre de cómo se va a distribuir los recursos y los procesos.

- Se tomarán algunas decisiones a largo plazo, pues modificarlas a corto plazo sale a un precio muy elevado.
- Se debe tomar en cuenta la inseguridad en las condiciones.

➢ **Planificaciones de la cadena de suministro**

- Se dice que son decisiones de un trimestre.
- La estructuración de la cadena de suministro es fija.
- Se configuran las restricciones dentro de las cuales debe hacerse la planificación.
- La meta es maximizar el **superávit** (este se refiere a la diferencia positiva que se puede encontrar en los ingresos sobre los gastos) manteniendo las restricciones.
- Incluye tomar decisiones sobre cuáles mercados serán abastecidos y desde qué ubicaciones, la subcontratación de fabricación, las políticas de inventario que se seguirán y la oportunidad y magnitud de las promociones de marketing y precio.

- **Operaciones de la cadena de suministro**

    - La línea de tiempo es semanal o diario.
    - Las empresas deben toman decisiones acerca de cada uno de los pedidos de cada cliente.
    - La estructuración de la cadena de suministro se considera como fija y las políticas de planificación se deben de haber fijado.

La meta de los procesos de la cadena de suministro es poder manejar los pedidos que llegan de los clientes de manera eficiente.

2.1.5. VISIONES DE UNA CADENA DE SUMINISTRO

Visión estratégica en una cadena de suministro

El camino al cual debe de dirigirse una compañía a largo plazo sirve como rumbo e incentivo para orientar las decisiones estratégicas de crecimiento frente a las competencias.

La visión de la cadena de suministro está divido en dos elementos fundamentales:

1. Valores fundamentales que debe de tener la empresa
2. Una descripción competitiva de cómo le gustaría ser frente a otras empresas

- La visión es como una fuerza con la cual se debe de dirigir una organización y para ello no basta solo con que sus valores estén bien legible sino que también deben ser genuino.

- La visión de los valores de una empresa, son para describir su propósito general, lo cual se debe hacer en una o dos frases, que deben expresar claramente y sin equivocaciones cómo satisface la empresa las necesidades básicas del cliente.

2.1.6. UNA CADENA DE SUMINISTRO MÁS EFICIENTE Y PRODUCTIVA

Las cadenas de suministro cada día serán más eficientes utilizando la tecnología Blockchain, cómo también este puede impulsar la eficiencia y reducir costos en el ecosistema empresarial a través de cuatro componentes principales, Shari Diaz (2017):

Privacidad: visibilidad completa de la cadena, las transacciones son seguras, autenticadas y verificables.

Contrato inteligente: las reglas comerciales y los términos implícitos en el contrato están integrados en el Blockchain y se ejecutan con transacciones.

Consenso: todas las partes aceptan una transacción verificada por la red.

En muchos entornos B2B (Business To Business), la comunicación es unidireccional y punto a punto. Cada organización tiene sus propios registros, en varias formas: correos electrónicos, registros telefónicos, mensajes de texto, etc. Conciliar estos documentos puede ser complicado y consumir mucho tiempo.

2.1.7. TRAZABILIDAD Y VISIBILIDAD TOTAL

Definición del Comité de Seguridad Alimentaria de AECOC:

"Se entiende trazabilidad como el conjunto de aquellos procedimientos preestablecidos y autosuficientes que permiten conocer el histórico, la ubicación y la trayectoria de un producto o lote de productos a lo largo de la cadena de suministros en un momento dado, a través de unas herramientas determinadas". "Trazabilidad y Cadena de Suministro" (Emprenda Negocios, 2012)

La norma UNE 66.901-92 define trazabilidad como la "capacidad para reconstruir el historial de la utilización o la localización de un artículo o producto mediante una identificación registrada"

La siguiente figura proporcionada por Carrefour en el internet es una representación gráfica del concepto de Trazabilidad. (Carrefour. Logística Inversa: el Negocio del Tercer Milenio. p. 6):

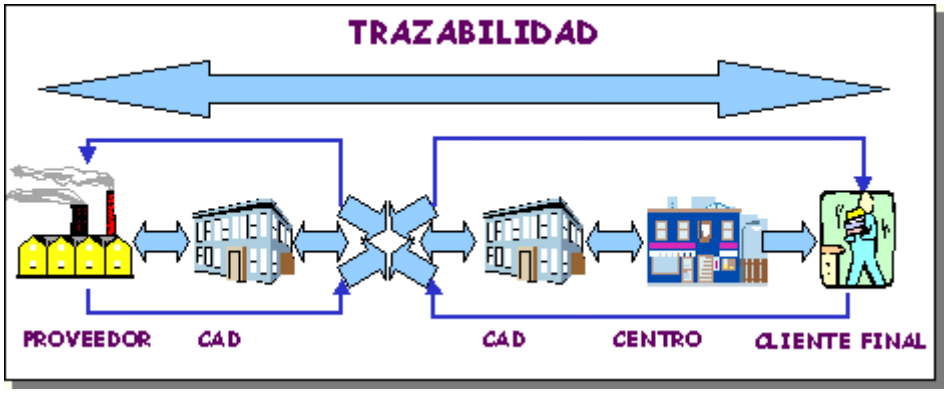


Fig. 12, Representación gráfica del concepto trazabilidad (Carrefour. Logística Inversa: el Negocio del Tercer Milenio. p. 6)

CAD: Centro de Almacenamiento y Distribución.

En la figura #12 se puede ver como se encuentra hoy en día una trazabilidad de un supermercado, en el cual a pesar de que todavía aún no tienen visibilidad completa de ella, en esta se ve en general como es el proceso o la secuencia que este sigue.

En la siguiente figura se puede tener una visibilidad total de la cadena de suministro utilizando tecnología Blockchain:

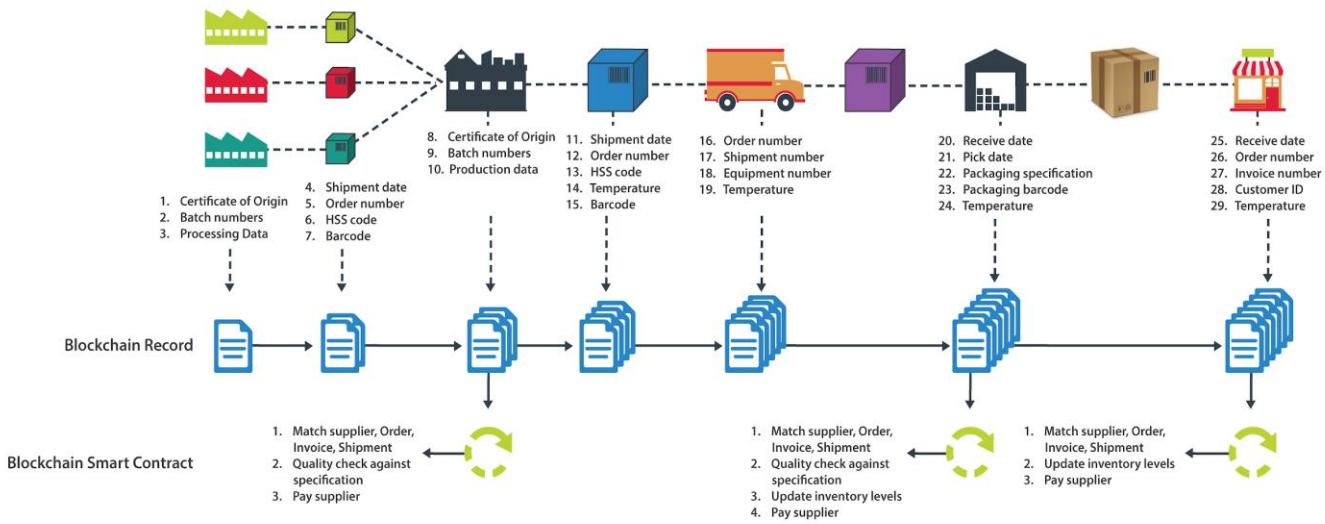


Fig. 13, Un Ejemplo de Blockchain con Contratos Inteligentes
Fuente: (Ryan Mullaney, S.F)

En la figura #13 se puede ver claramente un ejemplo de Blockchain con contratos inteligentes y como está te permite tener una visibilidad completa de la trazabilidad de la cadena de suministro.

2.2. BLOCKCHAIN

Blockchain es una base de datos compartida y distribuida que facilita el proceso de registro de las transacciones y el seguimiento de los activos en una red empresarial. Un activo puede ser tangible -una casa, un coche, dinero en efectivo, tierra- o intangible como la propiedad intelectual, como las patentes, los derechos de autor o la marca.

Prácticamente cualquier cosa de valor puede ser rastreada y comercializada en una red de cadena de bloques, reduciendo el riesgo y reduciendo los costos para todos los involucrados.

Marc Andreessen, creador de Netscape define Blockchain como, “Una cadena de bloques es esencialmente sólo un registro, un libro mayor de acontecimientos digitales que está “distribuido” o es compartido entre muchas partes diferentes.

Solo puede ser actualizado a partir del consenso de la mayoría de los participantes del sistema y, una vez introducida, la información nunca puede ser borrada.

La cadena de bloques de Bitcoin contiene un registro certero y verificable de todas las transacciones que se han hecho en su historia.”

2.2.1. ORIGEN

La cadena de bloques nació en el 2008 cuando Satoshi Nakamoto, cuya verdadera identidad aún se desconoce, publicó el whitepaper Bitcoin: A Peer to Peer Electronic Cash System en 2008 que describía una "versión puramente peer-to-peer de dinero electrónico" conocida como Bitcoin.

El Bitcoin Blockchain es un archivo de base de datos que se encuentra en miles de ordenadores en todo el mundo, donde las copias individuales se mantienen alineadas a través de las reglas del protocolo Bitcoin.

El archivo Bitcoin Blockchain (en realidad es una serie de archivos, porque los archivos grandes son difíciles de gestionar) contiene una lista de todas y cada una de las transacciones de bitcoin que han ocurrido: es el libro mayor de Bitcoin y ha ido creciendo desde enero de 2009.

Blockchain proporciona los medios para registrar las transacciones de bitcoin - el libro mayor compartido - pero este libro mayor compartido puede ser usado para registrar cualquier transacción y rastrear el movimiento de cualquier activo ya sea tangible, intangible o digital. Por ejemplo, la cadena de bloques permite que los valores se liquiden en minutos en lugar de días.

También se puede utilizar para ayudar a las empresas a gestionar el flujo de mercancías y los pagos relacionados, o para permitir a los fabricantes compartir los registros de producción con los fabricantes de equipos originales y regular la producción para reducir las retiradas de productos.

En la actualidad hay miles de cadenas de bloques públicas y privadas en funcionamiento, aunque muchas de ellas no tienen una aceptación significativa. Los sistemas públicos construidos con tecnología de cadena de bloques que han ganado prominencia incluyen Ripple, NXT y Ethereum.

Blockchain se ha convertido en la última década en una de las tecnologías pioneras más grandes de la actualidad, con potencial para impactar en todos los sectores, desde el financiero, pasando por el manufacturero, hasta el educativo.

2.2.2. CARACTERÍSTICAS DE LA BLOCKCHAIN

Las principales características de la cadena de bloques son:

- ➢ Consenso: Para que una transacción sea válida, todos los participantes deben estar de acuerdo en su validez.
- ➢ Procedencia: Los participantes saben de dónde proviene el activo y cómo su propiedad ha cambiado con el tiempo.
- ➢ Inmutabilidad: Ningún participante puede alterar una transacción después de que haya sido registrada en el libro mayor. Si una operación es errónea, se debe utilizar una nueva operación para anular el error y, a continuación, ambas operaciones serán visibles.
- ➢ La finalidad: Un único libro de contabilidad compartido proporciona un lugar a donde ir determinar la propiedad de un activo o la realización de una transacción.

En una cadena de bloques privada es posible tener las siguientes características:

- ➢ Mayor privacidad: Mediante el uso de IDs y permisos, los usuarios pueden especificar los detalles de la transacción que desean que otros participantes puedan ver. Los permisos se pueden ampliar para usuarios especiales, como auditores, que pueden necesitar acceso a más detalles de la transacción.

- Mejor capacidad de auditoría: Tener un libro mayor compartido que sirva como fuente única de verdad mejora la capacidad de supervisar y auditar las transacciones.

- Aumento de la eficiencia operativa: La digitalización pura de los activos agiliza la transferencia de propiedad, por lo que las transacciones pueden llevarse a cabo a una velocidad más acorde con el ritmo de la haciendo negocios.

Blockchain construye confianza a través de los siguientes cinco atributos:

- Distribuido y sostenible: El libro mayor se comparte, se actualiza con cada transacción y se replica selectivamente entre los participantes casi en tiempo real. Debido a que no es propiedad ni está controlada por una sola organización, la existencia continua de la plataforma de la cadena de bloques no depende de ninguna entidad individual.

- Seguro, privado e indeleble: Los permisos y la criptografía evitan el acceso no autorizado a la red y garantizan que los participantes sean quienes dicen ser. La privacidad se mantiene mediante técnicas criptográficas y/o técnicas de partición de datos para dar a los participantes una visibilidad selectiva. en el libro mayor; tanto las transacciones como la identidad de las partes que las realizan pueden enmascararse. Después de que se acuerden las condiciones, los participantes no pueden alterar

un registro de la transacción; los errores sólo se pueden anular con nuevas operaciones.

- Transparente y auditable: Porque los participantes en un tienen acceso a los mismos registros, pueden validar las transacciones y verificar las identidades o la propiedad sin necesidad de terceros intermediarios. Transacciones son sellados con la hora y pueden ser verificados en tiempo casi real.

- Basado en el consenso y transaccional: Toda la red relevante los participantes deben estar de acuerdo en que una transacción es válida. Este es mediante el uso de algoritmos de consenso. Cada la red de cadena de bloques puede establecer las condiciones bajo las cuales puede producirse una transacción o un intercambio de activos.

- Orquestado y flexible: Porque las reglas del negocio y contratos inteligentes (que se ejecutan en base a uno o más condiciones) pueden ser incorporados en la plataforma, la cadena de bloqueo las redes de negocios pueden evolucionar a medida que maduran para apoyar procesos de negocio de extremo a extremo y una amplia gama de actividades.

2.2.3. LA BLOCKCHAIN PARA EL NEGOCIO

La red de la cadena de bloques es económica y eficiente, ya que elimina la duplicación de esfuerzos y reduce la necesidad de intermediarios. También es menos vulnerable porque utiliza modelos de consenso para validar la información. Las transacciones son seguras, autenticadas y verificables.

Los participantes en ambos sistemas operativos son los mismos. Lo que ha cambiado es que el registro de transacciones ahora se comparte y está disponible para todas las partes.

Dentro de los principales beneficios para el negocio se encuentran:

- Ahorro de tiempo: Tiempos de transacción para empresas complejas y multipartitas las interacciones se reducen de días a minutos. Transacción es más rápida, ya que no requiere verificación por parte de una autoridad central.
- Ahorro de costes: Una red de bloqueo reduce los gastos en de varias maneras:

- Se necesita menos supervisión porque la red es autónoma vigilado por los participantes de la red, todos los cuales son conocidos en la red.
- Los intermediarios se reducen porque los participantes pueden intercambiar directamente artículos de valor.
- La duplicación de esfuerzos se elimina porque todos los participantes tienen acceso al libro de contabilidad compartido.

➢ Mayor seguridad: Las funciones de seguridad de Blockchain protegen contra la manipulación, el fraude y la ciberdelincuencia. Si una red está autorizada, permite la creación de una red sólo para miembros con la prueba de que los miembros son quienes dicen ser y que los bienes o activos comercializados son exactamente como están representados.

2.2.3.1. CONCEPTOS CLAVES DE LA BLOCKCHAIN PARA EL NEGOCIO

En lugar de tener una cadena de bloques que se basa en el intercambio de criptomonedas con usuarios anónimos en una red pública (como es el caso de bitcoin), una cadena de bloques para negocios es una red privada, permitida, con identidades conocidas y sin la necesidad de criptomonedas.

Para entender mejor cómo funciona una cadena de bloqueo para las empresas y apreciar su potencial para revolucionar las redes empresariales, es necesario comprender los cuatro conceptos clave de la cadena de bloqueo para las empresas, como se muestra en la figura 14.

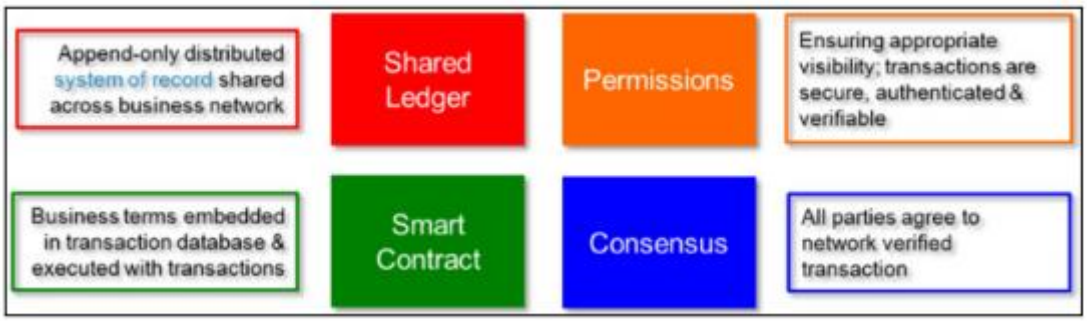


Fig. 14, Conceptos claves de la cadena de bloques para el negocio

Fuente: Blockchain for Dummies (Manav Gupta, 2017)

1. Libro de contabilidad compartido (Shared Ledger)

Los libros de contabilidad no son nada nuevo; se han utilizado en la contabilidad de doble entrada desde el siglo XIII. Lo que es nuevo es el concepto de un ledger compartido y distribuido - un registro inmutable de todas las transacciones en la red, un registro al que todos los participantes de la red pueden acceder. Con un libro de contabilidad compartido, las transacciones se registran sólo una vez, eliminando la duplicación de esfuerzos que es típica de las redes comerciales tradicionales.

Los libros compartidos tienen las siguientes características:

- ➢ Registra todas las transacciones a través de la red de negocios; el libro mayor compartido es el sistema de registro, la única fuente de verdad.
- ➢ Se comparte entre todos los participantes de la red; a través de la replicación, cada participante tiene una copia duplicada del libro mayor.
- ➢ Tienen privilegios, de modo que los participantes sólo vean las transacciones que están autorizados a ver. Los participantes tienen identidades que los vinculan a las transacciones, pero pueden elegir la información de la

transacción que otros participantes están autorizados a ver.

2. PERMISOS

Las cadenas de bloques pueden tener o no permisos. Cada participante tiene una identidad única, que permite el uso de políticas para limitar la participación en la red y acceso a los detalles de la transacción. Con la capacidad de restringir participación en la red, las organizaciones pueden cumplir más fácilmente con las normas de protección de datos.

Las cadenas de bloqueo permitidas también son más efectivas para controlar la consistencia de los datos que se añaden a la cadena de bloques.

Con la capacidad de restringir el acceso a los detalles de la transacción, se pueden almacenar más detalles de la transacción en el bloque y los participantes pueden especificar la información de la transacción que están dispuestos a permitir que otros vean. Además, algunos participantes pueden estar autorizados a ver sólo ciertas transacciones, mientras que otros, como los auditores, pueden tener acceso a una gama más amplia de transacciones.

(Con una cadena de bloqueo pública, el nivel de detalle de la transacción puede limitarse para proteger la confidencialidad y el anonimato.

Por ejemplo, si la Parte A transfiere un activo fijo a la Parte B, tanto la Parte A como la Parte B pueden ver los detalles de la operación. El Partido C puede ver que A y B han realizado, pero no pueden ver los detalles del activo fijo transferencia. Si un auditor o regulador se une a la red, los servicios de privacidad pueden asegurarse de que ven todos los detalles de todas las transacciones en la red. La tecnología criptográfica -esta vez mediante el uso de certificados digitales- lo hace posible.

Al igual que un pasaporte, un certificado digital proporciona información de identificación, es resistente a la falsificación y puede ser verificado porque fue emitido por una agencia de confianza. La red de la cadena de bloques incluirá una autoridad de certificación que emitirá el certificado digital.

3. CONSENSOS

En una red de negocios donde los participantes son conocidos y de confianza, las transacciones pueden ser verificadas y comprometidas con el libro mayor a través de varios medios de consenso (acuerdo), incluyendo los siguientes:

- ➢ Prueba de participación (Proof of Stake): Para validar las transacciones, los validadores deben tener un cierto porcentaje del valor total de la red. La prueba de participación podría proporcionar una mayor protección contra un ataque malicioso a la red al reducir los incentivos para y lo que hace que sea muy caro ejecutar ataques.

- ➢ Multifirma: Una mayoría de validadores (por ejemplo, tres de cada cinco) debe estar de acuerdo en que una transacción es válida.

- ➢ Tolerancia a faltas bizantinas (PBFT): Un algoritmo diseñado para resolver disputas entre nodos informáticos (participantes de la red) cuando un nodo de un conjunto de nodos genera una salida diferente de las otras en el set.

Cadena de bloques para características de negocio de consenso enchufable - una forma de implementar cualquier mecanismo de consenso que se considere mejor para cualquier segmento de la industria.

4. SMART CONTRACT

Un contrato inteligente es un acuerdo o conjunto de reglas que rigen una transacción comercial; se almacena en la cadena de bloques y se ejecuta automáticamente como parte de una transacción. Los contratos inteligentes pueden tener muchas cláusulas contractuales que podrían ser parcial o totalmente autoejecutables, auto-aplicables, o ambas. Su objetivo es proporcionar una seguridad superior a la del Derecho contractual tradicional, al tiempo que se reducen los costes y los retrasos asociados a los contratos tradicionales.

Por ejemplo, un contrato inteligente puede definir las condiciones contractuales bajo las cuales se produce la transferencia de bonos corporativos o puede encapsular los términos y condiciones del seguro de viaje, que puede ejecutarse automáticamente cuando, por ejemplo, un vuelo se retrasa más de seis horas.

2.2.4. APLICACIONES DE LA CADENA DE BLOQUES

Una de las mejores maneras de entender la Blockchain, apreciar su potencial y determinar si puede ser capaz de mejorar la forma en que su organización lleva a cabo sus negocios es analizar los casos potenciales de uso de la cadena de bloques.

En este subcapítulo se presenta una serie de casos de uso en una amplia diversidad de industrias.

- Servicios financieros: La industria de servicios financieros tiene varios casos de uso ejemplares para la cadena de bloques.

    - Financiación comercial:

      Las empresas necesitan comprar bienes y servicios a crédito con visibilidad de extremo a extremo para evitar y resolver disputas de transacciones.

      Por ejemplo, IBM Global Financing (IGF) proporciona financiación a sus socios globales, lo que les permite comprar bienes y servicios a proveedores con crédito aprobado por IBM. Con más de 4.000 socios y proveedores que utilizan sistemas diferentes y a menudo incompatibles, IBM trasladó toda la información a la

cadena de bloques y la presentó a los usuarios como un libro mayor distribuido.

Los beneficios de la implementación son:

- Visibilidad completa del canal de pedido a entrega.
- Reducción del número de litigios presentados.
- Reducción del tiempo necesario para resolver disputas.

- Trade comercial:

Las empresas necesitan una forma de agilizar el proceso de obtención de aprobaciones de múltiples entidades legales (aduanas, autoridades portuarias, empresas de transporte terrestre o ferroviario, etc.) para el movimiento de mercancías a través de las fronteras. La cadena de bloques puede ser utilizada por las personas jurídicas para firmar todas las aprobaciones y mantiene informadas a todas las partes sobre el estado de la aprobación, cuándo se reciben las mercancías y cuándo se transfiere el pago del banco del importador al del exportador.

2.2.5. ASPECTOS TÉCNICOS

La Blockchain es una lista ordenada de bloques de transacciones enlazadas de forma retroactiva, la misma puede almacenarse como un archivo plano o en una simple base de datos.

El cliente principal de bitcoin almacena los metadatos de la cadena de bloques utilizando la base de datos LevelDB de Google. Los bloques están vinculados "hacia atrás", cada uno de los cuales se refiere al bloque anterior de la cadena. La cadena de bloques a menudo se visualiza como una pila vertical, con bloques superpuestos y el primer bloque sirviendo como base de la pila. La visualización de bloques apilados unos encima de otros resultan en el uso de términos como "altura" para referirse a la distancia desde el primer bloque, y "parte superior" o "punta" para referirse al bloque añadido más recientemente.

Cada bloque dentro de la cadena de bloques está identificado por un hash, generado usando el **SHA256** algoritmo de hash criptográfico en la cabecera del bloque. Cada bloque también hace referencia a un el bloque anterior, conocido como bloque padre, mediante el campo "hash del bloque anterior" en la cabecera del bloque. En otras palabras, cada bloque contiene el hash de su padre dentro de su propio encabezado.

Mientras que un bloque tiene sólo un padre, puede tener temporalmente varios hijos. Cada uno de los hijos se refiere al mismo bloque que su padre y contiene el mismo hash (padre) en el campo "previous block hash". Múltiples hijos surgen durante un "fork" de cadena de bloques, lo cual es una situación temporal que ocurre cuando diferentes bloques son descubiertos casi simultáneamente por diferentes mineros. Finalmente, sólo un bloque hijo pasa a formar parte de la cadena de bloqueo y se resuelve el "fork". Aunque un bloque puede tener más de un hijo, cada bloque puede tener sólo un padre. Esto se debe a que un bloque tiene un único campo "hash de bloque anterior" que hace referencia a su padre único.

El campo "hash del bloque anterior" se encuentra dentro de la cabecera del bloque y afecta al hash del bloque actual. La propia identidad del hijo cambia si cambia la identidad de los padres. Cuando el padre es modificado de cualquier manera, el hash del padre cambia. El hash cambiado del padre necesita un cambio en el puntero "hash del bloque anterior" del hijo. Esto a su vez hace que el hash del hijo cambie, lo que requiere un cambio en el puntero del nieto, que a su vez cambia al nieto y así sucesivamente. Este efecto de cascada asegura que una vez que un bloque tiene muchas generaciones después de él, no se puede cambiar sin forzar un recálculo de todos los bloques subsiguientes. Debido a que tal recálculo requeriría una enorme computación, la existencia de una larga cadena de bloques

hace que la profunda historia de la cadena de bloques sea inmutable, una característica clave de la seguridad de bitcoin.

Una forma de pensar en la cadena de bloques es como capas en una formación geológica o núcleo glaciar. Las capas superficiales pueden cambiar con las estaciones, o incluso desaparecer antes de que tenga tiempo de asentarse. Pero una vez que se profundizan unos centímetros, las capas geológicas se vuelven más y más estables. Cuando se mira unos pocos cientos de metros hacia abajo, se está viendo una instantánea del pasado que ha permanecido inalterado durante milenios o millones de años. En la cadena de bloques, los bloques más recientes pueden ser revisados si hay un recálculo de cadena debido a una horquilla. Los seis bloques superiores son como unas pocas pulgadas de tierra vegetal. Pero una vez que se profundiza en la cadena de bloques, más allá de 6 bloques, los bloques son cada vez menos propensos a cambiar. Después de 100 bloques de vuelta hay tanta estabilidad que la transacción "Coinbase", la transacción que contiene bitcoins recién minados puede ser gastada. Unos pocos miles de bloques atrás (un mes) y la cadena de bloques es la historia establecida. Nunca cambiará.

2.2.5.1. RED PEER-TO-PEER (P2P)

Peer-to-peer (P2P) es un modelo de red alternativo al que proporciona la arquitectura tradicional de cliente-servidor.

Las redes P2P utilizan un modelo descentralizado en el que cada máquina, denominada peer, funciona como un cliente con su propia capa de funcionalidad de servidor. Un "par" juega el papel de un cliente y un servidor al mismo tiempo. Es decir, el par puede iniciar peticiones a otros pares, y al mismo tiempo responder a las peticiones entrantes de otros pares en la red. Se diferencia del modelo cliente-servidor tradicional en el que un cliente sólo puede enviar peticiones a un servidor y luego esperar la respuesta del servidor.

Con un enfoque cliente-servidor, el rendimiento del servidor se deteriora a medida que aumente el número de clientes que solicitan servicios del servidor. Sin embargo, en las redes P2P el rendimiento general de la red mejora a medida que se agrega un número creciente de pares a la red. Estos pares pueden organizarse en grupos ad-hoc a medida que se comunican, colaboran y comparten ancho de banda entre sí para completar las tareas en cuestión (por ejemplo, compartir archivos). Cada "par o nodo" puede subir y descargar al mismo tiempo, y en un proceso como este, nuevos pares pueden unirse al grupo mientras que los antiguos se van en cualquier

momento. Esta reorganización dinámica de los miembros del grupo es transparente para los usuarios finales.

Otra característica de una red P2P es su capacidad en términos de tolerancia a fallos.

Cuando un par se cae o se desconecta de la red, la aplicación P2P continuará utilizando otros pares. Por ejemplo, en un sistema BitTorrent, cualquier cliente que descargue un determinado archivo también actúa como servidor. Cuando un cliente encuentra que uno de los compañeros no responde, busca a otros compañeros, recoge partes del archivo donde estaba el compañero anterior y continúa el proceso de descarga. En comparación con un modelo cliente-servidor, en el que toda la comunicación se detendrá si el servidor se cae, una red P2P es más tolerante a fallos.

Las redes P2P pueden clasificarse en dos tipos: "redes P2P puras" y "redes P2P híbridas". En una red P2P pura, todos los pares participantes son iguales, y cada uno de ellos desempeña tanto el papel de cliente como el de servidor. El sistema no depende de un servidor central para ayudar a controlar, coordinar o gestionar los intercambios entre los pares. Sólo se mantiene un catálogo de archivos disponibles en el servidor, mientras que los archivos reales están dispersos entre

los pares de la red. La distinción central entre los dos tipos de redes P2P es que las redes P2P híbridas tienen una entidad central para realizar ciertas funciones administrativas, mientras que en las redes P2P puras no existe tal servidor. En comparación con la arquitectura híbrida P2P, la arquitectura P2P pura es más sencilla y tiene un mayor nivel de tolerancia a fallos. Por otro lado, la arquitectura híbrida P2P consume menos recursos de red y es más escalable que el enfoque P2P puro.

2.2.5.2. SISTEMA DE INTERCAMBIO PEER-TO-PEER

Bitcoin ha dado respuesta a la creciente necesidad de un sistema de pago que se adapte a la nueva forma de comunicación, una moneda rápida, segura y sin fronteras. (Antonopoulos 2014).

Sin embargo, la aparición de un dinero digital plenamente viable o de cualquier activo digital como acciones, bonos o licencias- presenta dos cuestiones técnicas principales: la confirmación de la autenticidad y el problema del doble gasto.

A diferencia de los activos físicos, el efectivo digital u otros activos digitales son simplemente un archivo informático (secuencia de bits) y, al igual que cualquier otro archivo digital, pueden copiarse.

Si no hay intermediarios que mantengan un libro de contabilidad de los saldos del titular de la cuenta (como efectivo o saldos de cuentas de valores), simplemente se puede enviar el archivo y conservar una copia del mismo.

Esto se conoce como el problema del doble gasto, y para prevenirlo, cada nota debe ser verificada en línea contra un libro mayor central cuando se gasta (Cham 1992). Por lo tanto, se necesita un registro fidedigno de todas las transacciones del activo digital. La solución propuesta por Nakamoto para evitar estos dos problemas se basa en un sistema de contabilidad constantemente actualizado y distribuido públicamente, combinado con una criptografía de clave pública o privada y un mecanismo de consenso particular.

“Proponemos una solución al problema del doble gasto utilizando un servidor distribuido peer-to-peer de timestamp para generar pruebas computacionales del orden cronológico de las transacciones” (Nakamoto 2009, p. 8).

Schollmeier (2002) define una red peer-to-peer como una arquitectura de red distribuida (Fig. 15), donde los participantes comparten una parte de su propio hardware como la potencia de procesamiento o la capacidad de almacenamiento. Estos

recursos compartidos son necesarios para proporcionar el servicio y el contenido que ofrece la red (por ejemplo, compartir archivos, almacenar o compartir espacios de trabajo para la colaboración), y son directamente accesibles por otros pares sin pasar por entidades intermediarias. Contrario al sistema bancario actual, las transacciones de Bitcoin, por ejemplo, son emitidas, grabadas y almacenadas por los numerosos participantes de la red y no en ningún servidor central propietario, lo que permite finalizar las transacciones en cuestión de minutos, ya que no se necesita ninguna conciliación o intervención manual en segundo plano.

Como menciona Dykes (1995), antes de que el dinero en efectivo digital pueda ganar una amplia aceptación, debe ganar y mantener la confianza del público. Por esta razón, la falsificación debe evitarse a toda costa. Dado que la moneda digital no es más que bits que representan valor, las transacciones monetarias digitales deben llevarse a cabo de manera que se evite la manipulación durante el tránsito, la recepción o el almacenamiento (Dykes 1995).

Este registro autoritativo es el blockchain, una base de datos compartida donde todas las transacciones son registradas en bloques por una red peer-to-peer distribuida arquitectónicamente.

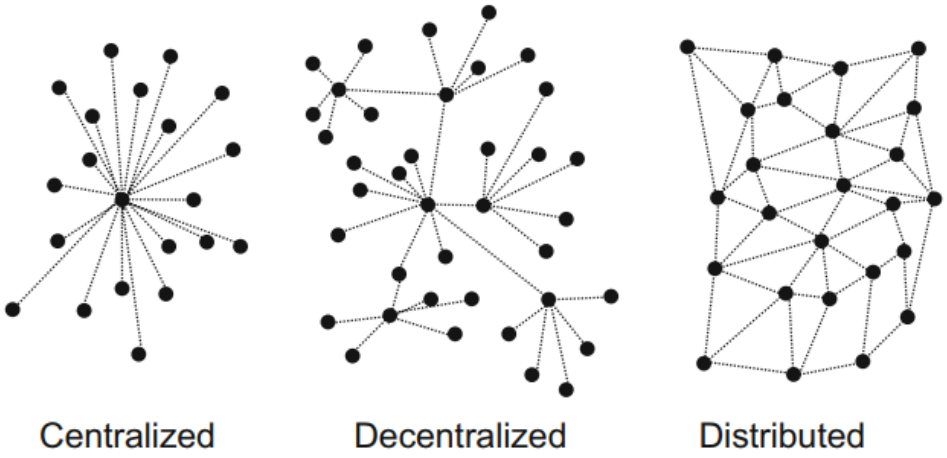


Fig. 15, Representación gráfica de centralizada a sistema distribuido
Fuente: (Swanson 2015)

Por "timestamp server" se entiende que todas las transacciones llevan un "sello de tiempo" para demostrar que los datos deben haber existido en un momento dado y para dar un orden cronológico a los bloques de transacciones. El historial de todas las transacciones define los propietarios de las monedas, creando los activos únicos (tokens digitales) que son imposibles de copiar. En el caso de criptomonedas como **Bitcoin**, de hecho, es teóricamente imposible que un participante malicioso rehaga parte de la historia (es decir, la cadena de bloques digitales en la que se registró la transacción) después de que se haya gastado una determinada moneda para cancelar la transacción y, por lo tanto, gastar la misma moneda dos veces (Nakamoto 2009).

La solución para evitar la manipulación se ofrece más bien a través de las firmas digitales, un concepto propuesto por primera vez en 1976 por **W. Diffie y M. Hellman** que Nakamoto integró en su diseño de cadenas de bloques. Una firma digital transforma el mensaje (es decir, la transacción) en un archivo criptográficamente firmado para que cualquiera que lo lea pueda estar seguro de quién lo envió.

Las firmas utilizan una clave secreta para firmar los mensajes y una clave pública para verificarlos, de forma que sólo los mensajes firmados con la clave privada puedan ser verificados por medio de la clave pública. Este proceso se conoce como prueba criptográfica, y las monedas electrónicas se definen como una cadena de firmas digitales (Chaum 1992). La posesión de las llaves para desbloquear las monedas equivale, por lo tanto, a la posesión de dinero en efectivo, y si se pierde la llave privada, también se pierden todas las monedas contenidas en el monedero digital correspondiente (Antonopoulos 2014, p. 231). Es decir, la llave privada es la más importante debido a que contiene la información necesaria para firmar las transacciones.

Criptografía de clave pública o privada

Las funciones Hash toman un mensaje como entrada y producen una salida que se denomina como un código hash, o simplemente un hash.

Cualquier dato que se ponga en uno de estos (una cadena), devuelve un número aleatorio del mismo tamaño de bit de modo que es imposible predecir lo que devolverán si reciben cierta información.

Además, el hash es una función unidireccional, y no se puede desencriptar, ofreciendo seguridad contra manipulaciones. La idea básica del hash criptográfico es que un valor hash sirve como una imagen representativa compacta (a veces llamado una impresión, huella digital o resumen de mensaje) de un y se puede utilizar como si fuera identificable de forma única con la cadena de entrada (Menezes et al. 1995).

Ejemplo de una prueba criptográfica:

Para gastar una moneda digital, uno tiene que demostrar ser el verdadero propietario de una dirección de clave pública desde donde se envía el dinero. El mensaje y la clave privada (entrada) son una secuencia de bits "n" que se analizan mediante la función de control criptográfico (f) descrita anteriormente.

signature = f (message, private key)

El receptor del mensaje puede entonces verificar a través de la función algorítmica matemática (v) detrás de la firma y la clave pública del remitente si la transacción corresponde realmente a la clave privada:

l = v (message, public key, signature)

En este ejemplo, si la función matemática devuelve un valor de '1', entonces el emisor es el verdadero propietario de la clave pública. Esta técnica evita la posibilidad de fraude manteniendo la privacidad de quienes la utilizan.

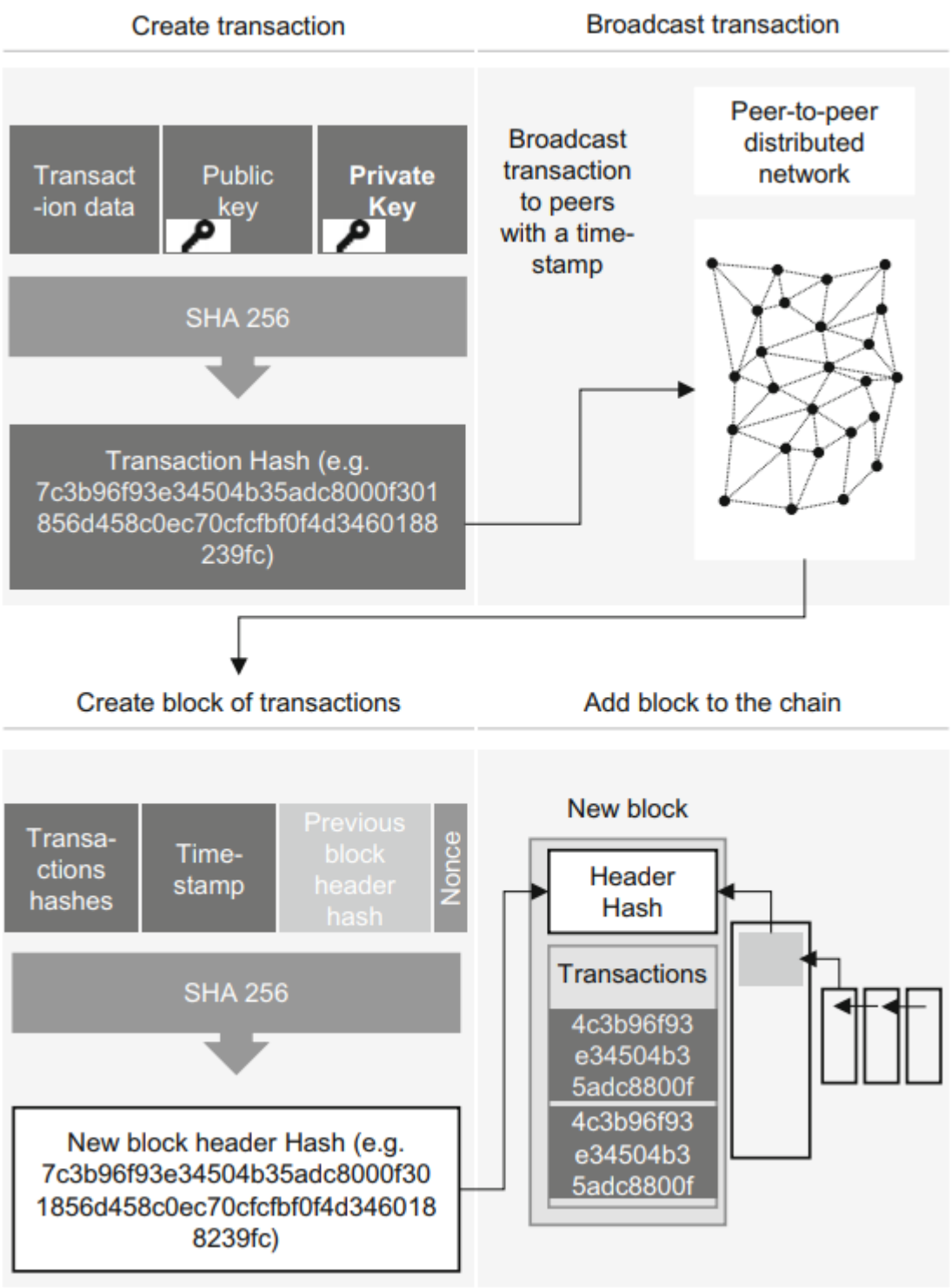


Fig. 16, Protocolo Blockchain de Bitcoin
Fuente: Supply Chain Finance and Blockchain Technology (Erik Hofmann, 2018)

Contrariamente a los actuales sistemas centralizados que gobiernan la economía dominante, el enfoque de libro mayor distribuido empuja la responsabilidad y el control a la amplia red a través de la prueba de trabajo de procesos basados en hash y, lo que es más importante, a los usuarios individuales.

Como ya se ha dicho, las claves privadas son la única prueba de propiedad de los activos digitales, por lo que la protección de las claves privadas es una cuestión central, porque si se piratea, se pierde todo el contenido de la cartera digital.

2.2.5.3. MECANISMOS DE CONSENSO DE GRUPO

Un sistema de contabilidad descentralizado y habilitado para la cadena de bloques plantea el problema de mantener una única verdad global entre los diferentes actores de la red que almacenan el historial de las transacciones. Para que los nodos puedan llegar a un consenso sobre la situación real del libro mayor, se necesita un mecanismo inequívoco de consenso entre los grupos.

La cadena de bloques de Bitcoin utiliza el mecanismo de consenso de prueba de trabajo (PoW). Este mecanismo

consiste en resolver un problema computacional difícil (un problema de hash) a la hora de crear nuevos bloques de transacciones. El protocolo de consenso se basa en un problema difícil de resolver pero fácil de verificar, evitando así la posibilidad de que otros nodos puedan rehacer todo el "PoW" para aceptar las transacciones. A través de este mecanismo, cada bloque se enlaza con el anterior, formando una cadena.

El mecanismo de consenso sobre la prueba de trabajo (PdT)

Un sistema contable descentralizado plantea el problema de mantener una verdad global única entre los diferentes actores de la red. Siguiendo los principios de las funciones de hash, la idea es insertar el "timestamp" (p.ej. 1456916388) en las entradas con el hash de todas las transacciones (merkle root) con el hash de cabecera del bloque anterior y un número arbitrario llamado "nonce" (Nakamoto 2009).

Se dice que los bloques están “encadenados”, porque la función hash contiene el hash de cabecera del bloque anterior (ver Fig. 17)

Excepto el “nonce”, todas las entradas son dadas. El problema a resolver es ahora encontrar el nonce correcto que produce un hash de salida (el nuevo hash de cabecera) con un valor que comienza con un gran número de ceros. Encontrar un

hash que comienza con un número dado de ceros es una tarea computacional difícil, y la única manera de resolver este problema es a través de la iteración (Antonopoulos 2014, p. 194). —se le pide a la computadora que ejecute miles de millones y miles de millones de cálculos hash hasta que resuelva el problema. Este valor calculado es “The proof of Work” y el trabajo realizado se llama **minería**.

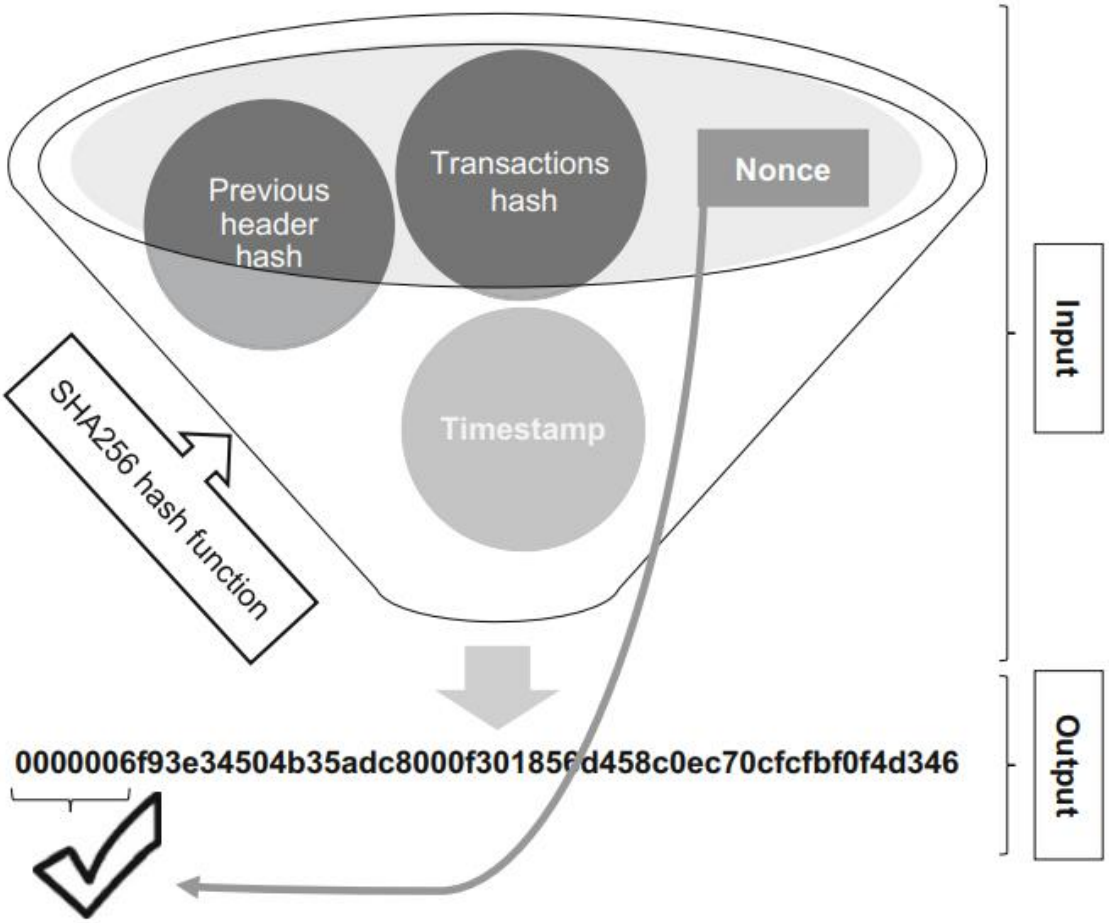


Fig. 17, Generación de un hash de encabezado de bloque "timestamped" SHA256. Fuente:

Cada vez que un nodo resuelve el problema de hash, transmite el bloque candidato junto con la prueba de trabajo a

los otros nodos para que puedan verificarlo insertando la transmisión nonce en la función de hash.

Si para la mayoría la salida comienza con el mismo número de ceros, el bloque es aceptado, y los nodos empiezan a hacer hash en la parte superior de ese bloque, continuando la cadena.

Con el mecanismo PoW, Bitcoin asegura la red y la integridad de la base de datos de transacciones, haciendo que la historia de la cadena de bloques sea prácticamente inmutable después de un cierto número de bloques. Se alcanza un nivel aceptable de seguridad después de seis bloques minados (es decir, una hora) (Antonopoulos 2014, pág. 160), mientras que las monedas recién extraídas sólo pueden gastarse cuando el bloque que contiene la primera transacción -la emisión de la moneda- está 100 bloques atrás (pág. 160), lo que lleva 17 horas de media.

Desde el lanzamiento de Bitcoin, han surgido alternativas al protocolo de consenso del PoW, como la prueba de trabajo con guion, la prueba de trabajo con múltiples algoritmos o las híbridas, que permiten acelerar el tiempo de generación de bloques (Antonopoulos 2014, p. 215).

El debate sobre cuál es el proceso de validación que mejor puede garantizar simultáneamente velocidad, eficiencia y seguridad parece no estar resuelto, pero el PdT parece ser el proceso más utilizado (Antonopoulos 2014). Con el tamaño real del bloque siendo limitado a 1 MB, las estimaciones antiguas y nuevas sitúan el máximo teórico en 7 por segundo (bitcoin.it), que desafortunadamente no es suficiente para servir a la de la corriente principal de la economía. En comparación, la red de Visa puede procesar más de 1000 por segundo, y en un comunicado oficial en 2013, Nasdaq afirmó ser capaz de más de 1 millón de transacciones por segundo en un día de negociación.

2.2.5.3.1. DIFERENTES MECANISMOS DE CONSENSO DE GRUPO

1. Prueba de Trabajo (PoW):

   Es el primer mecanismo de consenso distribuido, iniciado por el seudónimo creador de bitcoin, Satoshi Nakamoto.

   Muchas criptomonedas siguieron el ejemplo, incluyendo Ethereum. En PoW, todos los ordenadores de la red encargados de mantener la seguridad de la cadena de bloques -conocidos como Miners in bitcoin- trabajan para resolver un rompecabezas que consiste en una función matemática llamada hash. Esta tarea es sencilla (para una computadora), pero extremadamente repetitiva y, por lo tanto, costosa desde el punto de vista computacional.

   Las computadoras compiten para encontrar un hash con propiedades específicas. La computadora que encuentra la respuesta primero - la prueba de que han hecho el trabajo necesario - se le permite añadir un nuevo bloque de transacciones a la cadena de bloques. Se les recompensa con un tramo de bitcoins recién

acuñados, más todas las pequeñas comisiones de transacción que los usuarios han pagado por enviar monedas.

PoW funciona sobre la base del principio de que es caro añadir un tramo de nuevas transacciones a la cadena de bloqueo, pero es muy fácil comprobar si las transacciones son válidas debido a la naturaleza transparente del libro mayor. Los mineros verifican colectivamente toda la cadena de bloques, y las transacciones no se consideran completamente "confirmadas" hasta que se han añadido varios bloques nuevos encima de ellas. Si un actor malicioso intenta gastar monedas fraudulentamente, esas transacciones serán ignoradas por el resto de la red. La única manera de que un atacante pueda cometer un fraude de este tipo es poseer una enorme cantidad de poder computacional, de tal manera que puedan explotar bloque tras bloque, ganando la competencia de pruebas de trabajo una y otra vez. Esto se conoce como "ataque del 51%" debido a la necesidad de poseer más de la mitad del hashrate total de la red. La realidad es que ningún minero tiene tal proporción de poder total

de hashing. Por lo tanto, intentar tal fraude es 1) extremadamente costoso (ya que cuesta tanto como el hardware y la energía requeridos, más el costo de oportunidad de no soportar la versión válida de la cadena de bloqueo y recibir recompensas a cambio) y 2) extremadamente improbable que tenga éxito.

2. Prueba de Participación (PoS):

Debido a la cantidad de potencia computacional requerida, el PoW es costoso y requiere mucha energía. Toda una industria ha crecido alrededor de la creación de chips personalizados diseñados sólo para la minería. La prueba de participación (PoS) es un enfoque alternativo que ha ganado popularidad en los últimos años y que no requiere hardware especializado. En PoW, el hashrate determina la probabilidad de que un participante añada el siguiente bloque de transacciones a la cadena de bloques. En PoS, la participación en la moneda determina su probabilidad. Es decir, cada nodo de la red está vinculado a una dirección, y cuantas más monedas contenga esa dirección, más

probable será que extraigan (o `apoyen', en este caso) el siguiente bloque. Es como una lotería: el ganador es determinado por el azar, pero cuantas más monedas (billetes de lotería) tengan, mayores serán las probabilidades. Un atacante que quiera realizar una transacción fraudulenta necesitaría más del 50% de las monedas para procesar las transacciones requeridas de forma fiable; la compra de éstas aumentaría el precio y haría que este esfuerzo fuera prohibitivamente caro.

El sistema PoS fue pionero de Nxt. Dado que no consume mucha energía, como en el caso de PoW, no es necesario reembolsar los costes de la misma manera que en el caso de bitcoin. Por lo tanto, los sistemas PoS son muy adecuados para plataformas en las que hay un suministro estático de monedas, sin la inflación de las recompensas de bloque. Las recompensas de los Stackers consisten sólo en cargos por transacción. Este es el enfoque adoptado por la mayoría de las plataformas financiadas por la venta al por mayor, en las que las fichas se distribuyen sobre la base de la inversión, y diluir esto con más monedas se vería desfavorablemente.

PoS actualmente es un mecanismo de consenso bien establecido, pero no suele utilizarse en su forma original. Dos variantes, LPoS y DPoS, ofrecen ciertas ventajas.

3. Prueba de Importancia (PoI):

Una variación final de estos mecanismos de consenso es PoI. La primera plataforma de criptomonedas en implementar esto fue NEM. Con PoI, no es simplemente el balance de monedas lo que importa. El sistema de consenso de NEM se basa en la idea de que la actividad de la red productiva, no sólo la cantidad de monedas debe ser recompensada. Las probabilidades de apostar un bloque son una función de un número de factores, incluyendo el balance, la reputación (determinada por un sistema separado diseñado con un propósito), y el número de transacciones hechas desde y hacia esa dirección. Esto proporciona una imagen más holística de un miembro de la red "útil".

Existen muchas variaciones sobre estos enfoques amplios, y algunas plataformas utilizan una combinación de PoW y PoS - a menudo usando el primero para distribuir monedas, y luego cambiando al segundo en un punto posterior para mantener la red.

En todos los casos, el objetivo del enfoque de consenso es asegurar la red, predominantemente a través de medios económicos: debería ser demasiado caro atacar la red y más rentable ayudar a protegerla.

4. Prueba del tiempo transcurrido (PoET)

La prueba del tiempo transcurrido es un protocolo de consenso diseñado por Intel que funciona de alguna manera similar a la prueba de trabajo pero que consume mucha menos energía.

En lugar de requerir que los participantes resuelvan rompecabezas criptográficos, la prueba del tipo transcurrido se basa en un entorno de ejecución confiable para asegurarse de que los

bloques se generen a través de un mecanismo de lotería sin un trabajo intensivo de computación.

Se supone que puede escalar hasta mil nodos y ejecutarse de manera eficiente en cualquier CPU Intel que soporte SGX.

Sin embargo, hay un problema importante con la prueba del tiempo transcurrido. Para usarlo, tienes que confiar en un tercero, Intel. Por lo tanto, muchos piensan que desafía el propósito de la cadena de bloques.

2.2.5.4. REDES DE VALIDACIÓN DISTRIBUIDAS PÚBLICAS Y PRIVADAS

Incluso hoy en día, la cadena de bloques pública sin permiso requiere medidas de seguridad. (PoW) que limitan su aplicación más amplia a usos más amplios. Además, un estudio realizado en 2014 por la Universidad Nacional de Irlanda llegó a la conclusión de que el consumo de energía utilizado para generar la cadena de bloques de bitcoin y mantener el sistema en funcionamiento, bajo suposiciones razonables, es equivalente al consumo total de energía de Irlanda. El estudio también concluyó que toda la "industria" es teóricamente deficiente, dado que los costos de los mineros individuales (es decir, los participantes de la red que actualizan la cadena de bloques) exceden las recompensas (O'Dwyer y Malone 2014).

Además, la industria minera está compuesta por partes en gran medida desconocidas (grandes mineros), muchos de los cuales se oponen ideológicamente a las corporaciones o están ubicados en países con sistemas legales débiles (Greeenspan 2015, p. 11).

Por ejemplo, la red bitcoin está controlada por un gran grupo minero, como Bitfury o F2Pool, que podría controlar potencialmente más del 51% de la potencia de cálculo del hash y reescribir la información contenida en un bloque de reciente

creación. Por lo tanto, esta posibilidad podría socavar los requisitos reglamentarios de irrevocabilidad y firmeza de las transacciones financieras exigidos en los mercados de capitales (Swanson 2015, p. 23).

Por estas razones, varias instituciones financieras han comenzado a entender la idea de tener sus propias redes privadas o sistemas conjuntos con nodos de validación confiables y preseleccionados llamados libros mayores autorizados. Este concepto, como se subraya en un documento publicado por el Institute of International Finance (IFF) (2015), está claramente en conflicto con el diseño totalmente descentralizado de Bitcoin y de muchas otras criptomonedas o proveedores de servicios alternativos, pero probablemente siga siendo válido para el sector financiero.

> “Los libros de contabilidad privados pueden ser más útiles porque no necesita hacer pruebas de trabajo, por lo que de repente puede tener un modelo de negocio con un rendimiento de transacciones mucho mayor.” A. Batlin, Director Senior de Innovación de UBS, 2014

Esencialmente, en lugar de tener una red totalmente pública e incontrolada protegida por técnicas de computación dura, como el PoW, estas soluciones crean un sistema en el

que los permisos de acceso están estrictamente controlados y en el que los derechos para modificar o incluso leer el estado de la cadena de bloques están restringidos a usuarios seleccionados.

En un artículo del blog de 2015, Buterin identificó dos categorías de aplicaciones de cadenas de bloqueo autorizadas: (1) cadenas de bloques del consorcio y (2) cadenas de bloques totalmente privadas.

1. Las cadenas de bloques de consorcio son sistemas de ledger distribuidos en los que el proceso de consenso está controlado por un conjunto de nodos preseleccionados. Por ejemplo, un consorcio de 15 instituciones financieras, cada una de las cuales opera un nodo y de las cuales 10 deben firmar cada bloque para que el bloque sea válido. El derecho a leer la cadena de bloqueo puede ser público o restringido a los participantes.

2. En las cadenas de bloques totalmente privadas, los permisos permanecen centralizados en una organización, y los permisos de lectura pueden ser públicos o restringidos a un número cerrado de participantes. Las aplicaciones probables incluyen la

gestión de bases de datos, auditoría u otros usos internos para una sola empresa, por lo que la legibilidad pública puede no ser necesaria en muchos casos.

Las cadenas de bloques (Blockchain) privadas tienen la ventaja de que no es necesaria la creación de bloques computacionales duros, como se conoce a los nodos de validación (Greenspan 2015).

Esto permite procesos de validación más rápidos y una mayor escalabilidad, por lo que son más adaptables a los volúmenes de transacciones de la economía general y serían más favorables para los reguladores y legisladores (IFF 2015).

2.2.5.5. CONTRATOS INTELIGENTES (SMART CONTRACTS)

"El contrato inteligente es un programa basado en eventos que se ejecuta en un libro de contabilidad compartido replicado y que puede asumir la custodia de los activos de ese libro." (R. Brown, CTO en R3 CEV)

Un contrato inteligente viene siendo un programa informático que facilita, como también asegura, hace cumplir una serie de normas y ejecuta acuerdos registrado entre dos o más personas, es un sistema no controlado por ninguna de las partes del mismo, el cual ejecuta un contrato automático. Además, los contratos inteligentes no solo definen las reglas y sanciones en torno a un acuerdo de la misma manera que lo hace un contrato tradicional, sino que también hacen cumplir automáticamente esas obligaciones.

En la siguiente figura se encuentra la representación de un proceso Smart Contract:

Fig. 18, Representación de un proceso de Smart Contract.
Fuente: (Harwareate, 2018)

Uno de los principales innovadores en el espacio de la cadena de bloques es el proyecto Ethereum. El núcleo de sus principios fue propuesto por primera vez en 2013 en un libro blanco escrito por uno de sus inventores, V. Buterin. Ethereum es una BCT de código abierto con un lenguaje de programación Turing-completo incorporado (Buterin 2013).

El lenguaje de programación Turing-completeness permite a cualquiera crear y escribir código, comandos y aplicaciones descentralizadas en una cadena de bloques para crear sus propias reglas arbitrarias de propiedad, formatos de transacción y funciones de transición de estado (Buterin 2013), que básicamente funcionan como un pequeño programa informático.

Los activos digitales, por lo tanto, pueden ser controlados directamente por un código que implemente reglas arbitrarias, un principio descrito por primera vez en la década de 1990 por N. Szabo y denominado "contratos inteligentes". Para Szabo (1994), los contratos inteligentes son un protocolo de transacción computarizado que ejecuta los términos de un contrato. Los objetivos generales del diseño de Smart Contract son satisfacer condiciones contractuales comunes (tales como condiciones de pago, gravámenes, confidencialidad e incluso ejecución), minimizar las excepciones tanto maliciosas como accidentales y minimizar la necesidad de intermediarios de confianza.

Flood and Goodenough (2015) ilustra cómo las normas legales y las consiguientes estructuras de los contratos financieros podrían describirse directamente en términos computacionales. Demuestran que los contratos son sistemas de transición de estados que codifican reglas explícitas de transición para cambiar la relación de un estado a otro. Estos estados se activan por la realización de ciertos eventos predefinidos, tales como el desempeño de las propias contrapartes o la ocurrencia de contingencias particulares que pueden estar dentro o fuera de su control (por ejemplo, "fecha

de vencimiento vencida", "mercancía despachada" o "tasa LIBOR de 1 m = 0,45").

Los contratos inteligentes impulsados por cadenas de bloques pueden reaccionar con esos eventos (como entradas) y asegurar que la lógica se ejecute con precisión (proporcionar una salida) a través de entidades no confiables sin que ninguna de las partes la modifique (ni abuse) del programa escrito (Swanson 2015, p. 15). Hay tres elementos clave que distinguen los contratos inteligentes de los contratos ordinarios (Swan 2015, p. 16):

- Autonomía: Una vez que un contrato inteligente se lanza y se ejecuta, no necesita estar en contacto con su agente iniciador.
- Autosuficiencia: Un contrato inteligente tiene la capacidad de ordenar independientemente cualquier tipo de recurso. Por ejemplo, un contrato inteligente podría recaudar fondos mediante la prestación de servicios o la emisión de capital y podría gastarlos en los recursos necesarios, como el almacenamiento de energía de procesamiento.

- ➢ Descentralización: Los contratos inteligentes se registran en cadenas de bloques y se distribuyen y auto ejecutan a través de una amplia red de nodos.

Según Lang (2015), los contratos inteligentes pueden reaccionar a eventos externos y podrían aplicarse a activos representados fuera de una cadena de bloques (pág. 18). En primer lugar, las partes establecen las condiciones, los activos bajo custodia y las obligaciones, y registran los contrató inteligente en una cadena de bloques. Una vez que los eventos establecidos bajo las especificaciones condiciones desencadenan la ejecución del contrato, la lógica de programación automáticamente dicta los movimientos de valor en función de las condiciones cumplidas. Para activos digitales en un (p. ej. Bitcoin), las cuentas se liquidan automáticamente, mientras que en el caso de las cuentas digitales se liquidan automáticamente. Representación de activos fuera de una cadena de bloques (por ejemplo, valores, acciones), las cuentas son se considera liquidado cuando las cuentas fuera de la cadena coinciden con las instrucciones de liquidación (p. 18). La figura 4.4 ilustra un flujo inteligente de configuración y ejecución de contratos.

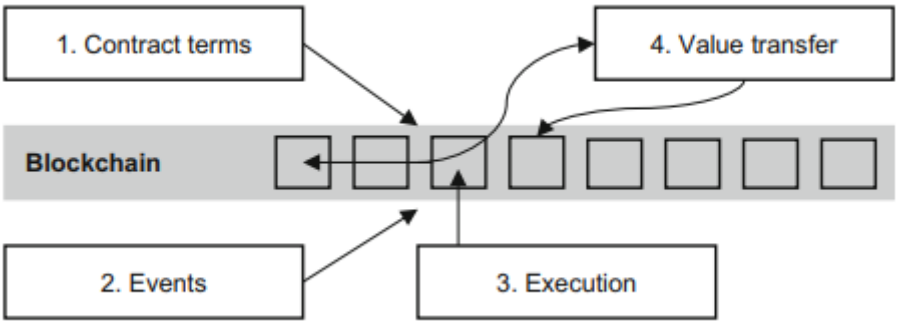


Fig. 19, Acciones sucesivas en el establecimiento y ejecución de un contrato inteligente
Fuente: (Swanson 2015, p. 18).

No está claro si la información de entrada tiene que estar en la misma cadena de bloques del contrato inteligente o no, porque según Greenspan (2016). Los insumos también deben ser sometidos a un proceso de consenso; de lo contrario, la red no podría ponerse de acuerdo sobre un determinado estado de salida. Gendal (2015) también está de acuerdo en que el éxito en la ejecución de contratos inteligentes depende de la calidad de los insumos que se les envían. Otro punto crítico viene dado por el escaso conocimiento de los lenguajes de codificación en los marcos legales (Flood and Goodenough 2015, p. 30), con la consecuencia de que es difícil para las jurisdicciones ver los contratos inteligentes como contratos legales reales y válidos.

2.2.5.6. LENGUAJES DE PROGRAMACIÓN ORIENTADOS A CONTRATOS

Un lenguaje de programación orientado a contratos es aquellos los cuales permiten escribir código y construir contratos inteligentes los cuales puedan ejecutarse de las siguientes formas:

- ➢ Funcionar como cuentas "multi-firma", de modo que los fondos se gastan sólo cuando un porcentaje requerido de personas está de acuerdo.
- ➢ Gestionar los acuerdos entre usuarios, por ejemplo, si uno compra un seguro del otro.
- ➢ Proporcionar utilidad a otros contratos (similar al funcionamiento de una biblioteca de software)
- ➢ Almacenar información sobre una solicitud, como información de registro de dominio o registros de membresía.

Unos de los lenguajes basados en contratos más utilizados hasta el momento son “**Solidity**”, el cual es un lenguaje de alto influenciado por C++, Python y JavaScript y está diseñado para apuntar a la máquina virtual Ethereum (EVM).

Esta plataforma tiene una sintaxis similar al lenguaje de programación JavaScript. Este tipo de lenguajes de programación ayudará y hará la comprobación en tiempo de ejecución en lugar de tiempo de compilación. Esta plataforma también soporta la herencia en la programación orientada a objetos, la herencia permite que los nuevos objetos tomen las propiedades de los objetos existentes.

Con los lenguajes basados en contratos es posible crear contratos para la votación, financiación de multitudes, subastas a ciegas, carteras con múltiples firmas y mucho más.

Actualmente, es recomendado utilizar remix para la creación de contratos pequeños, ya que es un entorno integrado de desarrollo (IDE) basado en un navegador el cual cuenta con un compilador y un entorno en tiempo de ejecución.

2.3. SENSORES

Para alimentar la Blockchain, es necesaria la captura de las informaciones que van arrojando los procedimientos involucrados en la cadena de suministros. En esta sección detallaremos cuales sensores estaremos utilizando para llevar a cabo la recolecta de datos.

2.3.1. SENSOR DE GEOLOCALIZACIÓN:

SIM7000A:

Fig. 20, Sensor SIM7000A
Fuente:

Este sensor está diseñado para aplicaciones que requieren comunicación de datos de baja latencia y rendimiento medio en una variedad de condiciones de propagación de radio. Debido a la combinación única de rendimiento, seguridad y flexibilidad, este módulo es ideal para aplicaciones M2M, como medición, telemática, seguimiento de activos, monitoreo remoto, E-health, etc. (“SIM7000A”, 2017)

Este sensor será utilizado para el alimentar la Blockchain con la ubicación continua de los bienes.

Especificaciones Técnicas:

- Quad-Band FDD-LTE B2/B4/B12/B13
- Control Via AT Commands
- Rango de voltaje: 3.0V~ 4.3V, Typ: 3.8V
- Temperatura operativa: -40℃ to +85℃
- Dimensiones: 24 X 24 X 2.6mm
- Peso: 3.0g
- GNSS (GPS, GLONASS and BeiDou/Compass, Galileo, QZSS)
- LTE CAT-M1(eMTC)
    - Uplink hasta 375 mbps, Downlink hasta 300mbps
- NB-IoT
    - Uplink hasta 66 kbps, Downlink hasta 34 mbps

2.3.2. SENSOR DE TEMPERATURA:

MCP9808:

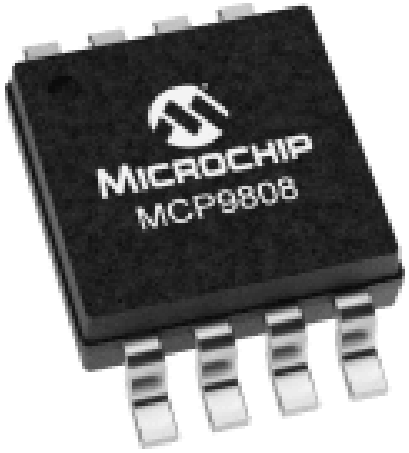


Fig. 21, Sensor MCP9808.
Fuente: ("MCP9808 - Thermal Management", 2018)

El sensor de temperatura digital MCP 9808 convierte las temperaturas entre -20 ° C y + 100 ° C en una palabra digital con una precisión de ± 0.5 ° C (máx.). El MCP 9808 viene con registros programables por el usuario que brindan flexibilidad para aplicaciones de detección de temperatura. Los registros permiten ajustes seleccionables por el usuario, tales como modos de Apagado o de baja potencia y la especificación de los límites de temperatura de eventos y de salida crítica. ("MCP9808 - Thermal Management", 2018)

Con esta herramienta la integridad de los bienes será resguardados pues ante cualquier evento que pudiera comprometerla las alertas serán emitidas con el fin de remediar el siniestro.

Especificaciones Técnicas:

- ±0.25°C (típico) de -40°C to +125°C
- ±0.5°C (máximo) de -20°C to +100°C
- 0.5°C, 0.25°C, 0.125°C, 0.0625°C
- Holgura de temperatura límite
- Límite de temperatura crítica
- Alertas programables en base a temperatura alcanzadas

2.4. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es definida como “La protección de la información y los sistemas de informa contra el acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción para proporcionar confidencialidad, integridad y disponibilidad. (Gobierno U.S.A., 2002).

Para poder satisfacer este requerimiento, se hace menester el establecimiento y fijación de normas que guíen hacia su cumplimiento con el fin de disminuir los riesgos que puedan afectar los principios CIA (Confidencialidad, Integridad y Disponibilidad).

La integridad se refiere a la habilidad de prevenir que la información puede ser modificada sin contar con la debida autorización o de una manera no deseada. Esto se refiere a la modificación o borrado de la información o porciones de ella, o también puede referirse a la manera autorizada, pero de una manera no deseada, el borrado o cambios de la información. Para mantener la integridad, no solamente debemos tener las herramientas que nos ayuden a prevenir los cambios desautorizados a nuestra da, pero también debemos contar con las herramientas que nos permitan los cambios que se hagan pertinentes recuperar.

La integridad de la información es vital cuando hablamos de que la misma es quien provee los fundamentos para la toma de decisiones. Si un ente nocivo pudiera llegar a alterar la información, por ejemplo, de la manipulación de alimentos, los clientes finales pudieran estar consumiendo bienes que no sean aptos para el consumo humano, pudiendo llegar a causar inclusive, la muerte.

La confidencialidad se refiere a la habilidad de proteger la información contra aquellos que no están autorizados a acceder a ella. Como un ejemplo, podemos considerar el caso de las informaciones generadas en la Blockchain para el mejoramiento de calidad de los procesos en la cadena de suministros de los supermercados, esta data en ningún momento debe ser accedida por entes nos autorizados pues puede ser utilizada sin posibilidades de competir dentro del mercado.

La confidencialidad puede ser comprometida inclusive con la pérdida de un equipo que contenga data relevante, una persona realizando Shoulder Surfing (mirando que escribe otro usuario), un correo enviado por equivocación o un intento, hacking exitoso.

La disponibilidad hace referencia a la habilidad de poder acceder a la información cuando se necesita. La pérdida de la disponibilidad puede referirse a un sin números de problemas que nos impidan el acceso, estos pudieran ser desde físicos, como lógicos. En el caso que nos concierne una falta de disponibilidad física puede ser

que los sensores presentes fallas debido a una irregularidad eléctrica y lógica que los nodos que reciben y envían las datas que viajan en la Blockchain sufra un ataque de denegación de servicio (DoS por sus siglas en inglés).

En los que concierne a los ataques que puedan comprometer alguno de estos principios podemos citar los siguientes:

- Confidencialidad: Intercepción.

  Un ataque de intercepción permitirá a un usuario no autorizado acceder a las informaciones, aplicaciones, ambientes, etc. La intercepción puede ir desde leer o copiar un archivo a escuchar conversaciones, capturar correos. Ejecutados de una manera pertinente, estos ataques pueden ser muy difíciles de detectar.

- Integridad y Disponibilidad: Interrupción.

  Los ataques de interrupción causan que nuestros activos se vuelvan inservibles o indisponibles para su uso pudiendo ser este siniestro temporal o permanente. Los ataques de interrupción casi siempre afectan la integridad pues existe la tendencia a la corrupción de la información cuando este tipo de ataques se materializan.

- Integridad y Disponibilidad: Modificación.

  Los ataques de modificación implican alterar los activos. Estos ataques podrían considerarse principalmente ataques a la integridad, pero también podría representar una amenaza a la disponibilidad.

  Si accedemos a un archivo de forma no autorizada y alteramos los datos que contiene, hemos afectado la integridad de los datos contenidos en el archivo. Sin embargo, si consideramos el caso donde el archivo en cuestión es un archivo de configuración que maneja el comportamiento de un servicio en particular, como por ejemplo un servidor Web, podría afectar la disponibilidad de ese servicio al cambiar los contenidos del archivo. Si continuamos con el concepto y decimos que la configuración alterada en el archivo de nuestro servidor web altera la forma en que el servidor trata las conexiones encriptadas, podríamos incluso hacer de esto un ataque de confidencialidad.

- Integridad y Disponibilidad: Fabricación.

  Los ataques de fabricación implican generar datos, procesos, comunicaciones u otras actividades similares con un sistema. Los ataques de fabricación afectan principalmente la

integridad, pero podría considerarse un ataque de disponibilidad también.

Si generamos información falsa en una base de datos, esto se consideraría un ataque de fabricación. Se puede también generar correos electrónicos, utilizado comúnmente como un método para propagar malware, como el que podemos encontrar en las propagaciones de los gusanos. En el sentido de un ataque de disponibilidad, si generamos suficientes procesos adicionales, tráfico de red, correo electrónico, tráfico web o casi cualquier cosa que consuma recursos, podemos potencialmente hacer que el servicio que maneja dicho tráfico no esté disponible a usuarios legítimos del sistema.

2.5. HARDWARE

En conjunto con los sensores definidos en el capítulo anterior se contarán con interfaces que sirvan de mediadores entre el Hardware y el Software. En esta sección le hablaremos sobre Arduino, quién será el intermediario.

2.5.1. DISPOSITIVO

Arduino:

Fig. 22, Arduino
Fuente: Arduino Uno - arduino.cc

Arduino es un fenómeno o una marca, no un microcontrolador. El proyecto Arduino se inició en Italia para desarrollar hardware de bajo costo para el diseño de interacción. Fundada por Massimo Banzi y David Cuartielles en 2005. Se basa en "Wiring Platform", que data de 2003. Es una plataforma de hardware de código abierto, tiene un entorno de desarrollo de código abierto, tiene un lenguaje y bibliotecas

fáciles de aprender (basado en Lenguaje de cableado), que tiene un entorno de desarrollo integrado (basado en el entorno de programación de procesamiento) y lo más importante disponible para los sistemas operativos Windows / Mac / Linux.

Arduino es una plataforma de creación de prototipos de electrónica de código abierto, por lo que el usuario puede hackearla como lo desee sin romper ninguna regla. Cuenta con herramientas de desarrollo amigables y soporta una gran cantidad de módulos de terceros para mejorar sus funciones con un mínimo esfuerzo y en menos tiempo y dinero. La filosofía de Arduino es alentar a los estudiantes, las mentes creativas, los aficionados y los profesionales a diseñar dispositivos integrados con menos esfuerzo y tiempo. Está teniendo sus propias líneas de productos de género para todas las necesidades de prototipos, como diferentes tipos de tarjetas disponibles [velocidad de chip, tamaño de memoria, pines de salida, etc. se eligen según la necesidad del usuario], se proporcionan módulos para mejorar las características de la placa e interactuar con otras tecnologías (como GSM, Ethernet, etc). La placa Arduino también admite otros componentes de terceros con el protocolo de interfaz adecuado. De modo que el usuario puede desarrollar cualquier concepto de producto / prototipo utilizando componentes disponibles localmente.

Este será el dispositivo que usaremos para interconectar los sensores con la blockchain.

2.5.1.1. COMPOSICIÓN DEL DISPOSITIVO

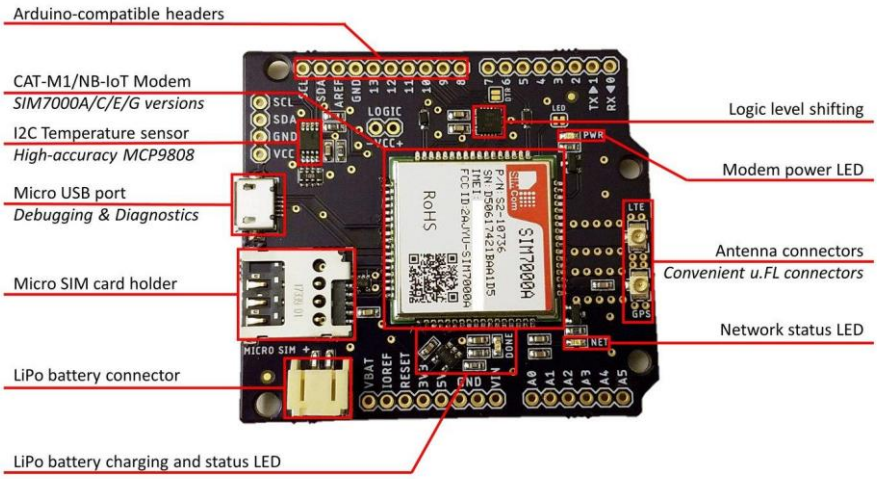


Fig. 23, SIM 7000 LTE CAT-M1/NB-IoT + GPS Shield Kit
Fuente: www.botletics.com

Para compenetrar los sensores y el arduino se utiliza el “GPS Shield Kit” (Que viene con los dos sensores por defecto) de Botletics que facilitara el proceso de ensamblaje.

El LTE Shield simplemente se conecta a los pines de Arduino (placa host) y le permite comunicarse con el módulo SIM 7000 y el sensor de temperatura.

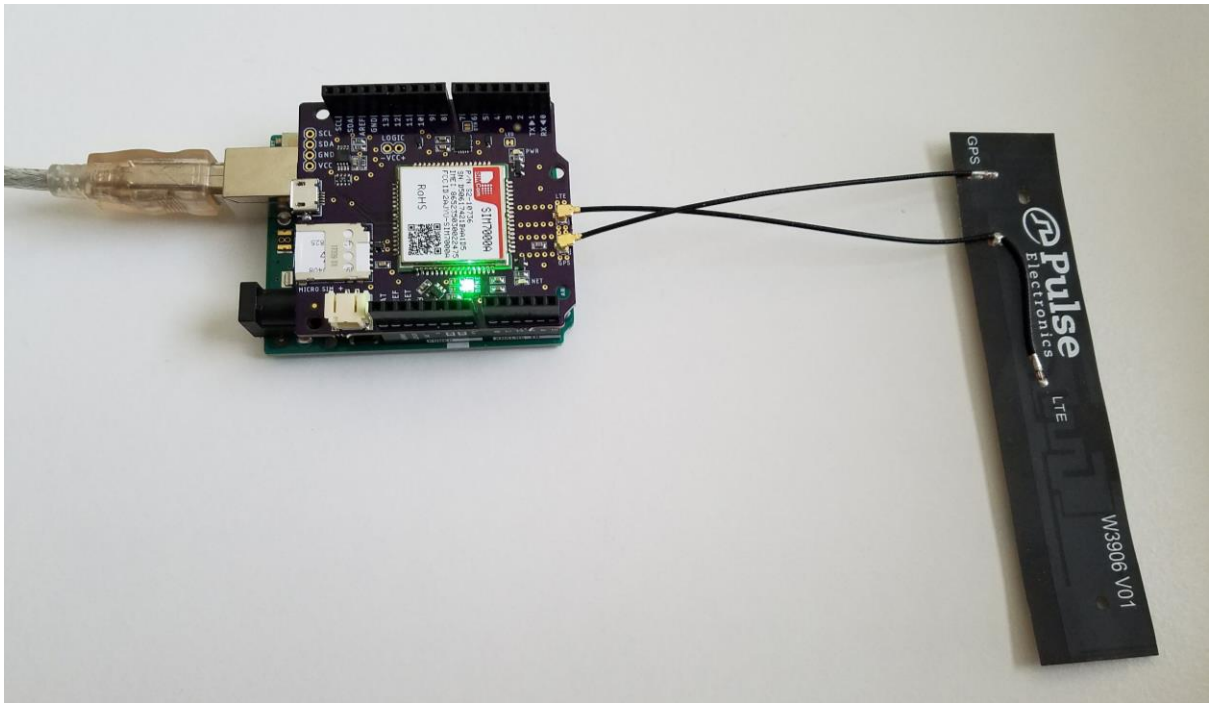


Fig. 24, Shield armado + Arduino + Antena
Fuente: http://www.instructables.com

2.5.1.2. COSTO DE LOS DISPOSITIVOS

- GPS Shield Kit US$80
- Arduino Uno US$20

Los precios de estos componentes son relativamente asequible y rentables por lo que la inversión en estos es mínima lo que facilita su escalabilidad.

CAPÍTULO III

ANÁLISIS Y DISEÑO DE LA SOLUCIÓN PROPUESTA

3. ANALISIS Y DISEÑO DE LA SOLUCION PROPUESTA

El objetivo de este capítulo es aplicar técnicas y principios con el fin de identificar y definir los procesos del sistema. A través de la ejecución de estas técnicas se podrá obtener suficientes detalles como para interpretar y realizar la solución.

En los próximos sub capítulos podremos visualizar la arquitectura general de la plataforma, las metodologías de trabajo con la cual se desarrollará la solución, las historias de usuarios, requisitos funcionales y no funcionales.

3.1. ALCANCE Y ARQUITECTURA GENERAL DE LA PLATAFORMA

3.1.1. ALCANCE DE LA PLATAFORMA

El alcance de la solución es transparentar los procesos realizados en una cadena de suministros, con el fin de generar información y estadísticas para posibles estrategias e inteligencia de negocios para la toma de decisiones las cuales ayudarán a sobrepasar los estándares de calidad y por tanto la satisfacción de los usuarios finales con los productos ofrecidos.

Además de visibilidad de los procesos, la plataforma a través de los sensores emitirá información sobre parámetros como temperatura, locación y humedad de los alimentos. Estas informaciones podrán ser consultadas a través del portal de gestión.

Entre los objetivos generales de la plataforma se encuentran:

- ➢ Proporcionar una visibilidad completa de la cadena de suministro.
- ➢ Generar reportes de estadísticas e inteligencias de negocios que ayuden a las tomas de decisiones.
- ➢ Mantener informado a los actores de la cadena sobre lo que está sucediendo vía notificaciones al instante.
- ➢ Simular la cadena de suministro en tiempo real por proveedores.

3.1.2. ARQUITECTURA GENERAL

La arquitectura de la plataforma está basada en Cloud Computing, debido a que el contexto y los diferentes elementos que la componen, demandan que la plataforma tenga poder de escalabilidad y elasticidad. Es una plataforma compartida, la cual tiene la ventaja de poder ampliarse y reducirse en función de la demanda.

La arquitectura de la solución propuesta está compuesta por varios elementos los cuales desempeñan una función única en todo el sistema. Cada elemento o subsistema utiliza diferentes tipos de redes, protocolos y consumen servicios web lo que permitirá que se puedan comunicar y entender uno al otro.

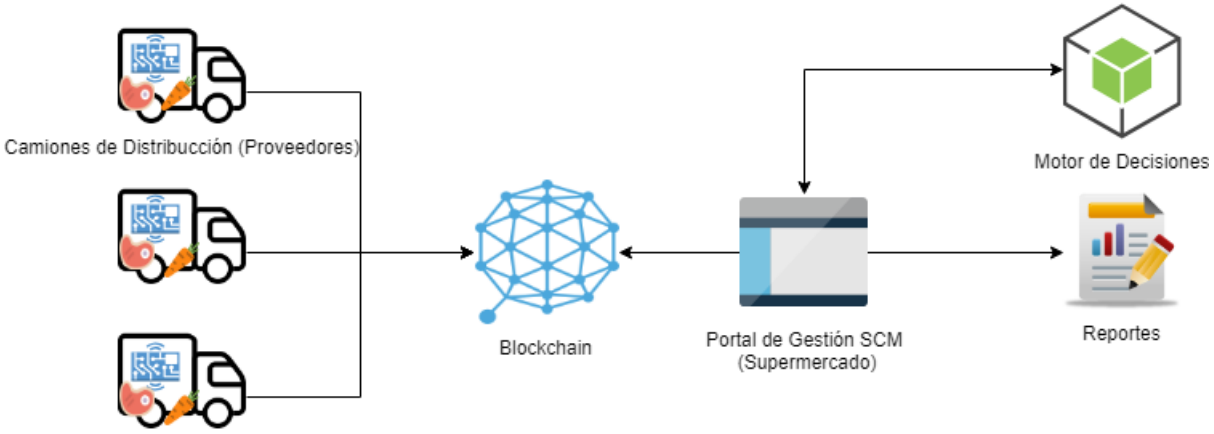


Fig. 25, Vista General de la Cadena de Suministros
Fuente: Propia

Como vemos en la figura 25, prácticamente el centro de la arquitectura está comprendido por la Blockchain (Hyperledger Sawtooh) y el portal de Gestión SCM. A estas se comunicarán diferentes elementos, como los sensores y Arduinos que se encuentran en los lotes de alimentos que viajaran en los camiones de los productores y el portal de gestión el cual se comunicará con el motor de decisiones y servidor de reportería.

Como toda la arquitectura funcionara en la nube, esto significa que si se presenta la oportunidad podría convertirse en un Software As A Service, lo cual es modelo de distribución de software lo cual todo el software está alojado en servidores de proveedores. Esto hace que el modelo sea muy eficiente, ya que habilita una propiedad llamada **"Multi Tenancy"**. Esto no es más que ofrecer la misma aplicación a múltiples usuarios finales y que exista un coste de infraestructura y mantenimiento compartido.

Queda explicado de forma generalizada la arquitectura de la solución propuesta. En el siguiente subcapítulo, se detalla cada uno de estos elementos, con el fin de que quede claro el desempeño y participación de cada uno de estos.

3.2. DISEÑO Y ELEMENTOS DE LA ARQUITECTURA

Con estas herramientas estaremos conformando la arquitectura que será utilizada para la recolección para su posterior transformación con el fin de generar las bases para la toma de decisiones inteligentes basadas en información. La arquitectura está conformada por varios elementos claves, estos son: Hyperledger Sawtooth, Arduinos y sensores, Portal de Gestión SCM, Motor de Inteligencia de Negocios y Amazon Web Services.

3.2.1. HYPERLEDGER SAWTOOTH

Hyperledger Sawtooth es una plataforma de cadena de bloques empresarial para la construcción de aplicaciones y redes de ledger distribuidas. La filosofía de diseño tiene como objetivo mantener los libros de contabilidad distribuidos y hacer que los contratos inteligentes sean seguros, especialmente para uso empresarial.

Una red Sawtooth en ejecución consta de las siguientes aplicaciones o procesos:

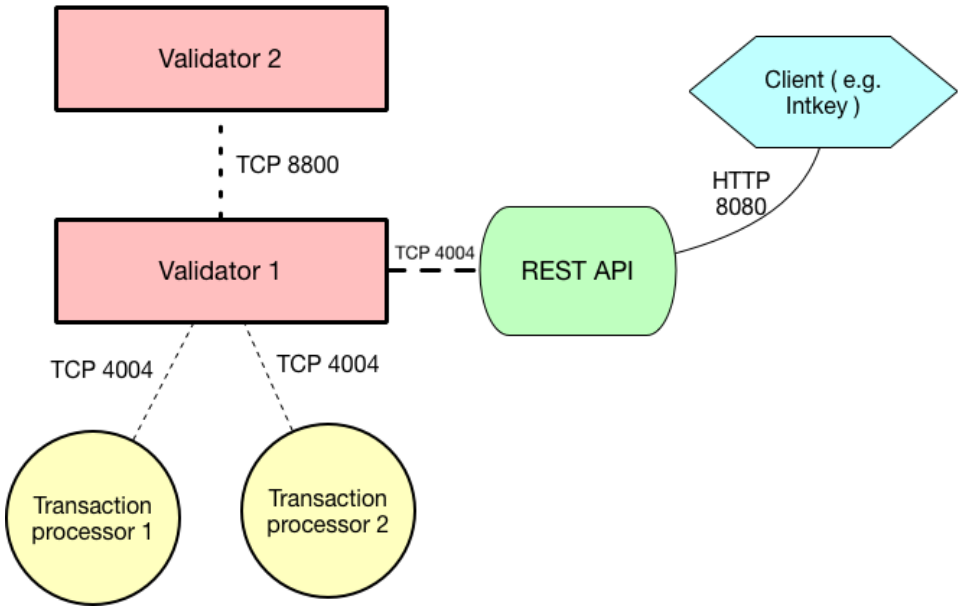


Fig. 26, Representación de una simple red con solo dos validadores y dos procesadores de transacciones.
Fuente: Hyperledger Sawtooth (https://sawtooth.hyperledger.org)

Envió de estados desde el Arduino (Client) hasta la Blockchain y por consiguiente validación de este.

Hyperledger Sawtooth proporciona una API REST pragmática para que los clientes interactúen con un validador utilizando estándares HTTP/JSON comunes.

Se trata de un proceso totalmente independiente que, una vez ejecutado, permite enviar transacciones y leer bloques con una interfaz común para cualquier lenguaje.

Con ese enfoque en los desarrolladores de aplicaciones, la REST API trata al validador principalmente como una caja negra, enviando transacciones y obteniendo los resultados. No es la herramienta para toda la comunicación con el validador.

Por ejemplo, no es utilizado por los procesadores de transacciones (Transaction Processor) para comunicarse con un validador, o por un validador para hablar con otros validadores.

Para estos y otros casos de uso similares, existe una interfaz ZMQ/Protobuf más eficiente y robusta, aunque algo más complicada.

Códigos de estado HTTP

La siguiente tabla mostrada a continuación muestra los códigos de estados HTTP que soporta el servicio web REST de la plataforma de Hyperledger Sawtooh.

Código	Título	Descripción
200	OK	Los recursos solicitados se obtuvieron con éxito. Se incluyen en la propiedad "data" de la respuesta.
201	Created	Los recursos enviados se presentaron y se crearon/comprometieron con éxito. Se incluye un "enlace" a los recursos.
202	Accepted	Los recursos enviados se enviaron al validador, pero todavía no se han comprometido. Se incluye un "enlace" para comprobar el estado de los recursos enviados. Si se le indica que espere a la confirmación, pero se ha agotado el tiempo, el estado en el momento de agotarse el tiempo también se incluye en la propiedad "data".
400	Bad Request	Algo en la solicitud del cliente estaba mal formado, y la solicitud no pudo ser completada.
404	Not Found	La solicitud estaba bien formada, pero no hay ningún recurso con el identificador especificado.
500	Internal Server Error	Algo está roto en el REST API o en el validador. Si se puede reproducir de forma consistente, se debe enviar un informe de fallo.
503	Service Unavailable	Indica que la API REST no puede ponerse en contacto con el validador.

Tabla 1, Hyperledger Sawtooh, REST API HTTP Status Codes
Fuente: https://sawtooth.hyperledger.org/docs

Respuesta de Datos

La API REST utiliza un objeto JSON para enviar metadatos a los clientes de una forma sencilla de analizar y personalizar. Todas las solicitudes aceptadas devolverán los datos en un objeto con al menos una de las cuatro posibles propiedades:

- `data` - Contiene el recurso o recursos reales que se están obteniendo.
- `head` - Id del bloque de cabecera de la cadena de la que se obtuvo el recurso, esto es particularmente útil para saber si no se estableció una cabecera explícita en la petición original.
- `link` - Un enlace a los recursos recuperados con los parámetros de cabecera y paginación explícitamente establecidos, siempre devolverá los mismos recursos.
- `paging` - Información sobre cómo se paginarón los recursos y cómo se pueden obtener más páginas.

Ejemplo de la respuesta:

```
{
  "data":          [{"fetched":          "resources"}],
  "head":                                "65cd...47dd",
  "link":    "http://rest.api.domain/state?head=65cd...47dd"
}
```

Manejo de Errores

Si algo sale mal mientras se procesa una solicitud, la REST API devolverá un objeto de respuesta con una sola propiedad: "error". Ese error contendrá tres valores que explican el problema que ocurrió:

- code - Código paralizable por la máquina específico de este error en particular.
- title - Título corto legible por humanos para el error
- message - Una explicación más larga y detallada de lo que salió mal.

Endpoints

Los endpoints incluyen referencias RESTful a recursos almacenados en el libro de Sawtooth en los que los clientes pueden estar interesados, como bloques y transacciones, así como metadatos RESTish, como estado de lotes.

Endpoints de Recursos

Para obtener los recursos almacenados en la cadena o en el estado del validador, se proporcionan varias rutas de recursos. Como es típico con las APIs RESTful, una petición GET obtiene uno o varios recursos, dependiendo de si se

especificó o no un identificador de recurso en particular (es decir, /resources vs /resources/{resource-identifier}).

- **/blocks** - Los bloques reales actualmente en la cadena de bloques, referenciados por id (aka header_signature)
- **/batches** - Los lotes almacenados en la cadena de bloques, referenciados por id
- **/transactions** - Las transacciones almacenadas en la cadena de bloques, referenciadas por id
- **/state** - El estado del libro mayor, almacenado en el Merkle Trie, referenciado por las direcciones de las hojas

Endpoints de Envíos

Para enviar transacciones a un validador de Sawtooth, deben estar envueltas en un lote. Por esta razón, los envíos se envían al endpoint **/batches** y sólo a ese endpoint. Debido a la naturaleza asincrónica de las cadenas de bloques, existe un punto final correspondiente para comprobar el estado de los lotes enviados. Ambas peticiones aceptarán el parámetro de consulta "wait", permitiendo a los clientes recibir una respuesta sólo una vez que se hayan confirmado los lotes.

- ➢ **/batches** - Acepta una petición POST con una BatchList de lotes a enviar.

➢ **/batch_statuses** - Obtiene el estado confirmado de uno o más lotes.

Ejemplo de respuesta del estado de lote:


```
[{
"id":"89807bfc9089e37e00d87d97357de14cfbc455cd608438d426a625a3
0a0da9a31c406983803c4aa27e1f32a3ff61709e8ec4b56abbc553d7d33063
5b5d27029c",
"status":"COMMITTED"},
{
"id":"c0c2075e708c04b34903c5374f65c9352f9dc9662f187e4bab0605ab
a3eb697e459bfa3a61a8050c428d1347d47a11b0cf81d481467a18cd48ab13
7001a5fa29",
"status": "PENDING"
}]
```

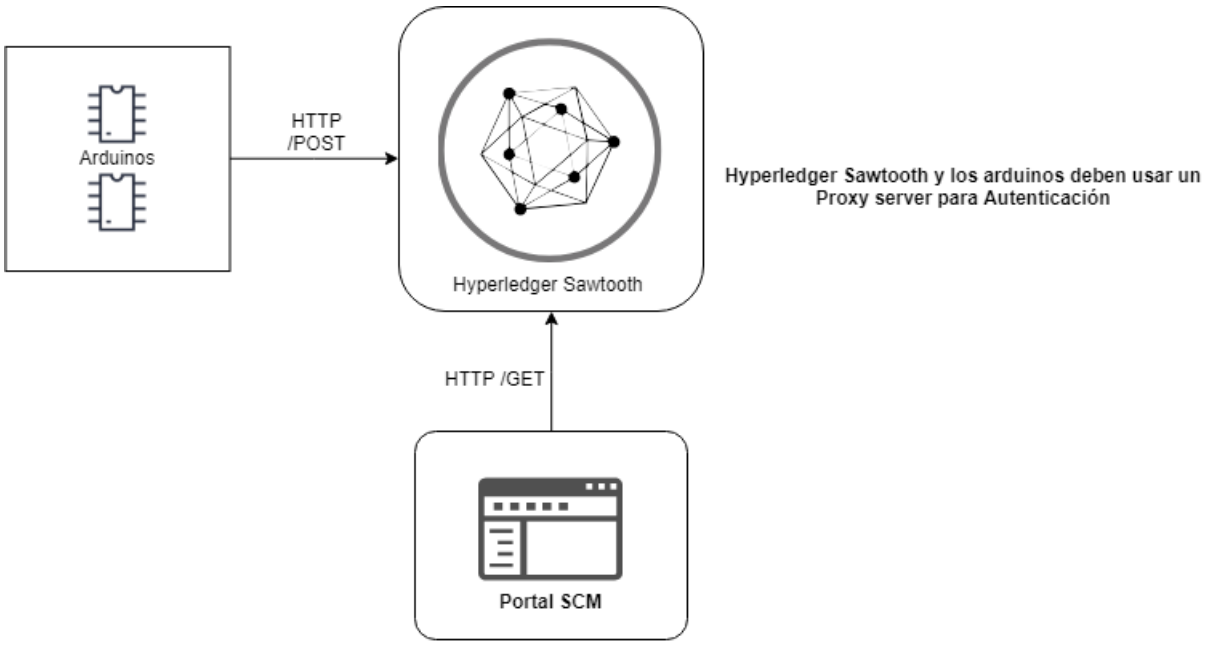



Fig. 27, Comunicación entre elementos a través de protocolo HTTP.

Fuente: Propia

Actualmente, la API de Hyperledger Sawtooth no ofrece ninguna autorización, pero es totalmente posible ponerla detrás de un proxy server que lo haga.

3.2.2. ARDUINO Y SENSORES

Los Arduino y sensores son los responsables de emitir los diferentes parámetros como temperatura, humedad y locación a la red de Blockchain.

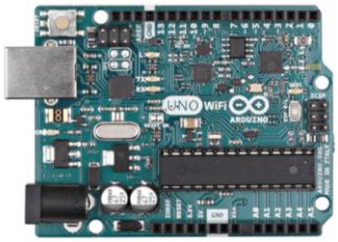


Fig. 28, Arduino UNO Wifi (ESP8266).
Fuente: Tienda BricoGeek (https://tienda.bricogeek.com)

Los dispositivos Arduino utilizados para la solución cuentan con conexión a internet, los mismos van a consumir un Servicio REST de Hyperledger Sawtooth el cual le permitirá enviar transacciones a la red. En la siguiente figura, se muestra cómo van a interactuar vía protocolo HTTP los dispositivos con la cadena de bloques.

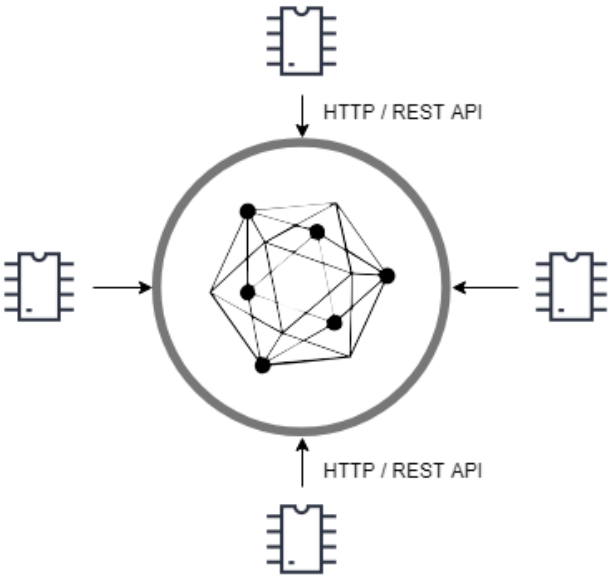


Fig. 29, Dispositivos Arduinos conectados a Hyperledger Sawtooth vía Protocolo HTTP
Fuente: Propia

Para enviar la información a los validadores, Hyperledger Sawtooth expone un servicio **POST /batches**. Este acepta un protobuf (Protocol Buffer) formateado BatchList como un archivo binario de flujo de octetos y lo envía al validador para que lo confirme.

Si el parámetro `wait` está establecido en la url, la API intentará esperar para responder hasta que todos los lotes hayan sido confirmados a la cadena de bloques, devolviendo una respuesta 201 con un enlace a los lotes confirmados.

Si la espera se establece en un número entero positivo, el tiempo de espera de la API se agotará y regresará después de que ese tiempo en segundos haya transcurrido. Si se establece en cualquier valor que no sea un número entero que no sea false (incluyendo simplemente wait?), la API todavía puede tener tiempo de espera, pero usará su propia configuración (normalmente 300s). Después del tiempo de espera, se devuelve un 202 con un objeto de datos que incluye los estados de cada lote (COMMITTED, INVALID, PENDING, o UNKNOWN) y un link a un punto final /batch_status para búsqueda.

Si la espera no está configurada, o está configurada como false, la API volverá inmediatamente con un estado de 202. No habrá

ningún objeto de datos, sólo un enlace a un punto final /batch_status que se comprobará para comprobar el estado de los lotes enviados.

Especificaciones del servicio `POST /batches`

Query Parameters:

- wait (integer) – Un tiempo en segundos para esperar la confirmación.

Status Codes:

- 201 Created – Enviados con éxito todos los lotes en BatchList
- 202 Accepted – Lotes presentados para su validación, pero aún no comprometidos
- 400 Bad Request – La solicitud fue mal formada
- 500 Internal Server Error – Algo salió mal en el validador
- 503 Service Unavailable – API no puede llegar al validador.

3.2.3. PORTAL DE GESTIÓN SCM

El portal de Gestión de la Cadena de Suministro (SCM) consiste en una aplicación web en la cual el usuario puede:

1. Clientes (Supermercado): realizar análisis de preferencias de los usuarios finales del supermercado, preludiar la demanda total, saber la disponibilidad de los productos, Solicitud cotización y órdenes de compra automáticas a los proveedores y establecer estrategias en base a la demanda real.

   Trazabilidad completa de toda la cadena de suministro, simulación de la cadena de suministro, envío de notificaciones.

2. Proveedores: Responder y aceptar a las solicitudes de cotizaciones del supermercado. Trazabilidad completa de la cadena de suministro desde el proveedor hasta el supermercado. Recepción de notificaciones sobre solicitud de cotizaciones del supermercado y notificaciones sobre el estado actual de la cadena de suministro.

3. Control de Stocks: El portal de gestión SCM se encargará de llevar un control de la disponibilidad de los productos, a modo que siempre haya existencia.

Además, hará optimización de almacenes para reducir espacio físico y reducir los costes por almacenamiento.

4. Recursos humanos: Como el sistema maneja en tiempo real la información de toda la cadena de suministro, el portal de gestión tiene la capacidad de notificar a los empleados el momento indicado en el cual realizar una tarea específica de acuerdo con sus funciones.

Como el sistema maneja toda la información de la cadena de suministro en su totalidad, los proveedores y fabricantes tendrán información en tiempo real sobre la necesidad de productos del supermercado.

3.2.4. ADAPA DECISION ENGINE

ADAPA es un motor de decisión de análisis predictivo basado en el estándar PMML (Predictive Model Markup Language). Con ADAPA, implemente uno o varios modelos predictivos de herramientas de minería de datos como R, Python, KNIME, SAS, SPSS, SAP, FICO y muchos otros. Califique sus datos en tiempo real utilizando Web-Services, o utilice ADAPA en modo batch para la calificación de Big Data directamente de su sistema de archivos local o desde un cubo de Amazon S3. Como una solución central para los entornos ricos en datos de hoy en día, ADAPA ofrece información precisa sobre el comportamiento de los clientes y la información de los sensores.

Análisis Predictivo usando Estándares Neutros para Proveedores: ADAPA utiliza el estándar de la industria Predictive Model Markup Language (PMML) para importar e implementar algoritmos predictivos y modelos de aprendizaje automático. ADAPA puede entender cualquier versión de PMML y es compatible con la mayoría de las herramientas de minería de datos, tanto de código abierto como comerciales.

Despliegue de Modelos de Forma Fácil: ADAPA permite que uno o varios modelos predictivos sean desplegados al mismo tiempo. Ejecuta muchos algoritmos, desde modelos de

regresión simples hasta los conjuntos de aprendizaje de máquina más complejos, por ejemplo, Random Forest y modelos potenciados.

Puntuación a la velocidad de los negocios: ADAPA es capaz de transformar instantáneamente sus puntajes en decisiones de negocios. El uso de reglas basadas en PMML permite emparejar diferentes rangos de puntuación con decisiones empresariales específicas. Las aplicaciones van desde la detección de fraudes y el scoring de riesgos hasta la optimización de campañas de marketing y el procesamiento de datos de sensores en la Internet de los objetos (IO).

3.2.5. Amazon Web Services (AWS): Computación en la Nube

La computación en la nube es un paradigma de computación, donde un gran número de sistemas están conectados en redes privadas o públicas, para proporcionar una infraestructura dinámicamente escalable para el almacenamiento de aplicaciones, datos y archivos.

Con la llegada de esta tecnología, el costo de computación, alojamiento de aplicaciones, almacenamiento de contenido y entrega se reduce significativamente.

La computación en la nube es un enfoque práctico para experimentar beneficios de costos directos y tiene el potencial de transformar un centro de datos de una configuración de

capital intensivo a un entorno de precio variable. La idea de la computación en la nube se basa en un principio fundamental de "reutilización de las capacidades de TI". La diferencia que aporta la computación en la nube frente a los conceptos tradicionales de "computación en red", "computación distribuida", "computación utilitaria" o "computación autónoma" es ampliar horizontes más allá de las fronteras organizativas.

Los proveedores de Cloud Computing ofrecen servicios que se pueden agrupar en tres categorías:

1. Software as a Service (SaaS): En este modelo, se ofrece al cliente una aplicación completa, como un servicio bajo demanda. Una única instancia del servicio se ejecuta en la nube y se da servicio a múltiples usuarios finales.

   Por el lado de los clientes, no hay necesidad de inversión inicial en servidores o licencias de software, mientras que, para el proveedor, los costos se reducen, ya que sólo una sola aplicación necesita ser alojada y mantenida. Hoy en día SaaS es ofrecido por compañías como Google, Salesforce, Microsoft, Zoho, etc.

2. Plataforma como un Servicio (Paas): Aquí, una capa de software, o ambiente de desarrollo es encapsulada y

ofrecida como un servicio, sobre el cual se pueden construir otros niveles más altos de servicio. El cliente tiene la libertad de crear sus propias aplicaciones, que se ejecutan en la infraestructura del proveedor.

3. Infraestructura como servicio (Iaas): IaaS proporciona capacidades básicas de almacenamiento y computación como servicios estandarizados a través de la red. Servidores, sistemas de almacenamiento, equipos de red, datos El espacio en el centro, etc., se agrupan y se ponen a disposición para manejar las cargas de trabajo.

La tendencia a nivel global es la computación en la nube, toda la infraestructura de la plataforma estará operando sobre Amazon Web Services (AWS). En la Fig. 30 se puede observar la Arquitectura de Amazon Web Services y los diferentes servicios a utilizar.

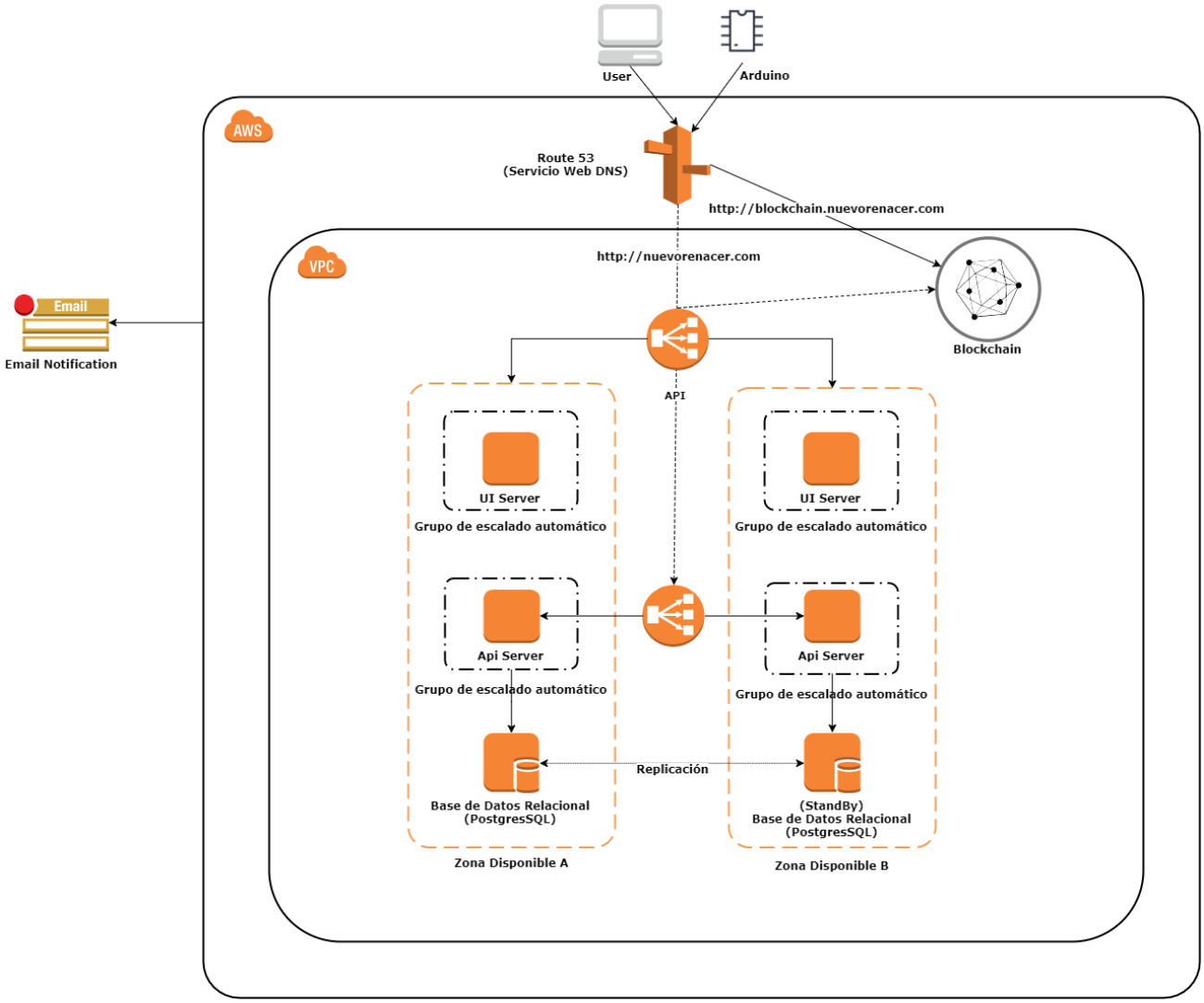


Fig. 30, Arquitectura General de Amazon Web Services para la plataforma.
Fuente: Propia

Los servicios de Amazon Web Services que serán utilizados para el correcto funcionamiento de la plataforma son:

- **Amazon Route 53:** es un servicio web de sistema de nombres de dominio (DNS) en la nube altamente disponible y escalable. Es utilizado dentro de la solución propuesta para configurar el nombre de dominio. Ej., *https://nuevorenacer.com*.

- **Amazon Virtual Private Cloud (Amazon VPC):** es un servicio de Amazon Web Services el cual permite lanzar recursos AWS en una red virtual definida por el administrador. La red es parecida a una red tradicional, pero con los beneficios de ser auto escalable.

  Dentro de la solución propuesta, Amazon VPC será utilizado para cubrir toda la seguridad de la plataforma. Es decir, creación de subnets, acceso al internet y enlaces con otros componentes de Amazon Web Services.

- **Amazon Elastic Load Balancer:** El balanceador de carga elástico de amazon se encarga de distribuir la carga entre las diferentes instancias de Amazon EC2 y direcciones IP.

  En la solución propuesta se utiliza para que, si existe una fuerte demanda, las peticiones de los usuarios sean balanceadas en los diferentes contenedores e instancias.

- **Amazon EC2:** Amazon Elastic Cloud Computer, es un servicio web que proporciona seguridad, capacidad de cálculo y redimensionable en la nube. Está diseñado para facilitar la computación escalable a los desarrolladores.

La solución propuesta utiliza Amazon EC2 para lanzar instancias con los distintos servidores web que correrán el frontend y backend del portal de administración.

- **Amazon EC2 Auto Scaling**: el cual ayuda a mantener la disponibilidad de la aplicación y le permite aumentar o reducir dinámicamente la capacidad de Amazon EC2 de forma automática según las condiciones que defina. Amazon EC2 Auto Scaling está habilitado por Amazon CloudWatch y no tiene cargos adicionales. Las tarifas de servicio de Amazon EC2 y Amazon CloudWatch se aplican y se facturan por separado.

  La solución propuesta utiliza Amazon EC2 Auto Scaling para mejorar la tolerancia a errores, poder contar con una mejor disponibilidad de servicio, mejor administración de costos y por último y más importante, cubrir la demanda variable que puede ocurrir en el portal lo cual disminuye significativamente los costos.

- **Amazon Marketplace: Hyperledger Sawtooth**: es una solución empresarial para la creación y despliegue de cadena de bloques. En la solución propuesta, Hyperledger Sawtooth es utilizado para el despliegue de la cadena de bloques y la trazabilidad de la cadena de suministro.

- **Amazon Relational Database Service (Amazon RDS)**: es un servicio de Amazon Web Services el cual facilita configurar, operar y escalar una base de datos relacional.

  Este servicio es utilizado en la solución propuesta para la base de datos relacional que es utilizada por el portal de administración, el servidor de reportería y el motor de decisión.

- **Amazon Simple Notification Service (SNS):** es un servicio de Amazon Web Services con el cual se puede gestionar mensajerías usando un patrón publish/subscribe para puntos finales y clientes suscritos.

  Gracias al uso de este tipo de arquitectura basada en computación en la nube, la plataforma tiene la capacidad de ser escalable, aumentar la disponibilidad de los servicios y reducir costes tantos iniciales como de operación.

3.3. METODOLOGÍAS DE TRABAJO

Para una buena gestión del ciclo de vida de desarrollo de Software, es necesario tener en cuenta que en todos los proyectos la principal prioridad es satisfacer al usuario final a través de la entrega temprana y continua de software que le aporte algún valor.

Para estos fines, en la solución propuesta se utilizará las metodologías ágiles como vía para mantener un desarrollo sostenido y que exista un método de comunicación efectiva.

3.3.1. METODOLOGÍA ÁGIL SCRUM

Es un framework dentro del cual las personas pueden abordar problemas complejos de adaptación, a la vez que entregan de forma productiva y creativa productos con el mayor valor posible (Ken Schwaber, 2013).

Scrum como metodología ágil puede ayudar al equipo de desarrollo a llevar una gestión de las expectativas del cliente, conseguir resultados anticipados y mantiene al equipo implicado en los objetivos del negocio.

La metodología ágil scrum está basado en los roles, equipos, eventos, artefactos y reglas. Cada elemento desempeña una función específica el cual hace que funcione con éxito.

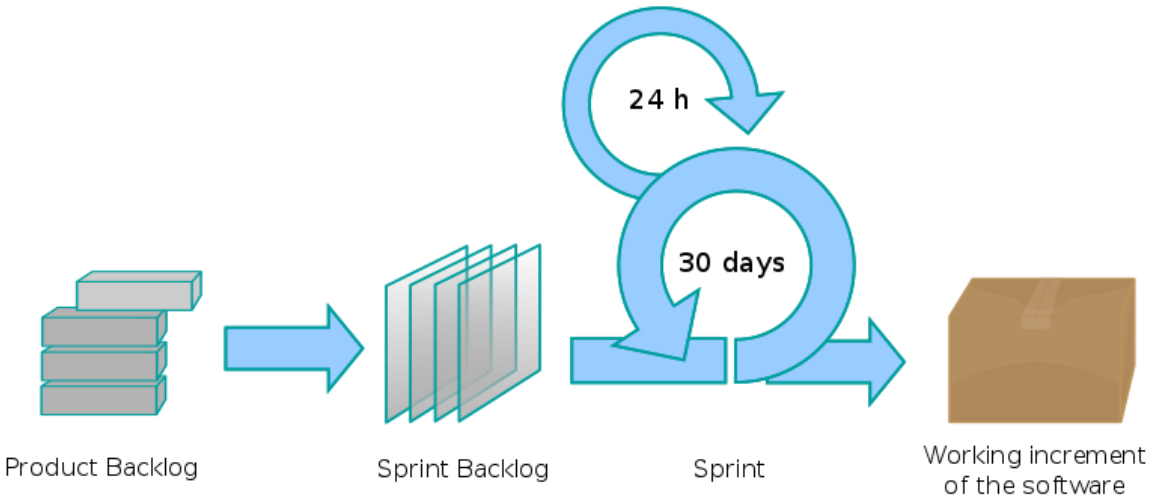


Fig. 31, Flujo del marco de trabajo de Scrum para un Sprint.
Fuente: Lakeworks, 2009

Roles:

Los equipos en el marco de trabajo entregan valor de forma iterativa e incremental, los mismos son organizados de forma autónoma y realizan funciones sin ser dirigidos por personas del exterior. Dentro de los equipos de Scrum existen diferentes roles los cuales desempeñan funciones específicas. Estos roles son los siguientes:

1. **Dueño del producto (Product Owner):**

   El propietario del producto Scrum suele ser el principal interesado en el proyecto. Parte de las responsabilidades del propietario del producto es tener una visión de lo que él o ella desea construir, y transmitir esa visión al equipo de scrum.

   Este rol es el responsable de definir y tener claros los requisitos funcionales. Crear historias de usuarios y determinar sus criterios de aceptación. En la solución propuesta tendremos

un dueño del producto encargado de recoger las necesidades del cliente y de alimentar el product backlog.

2. **Equipo de desarrollo (Development Team):**

El equipo de desarrollo en el marco de trabajo de Scrum, son aquellas personas las cuales tienen la responsabilidad de entregar un producto incrementar y funcional al final de cada sprint. Unas características del equipo de desarrollo es que son multifuncionales y autoorganizados.

El equipo de desarrollo de la solución está conformado por:

- 3 desarrolladores Back-end
- 2 desarrolladores Front-end
- 1 desarrollador de Ethereum Smart Contract
- 3 analistas de Aseguramiento de la Calidad
- 1 analista de base de datos
- 1 especialista Hyperledger Sawtooth
- 1 especialista Amazon Web Services (DevOps)
- 1 líder técnico de proyecto

Estos recursos anteriormente mencionados se encargados del desarrollo y despliegue de la plataforma.

3. **Scrum Máster:**

El scrum máster es el responsable de que se cumplan las reglas y se solucionen los problemas. El mismo gestiona el proceso, orienta al equipo para que se autogestionen y logren las metas y trata de que entiendan bien sin perder tiempo ni velocidad.

Eventos:

Los eventos en scrum se utilizan para minimizar la cantidad de reuniones y que se mantenga un patrón constante.

Todos los eventos de scrum se realizan en base a un tiempo de bloques (time-box). Este tiempo es definido para cada evento y no puede extenderse a menos que no se haya logrado el objetivo de la reunión.

En el desarrollo la convocación de estos eventos será importantes porque reducirán las reuniones y van a identificar y eliminar impedimentos que puedan surgir durante el ciclo de vida de desarrollo.

Los diversos eventos que se realizan dentro del marco de scrum son:

1. Sprint: Es un ciclo de tiempo que va alrededor de 2-4 semanas durante el cual se crea un incremento funcional del producto.

Este evento es el corazón de scrum y debe realizar a partir de un backlog detallado y priorizado. Para el desarrollo de la solución propuesta se harán sprint con un tiempo de duración de dos semanas.

2. Sprint Planning (Planificación del Sprint): La planificación del sprint es una reunión que se realiza previo al iniciar un nuevo sprint. En este evento se dice cuál será el objetivo del sprint y las tareas para lograrlo.
3. Daily Scrum: Es una breve reunión diaria donde los recursos comentan al equipo en que están trabajando y si tienen algún impedimento.

4. Revisión del Sprint (Sprint Review): La revisión del sprint es una especie de demo en la cual se muestra los avances del producto. En esta reunión participa los Stakeholders (Supermercado) invitados por el product owner y el equipo scrum completo.

5. Retrospectiva del Sprint (Sprint Retrospective): La retrospectiva es un evento de scrum en el cual el equipo realiza una inspección y recoge feedback sobre posibles mejoras a aplicar para el próximo sprint. En

esta reunión debe participar el equipo de scrum completo y durará 2 horas máximos.

Product Backlog:

El Product Backlog es una lista prioritaria de necesidades de los usuarios, historias de usuarios a realizar para crear, mantener y sostener un producto.

El Propietario del Producto (Product Owner) es dueño de la lista de tareas, él es quien la prioriza basándose en los comentarios de los clientes o en el valor del negocio.

Algunas de las características del Product Backlog son:

1. Es un documento muy activo en el que se recogen todos los deseos y necesidades de los usuarios.
2. El propietario del producto se asegura de que el contenido de las "historias de usuario" de los productos pendientes esté definido en el nivel detallado.
3. Todos los aspectos como escenarios de casos de uso, condiciones de satisfacción y criterios de aceptación deben ser proporcionados en cada una de las historias de usuarios.

Sprint Backlog:

El Sprint Backlog es el listado de tareas identificadas por el equipo para ser completadas durante ciclo de vida del Sprint actual. Las tareas del Sprint backlog serán asignadas a usuarios del equipo de desarrolladores y las mismas contienen pesos y prioridades.

Para el desarrollo de la solución, es de vital importancia que el equipo seleccione las tareas y tamaño del Sprint Backlog. Debido a que ellos son las personas que se comprometen a completar las tareas, ellos deben ser las personas que elijan lo que se comprometen durante el sprint de Scrum.

3.3.2. ACTORES E HISTORIAS DE USUARIOS

Dentro del marco de trabajo de scrum para la definición de los requisitos se utiliza las historias de usuarios. En la solución propuesta se utiliza las historias de usuarios para hacerle entender al equipo de desarrollo las tareas de una forma clara y precisa.

Dentro de los actores y las historias de usuarios relacionados se destacan:

Administrador de la plataforma

Es el usuario quien tiene la responsabilidad de mantener, configurar y gestionar accesos a la plataforma. Es un actor único dentro del sistema ya que tiene permiso a todos los recursos de la plataforma.

Historias de usuario del administrador general

1. *Como administrador del sistema quiero poder dar de altas a usuarios y asignarles roles para que cumplan con sus asignaciones.*
2. *Como administrador del sistema quiero poder crear nuevas sucursales para que puedan realizar sus operaciones.*

Gerente de Compras

Es el actor dentro del sistema quien tiene la responsabilidad de toda la división de compras, entre las acciones que puede ejecutar están realizar solicitudes de cotizaciones, órdenes de compra, recepción de facturas y autorización de entradas de productos.

Historias de usuario del gerente o encargado de compras

1. *Como gerente de compras quiero poder realizar solicitudes de cotizaciones a los proveedores para verificar y determinar si conviene comprar a dicho proveedor.*
2. *Como gerente de compras quiero poder realizar órdenes de compra para aprovisionar el almacén con productos.*
3. *Como gerente de compras necesito poder hacer recepciones de factura para proceder a pagar a los proveedores.*
4. *Como gerente de compras quiero poder autorizar unas entradas de productos para que el personal de almacén realice sus labores.*

Encargado Almacén General

Es el actor dentro del sistema quien, a pesar de tener un papel tradicionalmente muy manual, ahora con la solución propuesta podrá ejecutar acciones, realizar consultas y búsquedas de información de los productos, salida de productos y ya no tiene la responsabilidad de notificar al encargado de compras la necesidad de adquirir nuevos suministros.

Historias de usuario del gerente o encargado de almacén

1. *Como gerente o encargado de almacén quiero poder hacer búsquedas de información para saber la existencia de un producto.*
2. *Como gerente o encargado de almacén quiero poder realizar búsquedas sobre un lote de producto para saber los parámetros en los cuales se transporte desde su origen (Proveedor).*
3. *Como gerente o encargado de almacén quiero poder realizar salidas de productos para sacarlo de inventario o de existencia.*
4. *Como gerente o encargado de almacén quiero poder generar reportes sobre las existencias de un producto para facilitar a los recursos de base de datos en caso de que lo requieran.*

Encargado, Supervisor y Auxiliar de Inventario

Son los actores dentro del sistema quien tiene la facultad de generar reportes diarios, semanales y mensuales sobre los niveles de disponibilidad de la mercancía, realiza y programa inventarios en el almacén.

Historias de usuario del gerente o encargado de inventario

1. *Como encargado o supervisor de inventario quiero poder generar reportes diarios, semanales y mensuales sobre los niveles de disponibilidad de la mercancía para poder llevar a cabo los inventarios.*
2. *Como encargado o supervisor de inventario quiero poder agendar o programar la realización de inventarios para que las otras áreas puedan organizarse y estar preparadas para cumplir el objetivo en común.*
3. *Como encargado o supervisor de inventario quiero poder crear y almacenar por fechas los informes realizados sobre el inventario para que haya una constancia en el sistema del trabajo realizado.*
4. *Como encargado o supervisor de inventario quiero poder hacer búsquedas con filtros de fechas en el sistema de los inventarios realizados para suministrar la información a la división de compras.*

Supervisor de Fresco (Vegetales, Carnes)

Es un actor muy importante en el sistema porque es el responsable de confirmar y validar si el producto está en las condiciones de calidad para ser vendidos en las góndolas y mostradores.

Historias de usuario del supervisor de fresco

1. *Como supervisor de fresco quiero poder realizar una búsqueda de datos históricos de la cadena de suministro de un lote de producto para saber algunos factores como humedad y temperatura hasta llegar al supermercado.*
2. *Como supervisor de fresco quiero poder enviarle notificación a los encargados de las góndolas para que siempre haya disponibilidad de productos en unas determinadas áreas de la tienda.*
3. *Como supervisor de fresco quiero poder recibir notificaciones sobre el vencimiento de productos que se están ofreciendo en las góndolas para poder evitar posibles daños.*

Proveedores

Los proveedores son actores vitales dentro del sistema y la cadena de suministro. Tienen la facultad de ver la trazabilidad de sus productos, consultar los históricos de sus productos y la creación de usuarios del sistema pertenecientes a su empresa.

Historias de usuario de los proveedores

1. *Como proveedor quiero poder ver la trazabilidad de la cadena de suministro para ver algunos parámetros en los cuales viajan nuestros productos y poder mejorar precios y costos.*
2. *Como proveedor quiero consultar información e históricos sobre nuestros productos ofrecidos para poder tener mayor conocimiento y poder mejorar nuestros procesos internos.*
3. *Como proveedor quiero poder crear usuarios en el portal de gestión relacionados a nuestra empresa para que los recursos de nuestras empresas puedan realizar sus labores y asignaciones.*
4. *Como proveedor quiero responder a las solicitudes de cotizaciones emitidas por el supermercado para que todo esté centrado en la misma plataforma.*

3.4. TECNOLOGÍAS Y HERRAMIENTAS

Las tecnologías y herramientas de desarrollos están evolucionando a un ritmo muy rápido, lo cual es muy bueno o puede resultar un ciclo de cambios muy drásticos para los equipos de desarrollo de software. En la actualidad, es de vital importancia que se seleccione la tecnología adecuada para llevar a cabo los desarrollos de una solución porque de esto dependerá el éxito del equipo y del proyecto de software como tal.

3.4.1. Repositorio de Código y Control de Versiones

Un control de versión es la gestión que se realice sobre los diferentes cambios que se le hace a un producto o software. En la actualidad, el control de versiones por excelencia es Git. Debido a que está enfocado en la flexibilidad para los desarrolladores y cuenta con un conjunto de herramientas para gestionar el código del software.

Para el desarrollo de la solución propuesta se utilizará Git como control de versiones porque es open source y cuenta con la comunidad de desarrollo más grande de los controles de versiones. El control de versión Git almacena la información y datos en un repositorio. Los repositorios pueden ser tantos públicos como privados. Para la solución propuesta se utilizará Github, lo cual es una plataforma para alojar proyectos de software utilizando el control de versiones de Git.

3.4.2. Lenguajes de Programación

Los lenguajes de programación que se utilizara para la solución van a depender del proyecto para el cual se va a desarrollar.

Es decir, para el Portal de Administración de la Cadena de Suministro se va a utilizar Java para la creación de los servicios web y se utilizará Javascript para la creación del proyecto UI.

Para desarrollar funcionalidades para la Blockchain y Contratos Inteligentes se utilizará Solidity. Este último, es un lenguaje de programación de alto nivel orientado a contratos y es muy parecido al lenguaje de programación Javascript.

3.4.3. Entornos de Desarrollo Integrados (IDE)

Un entorno de desarrollo integrado (IDE) es un paquete de software que contiene las herramientas básicas que los desarrolladores necesitan para escribir y probar software.

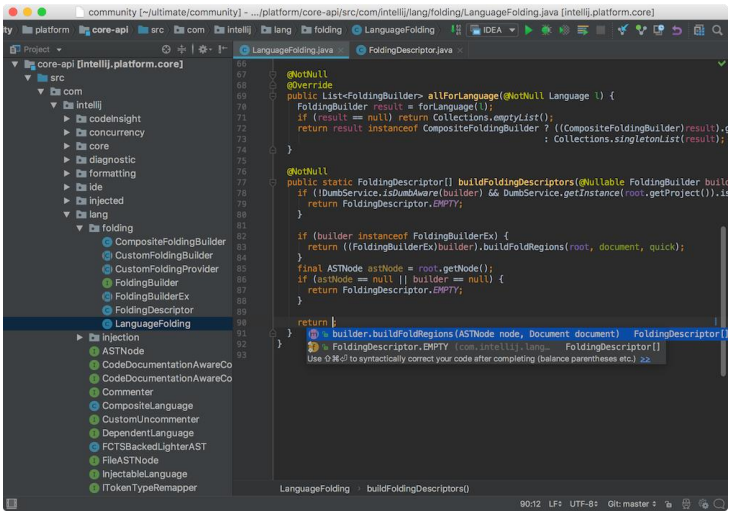


Fig. 32, Entorno de Desarrollo Integrado (IDE) IntelliJ IDEA. Fuente: Jetbrains, 2018

En el proyecto del Portal de Gestión de la cadena de Suministro (SCM) para la parte de los servicios web como se está utilizando el lenguaje de programación Java, el IDE ideal para los desarrollos es IntelliJ IDEA de la empresa Jetbrains. Como se puede apreciar en la Fig. 32 es un entorno muy completo con todas las necesidades que pueda tener el desarrollador. Para la parte visual del portal se va a utilizar Visual Studio Code, este es un editor de texto, pero es escalable y soporta muchas funcionalidades las cuales se les pueden agregar vía extensiones.

3.4.4. Base de Datos

El portal de Gestión de la Cadena de Suministro (SCM) utilizará como gestor de base de datos PostgreSQL. Este gestor es open-source y es mantenido por una amplia comunidad de desarrolladores.

Dentro de la arquitectura de la plataforma, el gestor de base de datos PostgreSQL será desplegado usando el servicio Amazon Relational Database Service (RDS), el cual nos permite dentro de la arquitectura tener una duplicación de la instancia de base de datos para contingencias en caso de fallas.

3.4.5. Frameworks y Librerías

Entre los frameworks y librerías que utilizaran los proyectos se encuentran:

Spring Framework (Spring Boot):

Es una plataforma Java que proporciona soporte de infraestructura integral para el desarrollo de aplicaciones Java. Spring maneja la infraestructura para que usted pueda concentrarse en su aplicación.

Dentro de la solución se utilizará para desarrollar los Servicios Web REST del Portal de Gestión de la Cadena de Suministro.

Hibernate y JPA:

Es un framework de Mapeo objeto-relacional (ORM) para el lenguaje de programación Java el cual nos permite hacer mapeo de atributos entre una base de datos y los objetos de una aplicación.

Dentro de la solución propuesta, este framework para mapeo de objetos se utilizará para hacer el modelo de base de datos con un enfoque CodeFirst. Es decir, no se realizará un diseño previo de base de datos, los objetos de la base de datos serán creados a partir de las clases del aplicativo.

Angular:

Angular es un framework que facilita la creación de aplicaciones web. Angular utiliza los conceptos de plantillas declarativas, inyección de dependencias y pruebas unitarias para el desarrollo. Es un framework totalmente basado en componentes y permite la creación de aplicaciones móviles.

Para el desarrollo de la solución, será utilizado para crear la parte visual (UI) del Portal de Gestión de la Cadena de Suministro (SCM).

3.5. REQUISITOS FUNCIONALES

Los requisitos funcionales son aquellos que representan una funcionalidad de la plataforma de Software o más bien de sus componentes. Es decir, describen cualquier actividad, funcionalidad y comportamiento que un sistema pueda tomar. Los requerimientos y sus diagramas de caso de usos representan la interacción que tendrá cada actor del sistema con el mismo.

- **Configuración de la plataforma:**

Este requerimiento especifica todo lo relacionado a la configuración inicial de la plataforma y todo lo relacionado con la gestión de sucursales, usuarios, roles y permisos de accesos. Como se puede visualizar en la figura. #33, el usuario administrador de los proveedores también tendrá la facultad de crear usuarios pero pertenecientes a su organización.

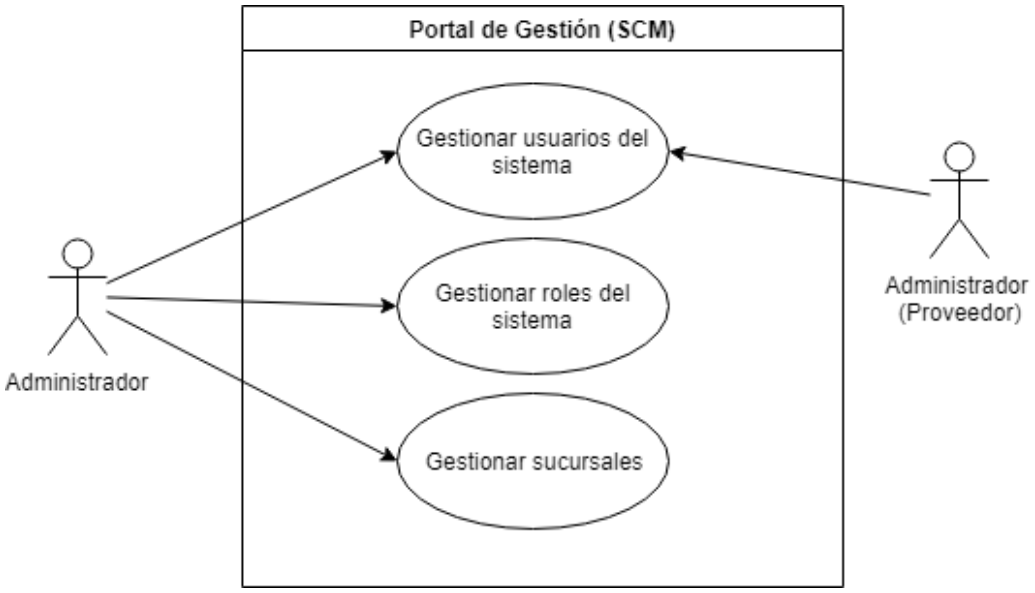


Fig. 33, Diagrama de Caso de Uso para la Configuración de la Plataforma.
Fuente: Propia

➢ **Gestión de Compras**

Este requerimiento especifica todas las funcionalidades que podrán realizar los usuarios de la división de compras. Estos podrán realizar el proceso entero desde gestionar una cotización hasta autorizar la entrada de los productos al almacén.

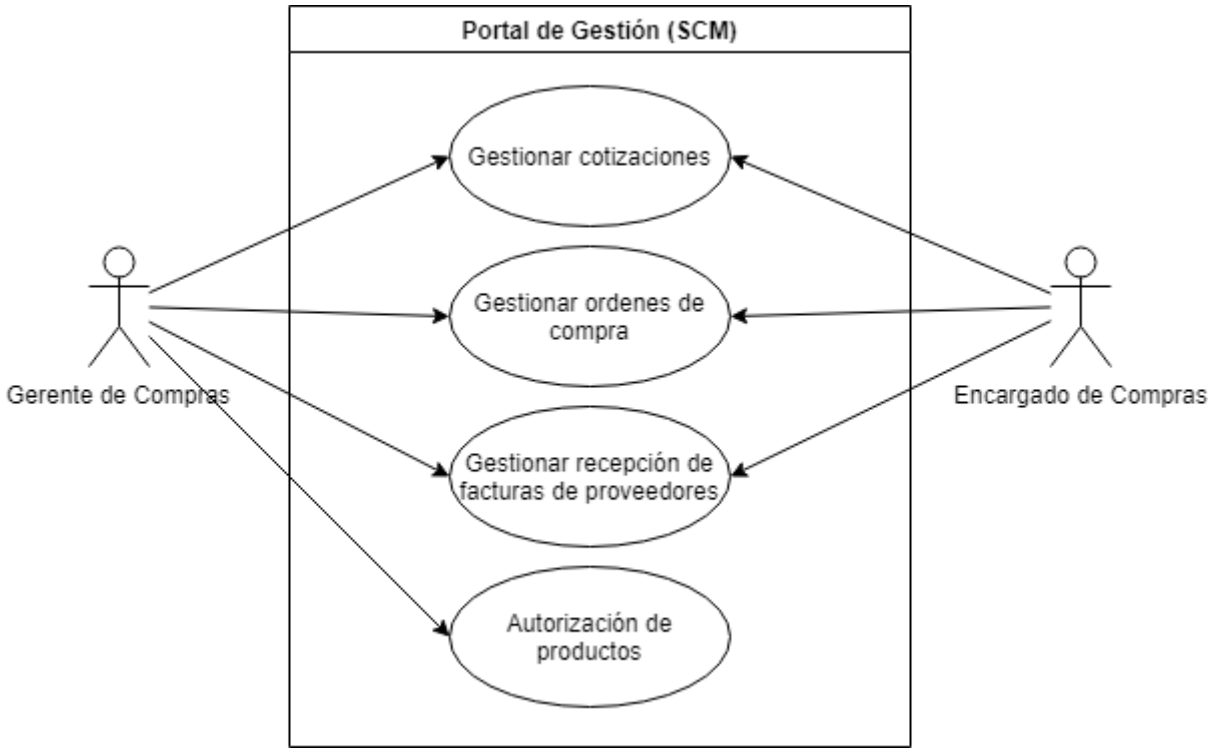


Fig. 34, Diagrama de Caso de Uso para la Configuración de la Plataforma.
Fuente: Propia

Como se puede visualizar en la figura. 34, los actores que intervienen en el proceso de compras podrán realizar las mismas funcionalidades a excepción de la autorización de los productos para que sean entrados al almacén debido a que esto requiere un proceso de autorización por parte de la gerencia.

➢ **Gestión de Almacén**

Este requerimiento especifica las funcionalidades que podrán realizar los encargados de almacén. Dentro de los requerimientos principales se encuentran consultas y búsquedas de información e históricos sobre los productos y salida de productos. En la siguiente imagen se puede visualizar como es la interacción de este actor con el sistema.

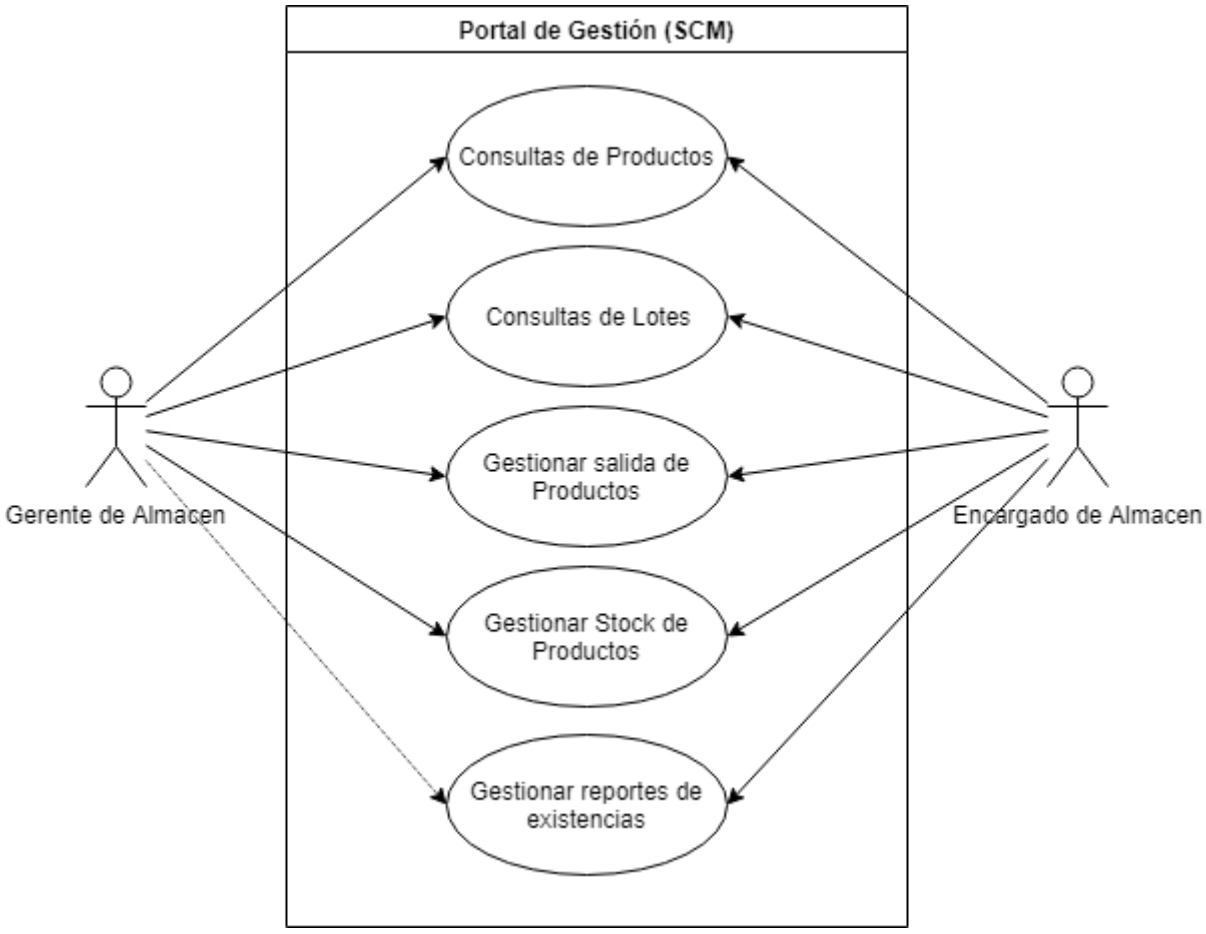


Fig. 35, Diagrama de Caso de Uso para la Gestión del Almacén.
Fuente: Propia

➢ **Gestión de Inventarios**

Este requerimiento especifica las funcionalidades que podrán realizar los recursos encargados del inventario. Estos poseen la facultad de generar estadísticas, reportes por periodos de tiempo (diarios, semanales, mensuales) sobre la disponibilidad de la mercancía y programar o agendar fecha para la realización de inventarios.

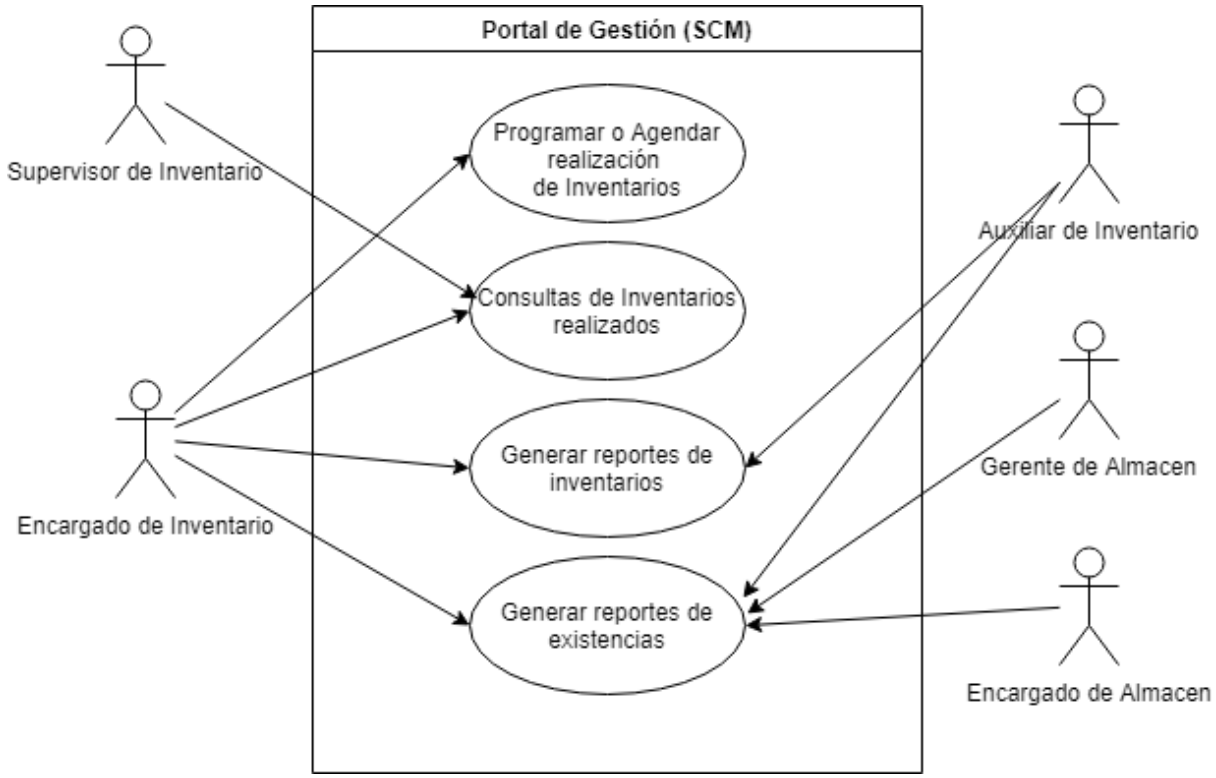


Fig. 36, Diagrama de Caso de Uso para la Gestión de Inventario.
Fuente: Propia

Como se muestra en la figura. 36, en el proceso de Gestión de Inventarios intervienen dos actores adicionales del sistema, el Gerente de Almacén y Encargado de Almacén.

➢ **Gestión de Tienda (Fresco)**

Este requerimiento especifica las funcionalidades que podrán realizar los recursos encargados del área de fresco del supermercado Nuevo Renacer. Dentro de sus funcionalidades están realizar búsqueda de datos históricos de la cadena de suministro de un lote de producto para saber algunos factores como humedad y temperatura hasta llegar al supermercado y envíos de notificación a los encargados de las góndolas para que siempre haya disponibilidad de productos en unas determinadas áreas de la tienda.

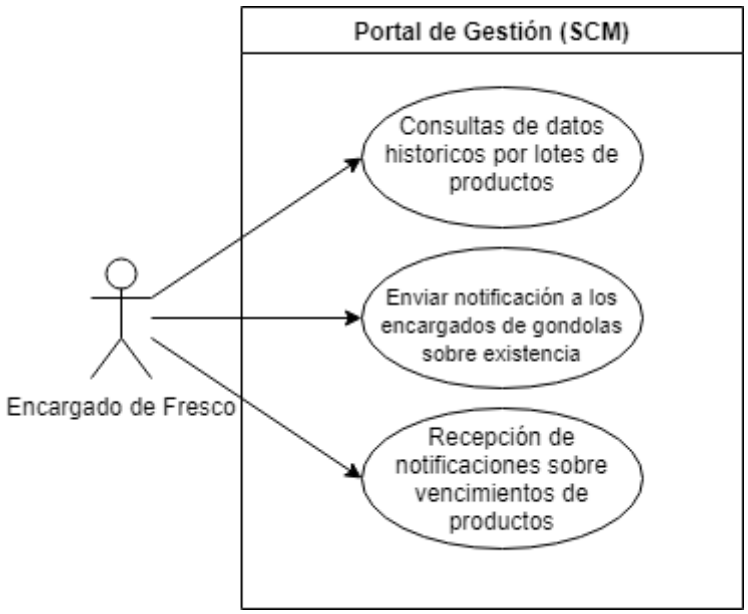


Fig. 37, Diagrama de Caso de Uso para la Gestión de Fresco (Vegetales, Carnes).
Fuente: Propia

➢ **Gestión operativa (Supermercado)**

Este requerimiento especifica las funcionalidades que podrían realizar los recursos encargados del área operativa del supermercado. Dentro de todas esas funcionalidades se encuentran: visualizar la trazabilidad de la cadena de suministro, generar reportes de inteligencia de negocios, administrar y dar seguimiento a casos.

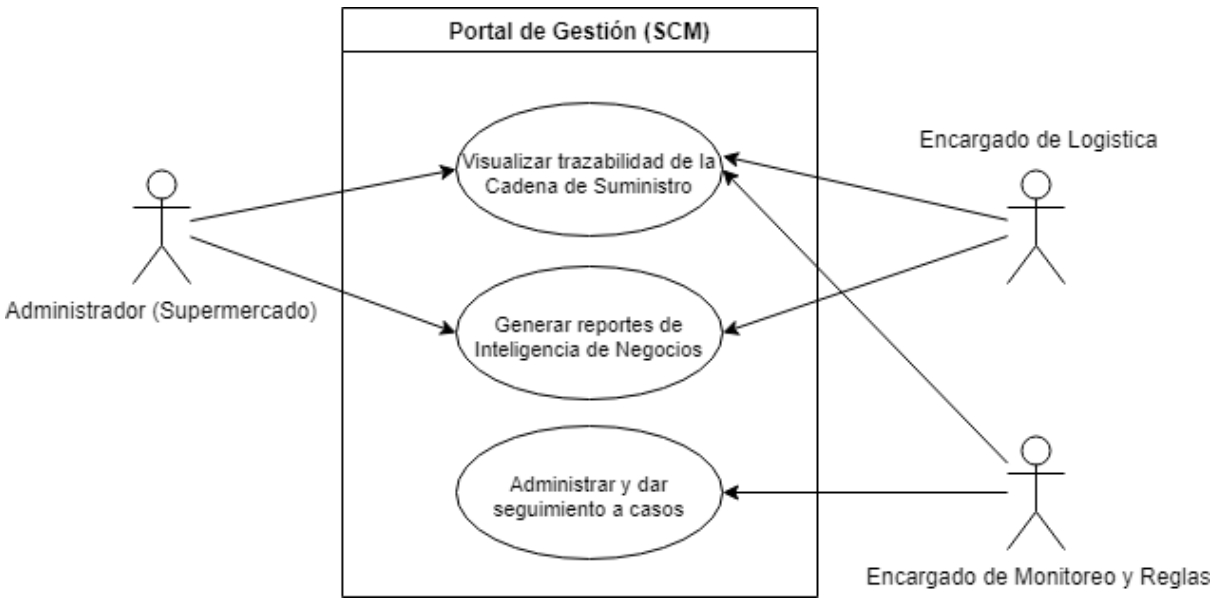


Fig. 38, Diagrama de Caso de Uso para la Gestión operativa del Supermercado. Fuente: Propia

➢ **Gestión operativa (Proveedores)**

Los proveedores son una pieza clave para el proceso de la Cadena de Suministro del supermercado y de cualquier organización. Debido a que la solución propuesta es Multi Tenancy, los proveedores van a contar con usuarios los cuales tendrán accesos a funcionalidades como: ver la trazabilidad de sus productos, consultar históricos de sus productos y la creación de usuarios del sistema pertenecientes a su organización.

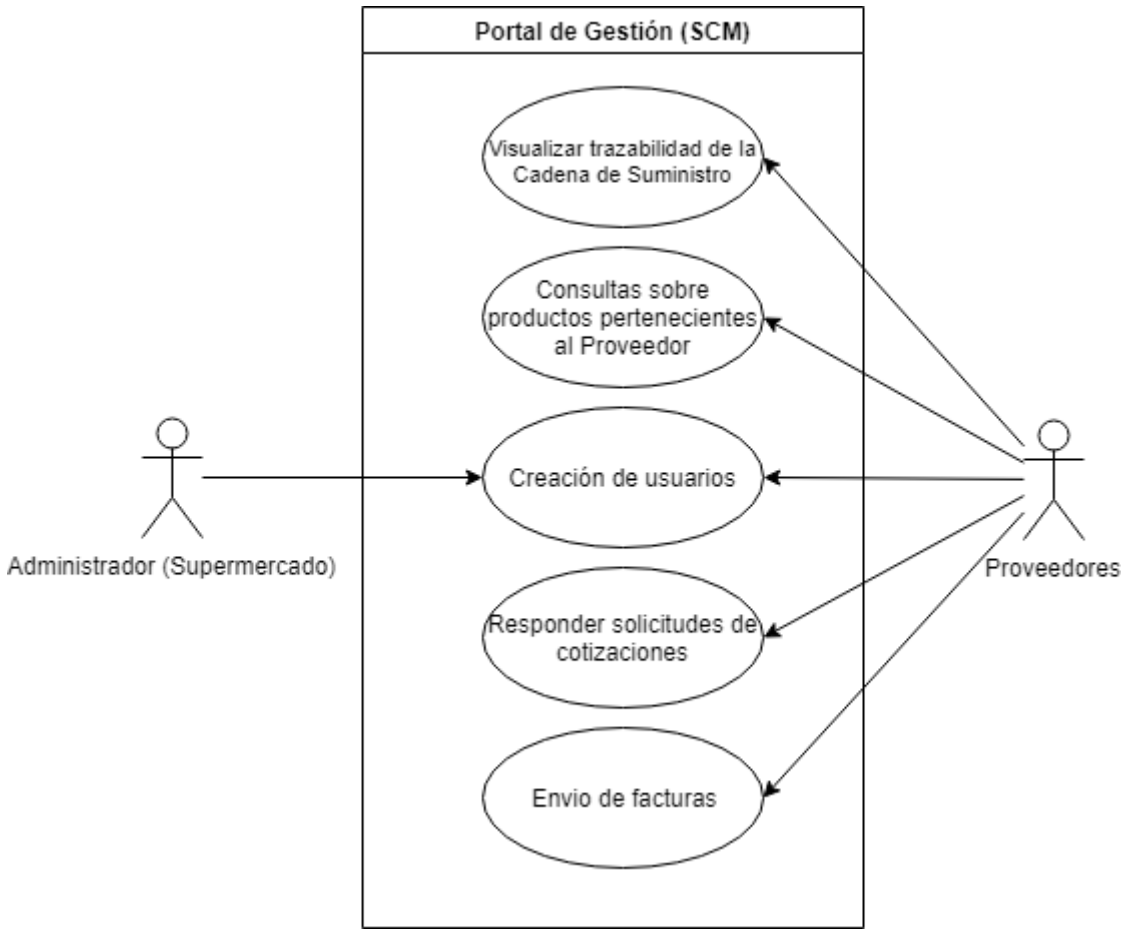


Fig. 39, Diagrama de Caso de Uso para la Gestión operativo de proveedores.
Fuente: Propia

3.6. REQUISITOS NO FUNCIONALES

Los requerimientos no funcionales son aquellas características que se deben tener en cuenta, ya que son necesarias para que se expongan de manera general sin hacer referencia o tomar en cuenta aspectos específicos de una aplicación.

Estos por lo general se presentan como un complemento a los requerimientos funcionales, su principal objetivo es el de procurar la mayor calidad durante el desarrollo y diseño.

Entre los requerimientos no funcionales especificados para la plataforma SCM están:

- **Arquitectura:**
  - Está conformada por varios elementos claves, estos son: Hyperledger Sawtooth, Arduinos y sensores, Portal de Gestión SCM, Motor de Inteligencia de Negocios y Amazon Web Services

- **Requerimientos de seguridad del sistema:**
  - La plataforma debe encriptar todas las contraseñas a nivel de base de datos.

- Los permisos de acceso al sistema podrán ser cambiados solamente por el administrador de acceso a datos.
- Las sesiones de usuarios deberán ser confirmadas cada dos horas, sin importar el nivel de actividad.
- Los permisos de acceso sólo serán modificados por el administrador general.
- Todas las bases de datos deberán ser respaldadas cada 24 horas.
- Todas las comunicaciones de bajo nivel serán encriptadas utilizando el algoritmo AES256.
- Las sesiones de un usuario deberán ser confirmada luego de 10 minutos de inactividad en ella.
- La comunicación que habrá entre los nodos deberá trabajar bajo la capa de seguridad SSL.

➢ **Requerimientos de usabilidad:**

- La apariencia de la aplicación debe promover la homogeneidad y armonía en el uso de colores e imágenes.
- La plataforma debe proporcionar mensajes de errores descriptivos, informativos y entendibles.

- La interfaz gráfica con la que el usuario final interactúa debe ser intuitiva, de manera que, sin un manual de uso, el usuario identifique rápidamente los componentes y las secciones del sistema.
- La presentación visual debe disponer de colores agradables a la vista para que el usuario pueda trabajar durante más de 2 horas seguidas sin tener mayores inconvenientes.
- El tiempo de aprendizaje del sistema por un usuario deberá ser menor a 4 horas.
- La interfaz de usuario debe garantizar la compatibilidad con los navegadores más comunes (Google Chrome, Firefox, Explorer).
- La interfaz de usuario debe permitir la escalabilidad en términos técnicos, sin que esta pierda de vista la homogeneidad ni la armonía.
- La plataforma debe contar con un manual de ayuda digital.

3.7. ESTRUCTURA DE BASE DE DATOS

La base de datos es un conjunto de información almacenada, en la cual se encuentran una serie de datos que están relacionadas entre sí y permite el acceso a ella, como también, es un conjunto de programas que puede ser manipulable por el usuario, cada una se componen de una o más tablas que dentro de esta guarda un conjunto de campos.

El diseño de la base de datos para el Portal de Gestión de la Cadena de Suministro (SCM) se estará basando en un modelo relacional, lo cual consiste en una estructura optimizada para hacer más eficiente al negocio, Además de monitorear procesos, asegurar la accesibilidad y disponibilidad en cualquier momento. Este ayuda a tener un incremento en la productividad y por último garantiza la eficiencia y agilidad.

Como se puede observar en la *Figura. 40*, en el modelo relacional de la solución propuesta del Portal de Gestión de la Cadena de Suministro existen un total de 15 entidades para el funcionamiento de toda la plataforma.

Para modelar la base de datos se utiliza un enfoque Code First con Hibernate, lo cual es una herramienta de mapeo objeto-relacional del lenguaje de programación Java.

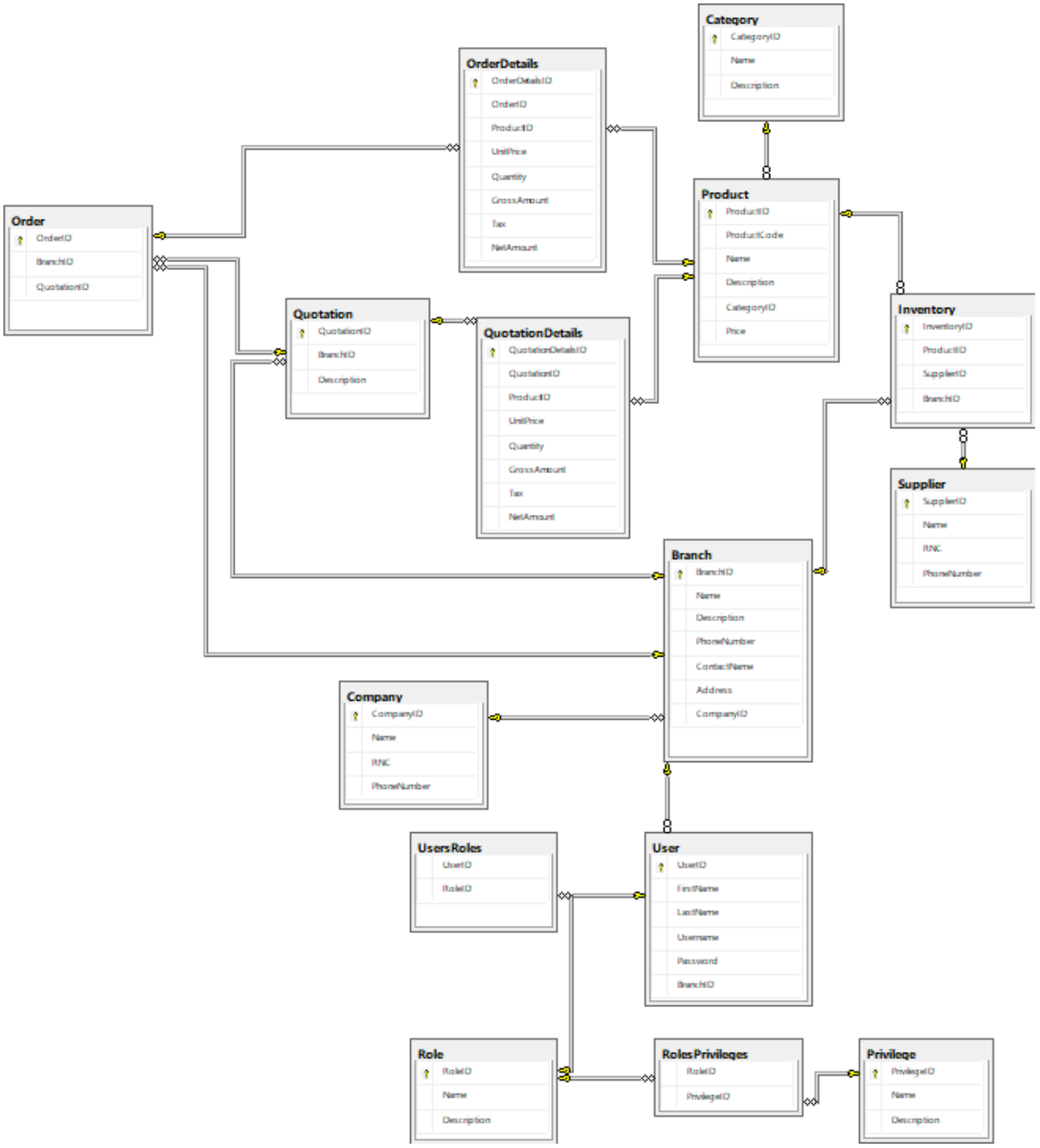


Fig. 40, Estructura de la Base de Datos de la Plataforma SCM.
Fuente: Propia

Con el hecho de tener una base de datos normalizada, se abre un abanico de oportunidades para evitar la duplicación de los datos y que se eliminen dependencias que no permitan a la eficiencia de los métodos de accesos a datos.

3.8. ANÁLISIS FINANCIERO

El análisis financiero es definido como uno del proceso que comprende la recopilación de información, interpretación, comparación y estudio de los estados financieros y los datos de operaciones de un negocio o proyecto con el principal objetivo de poder evaluar su viabilidad en términos económicos y si este es sustentante. Así mismo, esta busca mostrar información cuantitativa en términos financieros y operativos, para poder identificar y evaluar por medio del análisis la viabilidad económica que tiene un plan de negocio. En ese sentido, el valor de una empresa es un concepto cuya comprensión es muy compleja en la vida práctica, pero se puede decir que indica el valor de un mercado de cada acción o aporte a la sociedad, y que, de alguna manera, a través del tiempo, el valor promedio de la acción se refleja en el éxito o fracaso de la gestión financiera.

Parte principal de este proyecto es el ofrecer al cliente una solución que le permita controlar eficientemente sus operaciones, teniendo una visibilidad completa de su cadena de suministro y así poder detectar fallas en la calidad a tiempo, aprovechando al máximo los beneficios de sus recursos, de modo que incrementen sus utilidades y disminuyan las pérdidas.

A continuación, se conocerá el presupuesto referente al hardware y el software de la implementación de Blockchain. El presupuesto referente a software, hardware (equipos IT).

El cliente cuenta con el espacio físico y tiene todos los equipos necesarios para implementación del proyecto, este cuenta con una cantidad

de tres pc en el departamento, con el cual solo debe de conectarse a internet y este también cuenta con esto y así poder acceder al portal SCM.

A continuación, se le presenta una tabla con el presupuesto necesario para iniciar el proyecto:

Tasa del dólar	$49,00

Recursos	Cantidad	Monto	Precio x dólar	Monto total	Monto mensual
Equipos IT					
GPS Shield Kit(2 sensores y chip LTE)	10	$80,00	DO39,200.00	DO39,200.00	Solo comprado una vez
Arduino Uno	10	$20,00	DO9,800.00	DO9,800.00	Solo comprado una vez
Infraestructura y Software					
AWS Cloud	1	$0,00	DO0,00	DO0,00	DO0,00
Github	1	$7.00	DO 343.00	DO 343.00	DO 343.00
Amazon Route 53	1	$0.400	DO 19.06	DO 19.06	DO 19.06
ADAPA Decision Engine	1	$1680.0336	DO 82,321.6464	DO 82,321.646	DO 82,321.646
hosted zones	1	$0.50	DO 24.5	DO 24.5	DO 24.5
Amazon Virtual Private Cloud (Amazon VPC)	1	$19.048	DO 933.352	DO 933.352	DO 933.352
Amazon EC2	1	$141.412352	DO 6929.205248	DO 6929.205248	DO 6929.205248
Hyperledger Sawtooth	1	$0.07	DO 3.28	DO 3.28	DO2,363.76
Total de recurso				DO90.574,043248	DO92.934,523248

Tabla 2. Presupuesto de Recursos necesarios Pos-Proyecto de services Plan.
Fuente: Propia

En la tabla #2 se encuentra el presupuesto de los recursos para que se pueda implementar la propuesta para la visibilidad completa de la cadena de suministro.

3.9. GASTOS OPERATIVOS

"La noción de gastos de operación hace referencia al dinero desembolsado por una empresa u organización en el desarrollo de sus actividades. Los gastos operativos son los salarios, el alquiler de locales, la compra de suministros y otros." Julián Pérez Porto y Ana Gardey. Publicado: 2009. Actualizado: 2013.

Los gastos de operaciones se pueden definir como el mantenimiento a una propiedad, tales como servicios públicos, impuestos sobre la propiedad o el cómo también el seguro. Otros de sus principales objetivos es poder verificar los costos de operación teniendo en cuenta que esta no incluye financiación sin interés o impuesto sobre la renta que son el resultado de los ingresos de un negocio o proyecto.

En cuanto la nómina se tiene los siguientes gastos, desglosados primero generalizado y también la nómina de empleados:

Recursos	Cantidad	Monto	Monto total
Muebles:			
Sillas	30	13000	DO390.000,00
Sillas ejecutivas	10	18000	DO180.000,00
Escritorios	40	17000	DO680.000,00
Estantería	15	11000	DO165.000,00
Escritorio sala de juntas	1	80000	DO80.000,00
Sillas para escritorio de juntas	20	9000	DO180.000,00
Archivero	5	4000	DO20.000,00

Muebles	1	25000	DO25.000,00
Total			DO1.720.000,00
Alimentos:			
Café	864	120	DO103.680,00
Agua	432	60	DO25.920,00
Desayuno	5220	150	DO783.000,00
Almuerzo	5220	300	DO1.566.000,00
Azúcar	5039	72	DO362.808,00
Total			DO2.841.408,00
Desechables:			
Vasos	288	80	DO23.040,00
Platos	576	50	DO28.800,00
Servilletas	216	80	DO17.280,00
Papel higiénico	288	70	DO20.160,00
Fundas de basura	360	60	DO21.600,00
Utensilios de comida	1008	20	DO20.160,00
Total			DO131.040,00
Recursos tecnológicos:			
Sistema biométrico de control de acceso	1	14000	DO14.000,00
Computadores desktop:	20	48000	DO960.000,00
Computadores laptop:	5	86000	DO430.000,00
Impresora multifuncional pro:	3	25000	DO75.000,00
Memoria usb 64gb	25	750	DO18.750,00
Proyector	3	25000	DO75.000,00
Disco externo 5tb	3	7000	DO21.000,00
Total			DO1.593.750,00
Otros:			
Flota:	6	30000	DO180.000,00
Planta	1	500000	DO500.000,00
Aire acondicionado	4	110000	DO440.000,00
Camaras de seguridad	10	13000	DO130.000,00
Cableado estructurado	30	800	DO24.000,00

Cartuchos de impresora:	40	2500	DO100.000,00
Extintor	3	5000	DO15.000,00
Detector de humo	3	6000	DO18.000,00
Total			DO1.407.000,00
Servicios:			
Agua	6 meses	550 mensual	DO3.300,00
Luz	6 meses	25000 mensual	DO150.000,00
Basura	6 meses	550 mensual	DO3.300,00
Internet	6 meses	6000 mensual	DO36.000,00
Total			DO192.600,00
Transporte:			
Combustible:	108	20000	DO2.160.000,00
Total			DO2.160.000,00
Materiales de oficina:			
Resma de papel	450	200	DO90.000,00
Grapadoras	10	550	DO5.500,00
Grapas grandes	10	700	DO7.000,00
Post it	1000	25	DO25.000,00
Grapas	150	30	DO4.500,00
Grapas grandes	150	30	DO4.500,00
Clips	150	20	DO3.000,00
Folders	3000	5	DO15.000,00
Total			DO154.500,00
Licencias:			
Microsoft Office (excel, word, project, etc..)	10	53359	DO533.590,00
Photoshop	3 meses	1120 mensual	DO3.360,00
Jira	6 meses	13800 mensual	DO82.800,00
IDE oficial de Ethereum: Remix		0	DO0,00
LevelDB		0	DO0,00
Hyperledger Sawtooth	1	DO3.283,00	DO3.283,00
Total			DO623.033,00

Entrenamiento			
Curso SCRUM			DO770.000,00
Pago de certificación Blockchain expert	4	100	DO400,00
Pago de certificación Solidity developer	9	100	DO900,00
Pasaje a punta cana ida/vuelta	6	3000	DO18.000,00
Inscripción al congreso tecnología	6	45000	DO270.000,00
Inscripción congreso UI/UX	11	2500	DO27.500,00
Inscripción Congreso internacional de tecnología	1	60000	DO60.000,00
Pasaje ida y vuelta miami	1	35000	DO35.000,00
Estadía en hotel, comida, etc...	1	80000	DO80.000,00
Inscripción curso de finanzas	1	8000	DO8.000,00
Inscripción Curso de desarrollo ágil(TDD, BDD)	1	6000	DO6.000,00
Inscripción Curso de Microservices en Java	1	10000	DO10.000,00
Inscripción Curso de Jira	1	4000	DO4.000,00
Inscripción Curso de Docker	1	4000	DO4.000,00
Inscripción curso de SOA	1	10000	DO10.000,00
Inscripción curso de Selenium	1	3000	DO3.000,00
Inscripción curso de Microsoft Project	1	15000	DO15.000,00
Inscripción curso de ApiMan	1	5000	DO5.000,00
Inscripción congreso SOA	1	15000	DO15.000,00
Inscripción curso de Linux	1	5000	DO5.000,00
Inscripción curso Ethical Hacking	1	10000	DO10.000,00
Total			DO1.356.800,00

Capacitación	DO1.246.800,00
Recursos	DO21.023.629,00
Salario	DO 26.228.368,66
SubTotal	DO 48.498.797,66
Overhead	DO9.699.759,53
Utilidad neta (Ganancias)	DO 29.099.278,60

Total	**DO 87.297.835,79**
USD	**$1.857.400,76**

Tabla 3. Nomina General.
Fuente: Propia

Por cada segmento se puede observar el total que se tiene presupuestado como gastos operacionales, donde se tendrá un total de ganancias DO 29.099.278,60 y de Capacitación de los empleados se iría DO1.246.800,00 durante los seis meses que tendrá el proyecto vigente, como también esta tabla #3 representa la cantidad que se invertirá en capacitación de los empleados y en recursos.

Nómina de empleados del proyecto de software:

La nómina de empleado consiste en la suma total de todos los registros financieros de los sueldos de los empleados, en este también se incluye lo que es las bonificaciones que reciben cada uno, este es un pago que se le hace a los empleados por el tiempo que prestaron los servicios durante cierto periodo de tiempo.

Puesto	Sueldo	Precio(USD) x hora	Duración (Mes)	Sueldo a 6 meses
CEO	DO330.000,00	$42,09	6	DO1.980.000,00
Asistente Administrativo	DO95.000,00	$12,12	6	DO570.000,00
Consultor SCRUM	DO180.000,00	$22,96	6	DO1.080.000,00
Main Project Manager	DO220.000,00	$28,06	6	DO1.320.000,00
Líder técnico de proyecto	DO200.000,00	$25,51	6	DO1.200.000,00
Especialista Amazon Web Services (DevOps)	DO150.000,00	$19,13	6	DO900.000,00
Especialista Hyperledger Sawtooth	DO150.000,00	$19,13	6	DO900.000,00

Desarrollador de Ethereum Smart Contract	DO150.000,00	$19,13	6	DO900.000,00
Analistas de Aseguramiento de la Calidad	DO130.000,00	$16,58	6	DO780.000,00
Analistas de Aseguramiento de la Calidad	DO130.000,00	$16,58	6	DO780.000,00
Analistas de Aseguramiento de la Calidad	DO130.000,00	$16,58	6	DO780.000,00
Analista de Requerimiento 1	DO135.000,00	$17,22	6	DO810.000,00
Analista de Seguridad	DO110.000,00	$14,03	6	DO660.000,00
Arquitecto de Software	DO150.000,00	$19,13	6	DO900.000,00
Administrador de la configuración	DO100.000,00	$12,76	6	DO600.000,00
Documentador Técnico	DO80.000,00	$10,20	6	DO480.000,00
Analista de base de datos	DO140.000,00	$17,86	6	DO840.000,00
Ingeniero de Validación	DO120.000,00	$15,31	6	DO720.000,00
Ingeniero de Verificación	DO120.000,00	$15,31	6	DO720.000,00
Desarrolladores Back-end	DO135.000,00	$17,22	6	DO810.000,00
Desarrolladores Back-end	DO135.000,00	$17,22	6	DO810.000,00
Desarrolladores Back-end	DO135.000,00	$17,22	6	DO810.000,00
Desarrolladores Front-end	DO120.000,00	$15,31	6	DO720.000,00
Desarrolladores Front-end	DO120.000,00	$15,31	6	DO720.000,00
Diseñador Gráfico	DO100.000,00	$12,76	6	DO600.000,00
TOTAL				**DO21.390.000,00**

Tabla 4. Nómina de empleados.
Fuente: Propia

En la tabla #4 se puede ver los diferentes puesto que se tendrán presente en el proyecto, para poder lograr la meta y tener un sistema bien robusto, con recursos suficientes mentes capacitados en el área.

Desglose mensual de la nómina de empleados:

En está siguiente tabla se podrá ver el desglose mensual de la nómina de empleado, como también se verá detalladamente el tiempo que trabajaran cada recurso y que le toca a cada uno en el aporte que se le paga por trabajar por el tiempo indicado desde el principio de este proyecto.

Según la legislación, el doble sueldo es el equivalente a la duodécima parte de los ingresos percibidos en el año.

Es un derecho de todo el dominicano, el cual en el código laboral se encuentra las leyes dictadas, las leyes que rigen esto son: Ley No. 16-92 que establece el Código de Trabajo de la República Dominicana. Todo lo relativo a este salario queda contenido en los artículos 219 al 222.

El **artículo 219** establece que “el empleador está obligado a pagar al trabajador en el mes de diciembre, el salario de Navidad, consistente en la duodécima parte del salario ordinario devengado por el trabajador en el año calendario, sin perjuicio de los usos y prácticas de la empresa, lo pactado en el convenio colectivo o el derecho del empleador de otorgar por concepto de éste una suma mayor”.

El artículo 220 del Código de Trabajo expresa que el pago del salario de Navidad se hará a más tardar el día veinte del mes de diciembre, aunque el contrato de trabajo se hubiere resuelto con anterioridad y sin tener en cuenta la causa de la resolución.

El doble sueldo está liberado del Impuesto sobre la Renta, de modo que debe ser recibido sin deducción o descuento alguno. Al igual que el salario ordinario, el doble

sueldo tampoco puede ser objeto de embargo, cesión o venta.

A continuación, aquí se puede visualizar una tabla con todo el desglose, durante los 6 meses del proyecto:

Leyendas	Navidad	Vacaciones	Liquidacion

1	2	3	4	5	6	Liquidación
DO330.000,00	DO330.000,00	DO330.000,00	DO330.000,00	DO330.000,00	DO495.000,00	DO470.835,08
DO95.000,00	DO95.000,00	DO95.000,00	DO95.000,00	DO95.000,00	DO142.500,00	DO135.543,43
DO180.000,00	DO180.000,00	DO180.000,00	DO180.000,00	DO180.000,00	DO270.000,00	DO256.819,14
DO220.000,00	DO220.000,00	DO220.000,00	DO220.000,00	DO220.000,00	DO330.000,00	DO313.890,06
DO200.000,00	DO200.000,00	DO200.000,00	DO200.000,00	DO200.000,00	DO300.000,00	DO285.354,60
DO150.000,00	DO150.000,00	DO150.000,00	DO150.000,00	DO150.000,00	DO225.000,00	DO214.015,95
DO150.000,00	DO150.000,00	DO150.000,00	DO150.000,00	DO150.000,00	DO225.000,00	DO214.015,95
DO150.000,00	DO150.000,00	DO150.000,00	DO150.000,00	DO150.000,00	DO225.000,00	DO214.015,95
DO130.000,00	DO130.000,00	DO130.000,00	DO130.000,00	DO130.000,00	DO195.000,00	DO233.882,71
DO130.000,00	DO130.000,00	DO130.000,00	DO130.000,00	DO130.000,00	DO195.000,00	DO170.335,36
DO130.000,00	DO130.000,00	DO130.000,00	DO130.000,00	DO130.000,00	DO195.000,00	DO170.335,36
DO135.000,00	DO135.000,00	DO135.000,00	DO135.000,00	DO135.000,00	DO202.500,00	DO192.614,35
DO110.000,00	DO110.000,00	DO110.000,00	DO110.000,00	DO110.000,00	DO165.000,00	DO142.769,96
DO150.000,00	DO150.000,00	DO150.000,00	DO150.000,00	DO150.000,00	DO225.000,00	DO214.015,95
DO100.000,00	DO100.000,00	DO100.000,00	DO100.000,00	DO100.000,00	DO150.000,00	DO142.677,30
DO80.000,00	DO80.000,00	DO80.000,00	DO80.000,00	DO80.000,00	DO120.000,00	DO184.118,06
DO140.000,00	DO140.000,00	DO140.000,00	DO140.000,00	DO140.000,00	DO210.000,00	DO199.748,22
DO120.000,00	DO120.000,00	DO120.000,00	DO120.000,00	DO120.000,00	DO180.000,00	DO171.212,76
DO120.000,00	DO120.000,00	DO120.000,00	DO120.000,00	DO120.000,00	DO180.000,00	DO171.212,76
DO135.000,00	DO135.000,00	DO135.000,00	DO135.000,00	DO135.000,00	DO202.500,00	DO192.614,35
DO135.000,00	DO135.000,00	DO135.000,00	DO135.000,00	DO135.000,00	DO202.500,00	DO192.614,35
DO135.000,00	DO135.000,00	DO135.000,00	DO135.000,00	DO135.000,00	DO202.500,00	DO192.614,35
DO120.000,00	DO120.000,00	DO120.000,00	DO120.000,00	DO120.000,00	DO180.000,00	DO171.212,76

DO120.000,00	DO120.000,00	DO120.000,00	DO120.000,00	DO120.000,00	**DO180.000,00**	**DO171.212,76**
DO100.000,00	DO100.000,00	DO100.000,00	DO100.000,00	DO100.000,00	**DO150.000,00**	**DO142.677,30**

TOTAL	**DO 26.228.368,66**

Tabla 5. Nómina de empleados, desglosada mensualmente.
Fuente: Propia

En la tabla #5 se encuentra un desglose mensual de los 6 meses del proyecto, como también lo que es la liquidación, el doble sueldo que se encuentra calculado dentro de la liquidación ya que estas personas solo van a durar 6 meses.

CONCLUSIÓN

Según el Índice de Desempeño Logístico realizado por el Banco Mundial (2016) que tiene como objetivo mostrar y describir las tendencias globales en materia de Logística (Consejo Nacional de Competitividad, 2016) posiciona a la República Dominicana en un ostentoso puesto número 13 dentro Latinoamérica y el caribe lo que indica que el desarrollo en materia de logísticas (de cualquier índole) está avanzando a un paso considerable.

A pesar de este crecimiento, el país necesita centrarse en comenzar a desechar todos los procedimientos análogos, para poder así, aspirar a poder competir en esta nueva "carrera espacial" que las sociedades basadas en información están construyendo.

La tecnología Blockchain se está integrando rápidamente en muchas industrias a través de múltiples funciones, en algunos casos revolucionando procesos y transacciones. Creemos que las cadenas de suministros comprenden un escenario perfecto para la aplicación de esta tecnología emergente.

Por eso hemos presentado este modelo, que busca eficientizar la calidad de los productos que son ofrecidos a través de los supermercados que interactúan de una manera con las cadenas de suministros pues hemos visto detectado oportunidades de mejora que pueden generar beneficios desde el génesis del producto hasta que llegue a las manos del consumidor final basándonos en el principio de la transparencia que recientemente se ha vuelto fundamental para el desarrollo de las sociedades.

Se deben realizar investigaciones de cómo fortalecer la seguridad de los elementos de este modelo por la criticidad de las implementaciones a las cuales será objeto, como también su implementación de manera cotidiana en cualquier servicio donde exista una interacción humana.

RECOMENDACIONES

Fruto de los resultados obtenidos bajo esta investigación, se entregan estas recomendaciones de lugar:

- Las cadenas de suministros deben empezar a implementar ya, tecnologías basadas en Blockchain con el fin de transparentar sus operaciones para así, mejorar la calidad de los productos que ofrecen al público.

- Los supermercados necesitan comenzar a utilizar los motores de toma de decisiones alimentándose de la Blockchain pues con esto, la operatividad de los mismos se verá beneficiada exponencialmente.

- La edad análoga está consumiendo poco a poco la competitividad de los servicios ofrecidos por los supermercados tradicionales, para poder mantenerla ante entes de fuerza mayor (multinacionales extranjeras) los mismos deben incursionar en nuevas técnicas basadas en tecnología del conocimiento.

- La descentralización tecnológica debe ser fomentada como un estándar ya que la misma está basada en un eje central de transparencia que beneficia a cualquiera que interactúe con ella.

ANEXO

ANTEPROYECTO

UNIVERSIDAD APEC
UNAPEC

CURSO DE MONOGRAFICO DE EVALUACION FINAL
EVALUACION DE LAS PROPUESTAS
MAYO AGOSTO 2018

TITULO : MODELO DE SISTEMA DE TRAZABILIDAD PARA LA CADENA DE SUMINISTRO DE ALIMENTOS UTILIZANDO BLOCKCHAIN

MODULO : SISTEMA DE INFORMACION GEOGRAFICO (GIS)

PROFESOR (A) : LIC. SANTO NAVARRO

AUTOR : MATOS MANCEBO PAMIR | MIRELES MATEO MARIA DEL PILAR |
COPLIN CÁCERES RAYMOND AMADO

MATRICULA : 20120089 | 20132006 | 20132200 **AREA** INFORMATICA

APROBADO : X **APROBADO CON MODIFICACION** :

RECHAZADO : **FIRMA** : Santo Rafael Navarro

FECHA DE ENTREGA DEL TRABAJO AL PROFESOR :

OBSERVACIONES :
PROFESOR, EXPLIQUE LAS RAZONES POR LAS QUE USTED APROBO CON MODIFICACIONES O RECHAZO

Estructurado con imágenes el contenido, sólo corregir la bibliografía.

ys(20-05-2003)

INDICE DE CONTENIDO

1. Selección del título y definición del tema
   - 1.1. Definición del tema
   - 1.2. Mapa conceptual
2. Planteamiento del problema
3. Objetivos de investigación
   - 3.1. Objetivo General
   - 3.2. Objetivo Específicos
4. Justificación de la Investigación
   - 4.1. Justificación teórica
   - 4.2. Justificación metodológica
   - 4.3. Justificación práctica
5. Marco referencial
   - 5.1. Marco teórico
   - 5.2. Marco conceptual
   - 5.3. Marco espacial
   - 5.4. Marco temporal
6. Aspectos Metodológicos
   - 6.1. Tipos de investigación
   - 6.2. Métodos, procedimientos y técnicas de investigación
     - 6.2.1. Métodos
     - 6.2.2. Procedimientos
     - 6.2.3. Fuentes
     - 6.2.4. Técnicas de Investigación
     - 6.2.5. Palabras clave
7. Tabla de contenido preliminar
8. Referencias Bibliográficas

1. SELECCIÓN DEL TÍTULO Y DEFINICIÓN DEL TEMA

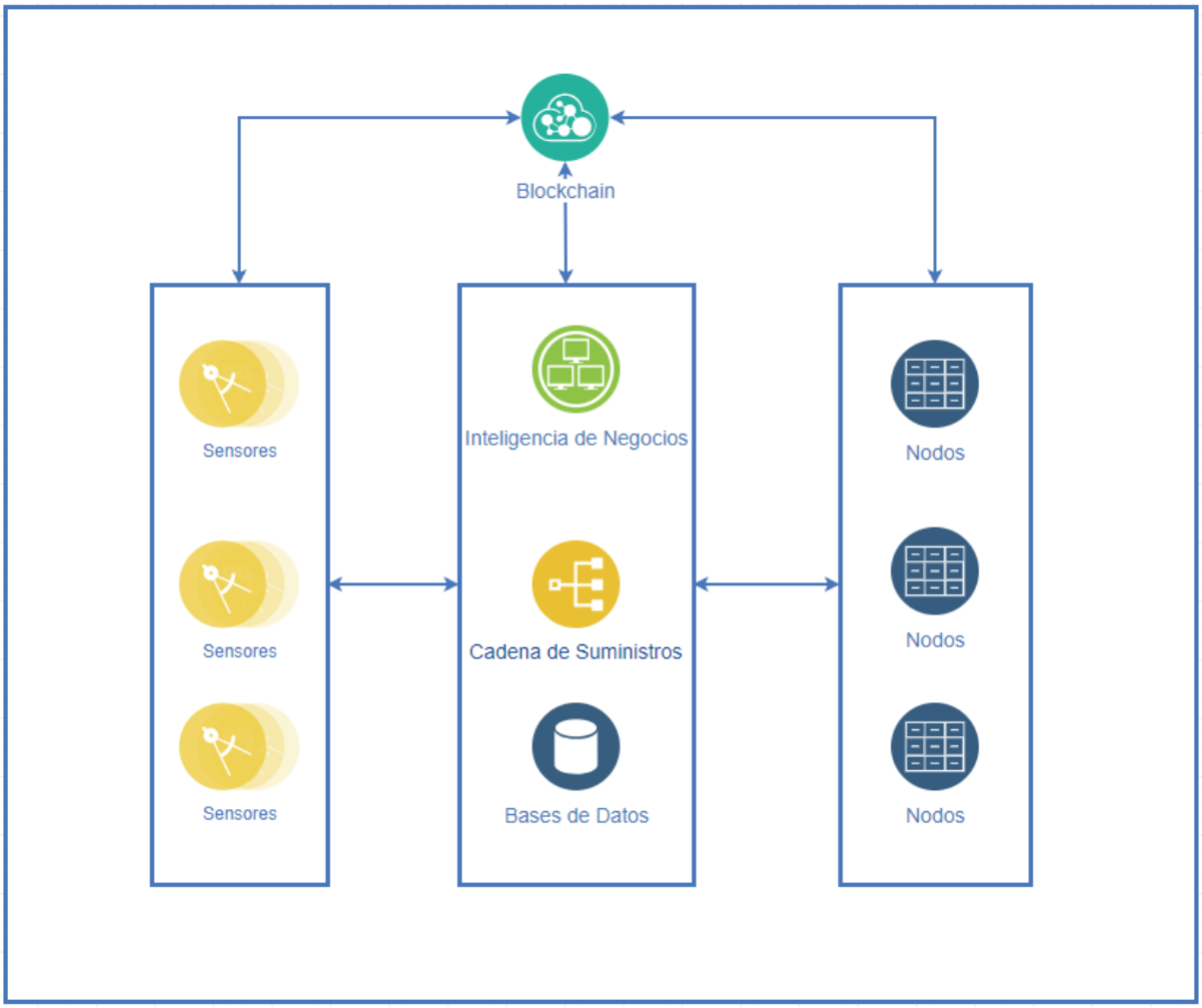
Modelo de sistema de trazabilidad de cadena de suministro de alimentos utilizando tecnología Blockchain para el Supermercado Nuevo Amanecer, en Santo Domingo Este, República Dominicana, año 2018.

1.1. Definición del tema

En el presente documento se propone el modelo o diseño de un sistema de información para la trazabilidad de alimentos dentro de una cadena de suministros utilizando Blockchain en el Supermercado Nuevo Amanecer en Santo Domingo Este, República Dominicana.

Este modelo busca transparentar los procesos realizados en una cadena de suministros, con el fin de generar información y estadísticas para posibles estrategias e inteligencia de negocios para la toma de decisiones las cuales ayudarán a sobrepasar los estándares de calidad y por tanto la satisfacción de los usuarios finales con los productos ofrecidos.

1.2. MAPA CONCEPTUAL



2. PLANTEAMIENTO DEL PROBLEMA

Actualmente, un gran porcentaje de los supermercados de la República Dominicana, cuentan con un sistema tradicional de gestión de cadena de suministro de alimentos (SCM), por lo tanto, estos sistemas no tienen la facultad de generar información valiosa, ni poseen la Inteligencia de Negocios necesaria para las tomas de decisiones. Por esta razón, los supermercados la mayoría de las veces se enfocan más en funciones operativas y no en funciones estratégicas y administrativas. Esto trae consigo que los mismos no puedan cumplir sus objetivos organizacionales.

Las estrategias son los medios a través de los cuales se pretende alcanzar los objetivos, pero estos objetivos sólo pueden ser alcanzados si la organización se siente en la capacidad de tomar decisiones.

Como es de saber, el conocimiento deriva de información, así como la información deriva de los datos, por ende, existe una correlación entre datos, información y conocimiento. Si la información se transforma en conocimiento, entonces ha ocurrido la intervención de un ente inteligente. Las acciones de generación del conocimiento se producen en los seres humanos (Davenport y Prusak, 2001). Las tecnologías de información y comunicación (TIC), a pesar de su capacidad de procesamiento de datos y creación de información, no pueden crear el conocimiento; este solo es posible a partir de la intervención de un ser humano (Bueno, 2000).

Hoy día, el activo más importante de una organización es la información y es evidente que la ociosidad de un proceso tan importante como lo es el flujo de la cadena de suministro en un supermercado puede representarse en pérdidas directas o indirectas a la organización.

Todo esto ocurre debido a que, durante el paso de un alimento por la cadena de suministro, el proveedor no retroalimenta al usuario final (supermercado) con información sobre el estado del producto, temperatura, locación, cantidad. El proceso es inseguro y no es trazable. Esto da paso a que el producto se encuentre en condiciones de almacenamientos inadecuadas, se realicen prácticas de alimentos no declaras y no reglamentadas, fraudes de carnes y pescados (Etiquetado Incorrecto).

3. OBJETIVOS DE INVESTIGACIÓN

3.1. Objetivo General

Diseñar modelo de sistema que permita recopilar información y brindar soporte a la cadena de suministro de alimentos utilizando tecnología Blockchain, así como medir la trazabilidad de los productos durante su vida dentro de la cadena de suministro.

3.2. Objetivos Específicos

- Verificar y analizar los mecanismos actuales que disponen los supermercados para gestionar la cadena de suministro.
- Diseñar arquitectura general de la plataforma en base a los procesos actuales y los procesos propuestos de mejora.
- Determinar los tipos de sensores necesarios para capturar las temperatura y locación de los alimentos.
- Generar reportes de inteligencias de negocios para las tomas de decisiones.

4. Justificación de la Investigación

4.1. Justificación Teórica:

Esta investigación tiene como propósito optimizar el proceso que se lleva a cabo hoy día en las cadenas de suministros de los supermercados. Los procesos de trazabilidad de alimentos pueden ser mejorados significativamente haciendo uso de tecnologías disruptivas como es el caso de Blockchain lo cual aporta un base de datos segura, inmutable e íntegra.

Para la cadena de suministro el sistema pretende sustituir completamente el proceso que se realiza actualmente por uno más viable que se apoye en datos compartidos, infraestructura en la nube y la inmutabilidad de los datos para evitar posibles corrosiones de información por parte de los entes participantes.

Para poder cumplir con el estándar de calidad que necesita el supermercado Nuevo Amanecer, se va a diseñar una plataforma que será capaz de validar la calidad de un producto de forma rápido y sencillo, por medio de una verificación que se hará bajo minería que permite analizar y verificar fraudes en el proceso. La plataforma manejara la información a través de servicios web, reduciendo el tiempo y atrayendo a más cliente a confiar más en lo que reciben de dicho supermercado.

4.2. Justificación Metodológica:

Para poder llevar a cabo esta investigación y cumplir con los objetivos establecidos se utilizarán técnicas de recolección de datos para determinar cómo funciona el proceso actual. Con la finalidad de adquirir esta información se realizará una entrevista a personas que conozcan el proceso completo y también se obtendrá información de los clientes en base a lo que encuentran al momento de visitar dicho establecimiento.

4.3. Justificación Práctica:

El resultado de esta investigación proveerá una base para consolidar el diseño del sistema y cómo será implementado, también se podrá determinar cuáles son los procesos que serán mejorados y cuáles serán sustituidos en el nuevo sistema, por último, se obtendrá documentación de todo el proceso con el fin de tener un proyecto estructurado y guiado por una metodología ágil.

5. MARCO REFERENCIAL

5.1. Marco teórico

“En el futuro, la competencia no se dará de empresa a empresa, sino más bien de cadena de suministros a cadena de suministros.”

Michael E. Porter, Ph.D., Harvard University

Los sectores de la ingeniería y la producción actualmente se están enfrentando a los nuevos modelos y condiciones del futuro. Dentro de todo este proceso la pieza clave más importante es la Cadena de Suministro.

La cadena de suministro es el nombre que se le otorga a todos los pasos involucrados en la preparación y distribución de un elemento para su venta, es decir, es el proceso que se encarga de la planificación o coordinación de las tareas a cumplir, para poder realizar la búsqueda, obtención y transformación de distintos elementos, de esta forma poder comercializar un producto para que el mismo sea de fácil acceso al público.

Figura 1. Cadena de Suministro

En la actualidad los participantes de las cadenas de suministros, en principal los consumidores a menudo tienen muy poca idea de dónde provienen los bienes que compran o cómo se fabrican.

Es posible que las empresas que venden estos productos ni siquiera lo sepan. Estas áreas grises son un problema, porque ofrecen oportunidades para el mal manejo o incluso para el fraude.

Otros muchos problemas como el mantenimiento de registros manuales casi siempre propensos a errores, condiciones inadecuadas de almacenamiento de alimentos, prácticas ilegales, no declarada y no reglamentada, fraudes en la etiquetación de alimentos y la falta de los vendedores y consumidores son los principales problemas por los cuales se enfrentan las cadenas de suministros tradicional.

5.2. Marco conceptual

API (Application Program Interface):

Proporciona un conjunto de funciones, que ayudan a interconectar servicios entre aplicaciones. (Microsoft Corp, 2001).

Blockchain:

Es una base de datos compartida y distribuida que facilita el proceso de registro de las transacciones y el seguimiento de los activos en una red empresarial.

Ethereum:

Es una plataforma open source, descentralizada que permite la creación de acuerdos de contratos inteligentes entre pares, basada en el modelo Blockchain.

Cadena de suministro:

Se deriva de la palabra latina cadena de abasto, que significa que es una red de empresas de suministro que es tomado desde el proveedor de la materia prima que requiere un producto hasta el producto final.

Smart Contract:

Es un programa informático que facilita, asegura, hace cumplir y ejecuta acuerdos registrados entre dos o más partes

(por ejemplo, personas u organizaciones). Como tales ellos les ayudarían en la negociación y definición de tales acuerdos que causarán que ciertas acciones sucedan como resultado de que se cumplan una serie de condiciones específicas. (Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, business, and the world. Don Tapscott,Alex Tapscott. Penguin Random House LLC. 2016)

Sistema de información geográfica (SIG):

Sistema de Información Geográfica (2018, febrero 10). Wikipedia. https://goo.gl/kCHYWb. Es un conjunto de herramientas que integra y relaciona diversos componentes (usuarios, hardware, software, procesos) que permiten la organización, almacenamiento, manipulación, análisis y modelización de grandes cantidades de datos procedentes del mundo real que están vinculados a una referencia espacial, facilitando la incorporación de aspectos sociales-culturales, económicos y ambientales que conducen a la toma de decisiones de una manera más eficaz.

5.3. Marco espacial

La investigación será realizada en la cadena de Supermercados Nuevo Amanecer en Santo Domingo, República Dominicana.

5.4. Marco Temporal

El desarrollo de esta propuesta será realizado dentro del período Mayo-Agosto 2018.

6. ASPECTOS METODOLÓGICOS

En esta sección se analizan y señalan los puntos relacionados con el tema en cuanto a la forma de desarrollo de la investigación, la utilización de técnicas y herramientas para el proceso de recopilación de información para la cercanía (aproximación) de resultados esperados y su factibilidad.

6.1. Tipos de investigación

La presente, se trata de una investigación descriptiva y explicativa donde se llevó a cabo algunas herramientas analíticas sobre el tema para aproximación de los resultados esperados.

Investigación Descriptiva:

La cual permite plantear una situación de forma concreta y consistente a la realidad en cuanto al manejo de los productos y alimentos desde su estado de cosecha o captura hasta que el usuario final adquiera el producto bajo los estándares recomendados. De modo que permita mejorar la calidad de productos que pasan por una cadena de suministros, interacción con los inter-usuarios, utilizando un sistema para registros de transacciones inmutables.

Investigación Explicativa:

Por medio de este tipo de investigación se busca establecer conclusiones y explicaciones para esclarecer las teorías y casos de estudios.

6.2. Métodos, procedimientos y técnicas de investigación

6.2.1. Métodos

- **Método de Observación:**

  Ayudará a recolectar datos sobre cuáles procesos dentro de las cadenas de suministros serán los más beneficiados con la implementación del Blockchain.

- **Método Inductivo:**

  A partir de la información generada con el método de la observación se determina las informaciones más relevantes para generarán reportes para la toma de decisiones para la mejora de la calidad de los productos involucrados.

- **Método de Análisis:**

  Al capturar los datos de los dos métodos descritos anteriormente, procederemos al análisis de los datos obtenido con el fin de establecer la relación de cada componente involucrado dentro de la investigación, ya sea de los involucrados en los diferentes tipos de cadenas de suministros para varios productos.

- **Método de Síntesis:**

  Nos permitirá que luego del análisis de los resultados obtenidos por los diversos métodos a emplear, se permita establecer un conocimiento y definición más precisa de los requisitos, objetivos principales, dirección, entre otros.

6.2.2. Procedimientos

El diseño de investigación de campo que se ha desarrollado contiene observación tanto estructurada como no estructurada, encuestas y entrevistas a agentes destinados al tema en general, recolección y análisis de información estadística, revisión bibliográfica, e Internet.

- Análisis de los Reglamentos y Estándares de Calidad de los Alimentos tales como la Ley General de Salud Ley No.42-01, la cual establece la exigencia de adquirir o recibir productos sanos correspondientes a calidad, naturaleza y seguridad de los mismos.

- Encuestas en línea a personas sobre la calidad, usabilidad y cotidianidad de los Supermercados.

- Encuestas en línea realizadas a profesionales (consultas a expertos) y la aplicación de las leyes(reglamentos) según área que competa con él/los alimentos.

- Los instrumentos de encuestas, a fin de conocer la opinión de terceros, para la recopilación fueron diseñados utilizando herramienta gratuita que ofrece Google Docs (Forms). Para difundir tal instrumento se utilizó el Correo Electrónico, y redes sociales como WhatsApp y Facebook. Se utilizaron para determinar el o los supermercados para mejorar la calidad de los productos y resultado final en base a las respuestas de los usuarios.

6.2.3. Fuentes

De acuerdo con lo redactado anteriormente se pueden subdividir las siguientes fuentes para la obtención de información tanto primarias como secundarias.

- Primarias: Informaciones obtenidas desde documentos, libros y reportes solicitados de parte de la cadena de suministros confiables al propósito de investigación y desarrollo del sistema.

- Secundarias: Informes, blogs, páginas de internet y análisis periodísticos que puedan contribuir al desarrollo del proyecto.

6.2.4. Técnicas de Investigación

- **Encuestas**:

  Se utilizará la técnica de investigación de encuestas para alcanzar resultados estadísticos tanto por parte del personal que interactúan con las cadenas de suministros y aportaran la mayoría de información al sistema como los consumidores finales de los productos procesado.

- **Entrevistas**:

  Se realizará la técnica de investigación de entrevistas a personas expertas en las cadenas de suministros del supermercado el amanecer.

6.2.5. Palabras clave

Calidad, trazabilidad, alimentos orgánicos, supermercados, cadena de suministros, Blockchain, clientes, productos, procesos.

7. TABLA DE CONTENIDO PRELIMINAR

Portada

Agradecimientos

Dedicatoria

Resumen

Introducción

Capítulo I - Antecedentes y Aspectos Generales

1. Situación actual de la cadena de suministro de los supermercados de la República Dominicana
2. Ley General de Salud 42-01
3. Las cadenas de suministros inteligentes
4. Blockchain como tecnología disruptiva

Capítulo II - Tecnologías y elementos del sistema

2.1. Blockchain
- 2.1.1. Origen
- 2.1.2. Características de la Blockchain
- 2.1.3. ¿Cómo funciona la cadena de bloques?
- 2.1.4. Contratos Inteligentes (SMART CONTRACT)
- 2.1.5. Beneficios claves de la cadena de bloques
- 2.1.6. Aplicaciones de la cadena de bloques

2.2. Cadena de Suministro
- 2.2.1. Origen Cadena de Suministro
- 2.2.2. Características de la Cadena de suministro
- 2.2.3. Procesos macro y funciones de la Cadena de Suministro en el Interior de una Empresa
- 2.2.4. Niveles de decisión en una cadena de suministro
- 2.2.5. Visiones de una cadena de suministro
- 2.2.6. Una cadena de suministro más eficiente y productiva
- 2.2.7. Trazabilidad y visibilidad total
- 2.2.8. Modelo de Transacciones

1. Lenguajes de Programación
2. Diseño, Desarrollo e Implementación de Base de Datos - Data Market
3. Diseño de Arquitectura del Sistema Trazabilidad - Blockchain
4. Desarrollo de Infraestructura Cloud Amazon AWS
5. Aplicaciones web y móviles
6. Sensores
7. Hardware
   - 7.1. Dispositivo
   - 7.2. Composición del dispositivo
   - 7.3. Aplicación
   - 7.4. Costo
8. Software
   - 8.1. Arquitectura
     - 8.1.1. Física
     - 8.1.2. Lógica

Capítulo lll - Diseño de la solución propuesta

- 3.1. Arquitectura del Sistema
- 3.2. Seguridad del Sistema
- 3.3. Análisis financiero
- 3.4. Documento anexo
- 3.5. Gastos operativos

Conclusiones

Recomendaciones

Bibliografía

Anexos

REFERENCIAS BIBLIOGRÁFICAS

1. Andress, J., & Rogers, R. (2011). The basics of information security (1st ed.). Amsterdam: Elsevier.

2. Antonopoulos MA (2014) Mastering Bitcoin—unlocking digital currencies. O'Reilly, Sebastopol Buterin V (2013) A next generation smart contract and decentralized application platform. https:// ethereumbuilders.gitbooks.io/guide/content/en/whitepaper.html

3. Autores: Julián Pérez Porto y Ana Gardey. Publicado: 2009. Actualizado: 2013.

4. Blockchain Becomes a Crucial Link in the Supply Chain | Aqurus, https://aqurus.ca/blockchain-crucial-link-supply-chain/

5. Buterin V (2013) A next generation smart contract and decentralized application platform. https://ethereumbuilders.gitbooks.io/guide/content/en/whitepaper.html

6. Cham D (1992) Achieving electronic privacy. Sci Am 267(2):96–101

7. Computing. (2018). Blockchain, el servicio cloud de IBM que crea redes financieras seguras. [online] Available at: http://www.computing.es/cloud/noticias/1096829046301/blockchain-servicio-cloud-de-ibm-crea-redes-financieras-seguras.1.html [Accessed 6 Jul. 2018].

8. Consejo Nacional de Competitividad (2016). Índice de Desempeño Logístico [PDF]. Santo Domingo. Consultado en http://www.competitividad.org.do/wp-content/uploads/2016/08/%C3%8Dndice-de-Desempe%C3%B1o-Log%C3%ADstico-2016.pdf

9. Decreto Número: 528-01 REGLAMENTO GENERAL PARA CONTROL DE RIESGOS EN ALIMENTOS Y BEBIDAS EN LA REPÚBLICA DOMINICANA. Santo Domingo, República Dominicana, 14 de mayo 2001.
   Definicion.de: Definición de gastos de operación (https://definicion.de/gastos-de-operacion/)

10. Definista (2018). ¿Qué es Cadena de Suministro? - Su Definición, Concepto y Significado. [online] Conceptodefinicion.de. Available at: http://conceptodefinicion.de/cadena-de-suministro/ [Accessed 6 Jul. 2018].

11. Dermody R (2015) Smart contract versus "token"-based systems. http://symbiont.io/uncategorized/ smart-contract-vs-token-based-systems/

12. Dykes JM (1995) Digital cash and the development of the apolitical currency. Ethics and Law on the Electronic Frontier Fall

13. Ethereum. (2018). Solidity - El lenguaje de programación de los Smart Contracts y Ethereum. [online] Available at: https://miethereum.com/smart-contracts/solidity/ [Accessed 5 Jul. 2018].

14. Flood N, Goodenough O (2015) Contracts as automaton: the computational representation of financial agreement. https://financialresearch.gov/working-papers/files/OFRwp-2015-04_Contractas-Automaton-The-Computational-Representation-of-Financial-Agreements.pdf

15. Gendal R (2015) A simple model for smart contract. https://gendal.me/page/2/

16. Greenspan A (2016) Why many smart contract use cases are simply impossible. http://www.coindesk.com/three-smart-contract-misconceptions/

17. Gupta, M. (2017). Blockchain For Dummies®, IBM Limited Edition. 1st ed. USA: John Wiley & Sons, Inc.

18. Harwareate. (2018). ¿Qué son los Contratos Inteligentes? Los Smart Contracts - Harwareate. [online] Available at: https://hardwareate.com/los-contratos-inteligentes [Accessed 5 Jul. 2018]

19. Hofmann, E., Strewe, U. and Bosia, N. (2018). Supply Chain Finance and Blockchain Technology. 1st era. Suiza: Springer.

20. Hugos, M. (2003). Essentials of supply chain management. Hoboken, N.J.: John Wiley & Sons.

21. IBM. (2018). IBM Blockchain Platform technical Overview [Ebook]. New York. Consultado en https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=KUW12555USEN

22. IFF (Institute of International Finance) (2015) The internet of finance: unleashing the potential of Blockchain technology. https://www.iif.com/sites/default/files/general/cmm_rn_20150416.pdf

23. Joint FAO/WHO Codex Alimentarius Commission. (1992). Codex alimentarius. Rome: Food and Agriculture Organization of the United Nations

24. Khaitan, R. (2017). Blockchain: One Truth Across Networks for Supply Chain. Consultado en: https://www.ibm.com/blogs/watson-customer-engagement/2017/04/11/blockchain-supply-chain/

25. Lang J (2015). In: Swanson T (Ed) Consensus as a service: a brief report of permissioned, distributed ledger systems. http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributedledgers.pdf

26. Lewis, A. (2016). Understanding Blockchain Technology And What It Means for Your Business. SECTOR BRIEFING, (19).

27. Lewis A (2015) The emergence of blockchains as activity registers. https://bitsonblocks.net/2016/ 08/05/the-emergence-of-blockchains-as-activity-registers/

28. Ley N° 41-02. Ley General de Salud. Santo Domingo, República Dominicana, Abril 2001

29. MCP9808 - Thermal Management. (2018). Consultado en: https://www.microchip.com/wwwproducts/en/en556182

30. Mearian, L. (2018). What is blockchain? The most disruptive tech in decades. Consultado en: https://www.computerworld.com/article/3191077/security/what-is-blockchain-the-most-disruptive-tech-in-decades.html

31. Menezes AJ, Oorschot PC, Vanstone SA (1995) A handbook for applied cryptography. http:// citeseer.ist.psu.edu/viewdoc/download?doi=10.1.1.99.2838&rep=rep1&type=pdf

32. Nakamoto S (2009) A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

33. O'Dwyer KJ, Malone D (2014) Bitcoin mining and its energy footprint. https://karlodwyer.github. io/publications/pdf/bitcoin_KJOD_2014.pdf

34. Sams R (2015) Bitcoin blockchain for distributed clearing: a critical assessment. J Financial Trans 42:39–46

35. Schollmeier R (2002) A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. Paper presented at the first international conference on peer-to-peer computing, Linkoping University, Sweden, 27–29 August 2001

36. SIM7000A. (2017). Consultado en http://simcomm2m.com/En/module/detail.aspx?id=173

37. Solidity.readthedocs.io. (2018). Solidity — Solidity 0.4.24 documentation. [online] Available at: http://solidity.readthedocs.io/en/v0.4.24/ [Accessed 5 Jul. 2018].

38. Soto, D., & Rovira, J. (2009). LA CADENA DE SUMINISTRO INTELIGENTE DEL FUTURO [PDF] (1st ed., pp. 6-19). New York: IBM. Consultado en https://www-03.ibm.com/press/es/es/attachment/27111.wss?fileId=ATTACH_FILE1&fileName=Presentacion%20prensa%20cadena%20de%20suministro%20inteligente.pdf

39. Swan E (2015) Blockchain: Blueprint for a New Economy. O'Reilly, Sebastpol

40. Swanson T (2015) Consensus as a service: a brief report of permissioned, distributed ledger systems. http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributedledgers.pdf

41. Szabo N (1994) Smart contracts. http://szabo.best.vwh.net/smart.contracts.html Vasin P (no date) BlackCoin's proof-of-stake protocol. http://blackcoin.co/blackcoin-pos-protocolv2-whitepaper.pd

42. U.S. Government, Legal Information Institute, Título 44, Capitulo 35, Subchapter 111, §3542, Cornell University Law School. Consultado en www.law.cornell.edu/uscode/44/3542.html

43. Woo, T. (2017). LTE CAT-M + NB-IoT Shield for Arduino. Consultado en http://www.instructables.com/id/LTE-NB-IoT-Shield-for-Arduino/