

TESIS DE MAESTRÍA

Maestría en Administración de Negocios

Título:

“Logística comparada entre método tradicional y la aplicación de la tecnología Blockchain. Estudio de caso en empresa metalmecánica argentina”

Autor: Mauricio Luis Prieto

Director de Tesis: Dr. Alfredo Gerardo Álvarez

Buenos Aires - 2020

1) INDICE GENERAL	
1) INDICE GENERAL.....	2
2) ÍNDICE DE FIGURAS.....	4
3) ÍNDICE DE TABLAS	5
4) PALABRAS CLAVES	6
5) INTRODUCCIÓN	6
6) OBJETIVOS.....	7
7) HIPÓTESIS.....	8
8) METODOLOGÍA	9
8.1) Estructura del Trabajo.....	10
9) MARCO TEÓRICO.....	11
9.1) LOGISTICA 4.0	11
9.2) BIG DATA	12
9.3) MACHINE LEARNING	13
9.4) INTERNET DE LAS COSAS (IoT).....	14
9.5) HISTORIA DE BLOCKCHAIN	17
9.6) QUE ES BLOCKCHAIN	22
9.7) PRINCIPALES CARACTERÍSTICAS DE BLOCKCHAIN	24
9.7.1) Inmutabilidad.....	24
9.7.2) Descentralización.....	25
9.7.3) Seguridad Mejorada.....	26
9.7.4) Encriptación Simétrica	27
9.7.5) Encriptación Asimétrica	28
9.7.6) Irreversible.....	29
9.7.7) Registros distribuidos	30

9.7.8)	Consenso.....	30
9.7.9)	Acuerdos más rápidos.....	31
9.8)	COMO SE COMPONE BLOCKCHAIN	31
	Criptografía de clave pública	31
9.8.1)	Base de datos distribuida:.....	32
9.8.2)	Algoritmos de consenso	32
9.8.3)	Hash	34
9.8.4)	Árbol de Merkle (Merkle root).....	39
9.8.5)	Tolerancia a Fallas Bizantinas (BFT).....	41
9.8.6)	Prueba de trabajo / Proof of Work (PoW)	48
9.8.7)	IV. Prueba de participación / Proof of Stake (PoS).....	51
9.8.8)	IV. PoA (Proof of Authority – Prueba de Autoridad)	55
9.9)	TIPOS DE BLOCKCHAIN.....	57
9.9.1)	Blockchain Públicas	57
9.9.2)	Blockchain Federadas.....	58
9.9.3)	Blockchain Privadas	59
9.10)	CONTRATOS INTELIGENTES (Smart Contracts).....	59
9.10.1)	Ether	62
9.10.2)	Las medidas de Ether.....	63
9.10.3)	Como se generan los Ether	64
9.10.4)	GAS en Ethereum.....	65
9.10.5)	Límite de Gas	66
9.10.6)	Gas utilizado por transacción	66
9.10.7)	Precio del Gas.....	66
9.10.8)	Coste actual de la Transacción – Comisión.....	67

9.10.9) Gas usado acumulado	67
10) APLICACIONES ACTUALES Y EN DESARROLLO	68
11) DESARROLLO DE BLOCKCHAIN EN LOGISTICA / SUPPLY CHAIN	81
11.1) Compras Locales	84
11.2) Compras al exterior	86
11.3) Producción.....	92
11.4) Almacenamiento.....	92
11.5) Transportes	92
11.6) Trazabilidad.....	93
11.7) Resumen	101
12) REGULACION	117
13) GLOSARIO.....	120
14) CONCLUSIONES.....	125
15) BIBLIOGRAFIA	128

2) ÍNDICE DE FIGURAS

Figura 1 - Aplicaciones de IoT	16
Figura 2 - Evolución Precio Bitcoin	17
Figura 3 - Red Descentralizada	22
Figura 4 - Funcionamiento de Blockchain	24
Figura 5 - Tipos de Redes.....	25
Figura 6 - Encriptación Simétrica.....	28
Figura 7 - Encriptación Asimétrica	29
Figura 8 - Función Hash MD5.....	36
Figura 9 - Función Hash SHA-256.....	37
Figura 10 - Árbol de Merkle.....	40
Figura 11 - Tolerancia a Fallas Bizantinas - Dilema 1	42

Figura 12 - Tolerancia a Fallas Bizantinas - Dilema 2	43
Figura 13 - Tolerancia a Fallas Bizantinas - Dilema 3	43
Figura 14 - Tolerancia a Fallas Bizantinas - Dilema 4	44
Figura 15 - Protocolo PoS	53
Figura 16 - Medidas del Ether	64
Figura 17 - Mercedes Benz Project	73
Figura 18 - Trazabilidad de diamantes	77
Figura 19 - Proyectos Blockchain	80
Figura 20 - Etapas de Supply Chain	81
Figura 21 - Proceso de Pedido de Transporte.....	85
Figura 22 - Medios de Pago Internacional	90
Figura 23 - Carta de Crédito Internacional.....	91
Figura 24 - Costos de Calidad	96
Figura 25 - El modelo tradicional de los CC. Fuente: Rao et al. (1996)	97
Figura 26 - El modelo emergente de los CC. Fuente: Rao et al.(1996)	98
Figura 27 - Trazabilidad con Blockchain	101
Figura 28 - Inventario	102
Figura 29 - Punto de Pedido	105
Figura 30 - Transportes	107
Figura 31 - Producción - Calidad	109
Figura 32 - Regulaciones desarrollándose.....	119
Figura 33 - Adopción Estimada de Blockchain.....	120

3) ÍNDICE DE TABLAS

Tabla 1 - Costos de Importación	89
Tabla 2 - Magnitudes relativas de los CC según sus diversas categorías.....	99

4) PALABRAS CLAVES

Blockchain, Contratos Inteligentes, Supply Chain¹, Blockchain aplicado a la logística, Blockchain en la cadena de suministro, Beneficios económicos de la aplicación de Blockchain en Logística.

5) INTRODUCCIÓN

En mis 25 años de experiencia en Logística y Supply Chain dentro de empresas multinacionales he transitado numerosos desafíos sobre innovaciones tecnológicas, principalmente por la demanda que este tipo de compañías tiene en replicar las mejores prácticas globales a todas sus filiales. Pero jamás como el que estamos atravesando actualmente, donde el avance del poder de cómputo y la creación de nuevas tecnologías parece haber logrado una simbiosis entre tecnologías pre existentes con otras que aún están experimentándose. Esta concatenación parece el inicio del fin de la logística tal cual la conocemos.

Entre estas tecnologías podemos nombrar: Big Data, Machine Learning, IoT, Cloud, Blockchain. ²

Es sobre la tecnología Blockchain la que se basará este trabajo; aunque como podrá observarse en el desarrollo, existe una interacción entre algunas de estas tecnologías que las complementan o las potencian.

Lo que termina siendo evidente es que hay un avance cada vez más acelerado en el desarrollo o aplicación de nuevas aplicaciones y tarde o temprano las empresas estarán obligadas a adoptarlas o posiblemente no puedan competir en un mundo digitalizado.

Empresas como Uber, Airbnb no tendrían razón de existir con Blockchain, cualquier usuario podría contratar directamente el servicio a otro usuario sin un intermediario fiscalizador como los que existen actualmente. *(Marr, 2018) (Schiller, 2018)*

Bienvenidos a la economía descentralizada, Blockchain trata sobre cambiar todo *(Warburg)*

¹ Supply Chain o Cadena de suministro está formada por todos aquellos procesos involucrados de manera directa o indirecta en la acción de satisfacer las necesidades de suministro

² Estos términos están desarrollados dentro del Marco Teórico

6) OBJETIVOS

El objetivo de este trabajo es establecer la aplicabilidad de la tecnología Blockchain en un proceso logístico en una empresa que fabrica en Argentina, evaluando y justificando en que partes del proceso resulta conveniente su implementación, sea por potenciales ahorros en costos, calidad del producto o servicio al cliente.

Para lograr entender su aplicabilidad, resultará necesario realizar una introducción en esta tecnología; aunque no sea el objetivo principal del trabajo el desarrollo de una explicación detallada del funcionamiento de la misma, la cual es técnicamente muy compleja y extensa y está perfectamente pormenorizada en numerosa bibliografía, mucha de ella mencionada en el transcurso de este trabajo.

Posterior a la explicación del funcionamiento sobre la tecnología, se realizará un detalle del proceso completo tradicional, justificando en cada una de las etapas donde podría aplicarse la ventaja que su implementación implicaría.

7) HIPÓTESIS

La hipótesis es un enunciado que realiza el investigador luego de conocer a fondo la teoría sobre el tema de interés (marco teórico). Las hipótesis indican lo que tratamos de probar y son definidas como explicaciones tentativas del fenómeno investigado. Derivan de la teoría existente (*Williams, 2003*) y deben formularse a manera de proposiciones De hecho, son respuestas provisionales a las preguntas de investigación.

En este trabajo se plantearán hipótesis operacionales de la empresa en estudio y serán contrastadas con posibles aplicaciones de Blockchain

Se desafiará la hipótesis que afirma que la implementación de esta tecnología en el proceso logístico causará una reducción en el costo total de la operación.

8) METODOLOGÍA

Una vez que se precisó el planteamiento del problema, este definió el alcance inicial en la investigación y formulada la hipótesis, el investigador debe visualizar la manera práctica y concreta de responder a las preguntas de investigación, además de cubrir los objetivos fijados. Esto implica seleccionar o desarrollar uno o más diseños de investigación y aplicarlos al contexto particular de su estudio. El termino diseño refiere al plan o estrategia concebida para obtener la información que deseada.

El enfoque cuantitativo es secuencial y probatorio. Cada etapa precede a la siguiente y no podemos “saltar o eludir” pasos; aunque desde luego, podemos redefinir alguna fase.

El proceso cualitativo es “en espiral” o circular, donde las etapas a realizar interactúan entre sí y no siguen una secuencia rigurosa.

En el enfoque cuantitativo los planteamientos a investigar son específicos y delimitados desde el inicio de un estudio. Además, las hipótesis se establecen previamente, esto es, antes de recolectar y analizar los datos. Esta recolección es fundamentada en la medición y el análisis en procedimientos estadísticos.

- La investigación cuantitativa debe ser lo más “objetiva” posible, evitando que afecten las tendencias del investigador u otras personas.
- Los estudios cuantitativos siguen un patrón predecible y estructurado (el proceso).
- En una investigación cuantitativa se pretende generalizar los resultados encontrados en un grupo a una colectividad mayor.
- La meta principal en los estudios cuantitativos es la construcción y la demostración de teorías.
- El enfoque cuantitativo utiliza la lógica o razonamiento deductivo.

(Sampieri, 2016)

8.1) Estructura del Trabajo

La composición del trabajo está determinada de la siguiente manera:

En la primera parte se ocupa de explicar brevemente las tecnologías inmersas en lo que se denomina Logística 4.0 y posteriormente Blockchain, con una profundidad razonable que permita el correcto entendimiento sobre los pasos posteriores y del propio trabajo.

Se presenta el marco teórico, diferentes antecedentes que existen sobre el tema a tratar; aunque debe considerarse que blockchain está en una etapa de desarrollo en áreas que no están incluidas en este trabajo (certificaciones de documentos, finanzas, seguridad informática, entre otros), y en etapa de pruebas en el sector que abarca el proyecto (*Schneider, 2019*)

En la segunda parte se realizará el análisis del proceso en detalle para entender las posibles implicancias y potencialidad de la tecnología.

Finalmente, la comparación entre modelos y las conclusiones del estudio

9) MARCO TEÓRICO

9.1) LOGISTICA 4.0

Logística 4.0 puede definirse como una logística moderna que incluye la digitalización, la interconexión y la informática en la nube. No está limitada al transporte únicamente, sino que sus responsables se encargan de coordinar de forma multifuncional la logística en la cadena de suministro. La logística 4.0 pretende una comunicación directa entre las instalaciones, los productos, las personas, la logística y las máquinas. Al integrar la logística en un momento temprano de la etapa de suministro, logrará una optimizará la producción justo a tiempo.³

De otro lado, los transportistas esperan una mayor seguridad para planificar y utilizar de forma óptima la flota de vehículos, reduciendo los tiempos en esperas en los puntos de carga. Cuáles son los retos de la Logística 4.0

Logística inteligente

Integrar la logística inteligente supone sacar partido a todas las oportunidades tecnológicas que hay disponibles en el mercado mediante varios softwares de gestión, que facilitarán la automatización de los procesos en los almacenes.

Anticipar las necesidades del cliente

Incorporar el Big Data a la logística permite predecir las necesidades de los clientes y, como consecuencia, anticipar desarrollando acciones sobre abastecimiento fiable.

Las herramientas de análisis desarrolladas cruzan los datos relacionados con los pronósticos meteorológicos, históricos de ventas, la actualidad local o las conversaciones en redes sociales. Tras este cruce, podremos obtener una aproximación real acerca del escenario al que nos enfrentaremos.

Reducir los tiempos de respuesta y limitar la producción

El sector retail trabaja con producciones cortas. Tienen una alta rotación de todas sus referencias en las tiendas online y en los establecimientos físicos, lo que obliga reducir el tiempo de respuesta en la entrega y trabajar con partidas más pequeñas.

³ Justo a Tiempo o Just in Time: es un sistema de organización de la producción para las fábricas, de origen japonés. También conocido como método Toyota, permite reducir costos, especialmente de inventario de materia prima, partes para el ensamblaje, y de los productos finales

Como consecuencia, se consigue un producto mejor adaptado a las exigencias de los consumidores, ganando flexibilidad y sin perder la eficiencia de la gestión de grandes volúmenes y la organización del trabajo en cadena.

Favorecer la omnicanalidad⁴

En la actualidad hay más canales de atención al cliente y cada uno aborda dicha atención de manera diferente, por lo que existe una discordancia en el tratamiento de las órdenes. Al unificar la gestión de mercancías y acelerar la preparación de los pedidos, esto podrá poner fin a dicha discordancia.

Trazabilidad

Mejorar la eficiencia logística supone un control de la trazabilidad de los productos durante toda la cadena de distribución. Son muy importantes las mencionadas etiquetas RFID, que se encargan de monitorizar la posición de los objetos, y los sistemas informáticos que integran la cadena de suministro. (*School, s.f.*) (*Amr, 2018*)

9.2) BIG DATA

No existe una definición única del significado de Big Data; por lo tanto, elijo una definición (*Marqués, 2015*). que me pareció acertada “Conjunto de datos que superan la capacidad del software habitual para ser capturados, gestionados y procesados en un tiempo razonable y por los medios habituales de procesamiento de la información”

Beneficios del Big Data en la logística

- El uso del Big Data permitirá controlar los vehículos y también los almacenes. Además al aproximarse al máximo al control en tiempo real, se optimizan las operaciones de distribución.
- La extracción de la información del Big Data permitirá un servicio más eficaz y costos más ajustados al ayudar en la reducción del inventario y en la optimización de los activos de la empresa.
- Los datos permitirán además sacar conclusiones para ajustar la oferta de un producto concreto a cada cliente en cada momento y por el canal idóneo.

⁴ Omnicanalidad: Omnichannel es una estrategia de contenido de canales cruzados que las organizaciones usan para mejorar su experiencia de usuario e impulsar mejores relaciones con su audiencia a través de puntos de contacto

- Todos los datos recogidos permitirán, en definitiva, conocer mejor al cliente, identificando sus necesidades. Con esto, conseguiremos ofrecer un mejor servicio, ajustando costos y siendo más rentables.

9.3) MACHINE LEARNING

Machine learning, también conocido en español como aprendizaje automático o aprendizaje de máquinas, nace como una idea ambiciosa de la Inteligencia Artificial en la década del 60. Exactamente es un campo de las ciencias de la informática que, de acuerdo con Arthur Samuel⁵ en 1959, les da a los ordenadores la habilidad de aprender sin ser explícitamente programados; es decir, se basa en la idea que existen algoritmos que pueden ofrecer conclusiones relevantes obtenidas de un conjunto de datos sin que una persona tenga que escribir instrucciones o códigos para ello.

En los años 90, machine learning se separa de la Inteligencia artificial para convertirse en una disciplina por sí sola. Actualmente el principal objetivo del machine learning es abordar y resolver problemas prácticos, que los ordenadores y las personas trabajen conjuntamente, ya que las primeras son capaces de aprender como lo harían las personas.

Las aplicaciones del machine learning dentro de la logística nos ayudan a obtener conclusiones, por lo que, por ejemplo, es perfecto para la previsión de las demandas, una de las tareas más complejas y delicadas dentro de la cadena de suministro. El machine learning es capaz de adaptarse continuamente sin intervención ajena. El aprendizaje automático aprende gradualmente qué variables son las que más afectan a nuestra demanda, adaptándose para futuros cálculos, sin necesidad que una persona tenga que volver a analizar todo el proceso.

Además, el machine learning en logística también puede ayudar con datos como la gestión de rutas, la sugerencia de productos, políticas de precios, optimización de inventarios, la evaluación y elección de proveedores o las relaciones inesperadas. Esto último quiere decir, por ejemplo, Walmart descubrió que había una relación entre el clima que hacía un día y el tipo de carne que se vendía, en resumen, datos que pueden ayudar a aumentar ventas.

⁵ Arthur L. Samuel fue un pionero en el campo de los juegos informáticos y la inteligencia artificial y el creador de uno de los primeros juegos didácticos como demostración muy temprana del concepto de la inteligencia artificial

(School E. B., 2018)

9.4) INTERNET DE LAS COSAS (IoT)

Como casi siempre ocurre el concepto y las herramientas que sustentan esta tecnología no son nuevas, lo nuevo y atractivo para los profesionales y empresas del sector logístico es el interés en su implementación y uso que puede dar como resultado un importante ahorro de costos en la actualidad.

A nivel logístico, el IoT se basa en que, en última instancia, las “cosas” (productos, materiales, etc., que pueda contener la supply chain) nos hablen y nos digan en tiempo real donde están ubicados (lugar) dentro de la cadena de suministro y, también, cómo se encuentran en el ámbito de calidad; es decir; si se ha producido algún tipo de desperfecto, obsolescencia por caducidad, etc.,

La pregunta que nos hacemos en este punto es ¿cómo podemos lograr la interconexión entre nuestros sistemas de información actuales y los bienes que circulan por nuestras cadenas de suministro? Bueno, la respuesta ya fue dada hace 20 años con la aparición de las primeras Smart Tags que estaban basadas en tecnología RFID.

Estas etiquetas “inteligentes” lo son, a diferencia del convencional código de barras, por que disponen de un chip con memoria regrabable que permite añadir y borrar información a lo largo de su paso por los diferentes eslabones que conforman la cadena de suministro (a diferencia del código de barras que es un código “muerto” en el sentido que es una etiqueta que suele añadirse al producto en origen o en un punto concreto en la supply chain; pero que luego no puede variar; es decir, nace y muere con él).

Con estos dispositivos o sensores informativos añadidos a un producto y actualizables en cualquier punto de la cadena de suministro se facilita la posibilidad de usar la IoT.

Existen en la actualidad diferentes usos dentro de la cadena de suministro para el IoT, todos muy interesantes y que suponen un importante ahorro de costos para las empresas que están innovando en sus procesos implementando estas herramientas.

En cuanto a transporte, el uso del IoT permite disponer de información en tiempo real sobre el servicio de distribución física (especialmente el denominado “última milla⁶” que está relacionado con la entrega directa al cliente). Este nivel informativo puede estar relacionado directamente con el vehículo que hace el reparto y su conductor (cumplimiento de rutas y horarios de entrega ajustados con ayuda de GPS, apertura de puertas del vehículo, seguridad de los productos por equivocación en reparto y también aspectos relacionados con mercancía a temperatura controlada, etc.), y/o también con los productos que se transportan para reparto dentro del mismo (error en dirección de entrega, confirmación sobre entrega correcta, indicación de posibles golpes o roturas en producto sin haber abierto el embalaje para su comprobación, etc.).

Dentro de lo denominado “intralogística⁷”, la gestión de almacenes también se ve favorecida por el uso del IoT. Esto lo hace con ayuda y combinación de otras tecnologías como, por ejemplo, el uso de drones dentro de almacenes. Si, decimos bien, dentro de almacenes. (ANNA, 2019)

La realización de inventarios cíclicos o anuales es una tarea habitual en todas las empresas, la misma es relativamente sencilla cuando el depósito o almacén tiene estanterías de poca altura; pero existen almacenes que tienen estanterías de más de 10 metros de altura, lo que hace muy complejo la realización de un inventario de forma rápida que no genere alteraciones importantes en el resto del proceso.

Se han realizado estudios (DHL, UPS entre otros) con drones en combinación con tecnología RFID basada en etiquetas inteligentes en HF (13,56 MHz) que nos indican que es posible leer hasta 600 ubicaciones paletizadas dentro de un almacén en una hora.

(Marco, s.f.)

⁶ La última milla, (conocida también como distribución capilar), es una gestión de transporte de paquetería centrado en el último trayecto que ha de realizarse en la entrega final

⁷ La Intralogística refiere a la optimización de los procesos logísticos de los materiales y mercaderías propios de una industria, en su punto de fabricación o almacén.



Figura 1 - Aplicaciones de IoT

Importancia de Blockchain en Internet de las Cosas

Los sistemas tradicionales de IoT dependen de una arquitectura centralizada. La información es enviada desde el dispositivo a la nube, donde se procesan los datos mediante análisis y luego son enviados nuevamente a los dispositivos IoT. Con miles de millones de dispositivos configurados para unirse a redes IoT en los próximos años, este tipo de sistema centralizado tiene una escalabilidad muy limitada, expone miles de millones de puntos débiles que comprometen la seguridad en la red y se volverá increíblemente costoso y lento si los terceros tienen que verificar y autenticar constantemente todas y cada una de las micro transacciones entre dispositivos.

Los contratos inteligentes en las redes descentralizadas permitirán que los dispositivos funcionen de forma segura y autónoma mediante la creación de acuerdos que solo son ejecutados al completar requisitos específicos. No solo permite una mayor automatización,

escalabilidad y transferencias más baratas (no requiere la participación de un tercero para supervisar las transacciones), sino que estos contratos inteligentes también pueden evitar anulaciones por parte de personas que desean utilizar los datos para su propio beneficio. La información es compartida en una red descentralizada y protegida criptográficamente, lo que resulta en una mayor complejidad para comprometer la seguridad de la red.

(Michael Casey, 2018)

Finalmente, con una red centralizada, el riesgo que un solo punto de falla deshabilite una red completa es una posibilidad muy real. Una red blockchain descentralizada mitiga este riesgo con millones de nodos individuales que transfieren datos en una base punto a punto (p2p) para mantener el resto de la red IoT funcionando sin problemas. *(Pauw, 2018)*

9.5) HISTORIA DE BLOCKCHAIN

Blockchain se dio a conocer por todos nosotros cuando en diciembre de 2017 el valor de Bitcoin llegó a 20000 USD,

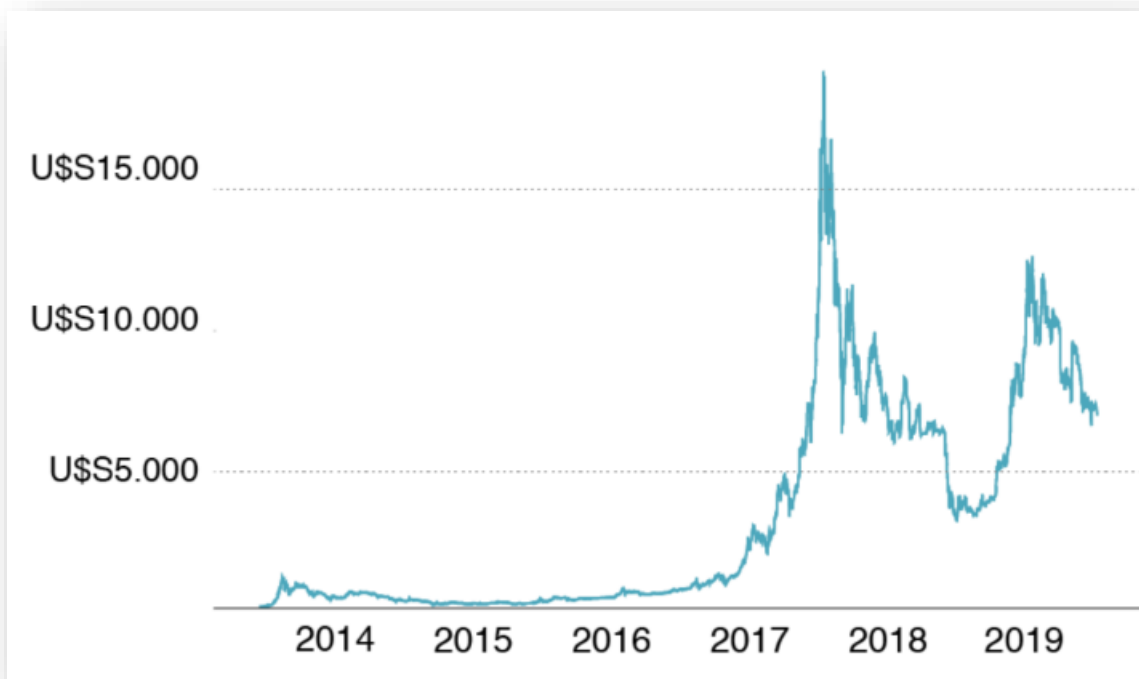


Figura 2 - Evolución Precio Bitcoin

en ese momento muy pocas personas (entre las que no me incluyo), podían distinguir Blockchain de Bitcoin, aún hoy esa asociación sigue vigente para muchos y resulta lógico que así suceda, Blockchain nació para ser una tecnología invisible, al igual que Internet, son las aplicaciones, páginas web y todo lo que alimenta el ecosistema lo que le brinda la visibilidad a la tecnología de fondo y hace que esto sea posible, en el caso de Blockchain, fue su primera aplicación llamada Bitcoin lo que despertó el interés general. Pero muchos años antes ya se realizaban pruebas y desarrollos por un movimiento denominado “Cypherpunks⁸” que enarboló la bandera de la privacidad, especialmente ante la amenaza del control y la censura por parte de gobiernos y autoridades centrales sobre el desarrollo tecnológico, la información y el intercambio de valor. En este caso, la privacidad podría entenderse como el legítimo derecho de cada ciudadano del mundo de revelar solo la información que desea. (Bastardo, 2019) (Vikram Dhillon, 2017). Es necesario destacar que esto es un manifiesto cyberpunk con ideología extrema en varios sentidos y sería imposible pensar siquiera vivir en semejante anarquía, solo para entender como ellos se autodefinían es que adjunto el primer párrafo del mismo:

“Somos las mentes electrónicas, un grupo de rebeldes de pensamientos libres.

Cyberpunks. Vivimos en el Ciberespacio, estamos en todos lugares, no tenemos límites.

Este es nuestro manifiesto. El manifiesto cyberpunk.

1/ Esos somos nosotros, lo Diferente. Ratas de la tecnología, nadando en el océano de la información.

2/ Estamos cohibidos, pequeños chicos de colegio, sentados en el último pupitre, en la esquina de la clase. 3/ Somos el adolescente que todos consideran extraño. 4/ Estamos estudiando hackear sistemas operativos, explorando la profundidad de su extremos. 5/ Nos criamos en el parque, sentados en un banco, con un ordenador portátil apoyado en las rodillas, programando la última realidad virtual.

6/ Lo nuestro está en el garaje, apilado con la porquería electrónica. El hierro soldado en la esquina

⁸ Cypherpunks es el nombre de un movimiento sin líderes que aboga por el uso de la criptografía para garantizar la privacidad de los individuos. El germen apareció a mediados de los años 80, cuando la criptografía era todavía cosa de espías y gobiernos, sobre la base de trabajos de personas del ámbito de la tecnología, básicamente un texto de David Chaum y el trabajo de criptografía de código público de Whitfield Diffie y Martin Hellman. El término fue acuñado como un juego de palabras en una de las primeras reuniones de un grupo convocado por Tim May, John Gilmore y Eric Hughes a finales de 1992; una treintena de personas que discutían acerca de política, filosofía, privacidad, anonimato, reputación y cómo manejarlo técnicamente. Crearon una lista de correo con ese nombre que para finales de los años 90 contaba con unos 2000 suscriptores.

de la mesa y cercana a la radio desmontada- eso es lo nuestro. Lo nuestro es una habitación con ordenadores, impresoras zumbeantes y modems pitando. 7/ Somos aquellos que vemos la realidad de forma distinta. Nuestro punto de vista muestra más de lo que la gente ordinaria puede ver. Ellos solo ven lo exterior, pero nosotros vemos lo interior. Eso es lo que somos- realistas con gafas de soñadores. 8/ Somos aquellas personas casi desconocidas para el vecindario. Personas, entregadas a sus propios pensamientos, sentadas día tras día ante el ordenador, saqueando la Red por algo. No salimos frecuentemente de casa, solo de vez en cuando para ir al cercano estudio de radio, o a un conocido bar a encontrarse a algunos de los pocos amigos que tenemos, o encontrarnos a algún cliente, o al camello de la esquina,... o simplemente para dar un paseo. 9/ No tenemos muchos amigos, sólo unos pocos con los que nos vamos de fiesta. Todos los demás que conocemos están en la Red, en el otro lado de la línea. Los conocemos de nuestro canal favorito de IRC, de los newsgroups, de los sistemas que frecuentamos : 10/ Nosotros somos aquellos los que nos importa una mierda lo que los demás piensen de nosotros, no nos importa lo que aparentamos o lo que la gente diga sobre nosotros en nuestra ausencia. 11/ La mayoría de nosotros viven escondidos, siendo desconocidos para todos menos a aquellos que inevitablemente están en contacto con ellos. 12/ Otros aman la publicidad, ellos aman la fama. Ellos son conocidos en su mundo underground. Sus nombres se escuchan con facilidad allí. Pero todos unidos somos una sola cosa- nosotros somos los cyberpunks.”
(As.Kirtchev, s.f.)

Algunos de los hitos más importantes que hicieron posible la aparición de Blockchain:

1982. El criptógrafo David Chaum⁹ publica el paper “Blind Signatures for Untraceable Payments” en la revista *Advances in Cryptology*, donde propone un sistema de cash digital anónimo llamado eCash. (Chaum, s.f.)

1990. Chaum funda la empresa DigiCash que ofrece un sistema de cash digital basado en las ideas de eCash.

⁹ David Chaum es el inventor de muchos protocolos criptográficos, así como eCash y DigiCash. Su artículo de 1981, "Correo Electrónico de rastro oculto, Direcciones de Regreso, y Seudónimos Digitales", sentó las bases para el campo de la investigación de las comunicaciones anónimas. https://es.wikipedia.org/wiki/David_Chaum

1997. Adam Back¹⁰ propone Hashcash, un sistema para combatir el spam basado en el proof of work, una idea que Satoshi Nakamoto retomaría en el algoritmo de minado del Bitcoin.

1998. DigiCash se presenta en quiebra. Algunos lo atribuyen a que el comercio electrónico aún no estaba lo suficientemente desarrollado. Otros sostienen que la quiebra se debió a malas decisiones en la gestión de Chaum.

1998. El criptógrafo Nick Szabo¹¹ propone un sistema de cash digital llamado Bit Gold, un precursor casi directo en la arquitectura del Bitcoin¹².

1999. En una entrevista, el economista Milton Friedman¹³ augura el advenimiento de una nueva tecnología anónima de cash digital. (*Friedman*)

¹⁰ Adam Back Nació en julio de 1970 en la ciudad de Londres, Inglaterra. Obtuvo un doctorado de ciencias de la computación de la Universidad de Exeter. Back es reconocido principalmente por sus diversos trabajos en criptografía y sistemas anónimos.

Su primer trabajo en ese sentido fue; “The Simple Key Search Protocol”. Gracias a este trabajo presentado en el año 1995, en conjunto con Andrew Brown y Piete Brooks, se pudo romper la seguridad SSL de Netscape. Además, durante su estadía en la empresa Zero Knowledge Systems, Back trabajó como consultor de la empresa Nokia, en un proyecto para integrar pagos electrónicos utilizando teléfonos móviles. <https://academy.bit2me.com/quien-es-adam-back/>

¹¹ Nick Szabo es un ciudadano estadounidense de ascendencia húngara. Hasta el momento se desconoce su fecha y lugar de su nacimiento. Obtuvo en 1989 la Licenciatura en Ciencias de la Computación por la University of Washington. Recientemente, en 2017, recibió el Doctorado Honoris Causa en Ciencias Sociales por la Universidad Francisco Marroquín.

<https://academy.bit2me.com/quien-es-nick-szabo/>

¹² Bitcoin es un protocolo, proyecto de código abierto y red peer-to-peer que es utilizado como criptomoneda, sistema de pago y mercancía

<https://es.wikipedia.org/wiki/Bitcoin>

¹³ Milton Friedman fue un estadístico, economista e intelectual estadounidense de origen judío ganador del Premio Nobel de Economía de 1976. Profesor en la Universidad de Chicago, fue uno de los fundadores de la Escuela de Economía de Chicago, una escuela económica de economía clásica defensora del libre mercado

https://es.wikipedia.org/wiki/Milton_Friedman

31 de octubre de 2008. Satoshi Nakamoto¹⁴ publica el paper “Bitcoin: A Peer-to-Peer Electronic Cash System” (*Nakamoto*) en un foro de criptografía.

3 de enero de 2009. El blockchain de Bitcoin entra en funcionamiento. Es minado el primer bitcoin.

12 de enero de 2009. Se desarrolla la primera transferencia de bitcoin entre Satoshi Nakamoto y el criptógrafo Hal Finney.

(Ast, 2017)

¹⁴ Satoshi Nakamoto es la persona o grupo de personas que crearon el protocolo Bitcoin y su software de referencia. En 2008, Nakamoto publicó un artículo en la lista de correo de criptografía metzdowd.com que describía un sistema P2P de dinero digital.
https://es.wikipedia.org/wiki/Satoshi_Nakamoto

9.6) QUE ES BLOCKCHAIN

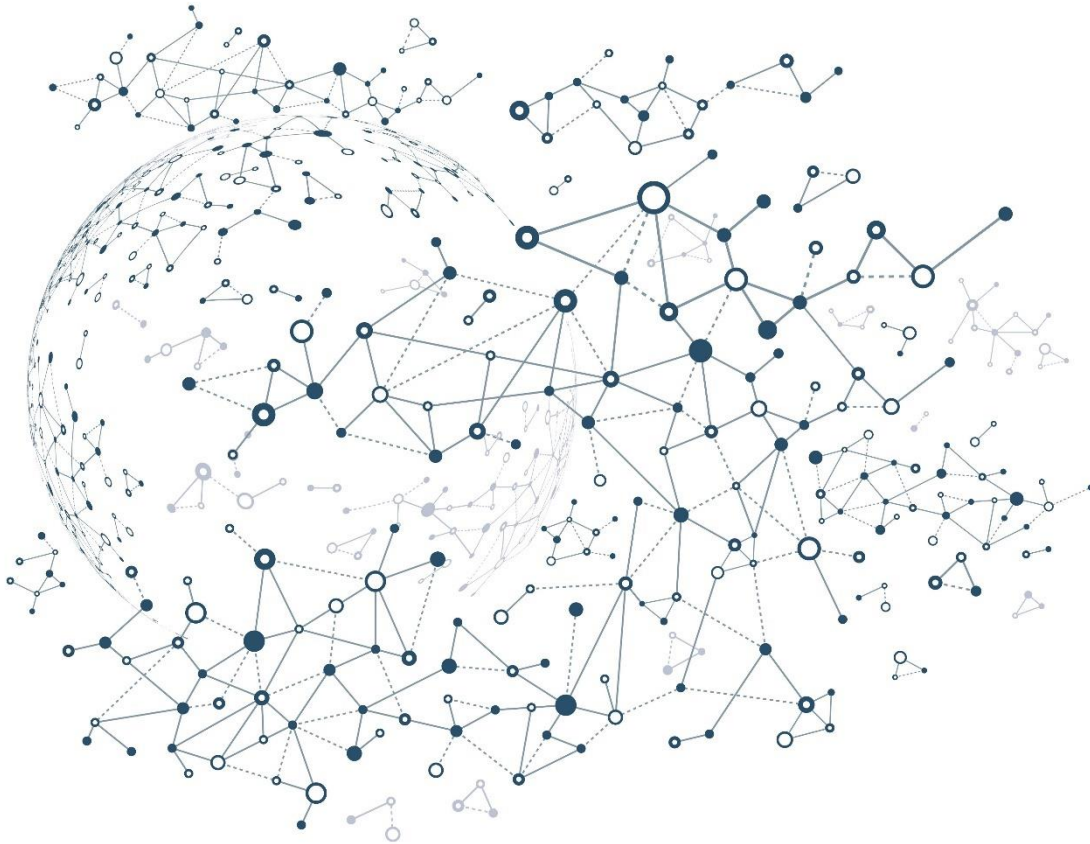


Figura 3 - Red Descentralizada

Blockchain (o cadena de bloques) es una base de datos compartida que funciona como un libro contable para el registro de operaciones de compra-venta o cualquier otra transacción. Es la base tecnológica que permitió la aparición de bitcoin en primera instancia. Consiste en un conjunto de bloques que están en una base de datos compartida, libre y on-line en la que se registran mediante códigos las operaciones, cantidades, fechas y participantes. Al utilizar claves criptográficas y al estar distribuido por muchos ordenadores (personas) presenta ventajas en la seguridad frente a manipulaciones y fraudes. Una modificación en una de las copias no serviría en absoluto, sino que hay que hacer el cambio en todas las copias porque la base es abierta y pública.

Este esquema distribuido es una de sus principales ventajas ante otras redes de almacenamiento: Resulta más complejo de hackear debido a que no basta con atacar uno o

dos nodos de la red, sino que tendrían que hacerlo con absolutamente todos para poder causar realmente daño. Esta propiedad está inspirada en las redes de almacenamiento y comunicación peer-to-peer (p2p), las cuales han sido popularizadas por el uso de los torrents¹⁵, que son servicios de descargas distribuidas en Internet.

Todos los bloques que conforman la cadena, tienen un hash (contraseña numérica) del bloque anterior, los bloques son ordenados en la cadena por orden cronológico, gracias a ese hash todos los bloques están referenciados por el bloque que los creó, por lo que solo los bloques que contienen un hash válido son introducidos en la cadena y replicados a todos los nodos. Gracias a este sistema, prácticamente es imposible modificar un bloque que ha permanecido en la cadena un tiempo determinado.

Los nodos “mineros” son los encargados de crear los bloques que forman la cadena, añadiendo a cada uno de ellos el hash correspondiente y todas las nuevas transacciones que han sido introducidas en la red. De esta manera podemos decir que blockchain nos permite llevar una “contabilidad” pública de manera totalmente transparente sobre todas las transacciones de la red, sin casi posibilidad de fraude, congestión o pérdida de datos, y totalmente trazable. (*Bikramaditya Singhal. Gautam Dhameja, 2018*)

En el siguiente punto se desarrolla con mayor profundidad el significado de hash, mineros, bloques.

¹⁵ Un archivo torrent almacena metadatos sobre archivos y carpetas que son distribuidas y serán utilizados por un cliente de BitTorrent. Está definido en la especificación de BitTorrent.

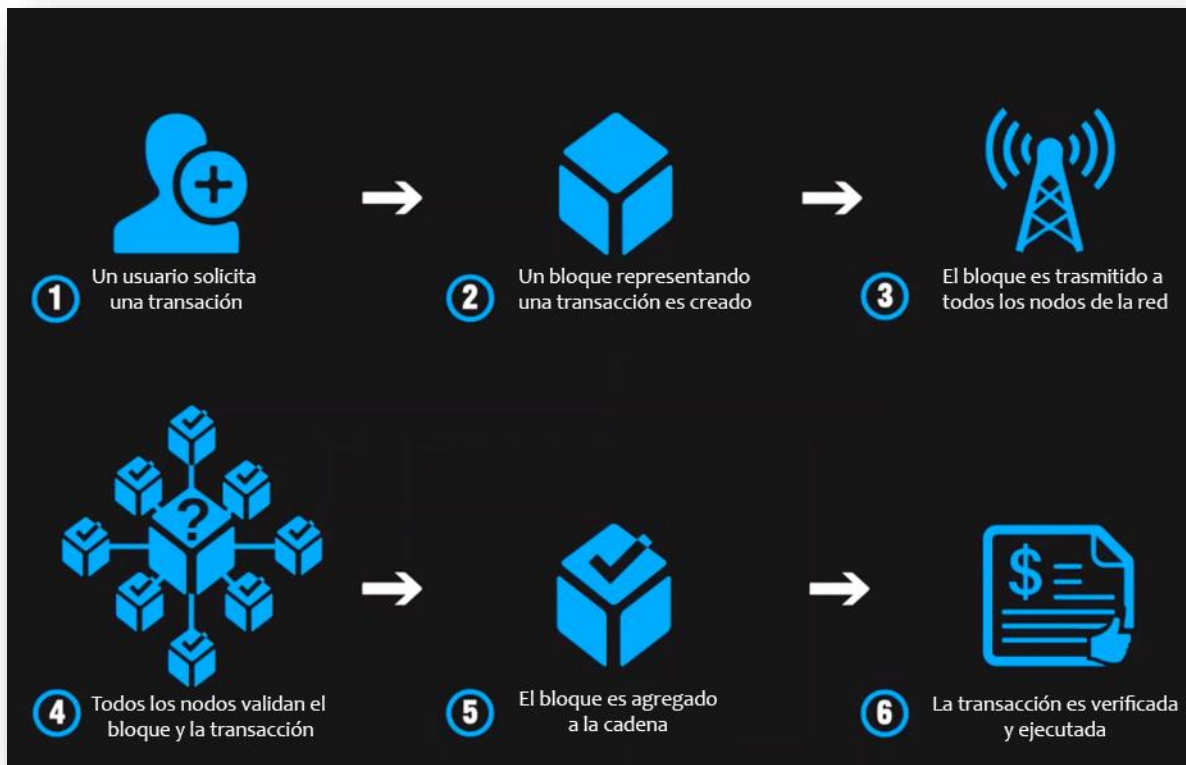


Figura 4 - Funcionamiento de Blockchain

9.7) PRINCIPALES CARACTERÍSTICAS DE BLOCKCHAIN

9.7.1) Inmutabilidad

Hay algunas características interesantes de blockchain; pero entre ellas la “Inmutabilidad” es sin duda una de las características clave de la tecnología.

Inmutabilidad significa que algo no puede ser cambiado o alterado. Esta es una de las características que ayuda a garantizar que la tecnología se mantenga como está: una red permanente e inalterable.

La tecnología Blockchain funciona ligeramente diferente a la del sistema bancario típico. En lugar de confiar en las autoridades centralizadas, esta garantiza las características de la blockchain a través de una colección de nodos.

Cada nodo en el sistema tiene una copia del registro digital. Para agregar una transacción, cada nodo necesita verificar su validez. Si la mayoría entiende que es válido, entonces es agregado al registro. Esto promueve la transparencia y la hace incorruptible.

Por lo tanto, sin el consentimiento de la mayoría de los nodos, nadie puede agregar bloques de transacciones al registro.

Otro hecho, que respalda las características de la blockchain, es que una vez que los bloques de transacciones han sido agregadas en el registro, nadie puede regresar y cambiarlo. Por lo tanto, ningún usuario dentro la red podrá editarlo, eliminarlo o actualizarlo.

9.7.2) Descentralización

La red está descentralizada, lo que significa que no tiene ninguna autoridad que la gobierne o una sola persona que ejerce control total. Más bien, un grupo de nodos mantiene la red descentralizada.



Figura 5 - Tipos de Redes

Esta es una de las características clave de la tecnología blockchain que funciona perfectamente. Blockchain nos pone a los usuarios en una posición directa. Como el sistema no requiere ninguna autoridad del gobierno, podemos acceder directamente desde la web y almacenar nuestros activos allí.

Puedes almacenar cualquier cosa desde criptomonedas, documentos importantes, contratos u otros activos digitales valiosos. Y con la ayuda de blockchain, tendrás control directo sobre

ellos usando tu clave privada. Entonces, verás que la estructura descentralizada le está dando a la gente común el poder sobre sus activos.

Esto genera:

Menos fallos: todo en blockchain está completamente organizado, y como no depende de cálculos humanos, es altamente tolerante a fallos. Por lo tanto; las fallas accidentales en este sistema no son una salida habitual.

Control de usuario: con la descentralización, los usuarios ahora tienen control sobre sus propiedades. No tienen que depender de terceros para mantener sus activos. Todos ellos pueden hacerlo simultáneamente por sí mismos.

Menos propenso a averías: como ser descentralizado es una de las características clave de la tecnología blockchain, resulta más complejo de vulnerarse. Esto es debido a que atacar el sistema puede ser más costoso para los piratas informáticos y no es una solución fácil. Por lo tanto, existe menos posibilidad que pueda averiarse.

Sin terceros: la naturaleza descentralizada de la tecnología la convierte en un sistema que no depende de empresas de terceros; Sin terceros, no hay riesgo añadido.

Cero estafas: Gracias a que el sistema es ejecutado con algoritmos, no hay posibilidad que otras personas puedan estafar a su contraparte. Nadie puede utilizar blockchain para sus ganancias personales.

Transparencia: la naturaleza descentralizada de la tecnología crea un perfil transparente de cada participante. Cada cambio en el blockchain es visible y lo hace más concreto.

Naturaleza auténtica: esta naturaleza del sistema lo convierte en un tipo único de sistema para todo tipo de personas. Y los piratas informáticos tendrán dificultades para descifrarlo.

9.7.3) Seguridad Mejorada

A medida que es eliminada la necesidad de una autoridad central, no puede simplemente cambiarse cualquier característica de la red para su beneficio. El uso del cifrado garantiza otra capa de seguridad para el sistema.

Agregado con la descentralización, la criptografía establece otra capa de protección para los usuarios. La criptografía es un algoritmo matemático bastante complejo que actúa como un firewall para ataques.

Toda la información en la blockchain es cifrada criptográficamente. En términos simples, la información en la red oculta la verdadera naturaleza de los datos. Para este proceso, cualquier dato de entrada pasa por un algoritmo matemático que produce un tipo diferente de valor; pero manteniendo la longitud siempre fija.

Podrías considerarlo como una identificación única para cada dato. Todos los bloques en el registro vienen con un hash único y contienen el hash del bloque anterior. Por lo tanto, cambiar o intentar manipular los datos significa cambiar todas las ID de hash. Y hacerlo con la tecnología existente, resulta imposible.

Tendrás una clave privada para acceder a los datos; pero también tendrás una clave pública para realizar transacciones.

Si un hacker quisiera hacer daño a Blockchain tendría que penetrar en cada uno de los nodos que la componen, en sistemas centralizados solo se requiere ingresar a sus servidores centrales. Un ejemplo cercano es el considerado el mayor hackeo de la historia realizado contra Yahoo que comprometió 3.000 millones de cuentas. (*Valinsky, 2019*).

9.7.4) Encriptación Simétrica

En este tipo de encriptación es utilizada la misma clave para encriptar y desencriptar el mensaje (*Anderson, Narus, Narayandas, & Seshadri, 2011*). Debido a su mayor velocidad, la encriptación simétrica es empleada de forma generalizada para la protección de información en muchos sistemas de computación modernos. El Advanced Encryption Standard (AES), por ejemplo, es empleado por el gobierno de los Estados Unidos para encriptar información clasificada y sensible. El AES reemplazó a su predecesor, el Data Encryption Standard (DES), desarrollado en la década de 1970 como estándar de encriptación simétrica. (*binance*)



Figura 6 - Encriptación Simétrica

9.7.5) Encriptación Asimétrica

Son utilizadas diferentes claves (públicas y privadas), para encriptar y desencriptar. La encriptación asimétrica puede aplicarse en sistemas en los que muchos usuarios pueden requerir la encriptación y desencriptación de mensajes o conjuntos de datos, especialmente, cuando la velocidad y la potencia computacional no son preocupaciones primarias. Un ejemplo de este tipo de sistemas; el correo electrónico cifrado, en el que una clave pública puede ser empleada para encriptar un mensaje, y una clave privada para desencriptarlo.

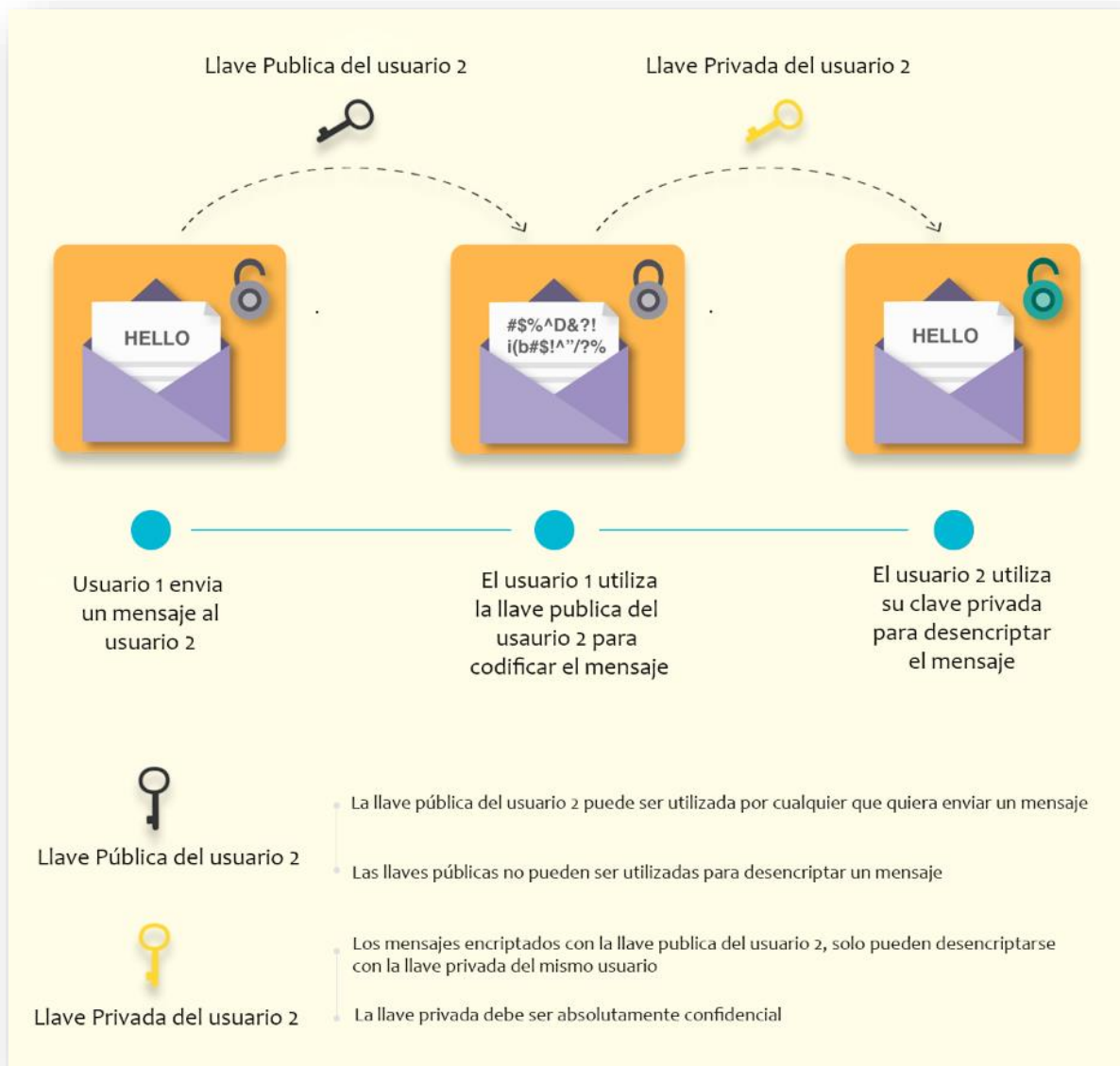


Figura 7 - Encriptación Asimétrica

9.7.6) Irreversible

Los hashes son bastante complejos, y prácticamente imposible alterarlos o revertirlos. Nadie puede tomar una clave pública y crear la clave privada. Además, un solo cambio en la entrada podría llevar a una ID completamente diferente, por lo que los pequeños cambios no son un lujo en el sistema.

Si alguien quiere corromper la red, deberá modificar todos los datos almacenados en cada nodo de la red. Podría haber millones y millones de personas, donde todos tengan la misma copia del registro.

9.7.7) Registros distribuidos

Por lo general, un registro público proporcionará toda la información sobre una transacción y el participante. Todo está a la vista y no hay dónde esconderse. Aunque en el caso de la blockchain privada o federada es un poco diferente. Pero, aun así, en esos casos muchas personas pueden ver lo que realmente sucede en el registro.

Esto se debe a que todos los usuarios del sistema mantienen el registro en la red. Distribuyendo el poder computacional para asegurar un mejor resultado.

El resultado siempre será un sistema de registro más eficiente que puede superar los tradicionales.

No hay cambios maliciosos: el registro distribuido responde realmente bien a cualquier actividad sospechosa o manipulación. Como nadie puede cambiar el registro y todo se actualiza muy rápido, el seguimiento de lo que sucede en el registro es bastante fácil con todos estos nodos.

Verificación de propiedad: aquí, los nodos actúan como verificadores del registro. Si un usuario desea agregar un nuevo bloque, otro tendría que verificar la transacción y luego dar el visto bueno. Esto proporciona al usuario una participación justa.

Sin favores adicionales: Nadie en la red puede obtener favores especiales de la red. Todos tienen que pasar por los canales habituales y luego agregar sus bloques.

Administración: para hacer que las características de la blockchain funcionen, cada nodo activo debe mantener el registro y participar para la validación.

9.7.8) Consenso

Cada blockchain prospera debido a los algoritmos de consenso. La arquitectura está diseñada inteligentemente y los algoritmos de consenso están en el centro de esta arquitectura. Cada una de ellas tiene un consenso para ayudar a la red a tomar decisiones.

En términos simples, el consenso es un proceso de toma de decisiones para el grupo de nodos activos en la red. Aquí, los nodos pueden llegar a un acuerdo de forma sencilla y relativamente más rápida. Cuando millones de nodos están validando una transacción, es

absolutamente necesario un consenso para que un sistema funcione sin problemas. Podrías considerarlo como una especie de sistema de votación, donde la mayoría gana y la minoría tiene que apoyarlo para que el sistema logre funcionar.

El consenso es responsable que la red no necesite confianza. Hay posibilidad que los nodos no confíen entre sí; pero pueden confiar en los algoritmos que son ejecutados en su núcleo.

Hay muchos algoritmos de consenso diferentes para las blockchain en todo el mundo. Cada uno tiene su propia y única manera de tomar decisiones y perfeccionar errores previamente introducidos. Esta arquitectura crea un reino de justicia en la web.

Sin embargo, para que la descentralización continúe, cada blockchain debe tener un algoritmo de consenso, de lo contrario; se perderá su valor central.

9.7.9) Acuerdos más rápidos

Los sistemas bancarios tradicionales son bastante lentos. A veces puede llevar días procesar una transacción después de finalizar todas las liquidaciones. También puede ser corrompido con bastante facilidad. Blockchain ofrece una liquidación más rápida en comparación con los sistemas bancarios tradicionales. De esta manera, un usuario puede transferir dinero relativamente más rápido, lo que ahorra mucho tiempo a largo plazo.

9.8) COMO SE COMPONE BLOCKCHAIN

El motivo de la tesis no es profundizar en detalle sobre cada aspecto de tan compleja tecnología; pero resulta inevitable explicar el funcionamiento de blockchain para evaluar el alcance y limitaciones que tiene; por lo tanto, se realizará una breve introducción sobre los elementos que la componen.

Técnicamente, blockchain es una brillante amalgama entre los conceptos de criptografía, teoría de juegos e ingeniería de ciencias de la computación. (*Bikramaditya Singhal, 2018*)

Entre los elementos más importantes que componen esta tecnología se encuentran:

Criptografía de clave pública: también conocida como criptografía asimétrica, utiliza la implementación de curva elíptica para mejorar el rendimiento respecto a implementaciones

tradicionales como RSA¹⁶. De esta forma es validada la autenticidad del emisor de la transacción (*Gates, 2017*) por parte de todos los nodos de la red. Para las implementaciones más populares (Bitcoin y Ethereum¹⁷) esta validación es realizada comparando la clave pública del remitente con el elemento firmado con su clave privada (el elemento a firmar es una versión “hasheada” de la transacción).

9.8.1) Base de datos distribuida:

Cada uno de los nodos replica completamente la base de datos al unirse a la red de la Blockchain correspondiente. Este proceso de réplica sincroniza todos los bloques de la cadena. Una vez sincronizada, el nodo podrá empezar a operar con normalidad sobre la red (balance de criptomonedas, envío y recepción de transacciones). Es importante destacar que la base de datos se nutre de bloques. Es decir, hasta que una transacción no es confirmada mediante su inclusión en un bloque aceptado, la transacción en sí no es considerada válida en la Blockchain.

9.8.2) Algoritmos de consenso

la característica que marca la diferencia entre otros sistemas distribuidos y Blockchain es el algoritmo de consenso. Dicho algoritmo incentiva a participar mediante el envío de recompensas a los mineros encargados de crear los bloques.

Los más destacados por el momento son los siguientes:

Proof-of-Work: es el algoritmo más extendido, utilizado por Bitcoin y la versión estable de Ethereum y está orientado a redes públicas.

¹⁶ RSA - En criptografía, RSA es un sistema criptográfico de clave pública desarrollado en 1979. Es el primer y más utilizado algoritmo de este tipo y válido tanto para cifrar como para firmar digitalmente. La seguridad de este algoritmo radica en el problema de la factorización de números enteros

¹⁷ Ethereum es una plataforma open source, descentralizada que permite la creación de acuerdos de contratos inteligentes entre pares, basada en el modelo blockchain. Cualquier desarrollador puede crear y publicar aplicaciones distribuidas que realicen contratos inteligentes

Se basa en la generación de un hash teniendo en cuenta el Merkle Root (raíz hash del árbol que toma a pares los hashes de las transacciones a incluir en un bloque), el hash del bloque anterior, la hora, la dificultad y el nonce (“valor único”).

Los valores se van combinando por los mineros hasta generar un hash que tenga N 0s (en la elaboración de esta presentación, el valor de N para Bitcoin es 18).

El valor N se va modificando por el protocolo para encajar con los tiempos medios de subida de bloques (10’ para Bitcoin, 15” para Ethereum).

Una vez generado el hash de bloque correcto, es enviado al resto de la red. La aceptación de dicho bloque es conseguida cuando los mineros en la red empiezan a utilizar dicho hash como valor del bloque previo.

A cambio del bloque subido, se obtiene una recompensa por bloque y transacciones. En el caso de lograrse una solución del hash; pero no se consiga llegar a ser el nuevo bloque de la cadena (porque alguien lo haya conseguido antes). No se obtendrá recompensa en Bitcoin; pero sí en Ethereum (bloques huérfanos y tíos).

Proof-of-Authority: algoritmo utilizado por Ethereum para la gestión de redes privadas.

El coste de PoW no tiene sentido en redes privadas en las que todas las partes se conocen.

Para acelerar la subida de bloques y sus transacciones son definen autoridades, una por cada parte implicada.

Cada autoridad dispone de una clave privada en la red que permite firmar las transacciones.

La parte pública de la misma es distribuida al resto de autoridades.

Cuando es emitida una transacción, se valida la firma del remitente y es incluido en un bloque que sube “inmediatamente”.

De esta forma los tiempos pueden reducirse exponencialmente, basado en una confianza predefinida.

Proof-of-Stake (en desarrollo): algoritmo en desarrollo por Ethereum (y otros protocolos de criptomonedas) que es basado en que las direcciones que tienen una mayor participación en la red (mayor número de criptomonedas, “stake”) tendrán una mayor posibilidad de subir nuevos bloques.

9.8.3) Hash

El nombre de hash es utilizado para identificar una función criptográfica muy importante en el mundo informático. Estas funciones tienen como objetivo primordial codificar datos para formar una cadena de caracteres única. Todo ello sin importar la cantidad de datos introducidos inicialmente en la función. Estas funciones sirven para asegurar la autenticidad de datos, almacenar de forma segura contraseñas, y la firma de documentos electrónicos.

Las funciones hash son ampliamente utilizadas en la tecnología blockchain con el fin de agregar fiabilidad a las mismas. El Bitcoin, es un claro ejemplo de cómo los hashes pueden usarse para hacer posible la tecnología de las criptomonedas.

Historia de las funciones Hash

La aparición de la primera función hash data del año 1961. En ese entonces, Wesley Peterson¹⁸ creó la función Cyclic Redundancy Check (Comprobación de Redundancia Cíclica). Fue creada para comprobar cuán correctos eran los datos transmitidos en redes (como Internet) y en sistemas de almacenamiento digital. Fácil de implementar y muy rápida, ganó aceptación y es hoy un estándar industrial. Con la evolución de la informática y los computadores, estos sistemas fueron especializándose cada vez más.

Esto permitió crear nuevas y mejores funciones hash entre las que pueden destacarse:

MD2: es una de las primeras funciones hash criptográficas. Creada por Ronald Rivest¹⁹, en el año 1989. Con un alto nivel de eficiencia y fiabilidad para el momento. Su consecuente

¹⁸ William Wesley Peterson, Ph.D.1 (22 de abril de 1924, Muskegon, Míchigan – 6 de mayo de 2009) fue un matemático y científico computacional estadounidense. Fue conocido por inventar el método de comprobación de redundancia cíclica, por cuya investigación fue galardonado con un Premio Japón en 1999.

Peterson fue profesor de Ciencias de la computación de la Universidad de Hawaii en Manoa. Coescribió varios libros sobre códigos de corrección de errores, incluyendo la 2ª edición revisada de: Código de Corrección de Errores (coautoría con E. J. Weldon).

Además hizo investigaciones y publicaciones en los campos de lenguajes de programación, programación de sistemas y redes. Además del Premio Japón, ha ganado el Premio Claude Shannon en 1981 y la medalla Centenaria de IEEE en 1984.

¹⁹ Ronald Linn Rivest es un criptógrafo y profesor en el MIT. En dicha institución, miembro del departamento de ingeniería eléctrica y ciencias de la computación, y del laboratorio de ciencias de la computación e inteligencia artificial

evolución llevó a la creación de la función hash MD5. La cual es aún usada en ambientes donde la seguridad no es una alta prioridad.

RIPEMD: es una función hash criptográfica creada por el proyecto europeo RIPE en el año 1992. Su principal función era la de sustituir al estándar del momento, la función hash MD4. En la actualidad aún se considera muy seguro, especialmente en sus versiones RIPEMD-160, RIPEMD-256 y RIPEMD-320.

SHA: el estándar actual de hashes criptográficos. Creada por la NSA²⁰ en 1993, como parte de su proyecto interno para autenticar documentos electrónicos. SHA y sus derivadas son consideradas las funciones hash más seguras hasta el momento. Es de especial interés, SHA-256 por ser fundamental en la tecnología que hizo posible el Bitcoin.

Funciones Hash – ¿Cómo funcionan?

Las funciones hash funcionan gracias a una serie de complejos procesos matemáticos y lógicos. Estos procesos, son trasladado a un software de ordenador con el fin de usarlos desde el propio ordenador. Desde allí, podemos tomar cualquier serie de datos, introducirlos en la función y procesarlos. Con esto se busca obtener una cadena de caracteres de longitud fija y única para los datos introducidos. A la vez que se hace prácticamente imposible realizar el proceso contrario. Es decir, es prácticamente imposible obtener los datos originales desde un hash ya formado. Esto gracias a que el proceso de creación de hashes, es un proceso de un solo sentido.

Un ejemplo sencillo y de la vida diaria de este proceso sería; la realización de un pastel. Cada uno de los ingredientes del pastel, sería el equivalente a la entrada de datos. El proceso de preparación y cocción del pastel, sería el proceso de codificación de dichos datos (ingredientes) por la función. Al finalizar, obtenemos un pastel con características únicas e irrepetibles dadas por los ingredientes del mismo. Mientras que el proceso contrario (llevar al pastel a su estado de ingredientes inicial), es prácticamente imposible de realizar.

²⁰ NSA La Agencia de Seguridad Nacional es una agencia de inteligencia del Gobierno de los Estados Unidos. Encargada de todo lo relacionado con la seguridad de la información

Un ejemplo visual del proceso puede mostrarse utilizándose las funciones MD5 y SHA-256, en dos casos de uso distintos.

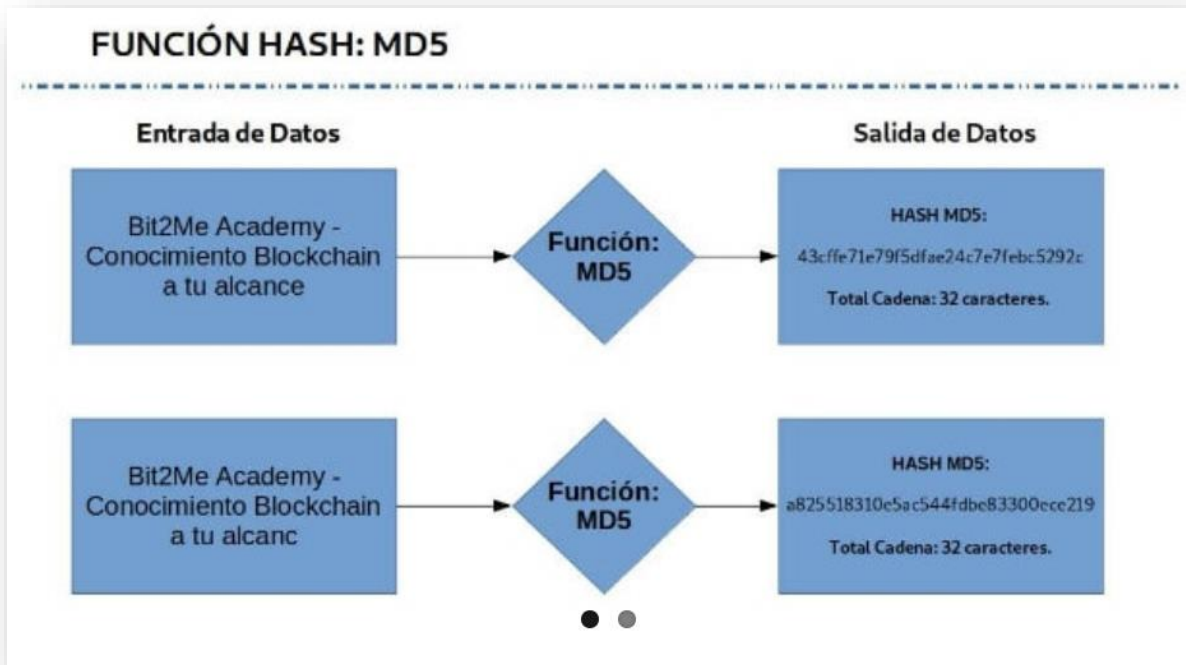


Figura 8 - Función Hash MD5

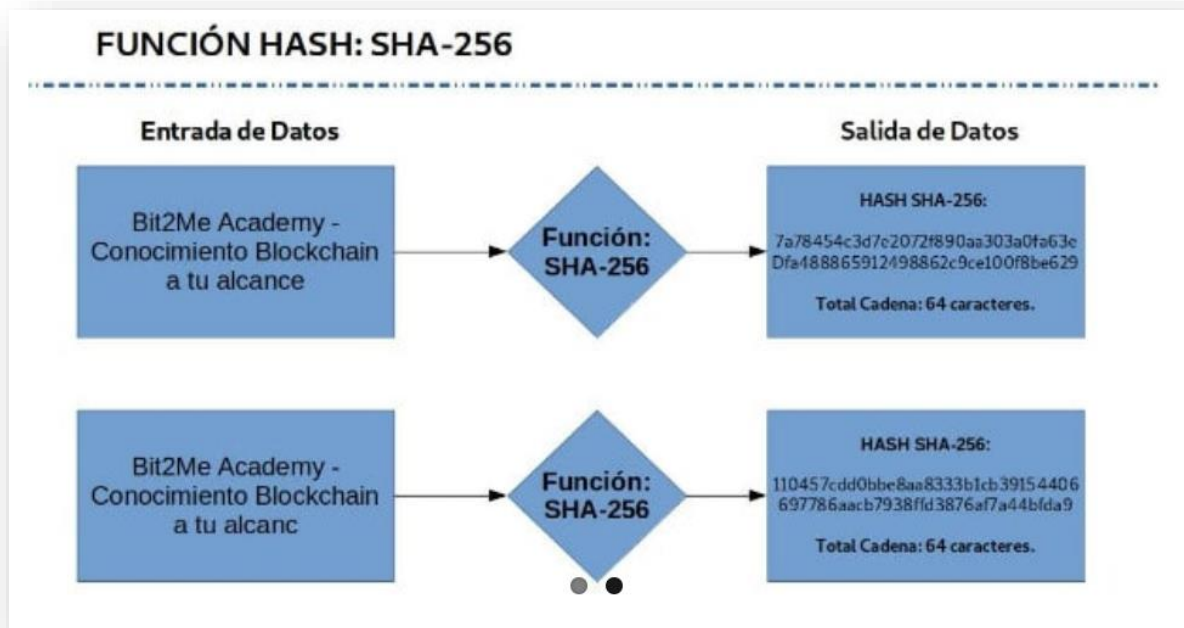


Figura 9 - Función Hash SHA-256

La segunda entrada se ha realizado una pequeña modificación en el texto. Esta; aunque es mínima, alteró completamente el resultado de los hashes para MD5 y SHA-256.

Esto prueba que los hashes serán únicos en todos los casos. Lo que nos permite estar seguros que ningún actor malicioso podrá forzar hashes de forma sencilla. Aunque lograr esto no sea imposible, un hacker podría pasar cientos de años procesando datos para lograr su cometido. Son estas dos observaciones las que nos dan la fiabilidad de usar este método en distintas áreas sensibles. Certificados digitales, firmas únicas de documentos sensibles o secretos, identificación digital y almacenamiento de claves, son algunos casos de uso. Pero no se detiene allí, puesto que la flexibilidad y seguridad de esta tecnología la hace idónea en muchas áreas. (Anderson, Narus, Narayandas, & Seshadri, 2011)

Características de las funciones hash

Entre las principales características de las funciones hash, pueden mencionarse las siguientes: Son fáciles de calcular. Los algoritmos de hash son muy eficientes y no requieren de grandes potencias de cálculo para ejecutarse.

Es compresible. Esto quiere decir que, sin importar el tamaño de la entrada de datos, el resultado siempre será una cadena de longitud fija. En el caso de SHA-256, la cadena tendrá una longitud de 64 caracteres.

Por ejemplo, si encriptamos dos palabras con diferente cantidad de caracteres obtendremos la misma cantidad de caracteres de hash

UTN	4BB772E13AA19E12612A514531E0A062111E6312EDAE401F59DE3CE06DE91A2A
MAURICIO	668C2FAA19C77BDF43CE287D4568CF8A092F8AF8CE097C430F4D68E1BA5E734B

Funcionamiento tipo avalancha. Cualquier mínimo cambio en la entrada de datos, origina un hash distinto a la entrada de datos original.

Resistencia débil y fuerte a colisiones. Hace referencia a que es imposible calcular un hash, que permita encontrar otro hash igual. Mejores conocidos como preimagen y segunda preimagen, es el concepto base de la seguridad de los hashes.

Son irreversibles. Tomar un hash y obtener los datos que dieron origen al mismo, en la práctica no puede ser posible. Esto es uno de los principios que hacen a los hashes seguros.

Nivel de seguridad de las funciones hash

Una explicación más cercana

Observando ambos casos de uso podemos notar lo siguiente:

La primera entrada de datos, da como resultado un hash único, para los casos de MD5 y SHA-256. Resultados que están ajustados a la realidad de cada una de esas funciones.

Las actuales funciones hash tienen un alto nivel de seguridad; aunque esto no significa que sean infalibles. Un buen ejemplo de esto es; la función hash MD5. En principio, las especificaciones de la misma prometían una seguridad muy alta. Su uso fue extendido en Internet por la necesidad de un sistema de hash para mantener su seguridad. Pero en el año 1996, se pudo romper la seguridad de la función. Con ello quedó obsoleta y se recomendó abandonar su utilización.

Por otro lado, funciones como RIPEMD-160 y SHA-256, son tan complejas que su seguridad aún está garantizada. Por ejemplo, para SHA-256 se calcula que para romper su seguridad harían falta miles de años usando supercomputadores actuales. Lo mismo aplica en el caso

de RIPEMD-160 y sus consecuentes evoluciones. Esto significa que ambas funciones aún brindan un alto nivel de seguridad y pueden utilizarse sin problemas.

Pero pese a que estas funciones son muy seguras, no significa que no se investiguen y desarrollen otras opciones. Esta constante evolución nos dice que siempre tendremos a disposición herramientas seguras para usar, en cualquier caso.

9.8.4) Árbol de Merkle (Merkle root)

Un árbol Merkle, es una estructura de datos dividida en varias capas que tiene como finalidad relacionar cada nodo con una raíz única asociada a los mismos. Para lograr esto, cada nodo debe estar identificado con un identificador único (hash). Estos nodos iniciales, llamados nodos hijos (hojas), se asocian luego con un no superior llamado nodo padre (rama). El nodo padre, tendrá un identificador único resultado del hash de sus nodos hijos. Esta estructura es repetida hasta llegar al nodo raíz o raíz Merkle (Merkle root), cuya impronta está asociada a todos los nodos del árbol.

Gracias a esta estructura única, los árboles Merkle permiten relacionar una gran cantidad de datos en único punto (Merkle root). De esta forma, la verificación y validación de esos datos, puede pasar a ser muy eficiente, al tener que solo verificar el Merkle root en lugar de toda la estructura.

Este diseño fue creado por Ralph Merkle²¹, en el año 1979, con el fin de agilizar el proceso de verificación de grandes cantidades de datos.

¿Cómo funciona un árbol Merkle?

Un árbol Merkle es una estructura que relaciona todas las transacciones y las agrupa entre pares para obtener un Root Hash o “dirección raíz”. Este Root Hash, está relacionado con todos los hashes del árbol. Verificar todas las transacciones de una red sería algo extremadamente lento e ineficiente. Por esta razón, se implementó este sistema. Ya que, si un hash es cambiado, cambiarían todos los demás hasta llegar a la raíz (root hash). Esto

²¹ Ralph C. Merkle es uno de los inventores de la criptografía de clave pública, el inventor de hash criptográfica, y más recientemente, un investigador y conferencista en la nanotecnología molecular y la criónica. Merkle aparece en la novela de ciencia ficción La era del diamante, que implica la nanotecnología

invalidará la autenticidad de la información de todo el árbol. Es precisamente esta función, la que permite a los árboles Merkels otorgar el alto nivel de seguridad que los caracteriza.

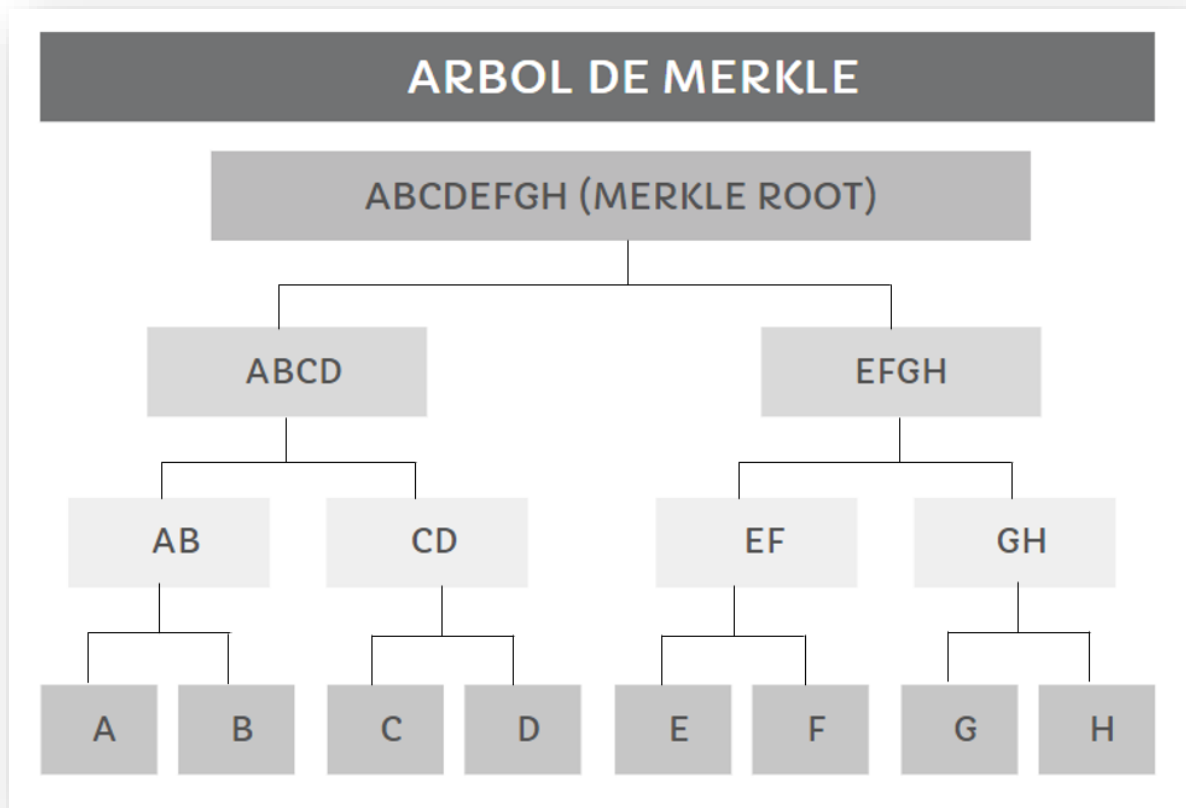


Figura 10 - Árbol de Merkle

Características de los árboles Merkle

Algunas de las características más destacables de los árboles Merkle son:

- Medio eficiente para generar una estructura distribuida de datos.
- Proveen una gran seguridad y resistencia a alteraciones de datos.
- Permiten un alto nivel de rendimiento en transmisión de datos en redes distribuidas. Gracias a esto, disminuyen la cantidad de datos necesarios para su correcto funcionamiento.
- Son computacionalmente poco costosos y eficientes a la hora de crear, procesar y verificar información.

- Permiten “disección” para hacer búsquedas de verificación más rápidas. Todo ello, sin comprometer la seguridad y trazabilidad de las transacciones que se realicen.
- Gracias a la característica de “disección” también son capaces de permitir ahorrar recursos de almacenamiento.
- Ofrecen una gran adaptabilidad a distintos problemas informáticos. Gracias a esto, los árboles Merkle han sido ampliamente utilizados en distintos sistemas. Por ejemplo, software de base de datos, sistemas de archivos, estructuras de llaves públicas, sistemas de versionamiento, redes distribuidas (P2P), entre otros.

El uso de los árboles Merkle en la tecnología blockchain es vital. Gracias a su uso, el software cliente puede descargar todo el historial de la red y verificarlo en caliente. De hecho, su uso facilita el proceso al permitir “podar” (tomar solo una parte del historial) el historial y reducir el tamaño de la descarga.

Por ejemplo, un usuario que desea instalar un cliente Bitcoin no tiene por qué descargarse todo el historial de la blockchain. En su lugar, puede reducir su descarga a solo unos cientos o miles de bloques atrás. De esta forma, tiene acceso a una versión más ligera del historial que se ajusta más a sus requerimientos.

Al contrario de lo que puedan pensar, esto no resta seguridad al cliente. Pues gracias al árbol Merkle, es posible bajar un “root hash” específico y desde allí comenzar a crear un historial. Como ese “root hash” está relacionado con los bloques anteriores a él, lo único que debe hacerse es verificarlo. Para ello, puede acudir a una serie de nodos completos de Bitcoin (con todo el historial) y verificar que el “root hash” tomado coincida. Teniendo absoluto consenso en este punto, se da el “root hash” como válido. Y desde ese punto, el usuario puede usar perfectamente su nuevo nodo cliente Bitcoin.

9.8.5) Tolerancia a Fallas Bizantinas (BFT)

¿Qué es el "problema de los generales bizantinos" y por qué explica el origen del bitcoin?

Los generales de un ejército bizantino rodean una ciudad enemiga. Se posicionan con sus respectivas tropas en los alrededores, a cierta distancia entre sí, y no se deciden entre ordenar un ataque o una replegada.

Es necesario, pues, que acuerden un plan de guerra.

Los altos cargos militares sospechan que entre ellos hay al menos un traidor, lo que hace difícil tomar la decisión en conjunto.

Si van a atacar, deben hacerlo todos y bien coordinados, pues de lo contrario es muy probable que pierdan la batalla.

Un general podría enviar un mensaje a los demás anunciando que va a atacar, cuando en realidad pretende ordenar el repliegue y hacer que el resto falle.

Pero ¿cómo ponerse de acuerdo?

Gráficamente explicado:

Supongamos que el comandante es un traidor. Si el comandante envía una orden distinta a cada teniente entonces habrá un teniente que no sepa qué acción realizar:

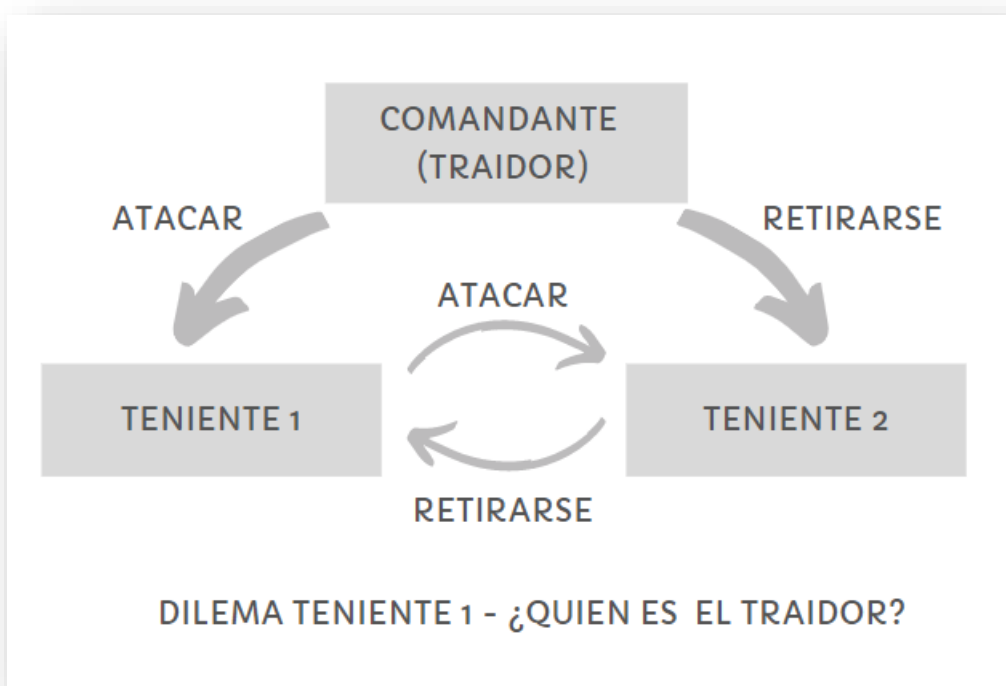


Figura 11 - Tolerancia a Fallas Bizantinas - Dilema 1

Supongamos que un teniente es el traidor. Entonces este retransmite al otro teniente información distinta a la que recibió del comandante. Por tanto el otro teniente no sabrá qué acción realizar:

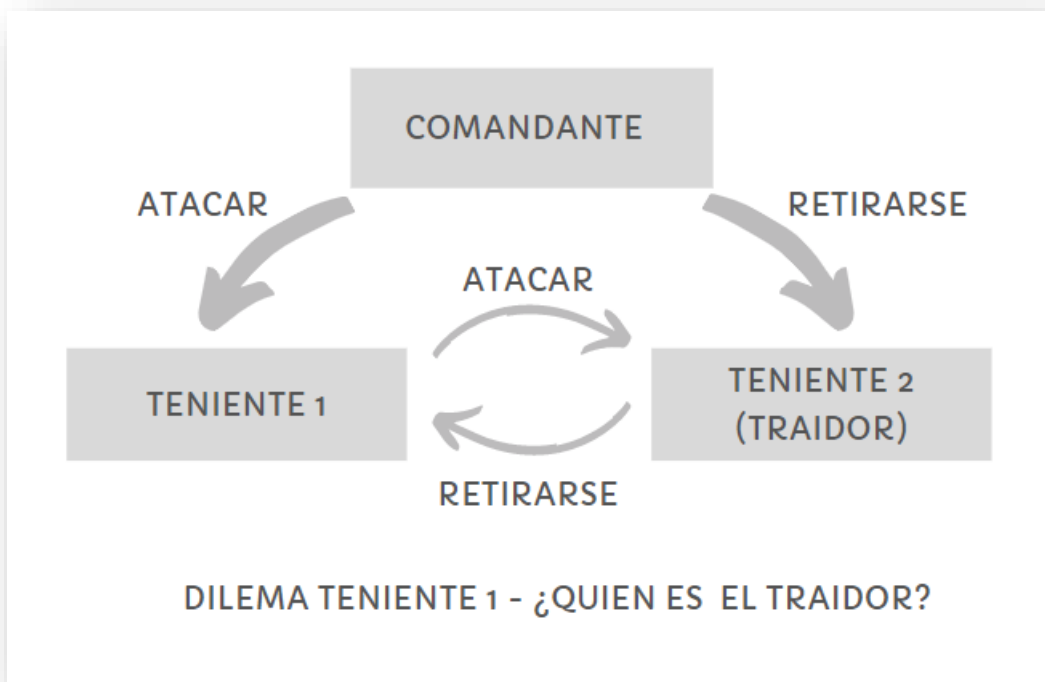


Figura 12 - Tolerancia a Fallas Bizantinas - Dilema 2

Veamos el esquema si el comandante es leal y un teniente es traidor:

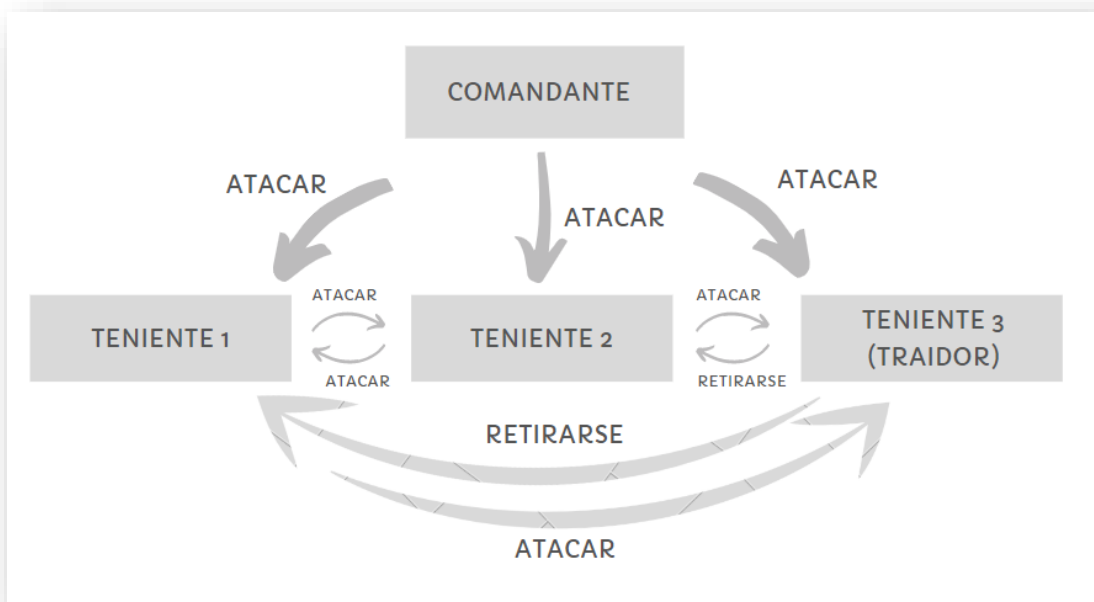


Figura 13 - Tolerancia a Fallas Bizantinas - Dilema 3

Veamos el esquema si el comandante es traidor y los tenientes leales:

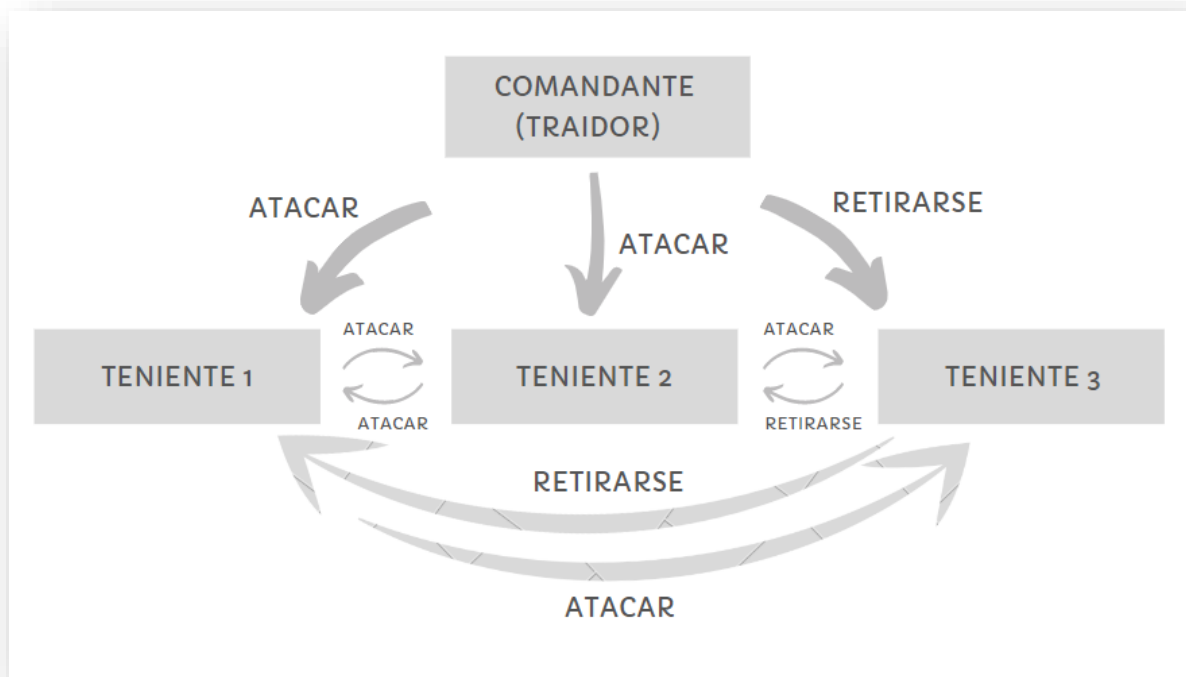


Figura 14 - Tolerancia a Fallas Bizantinas - Dilema 4

Problema de lealtad

Este planteamiento fue hecho por Robert Shostak²² y desarrollado con Leslie Lamport²³ y Marshall Pease en 1982 en el centro de investigación científica y tecnológica SRI International.

²² Robert Shostak es un informático estadounidense y empresario de Silicon Valley, más conocido académicamente por su trabajo seminal en la rama de la computación distribuida conocida como Tolerancia a fallos bizantinos.

²³ Leslie Lamport es un matemático y científico de la computación estadounidense, especialmente conocido por sus trabajos en sistemas distribuidos y por ser el desarrollador inicial del sistema de formateo de textos LaTeX, y de BibTeX.

Lo llamaron el "problema de los generales bizantinos" y lo que querían era solucionarlo para luego aplicar el proceso a sistemas informáticos conformados por varias computadoras.

"Los sistemas informáticos confiables deben manejar componentes que funcionan mal y que brindan información conflictiva a diferentes partes del sistema", plantearon Shostak, Lamport y Pease.

"El problema es encontrar un algoritmo que garantice que los generales leales lleguen a un acuerdo. Se muestra que, usando solo mensajes orales, este problema es solucionable si y solo si más de dos tercios de los generales son leales. Un solo traidor puede confundir a dos generales leales", explican en su estudio.

Para resolverlo, ofrecieron una serie de ecuaciones y algoritmos que llevan a la solución a través de un sistema de mensajes "inviolables".

¿Qué uso práctico tiene?

El "problema de los generales bizantinos" y su solución han sido aplicados desde la década de 1980 en diversos ámbitos, desde los sistemas informáticos a la industria aeroespacial y a la nuclear. Pero más recientemente se ha usado en el desarrollo de las criptomonedas.

"Este problema fue planteado para explicar una situación en la que los involucrados deben consensuar una estrategia para evitar el caos del sistema", explica Eloisa Cadenas²⁴, una especialista en el tema.

"Cuando hay un miembro malicioso, el consenso es la clave"

Si tenemos una molestia en los ojos, ejemplifica Cadenas, y el oftalmólogo asegura que están bien; pero el neurólogo dice que no lo están, se presenta un conflicto que hace que la búsqueda de una solución se convierta en un problema.

Lo mismo ocurre con los sistemas computacionales.

"Cuando tenemos un sistema informático distribuido -que tiene muchos nodos o computadoras- puede haber una condición en la que no se sepa que un componente que falló realmente lo hizo"

²⁴ Eloisa Cadenas: Doctora en Ingeniería en la UNAM, realizando investigación sobre valuación de empresas que aceptan criptoactivos como forma de pago| Consultora de Crypto & Blockchain. Profesora de la Bolsa Mexicana de Valores| Miembro de la Comisión de Fintech Colegio de Contadores Públicos de México.

"Podrían estar presentando síntomas; pero que algunos sistemas lo detecten como bueno y otros como malo", añade.

A ese problema se enfrentaban los creadores del dinero digital o criptomonedas en las décadas de 1990 y 2000, quienes buscaban eliminar de la ecuación de las transacciones personales a los poderosos bancos y a los gobiernos que dominan el sistema financiero mundial.

Satoshi Nakamoto es un nombre clave para resolver el reto.

En 2008 este supuesto individuo -nadie sabe quién es realmente, si una persona o un grupo de personas- publicó un estudio llamado "Bitcoin: un sistema de dinero electrónico punto a punto" que proveía una solución infalible al "problema de los Generales Bizantinos".

Creó el algoritmo de consenso, "el mecanismo a través del cual una red de blockchain va a poder tener lugar"

"Nakamoto supo cómo integrar cosas que no estaban resueltas, la prueba de trabajo, el sistema de consenso, muchas cosas que eran necesarias dentro de la tecnología".

Hoy esto es la base del bitcoin y los miles de criptomonedas similares que existen y que tienen "tolerancia a fallas bizantinas" (BFT, por sus siglas en inglés).

La solución Blockchain

Cada unidad de bitcoin u otra criptomoneda está asentada en el blockchain, una especie de libro de contabilidad que registra cada movimiento de la unidad.

El libro es distribuido a un número de computadoras (nodos) alrededor del mundo, que se actualizan instantáneamente con cada transacción, de manera que cada parte interesada en un bitcoin -un comprador y un vendedor- puede confiar en los movimientos de esa moneda.

Si cada general bizantino tuviera la tecnología de Blockchain, con una copia de los planes de cada uno de sus colegas, entonces habría prácticamente un margen nulo para las fallas BFT producto de una traición.

Eso pasa con el blockchain de bitcoin y otras criptomonedas.

"Cuando todos están de acuerdo que tienen el mismo resultado, entonces los nodos validan un bloque. Aunque alguien quisiera meter información equivocada -y aquí entra el problema

de los generales bizantinos- no lo va a poder lograr, porque ya todos están de acuerdo", explica Cadenas.

En el mundo del blockchain, aquellas personas que se ofrecen a dar mantenimiento a los libros de contabilidad de las criptomonedas reciben un pago por hacerlo con la misma criptomoneda. La labor es denominada "minar".

En la actualidad, la confianza en las criptomonedas está en uno de sus puntos más altos de la última década: un bitcoin vale un 17.000% más de lo que valía hace 10 años.

Y; aunque expertos advierten que es una "burbuja" financiera que en algún momento explotará, lo cierto es que su estructura basada en el blockchain y la respuesta al "problema de los generales bizantinos" lo ha hecho realidad.

(Brooks, 2019)

El término “falla bizantina”, se deriva del Problema de los Generales Bizantinos. Este problema lógico supone, en pocas palabras, que los actores deben acordar una estrategia concertada para evitar una falla catastrófica del sistema. Pero existe la posibilidad que dentro del sistema haya actores que pueden no ser confiables. Ante este hecho, el sistema debe crear mecanismos que garanticen que esos actores maliciosos no puedan conducir a la falla sin más remedio. La creación de esos mecanismos son los que precisamente otorgan la tolerancia a las fallas bizantinas.

Puede sonar algo sencillo; pero la realidad es muy distinta. Alcanzar la Tolerancia a Fallas Bizantinas, es uno de los desafíos más difíciles en informática. Hasta el punto, que el primer diseño en resolverlo de forma satisfactoria fue el Bitcoin, de Satoshi Nakamoto. Con ello marcó un hito, uno que ha acompañado a la tecnología blockchain hasta ahora.

La Tolerancia a Fallas Bizantinas funciona definiendo un conjunto de reglas que permite resolver el Problema de los Generales Bizantinos de forma satisfactoria. Alcanzar esto es complejo, pues estas clases de fallos no implican restricciones. Esta situación hace al problema más complejo y difícil de tratar. Sin embargo, en muchos sistemas informáticos esta tolerancia es un requisito. Por ello, para poder alcanzar este objetivo, un sistema tolerante a fallos bizantinos debe cumplir como mínimo lo siguiente:

- Se debe iniciar cada proceso con un estado no decidido (ni SI, ni NO). En este punto, la red propone una serie de valores determinísticos aplicables al proceso.

- Para compartir los valores, debe garantizarse un medio de comunicación. Esto con el fin de desplegar mensajes de forma segura. El medio, también servirá para comunicar e identificar las partes de forma inequívoca.
- Llegados a este punto, los nodos computan los valores y pasan a un estado decidido (SI o NO). Cada nodo debe generar su propio estado, el cual es parte de un proceso puramente determinístico.
- Una vez decididos, totalizan y gana el estado con mayor cantidad de decisiones a favor.

Estos cuatro puntos definen el funcionamiento básico de un algoritmo tolerante a fallos bizantinos.

Los protocolos de consenso en blockchain como PoW son tolerantes a fallos bizantinos. Estos permiten alcanzar a una red distribuida un consenso en condiciones bizantinas. Cuando Satoshi Nakamoto diseñó Bitcoin, tomó en cuenta este tipo de tolerancia. Para ello, creó una serie de reglas y aplicó el protocolo de consenso PoW para crear un software con tolerancia fallos bizantinos. Sin embargo, esta tolerancia no es del 100%.

Pese a ello, PoW ha demostrado ser una de las implementaciones más seguras y confiables para redes de blockchain. En ese sentido, el algoritmo de consenso de prueba de trabajo, diseñado por Satoshi Nakamoto, es considerado por muchos como una de las mejores soluciones para las fallas bizantinas. PoS y DPoS por su parte no son completamente tolerante a fallos bizantinos, razón por la cual suelen complementarse con otras medidas de seguridad.

9.8.6) Prueba de trabajo / Proof of Work (PoW)

El protocolo de Prueba de Trabajo, nos sirve para evitar ciertos comportamientos indeseados en una red. Su nombre proviene del inglés Proof of Work (PoW). Este protocolo funciona bajo el concepto de requerir un trabajo al cliente, que luego es verificado por la red. Normalmente el trabajo solicitado, consiste en realizar complejas operaciones de cómputo. Estas operaciones que luego son verificadas por la red. Una vez que son aprobadas, se da acceso al cliente para que use los recursos de la misma. Con ello se busca impedir que clientes maliciosos puedan consumir todos los recursos de forma incontrolada. Una situación que puede acabar por denegar el servicio prestado al resto de los clientes en la red.

Un ejemplo muy simple de entender es el famoso captcha²⁵ que es colocado cuando se quiere hacer un registro en una web. La web pone este reto que el visitante debe resolver. Si lo resuelve tendrá acceso al servicio. Esto evita que un atacante pueda crear millones de registros y así colapsar la página web. No obstante, el reto en una comunicación entre ordenadores no puede ser tan complejo. Debe ser solventable; aunque con una complejidad relativa.

La principal característica de esta estrategia es su asimetría. El trabajo por parte del cliente es moderadamente difícil de realizar; pero la verificación por parte de la red es sencilla. Esto quiere decir, que la prueba de trabajo lleva mucho tiempo en producirse y es computacionalmente costosa. Pero verificarla es sencillo, pues la prueba diseña patrones que facilitan la verificación.

Fue precisamente esta característica, la que llamó la atención de Satoshi Nakamoto a la hora de diseñar el Bitcoin. Es por ello que implementó el sistema HashCash (un sistema PoW) en su reconocida criptomoneda.

La Prueba de Trabajo, funciona de una forma bastante sencilla. De hecho, el proceso que es llevado a cabo, puede dividirse en las siguientes grandes etapas:

El cliente o nodo establece una conexión con la red. En este punto, la red le asigna una tarea computacionalmente costosa. Esta tarea debe ser resuelta a los fines de recibir un incentivo económico.

Comienza la resolución del acertijo. Esto conlleva el uso de mucha potencia de computación hasta resolver el enigma entregado. Este proceso es el que recibe el nombre de minería.

Una vez resuelta la tarea computacional, el cliente comparte esta con la red para su verificación. En este punto, se verifica rápidamente que la tarea cumpla con los requisitos exigidos. Si lo hace, brinda acceso a los recursos de la red. En caso contrario, se rechaza el acceso y la solución presentada del problema. Es en este punto, donde son realizadas las verificaciones de protección contra el doble gasto. Una protección que evita, que se presente más de una vez, una tarea ya asignada y verificada por la red.

²⁵ Recaptcha o reCAPTCHA es una extensión de la prueba Captcha utilizada para reconocer texto presente en imágenes. Emplea; por tanto la prueba desafío-respuesta utilizada en computación para determinar cuándo el usuario es o no humano para, a su vez, mejorar la digitalización de textos

Con la confirmación que la tarea ha sido cumplida, el cliente accede a los recursos de la red. Gracias a esto, recibe una ganancia por el trabajo computacional realizado.

Son estas cuatro etapas, las que permiten y modelan el funcionamiento de la Prueba de Trabajo. La facilidad de este modelo permite trasladar el mismo a distinto software para aprovechar su potencial. Pero es en las blockchains donde observamos una mayor utilidad, brindando unos niveles de seguridad excepcionales a pesar de la baja complejidad del protocolo. Y al mismo tiempo, permitiendo que millones de personas puedan participar de forma concurrente en la red.

Características del protocolo PoW

Es un protocolo muy seguro. La Prueba de Trabajo garantiza grandes niveles de seguridad, si la red está formada por miles de mineros. De hecho, mientras más mineros más segura es la red. Esto lo hace ideal para su uso en la formación de enormes redes distribuidas.

Es sencillo y muy fácil de implementar algorítmicamente. Una de las principales ventajas de PoW es que es muy sencillo de implementar. Esta facilidad es traducida en el fácil mantenimiento de los softwares que hacen uso del mismo. Además de permitir auditorías de forma mucho más sencilla con el fin de mantener la seguridad de la red.

Fácilmente adaptable a las necesidades de hardware, pudiéndose diseñar resistencia a determinados equipos (ASIC, GPU, FPGA, CPU). Otra ventaja del protocolo es su adaptabilidad a la tecnología. Se puede hacer más fácil o difícil, con el fin de adaptarlo a los avances tecnológicos. Permitiendo que la evolución del hardware no deje atrás la dificultad de minado. Que por ende termina centralizando el poder minero en quienes tienen hardware más nuevo y poderoso.

Excelente capacidad de resistencia a ataques de Denegación de Servicios. La principal razón de la creación de los protocolos PoW fue; evitar la denegación de servicios. Una tarea que cumplen a la perfección y que han mejorado mucho los actuales esquemas del protocolo.

El sistema consume una gran cantidad de energía eléctrica. El intensivo trabajo computacional de PoW necesita grandes cantidades de energía eléctrica. Estimaciones ubican que el consumo asciende a los 24 Teravatios de energía al año y seguirá ascendiendo a medida que sea necesaria más potencia para realizar este intensivo trabajo.

9.8.7) IV. Prueba de participación / Proof of Stake (PoS)

La Prueba de Participación, es uno de los dos protocolos de consenso más utilizados en la tecnología blockchain. Su nombre en inglés es Proof of Stake. De allí derivan las siglas PoS, con las que son conocidas comúnmente. El objetivo de este algoritmo, al igual que en PoW, es crear consenso entre todas las partes que integran la red.

A los nodos que minan en PoS se les llama validadores. La decisión sobre qué nodo ha de validar un bloque se realiza de forma aleatoria; pero dando mayor probabilidad a quienes cumplan una serie de criterios. Entre estos criterios podemos mencionar la cantidad de moneda reservada y el tiempo de participación en la red; pero pueden definirse otros. Una vez establecidos, es iniciado el proceso de selección de nodos de forma aleatoria. Una vez terminado el proceso de selección, los nodos elegidos podrán validar transacciones o crear nuevos bloques.

Esto revela que Proof of Stake es un proceso completamente distinto al conocido protocolo de Prueba de Trabajo (PoW). Donde cada uno de sus nodos realizan un arduo trabajo de cómputo para resolver acertijos criptográficos. Lo que significa que PoW, a diferencia de PoS, necesita grandes cantidades de energía y equipo especializado para realizar sus operaciones. En PoS, por el contrario, esto no es necesario. En PoS el proceso es mucho más sencillo y energéticamente amigable. Son estas razones por la que muchos proyectos blockchain en la actualidad se interesan por este nuevo protocolo.

La primera moneda en usar este protocolo fue PeerCoin en el año 2012. Luego aparecieron otros proyectos como NXT y Bitshares que también usan dicho protocolo.

El protocolo de Proof of Stake fue creado por el reconocido desarrollador Sunny King, en el año 2011. En 2012 King presentó formalmente el whitepaper PPCoin, donde dejaba en claro cómo funcionaba el algoritmo PoS. El objetivo, era solucionar algunos problemas conocidos de protocolo PoW. Entre ellos se destacan los siguientes:

La falta de escalabilidad y velocidad. El proceso de minería agrega un alto nivel de latencia para poder aprobar transacciones y producir nuevos bloques. Sin embargo, PoS evita esta situación. En las blockchains que usan el protocolo PoS, las verificaciones son realizadas por nodos con una alta tenencia de monedas. De esta forma las verificaciones se hacen rápidamente impactando positivamente en la escalabilidad y velocidad de la red.

El alto consumo energético del proceso de minería. El proceso de minería en PoW requiere de alto poder de cómputo. Un poder que generalmente proviene de máquinas con un alto consumo de electricidad. Pero PoS cambia radicalmente esta visión. Cambia el proceso de minería por un proceso de participación. Una participación reflejada en la tenencia de monedas o tiempo dentro de la red

La descentralización de la red. Este es un problema que afecta fuertemente a las redes PoW en la actualidad. Un hecho que se hace cada vez más palpable, especialmente al ver a los grandes grupos mineros. Una situación que centraliza la red en manos de unos pocos. PoS busca solucionar esto, diversificando y democratizando el acceso a los participantes en las diferentes tareas de la red.

Restar interés financiero a los ataques de 51%. Los ataques de 51%, son uno de los temores concurrentes en las redes PoW. Basta con que un grupo minero malicioso tenga el 51% del poder de cómputo de la red para el desastre. Pues con esa capacidad, el grupo minero puede manipular la blockchain a su antojo. Pero en un sistema PoS, esto solo es posible si el atacante posee el 51% de todas las monedas. Si el atacante realiza un ataque de este tipo, el valor de la moneda tiende a caer. Lo que conlleva a pérdidas económicas muy grandes para el atacante. Esta situación sirve de disuasivo para evitar estos ataques, manteniendo al mismo tiempo la seguridad de la red.

El funcionamiento de protocolo de Prueba de Participación es bastante particular. Este sistema busca incentivar a los participantes para que posean en todo momento, una determinada cantidad de monedas. La posesión de monedas, les permite ser elegidos por el proceso de selección aleatoria que es realizado para designar tareas. Bajo este esquema, aquellos que tengan más reservas, tienen mayor peso en la red y mayores oportunidades de ser elegidos. Una vez elegidos pueden validar transacciones y crear nuevos bloques dentro de la red. Permitiéndoles recibir ganancias e incentivos por el trabajo realizado.

Ejemplo de protocolo PoS

Una forma más sencilla de explicar este proceso sería el siguiente ejemplo:

Imagine que usted forma parte de una red de 100 inversores. De esa red, un primer grupo compuesto de 50 inversores poseen 1,000 monedas cada uno. Otro grupo de 30 inversores, poseen 2,500 monedas cada uno. Y un último grupo de 20 inversores, poseen 10,000

monedas cada uno. En la siguiente tabla, puede ver los datos de cada uno de los grupos mencionados y su peso en la participación en la red.

GRUPO DE INVERSORES	INVERSORES	MONEDA DE RESERVA	TOTAL MONEDA DE RESERVA	% PARTICIPACIÓN
GRUPO A	50	1000	50000	15,38%
GRUPO B	30	2500	75000	23,08%
GRUPO C	20	10000	200000	61,54%
TOTAL	100	325000	3250000	100,00%

Figura 15 - Protocolo PoS

De este modo, puede evidenciarse claramente que el Grupo C, es quien tiene mayor participación en la red. Un total de 61,54 % y 200.000 monedas para ser exactos. Ahora bien, es hora de realizar el proceso de selección aleatoria en la red. Esto significa que quienes estén en el Grupo C, tienen mayor probabilidad de ser seleccionados. Pero no solo ellos son seleccionados. También participan miembros de los Grupos A y B. Esto es realizado con el fin de democratizar y descentralizar la red.

La mayor tenencia, no garantiza la selección como nodo; pero brinda mayores oportunidades. Con esto se busca que todos los que están dentro de la red puedan beneficiarse sin sufrir detrimentos. Adicionalmente, cualquiera de los inversores en los Grupos A y B, pueden invertir más para incrementar su nivel de participación. Una vez seleccionados, los inversores tienen la capacidad de realizar las tareas que se les permite. Los inversores realizan dichas tareas con el fin de recibir incentivos y ganancias proporcionales a su participación dentro del sistema. Terminada la ronda, reinicia el proceso de selección para que otros inversores puedan participar.

Además de esto, los fondos usados como tenencia no pueden utilizarse y deben ser bloqueados dentro de la blockchain. De esta forma se garantiza que los fondos siempre estarán disponibles como garantía del nodo validador. Sin embargo, el nodo puede agregar nuevos fondos en cualquier momento, con el fin de aumentar aún más su nivel de participación.

Características de PoS

El protocolo de Proof of Stake (PoS) cuenta con una gran variedad y potentes características, entre las que podemos mencionar:

Es una tecnología más respetuosa con el medio ambiente. Esto es gracias a que no necesita potentes máquinas para actividades de minería. Lo que significa que su consumo energético es reducido.

Permite una mejor alineación de objetivos e incentivos entre los integrantes de la red. De esta forma, cada uno de los que forman parte de la red buscan mantener a dicha red por un largo periodo de tiempo.

Mejora la descentralización y democratiza el acceso a la red. Esto gracias a que todos pueden participar en la red, siempre y cuando cumplan con su cuota de participación. En las redes PoS no aplican los conceptos de minería y los equipos que esta tarea conlleva. Lo que evita la concentración de poder en pocas manos debido a lo costosa que pueda ser su actividad.

La entrega de recompensas es más proporcional. Esto gracias al sistema de selección aleatoria dentro de la red, el cual tiene como finalidad asignar tareas a aquellos que tienen tenencia de monedas. Quienes tienen mayor posesión tienen mayor posibilidad de ser elegidos, hacer verificaciones y recibir ganancias con ello.

La seguridad de la red es mucho mayor. Esto gracias a que solventa o dificulta ciertos esquemas de ataques ya conocidos, como el ataque de 51%.

Ofrece una mayor escalabilidad. Esta es esgrimida como una de sus principales características. La velocidad y escalabilidad de las redes PoS supera por mucho a las redes PoW. Esto gracias a que no hace ningún trabajo computacional intensivo que consuma una gran cantidad de tiempo. Esto hace a PoS perfecto para blockchain que quieran usarse como sistemas de pagos al menudeo, donde se requiera verificar grandes cantidades de transacciones por segundo.

Existe el riesgo de perder los fondos por ataques maliciosos. Los sistemas PoS requieren que la cartera del usuario siempre esté abierta y conectada a Internet. Esto genera un problema de seguridad que puede permitir a los hackers aprovechar vulnerabilidades para robar fondos de dichas carteras. Una razón más para seguir criterios comunes de seguridad cuando se use este sistema.

9.8.8) IV. PoA (Proof of Authority – Prueba de Autoridad)

La Prueba de Autoridad, está diseñada para ser una solución práctica y eficiente, especialmente dirigida a blockchains privadas. El término PoA fue propuesto por Gavin Wood, cofundador y ex-CTO de Ethereum. Este protocolo de consenso, tiene una marcada diferencia a otros como PoW y PoS. Ello es debido, a que PoA se aprovecha de las identidades reales para permitir la validación dentro de una blockchain. Esto significa, que los validadores ponen su identidad real y reputación como garantía de transparencia. Un proceso que incluye, una selección arbitraria de dichos validadores confiables. Una situación totalmente distinta a la minería de PoW; pero con similitudes al esquema de participación PoS.

Además, PoA se basa en un número limitado de validadores. Esta característica le otorga una clara ventaja, la alta escalabilidad de la blockchain. Lo que tiene un impacto positivo en aplicaciones donde la velocidad es primordial. Además, mantiene un alto nivel de control de acceso a dicha blockchain, pues solo los nodos con permiso pueden participar.

El funcionamiento del protocolo PoA es bastante sencillo. En primer lugar, para que el sistema funcione debe elegirse de forma aleatoria los validadores. La inclusión y selección de nodos es realizada gracias, a un sistema de votación de otros nodos ya previamente autorizados. De esta forma, se evita que nodos maliciosos puedan ser incluidos y afectar el funcionamiento de la red. Sumado a esto, cada validador puede firmar como máximo uno de una serie de bloques consecutivos durante su turno de validación. Adicionalmente, PoA no requiere un esquema de minería como ocurre en Bitcoin, por lo que resulta muy eco-friendly. Al igual que en PoS, donde es utilizada la participación como medida de selección y confianza dentro de la red, PoA hace uso de la identidad y la reputación. La identidad de una persona o institución es escasa, y la reputación de la misma es muy valiosa. Su uso dentro del protocolo significa, que el validador debe revelar quien es de forma voluntaria. Al hacerse pública esta información, es fácil establecer responsabilidades en el funcionamiento de la blockchain. Cualquier acto que atente contra la fiabilidad y transparencia de la red, recaerá directamente sobre esa persona o institución. Algo que puede socavar o destruir su reputación en todas partes.

De esta forma, los validadores de una blockchain, haciendo uso del protocolo PoA cuidarán su reputación e identidad. Y es por esa razón, que velarán por el buen funcionamiento, la

transparencia y confiabilidad de la operación de la misma. En este sentido, la identidad puesta en juego puede servir como un gran ecualizador, entendida y valorada por todos los actores. Las personas o instituciones cuya identidad está en juego, se sentirán incentivadas para preservar la red.

Condiciones de funcionamiento de PoA

Las condiciones de funcionamiento de PoA, son los pasos necesarios para el cumplimiento del protocolo. Entre ellos, podemos destacar los siguientes:

Es necesario validar las identidades de los posibles validadores. Esto significa que quienes quieran participar en la red, deben verificar y hacer públicas sus identidades reales.

El candidato a validador debe estar dispuesto a invertir dinero y poner su reputación como garantía. Este proceso, garantiza que los candidatos tengan motivaciones de participación a largo plazo dentro de la red.

Se debe tener un sistema estándar para la aprobación de un validador. Con esto, se busca que el método de selección sea el apropiado para seleccionar por igual a los candidatos a validadores.

El sistema debe ser capaz de eliminar a posibles actores maliciosos. Si un validador dentro de la red actúa de forma nefasta, la red debe eliminarlo. Todo ello con el fin de mantener la confianza y la transparencia del resto de partes de la red.

Implementaciones del protocolo PoA

Como fue mencionado anteriormente, el consenso del PoA es utilizado en la red de pruebas Kovan y Rinkeby de Ethereum. Además, es utilizado por varias plataformas bastante conocidas y, a partir de este punto, parece ser el mecanismo de consenso más plausible para las instituciones que buscan implementar redes privadas de cadenas de bloques.

La más conocida de estas redes es POA Network. Una red pública para contratos inteligentes que funciona como una sidechain (cadena lateral) de Ethereum. En la misma todos sus nodos están formados por validadores independientes. Utilizan la base de datos de notarios públicos como mecanismo para la elegibilidad de los validadores. Esencialmente, los validadores pasan por una verificación formal de la identidad utilizando dos pasos. Un cliente que hace uso del software POA Network DApp, así como del sistema de notarios públicos.

Hyperledger y Ripple también hacen uso del protocolo PoA en sus blockchain. En el caso de Hyperledger Fabric está basado en la Tolerancia a Fallas Bizantinas; pero emplea el consenso del PoA como parte de su marco general de código abierto para las cadenas de bloques del consorcio. Ripple utiliza una forma iterativa de consenso del PoA.

Otra cadena que usa PoA es VeChain. Esta es una blockchain pública de nivel empresarial especializada en el manejo transparente de información empresarial. Enfocada sobre todo en el manejo de la cadena de suministro y logística.

9.9) TIPOS DE BLOCKCHAIN

9.9.1) Blockchain Públicas

Las redes de blockchain públicas son aquellas a las que cualquier persona tiene acceso. En general estas redes son transparentes y los usuarios son anónimos. Ningún participante tiene más derechos que los demás, por lo cual no hay administradores de la red. Las redes públicas más conocidas son Bitcoin, Bitcoin Cash, Ethereum y Litecoin, que tiene además una criptomoneda asociada.

El procedimiento para participar es descargarse la aplicación correspondiente y conectarse de forma automática con un determinado número de participantes o nodos, a los que se les solicita la versión más actualizada de la cadena de registros, lo que puede tomar minutos u horas. Una vez que el usuario hace con la copia actualizada de toda la cadena, tiene los mismos derechos y deberes que el resto de los participantes a la hora de proponer y validar transacciones.

La forma de validar las transacciones es mediante lo que es conocido como protocolos de consenso. De forma aleatoria es elegido un participante cada vez para proponer un nuevo bloque. Si el elegido propusiese un bloque con información errónea, el resto de los participantes podrían rechazarlo. Para incentivar a los nodos para que propongan bloques válidos, muchas redes dan recompensa en forma de criptomoneda al nodo que propone un bloque cuando este es aceptado. Los nodos que compiten por validar los bloques, encontrando el hash válido del bloque, son conocido como mineros. La labor del minado en las redes públicas es el corazón que las mantiene vivas. Es la responsabilidad de los usuarios o nodos mineros seguir realizándolo.

9.9.2) Blockchain Federadas

Las redes de blockchain federadas son las más solicitadas a la hora de construir soluciones compartidas para gobiernos, empresas, y asociaciones. En general no son abiertas a la participación del público, sino que un número determinado de organizaciones, entidades o compañías se encargan de administrar la red en conjunto y mantener copias sincronizadas del registro. El acceso mayoritario es mediante una interfaz web que los administradores ponen a disposición del usuario medio, en lugar de compartirles una copia de la cadena como en las redes públicas.

Una red de blockchain federada puede ser, por ejemplo, una buena opción para industrias como salud y finanzas, donde tienen lugar grandes volúmenes de transacciones entre distintas entidades con una alta necesidad de confianza. A la hora de diseñar e implementar una solución de este tipo, es fundamental acompañar a la herramienta blockchain con un plan estratégico adecuado consistente en definir desde quiénes y cómo van a administrar la red hasta qué información se les va a mostrar a los usuarios vía interfaz web. En muchos casos el usuario que accede vía web puede no tener interés ni conocimiento sobre blockchain; pero sí necesitar una plataforma que involucre entidades diferentes, necesidad de confianza y transparencia. Es importante señalar que al ser su acceso vía web y no como “nodos” de la red; es decir, que no tienen una copia de la cadena-, los usuarios comunes tendrán acceso a tanta información como los administradores decidan mostrarles a través de la misma. Se tendrán entonces opciones que varíen desde un gran nivel de transparencia hasta una transparencia nula.

Al contrario de las redes públicas, las redes federadas no recompensan al usuario para la creación del hash a través del minado de bloques y ni siquiera tienen una criptomoneda asociada. Los propios administradores o entidades a cargo de la red proporcionan los recursos computacionales necesarios que cumplan con el propósito de generar el hash.

Aunque las redes de blockchain federadas no tienen un modelo de participación abierto al público, el software que las respalda sigue siendo en general de código abierto, lo que permite a la comunidad desarrolladora reutilizar código en muchos casos. Algunos de los softwares más comunes de código abierto utilizados para crear redes federadas son Hyperledger, Corda, EFW o Multichain, que permiten descargar la aplicación de blockchain y programar la cadena a tu gusto, decidiendo quién quieres que participe y bajo qué reglas son reguladas las

transacciones. También es posible y común crear entornos federados haciendo un fork de una red pública, generando así tu propia red customizada.

9.9.3) Blockchain Privadas

Las redes de blockchain privadas son aquellas donde el control está reducido a una única entidad que es encargada de mantener la cadena, dar permisos a los usuarios que se desea que participen, proponer transacciones y aceptar los bloques. Son iguales que las federadas; pero con solo una entidad a cargo.

En estas redes no hay ningún tipo de descentralización ni de consenso puesto que toda la información es controlada por una única entidad que administra la red. La mayor parte de la comunidad no considera a estas redes como verdaderos blockchain, ya que no cumple con prácticamente ninguno de los propósitos para los que idealmente es utilizada esta tecnología. Los mismos softwares que son utilizados para blockchain federadas son también empleados para blockchain privadas.

(López, 2018)

9.10) CONTRATOS INTELIGENTES (Smart Contracts)

Un contrato inteligente (Smart Contract en Ingles), es un programa informático que ejecuta acuerdos establecidos entre dos o más partes haciendo que ciertas acciones sucedan como resultado que puedan cumplirse una serie de condiciones específicas.

Es decir, cuando se da una condición programada con anterioridad, el contrato inteligente ejecuta automáticamente la cláusula correspondiente.

Como puede observarse en la historia de Blockchain, Nick Szabo ya pensaba en este tipo de contrato en 1993; pero no existía en ese momento la tecnología apropiada para soportar esta idea, este sistema de pagos no apareció hasta la creación de Bitcoin en el año 2009

No obstante, Bitcoin no estaba pensado para nada más que ser una herramienta financiera: una criptomoneda.

Por el contrario, la tecnología con la que funcionaba – el blockchain o cadena de bloques-, sí que hacía posible estos contratos inteligentes y fue a principios de 2014, con la creación de Ethereum, cuando, por fin, pasaron a ser una realidad. (Swan, 2015)

Estos smart contracts transcurren en una atmósfera no controlada por ninguna de las partes implicadas en el contrato, en un sistema descentralizado.

Esto significa que

- Se programan las condiciones, las cuales tienen que estar perfectamente definidas y detalladas debido a que no hay posibilidad posterior de realizar un ajuste en este tipo de contrato
- Se firma por las partes implicadas
- Se carga en Blockchain para que no pueda modificarse.

Y, por otra parte, tienen como objetivo principal:

- Implementar un estado de seguridad mayor al del contrato tradicional, en este tipo de contratos el lenguaje no es natural, sino virtual a través de un lenguaje de programación. Esta rigidez quita la subjetividad de los contratos como los conocíamos.
- Reducir costos. En este tipo de contrato, la falta de necesidad de un intermediario de confianza (escribano), reduce los costos por los honorarios que no se contemplan.
- Reducir el tiempo asociado a este tipo de interacciones, la ejecución es automática cuando se cumplen las condiciones, sin posibilidad de interpelación o interpretación que demore la ejecución del contrato.

Un ejemplo simple de funcionamiento de Smart Contract es el que es producido con cualquier máquina expendedora, la máquina está programada para que cuando el usuario deposite determinada cantidad de dinero y ejecute determinada combinación de teclas, el producto sea entregado, además de devolver el cambio si hiciera falta y de informar si el producto no está disponible. Esta secuencia no es más que sentencias IF y THEN en programación. Este ejemplo simple de la expendedora puede ser aún más eficiente si además la señal de producto agotado llegará al proveedor que tiene que abastecerla, o más aún, que esta señal llegue en el punto de reabastecimiento calculado para cada tipo de producto.

Actualmente existen muchas aplicaciones que utilizan Smart Contracts y otras tantas que están en desarrollo. (*Bashir, 2018*)

Servicios Financieros

Préstamos: si la persona que contrata el préstamo no realiza el pago en el tiempo estipulado, se ejecutaría el contrato para retirarle las garantías.

Liquidación de operaciones: los contratos calculan importes de liquidación y transfiere fondos automáticamente.

Pagos de cupones y bonos: los contratos calculan y pagan automáticamente de forma periódica los cupones y devuelve el capital al vencimiento de los bonos.

Microseguros: Calculan y transfieren micropagos basados en datos de uso de un dispositivo conectado a Internet (por ejemplo, un seguro automotor de pago por uso)

Depósito en garantía en el registro de la propiedad: el contrato supervisa la información externa a la cadena de bloques y una vez transferida la propiedad de un vendedor a un comprador, el contrato ingresa automáticamente los fondos al vendedor.

Herencias: una vez que el contrato puede verificar el fallecimiento de la persona, automáticamente las propiedades quedan repartidas y asignadas entre los herederos.

Automatización de pagos y donaciones: Pueden acordarse pagos o donaciones periódicas o puntuales a personas o entidades. El contrato inteligente verificaría que se cumplen las reglas para realizar automáticamente la donación.

Servicios de la salud

Expedientes médicos electrónicos: los contratos proporcionan transferencias y accesos a los historiales médicos tras la aprobación de múltiples firmas entre pacientes y proveedores.

Acceso a los datos sanitarios de la población: se conceden a las organizaciones de investigaciones sanitarias el acceso a determinada información sanitaria personal. A cambio, a través de los contratos, se realizan micropagos automáticamente al paciente para su participación.

Seguimiento de la salud personal: se realiza un seguimiento de las acciones relacionadas con la salud de los pacientes a través de dispositivos IoT -Internet of Things- (conectados a Internet). Los contratos generan automáticamente recompensas basadas en hechos específicos.

Servicios de propiedad intelectual

Distribución de royalties: el smart contract calcula y distribuye los pagos de royalties a artistas y otras partes asociadas según los términos acordados.

Servicios energéticos

Estaciones autónomas de recarga para vehículos eléctricos: el contrato procesa un depósito, habilita la estación de recarga y devuelve los fondos restantes una vez completados.

Servicios del sector público

Votación: valida los criterios del votante, registra el voto en la cadena de bloques e inicia acciones específicas como resultado del voto mayoritario. Esto es posible en una votación tanto en el ámbito de encuesta como a nivel estatal.

Apuestas: dos o más partes pueden apostar sin que se resienta su seguridad y sin necesidad de un tercero a través de un contrato inteligente que asegure unas condiciones concretas.

Propiedades inteligentes: una casa, un coche, una heladera, un lavarropas... todos los objetos que puedan conectarse a Internet son consideradas propiedades inteligentes (del inglés, smart property). Y todos pueden ser gestionados con contratos inteligentes para poder venderlos o alquilarlos de forma automatizada.

9.10.1) Ether

Ethereum pretende funcionar como una especie de Internet descentralizado y una plataforma para soportar contratos inteligentes y aplicaciones llamadas Dapps.

Pero; aunque nadie controle Ethereum, el sistema no es gratuito. Este necesita 'Ether', un token que puede utilizarse para pagar los recursos computacionales necesarios para ejecutar aplicaciones o programas.

Al igual que Bitcoin, el Ether es un activo digital (y para simplificarlo lo solemos llamar criptomoneda). Y al igual que cuando utilizamos dinero en efectivo, no requiere que un tercero procese o apruebe una transacción.

Para publicar, eliminar o modificar algo en la red Ethereum, debemos pagar una tarifa de transacción en Ether (sus siglas son ETH) para que la red procese ese cambio.

La red Ethereum, además, está formada por todos y cada uno de los ordenadores que trabajan verificando operaciones en la Blockchain, también llamados mineros. Estos mineros reciben Ether como recompensa por ejecutar las operaciones de la plataforma.

Los desarrolladores de Dapps (aplicaciones descentralizadas) también forman parte de Ethereum, pues su trabajo de desarrollo es lo que luego dará como resultado mejores aplicaciones.

Estos, al igual que los mineros, reciben Ether por su trabajo. Podríamos decir que el Ether es el incentivo para garantizar que los desarrolladores escriban aplicaciones de calidad y que la red pueda mantenga estable.

9.10.2) Las medidas de Ether

Al igual que con el resto de las monedas fiduciarias que tienen submedidas de sus monedas (centavos, céntimos, etc.). Ether tiene sus propias medidas a saber:

Wei

Lovelace (1000 wei),

Babbage (1000 lovelace)

Shannon (1000 babbage)

Szabo (1000 shannon)

Finney (1000 szabo)

Ether (1000 finney)

Estas están ordenadas de orden ascendente de la más pequeña a la principal. Existen medidas por encima del valor del Ether, estas están detalladas en el siguiente cuadro:

Guía de medidas del Ether				
	wei		0,000000000000000001	10^{-18}
kwei	lovelace	femtoether	0,000000000000001	10^{-15}
mwei	babbage	picoether	0,000000000001	10^{-12}
gwei	shannon	nanoether	0,000000001	10^{-9}
	szabo	microether	0,000001	10^{-6}
	finney	miliether	0,001	10^{-3}
	ETHER		1	1
	kether		1.000	10^3
	mether		1.000.000	10^6
	gether		1.000.000.000	10^9
	tether		1.000.000.000.000	10^{12}

Figura 16 - Medidas del Ether

9.10.3) Como se generan los Ether

Según la web oficial de Ethereum, la oferta total de Ether y su tasa de emisión fue decidida por las donaciones reunidas en la ICO de 2014.

Los resultados aproximados fueron:

- 60 millones de Ether creados a los contribuyentes de la preventa
- 12 millones de Ether (20% de los anteriores) para el fondo de desarrollo, la mayor parte de los cuales son destinados a contribuyentes y desarrolladores iniciales y el resto a la Fundación Ethereum.
- 5 Ether son creados en cada bloque (aproximadamente 15-17 segundos) al minero del bloque
- 2-3 Ether a veces se envían a otro minero si ellos también pudieron encontrar una solución; pero su bloque no fue incluido (llamado recompensa de tío/tía).

La oferta de Ether no es infinita, sino que su emisión está limitada a 18 millones de Ether por año (25% del suministro inicial), según los términos acordados al inicio.

Esto significa que; aunque la emisión absoluta es fija, la inflación relativa disminuye cada año.

No obstante, en algún Ethereum pasará del sistema Prueba de Trabajo (PoW) a un nuevo algoritmo de consenso en desarrollo, llamado Casper²⁶, que se espera sea más eficiente y requiera menos subsidios mineros.

El método exacto de emisión y la función a la que servirá es un área de investigación activa; pero lo que puede garantizarse ahora es que:

El máximo actual es considerado un techo y la nueva emisión bajo Casper no lo superará (y se espera que sea mucho menor).

Cualquier método que sea escogido finalmente para emitir, será un contrato inteligente descentralizado que no dará un trato preferencial a ningún grupo particular de personas y cuyo propósito sea beneficiar la salud y seguridad general de la red.

9.10.4) GAS en Ethereum

La ejecución Smart Contracts se realiza mediante Ethereum Virtual Machine (EVM), esta es una red distribuida de Ethereum donde cada computadora conectada recibe el nombre de nodo. Estos nodos son los que cumplen la función de los mineros en Bitcoin; pero solo es aplicable a Ethereum y como en el caso de la criptomoneda, es necesario que los que prestan servicio de cómputo y consumo eléctrico, reciban su recompensa. Debido a que el ecosistema es diferente al de Bitcoin, se determinó al gasto temporal, computacional y de tiempo con el concepto de GAS.

Con esta unidad de medida se puede establecer el costo que tendrá la ejecución de un Smart Contract o el desarrollo de una aplicación descentralizada. El gasto será directamente proporcional a la complejidad que se requiera. En definitiva, el GAS cumple dos funciones principalmente, mantener un equilibrio en la plataforma y recompensar a los “mineros”.

A diferencia del Bitcoin, el Gas no es una criptomoneda o moneda electrónica, no sirve como unidad de intercambio. Entonces, el Gas solo es una unidad de medida, no se almacena en billeteras electrónicas ni tiene un valor por sí mismo, para valorizar esta unidad de medida se calcula al precio denominado “Gas Price”. Esta valorización la desarrollaremos después de explicar otros conceptos asociados a como son ejecutados los Smart Contracts; pero para tener una idea básica sobre cómo funciona podemos decir que una transacción simple en

²⁶ Casper: El protocolo Casper se convertiría en un paso intermedio en la transición del PoW al PoS, combinando las posibilidades de ambos principios:

Ether tiene un valor de 21000 unidades de Gas, Si ese Gas tiene un precio de 0.0005 Ether por cada 100 unidades, el coste de esa transacción será de $(21.000 / 100) \times 0,0005 = 0,105$ Ether. Lo que cobraría el minero no sería 21.000 Gas, sino que sería 0,105 Ether por procesar esa transferencia. El valor de Ether que fue dado en el ejemplo es un valor aleatorio simple para utilizarlo a modo de ejemplo.

Debido a la volatilidad que tienen todas las criptomonedas, se utiliza Gas y no Ether para establecer el costo estándar de una transacción.

9.10.5) Límite de Gas

Este dato indica el valor máximo de Gas que una transacción puede llegar a consumir para ser válida.

Normalmente, el software que suele utilizarse para realizar transacciones en la red Ethereum calcula de forma automática una estimación de la cantidad de Gas necesaria para llevar a cabo dicha transacción y nos lo muestra inmediatamente.

9.10.6) Gas utilizado por transacción

Este dato, también conocido a secas como ‘Gas used’, indica el Gas que ha necesitado la transacción para que se llevase a cabo. En otras palabras, el gasto computacional o el trabajo de los mineros que ha sido necesario para procesar la transacción.

Lo que resulta imposible es que el Gas usado sea mayor que el límite de Gas, ya que, como su propio nombre indica, el límite no puede superarse.

Sin embargo, si el gasto computacional ha sido mayor que el límite de Gas que se ha seleccionado para la transacción, esta aparecerá como fallida.

En ese caso, no se perderá el valor que queríamos enviar mediante esa transacción; pero si deberá pagar por el total del Gas usado por la misma.

Explicado con números, si queríamos enviar 5 Ether y la transacción es fallida porque el Gas usado es mayor que el límite de Gas, esos 5 Ether quedarán en nuestro wallet de Ethereum; pero deberemos pagar lo correspondiente a esas 21.000 unidades de Gas que costó la transacción.

9.10.7) Precio del Gas

El valor 'Gas price' señala el precio de cada unidad de Gas. Este es variable y son los mineros los que acuerdan subir su precio o bajarlo. Para ver cuál es el precio actual del Gas recomendamos visitar la web ETH Gas Station que tiene como objetivo aumentar la transparencia de los precios y de los tiempos de confirmación de las transacciones en la red Ethereum.

Este precio viene dado en GigaWei (Gwei), una submedida del Ether. Al cambio, 1 Gwei equivale a 0,000000001 Ether.

También debemos mencionar que; aunque el precio del Gas es el que es, nosotros podemos determinar tanto su precio como el límite de Gas que queremos pagar a la hora de realizar una transacción en Ethereum.

Cuando realizamos una transacción, nosotros podemos pagar más Gas del establecido para que la transacción pueda llevarse a cabo más rápido.

9.10.8) Coste actual de la Transacción – Comisión

Este dato nos da la comisión total que es cobrado por una transacción concreta. Depende directamente de las variables 'Gas used' y 'Gas price'.

Para explicarlo de una forma más clara y sencilla podríamos poner estas dos variables de forma que el precio del Gas sería similar al precio por hora trabajada de un minero, y el Gas usado sería las horas trabajadas por ese minero.

En este caso, para sacar el salario del minero deberíamos multiplicar el número de horas por el precio por hora.

La fórmula llevada al entorno Ethereum sería: Coste Actual de la Transacción – Comisión = Gas usado * precio del Gas

Si el Gas es sobreestimado, será reembolsado en nuestra cuenta cualquier cantidad adicional, por pequeña que sea.

9.10.9) Gas usado acumulado

Aunque este dato no sea muy relevante, nos permite hacernos una idea general. Este Gas usado acumulado refiere al total de Gas usado por todas las transacciones que están añadidas a ese bloque.

10) APLICACIONES ACTUALES Y EN DESARROLLO

Existen actualmente muchísimas aplicaciones funcionando y otras tantas en pruebas, las aplicaciones que lograron mayor madurez son las dedicadas a las finanzas o donde la desintermediación no genera la necesidad de modificaciones regulatorias.

Debido a que el presente trabajo es sobre Logística, haré hincapié en los proyectos más importantes en gestión; pero previamente realizaré una breve enumeración de otros proyectos para evidenciar la importancia que podría tener esta tecnología:

Transferencias de dinero Internacionales: Empresas dedicadas a este rubro serían las primeras en verse impactadas, con un simple smart contract una persona podría transferirle dinero a otra con un mínimo de costo y de manera instantánea. Las transferencias bancarias sin dudas se verán amenazadas, actualmente son muy costosas y demoran mucho tiempo en concretarse.

Industria de seguros: La industria de los seguros podría rehacer gran parte de su operativa gracias al blockchain y a la posibilidad de trabajar con los Smart Contract o contratos inteligentes, esto es explicado de forma sencilla, un contrato con capacidad de autoejecutarse sin intermediarios. Gracias a los Smart Contract, las aseguradoras podrían trabajar, digámoslo así, “de oficio”, ante cualquier incidente. Por ejemplo, si un pasajero tiene un billete de avión con seguro de reembolso y finalmente no embarca en su vuelo, recibirá directamente la cantidad acordada en el contrato con su aseguradora porque existe un contrato inteligente. Este sistema reduce costos, acelera el procedimiento y genera una experiencia de usuario totalmente satisfactoria.

Otro ejemplo podemos verlo en los seguros de coches. Imaginemos que un conductor quiere asegurar su vehículo y, gracias al blockchain, pudiera transmitir de forma anónima su historial de siniestros. Incluso, si su coche estuviera conectado, (damos paso aquí al Internet de las cosas), podría enviar un informe sobre sus hábitos de conducción. Una vez analizada esta información, la aseguradora podría mandarle un Smart Contract adaptado a su perfil, y con un coste y coberturas completamente personalizados. El conductor demostraría ser el

propietario, ingresaría el dinero y recibiría el certificado. Todo, gracias a la red de verificación, codificación, seguridad y transparencia que ofrece blockchain.

Esta misma idea puede ser aplicada a sectores como el de las operadoras de teléfono, alquiler de coches y muchos otros servicios.

Industria Energética: Blockchain podría hacer posible la compraventa de energía punto a punto, al menos ya conocemos algunas iniciativas en los Países Bajos o en el Reino Unido. Las Virtual Power Plant (*Najafi, 2017*), un sistema de generación de energía distribuida en la que los consumidores se convierten en productores de esa energía, sería uno de los grandes beneficiados. En el Reino Unido la empresa Electron (<https://www.electronjs.org/>), tiene como objetivo, precisamente, desarrollar la industria de renovables con el blockchain para hacerla más eficiente y flexible.

ONG's: una nueva forma de donaciones más segura y transparente. Los donantes podrían rastrear sus aportaciones e informarse sobre cómo están utilizándose. Y de paso mucho más justa, porque no habría intermediarios en la gestión que cobrarán un porcentaje de ese dinero donado. Todo de forma anónima y veraz. Ya hace tiempo organizaciones como Save the Children o Wikileaks comenzaron a aceptar criptomonedas de financiación, y el futuro de la tecnología de la cadena de bloques en este sector es muy prometedor.

Entidades Públicas: La digitalización con el desarrollo de sistemas basados en el blockchain está explorando en algunos países aplicarlo en el registro de títulos de propiedad, licencias de vehículos, subvenciones, registros sanitarios, etc. Incluso en la educación, Blockchain puede prestar un servicio al evitar que los títulos sean apócrifos, La Universidad Provincial del Sudoeste en Argentina es la primera del país en emitir sus diplomas a través de la red (*Fernandez, 2019*)

Derechos de Propiedad Intelectual: De la fusión del blockchain y la propiedad intelectual nacen bases de datos como la IPChain, cuyo interés principal es proteger la autoría de manera segura y fácil; pero que es capaz de ofrecer a la vez que los usuarios compartan información, como documentos, por ejemplo, resguardando su carácter confidencial.

La IPChain es caracterizado por su cercanía con las Oficinas de Propiedad Intelectual y mantiene una relación de colaboración con entidades como WIPO Green (<https://www3.wipo.int/wipogreen/en/>), asociación de la Organización Mundial de la Propiedad Intelectual que promueve innovación y la difusión de tecnologías; el Dennemeyer Group (<https://www.dennemeyer.com/>), firma de propiedad intelectual más grande del mundo; y la Marie Curie Alumni Association MCAA (<https://www.mariecuriealumni.eu/>), que representa los intereses de más de 10.000 investigadores europeos.

Es la seguridad de la plataforma lo que la ha hecho muy atractiva en operaciones tan delicadas como transferencias o acuerdos contractuales. Si miramos específicamente los derechos de autor, blockchain impide que terceros puedan copiar las creaciones.

Otro de sus usos permite calcular las ganancias que puede obtener un compositor con su creación musical, lo cual puede ser complicado teniendo en cuenta lo difícil que resultaría tener un registro de todas las veces que es escuchada una canción determinada.

Mycelia (<http://myceliaformusic.org/>) es una base de datos musical en la que se puede consumir distintos tipos de música y pagar por ello. Fue creada por la cantante Imogen Heap²⁷, quien en una entrevista dio a conocer su motivación: “Una de las normas debería exigir que todos los servicios devuelvan información. En concreto, datos sobre dónde, cuándo y cómo se interactúa con nuestra música y quién lo hace. Esta información es oro en polvo para los artistas, porque si la sabemos interpretar podemos conocer mejor a nuestra audiencia y crear oportunidades de promover con mayor eficacia nuestra obra y de obtener una retribución económica por nuestro trabajo”.

En el mundo de las patentes ya se han generado debates respecto de cuál sería el papel de esta herramienta. Tal es el caso de un documento elaborado para diputados y personal del Parlamento Europeo, en el cual está en discusión el desarrollo y rol que desempeña el blockchain en la protección de la innovación.

Hoy, los costos ocasionan que algunos titulares opten por comercializar sus creaciones sin recurrir a alguna protección. También influye el problema que se presenta toda vez que no existe un sistema de patentes unificado a nivel mundial: tenemos uno por cada país.

²⁷ Imogen Jennifer Jane Heap, es una cantautora y productora musical británica ganadora de un premio Grammy, conocida por su trabajo en el dúo musical Frou y sus cuatro álbumes solistas. https://es.wikipedia.org/wiki/Imogen_Heap

El documento también aborda el problema de los “troles de patentes”, quienes adquieren patentes para luego solicitar indemnizaciones por daños y perjuicios por su infracción.

Es útil analizar las ventajas jurídicas y económicas de la aplicación de esta tecnología en el campo de la propiedad intelectual, al proveer registros seguros y estables que son difíciles de eliminar, permitiendo la participación de diferentes usuarios que almacenan copias actualizadas de información, quienes tienen control sobre las operaciones e información que ingresan.

Falsificaciones, un proyecto que patentó Nike llamado CryptoKick para evitar que sigan falsificándose sus calzados (*Cortés, 2019*)

Identificación Personal: "¿Quién eres?" podría ser la pregunta más común del mundo. En una página web, en una discoteca, en un aeropuerto o delante del mostrador de un banco, todo el mundo quiere que demostremos que realmente somos quienes afirmamos ser. Pero 2.400 millones de personas pobres a nivel mundial, alrededor de 1.500 millones de las cuales tienen más de 14 años de edad, no pueden dar a las autoridades una respuesta satisfactoria a esa pregunta. A pesar que ellas saben desde luego quiénes son, no poder demostrarlo les excluye de derechos como la propiedad, la libertad de circulación y las ayudas sociales. Simplemente, no pueden demostrar su identidad. Este vacío las expone en mayor medida a la corrupción y el crimen, incluidas la trata de personas y la esclavitud. De manera perspicaz, Naciones Unidas intenta cambiar la situación con el Objetivo de Desarrollo Sostenible #16 de la ONU de Paz, Justicia e Instituciones fuertes dirigido a "proporcionar una identidad legal a todos, incluidos los certificados de nacimiento, para 2030". (*Mainelli, 2017*)

El Blockchain en la Lucha contra el Cambio Climático

La ONU está fuertemente involucrada en incentivar ideas y atraer personas interesadas en el uso de la tecnología blockchain para el clima. Por eso, en diciembre de 2017, se desarrolló en Bonn el hackaton Hack4Climate [www.hack4climate.org], donde han sido presentados más de 100 desarrolladores para proponer soluciones de blockchain para el cambio climático. Algunos de los temas que se trabajaron fueron el desarrollo de aplicaciones de blockchain para combatir el cambio climático en áreas como el monitoreo de bosques, las transacciones

de energías renovables y de bonos de carbono. (Ast, *El Blockchain en la Lucha contra el Cambio Climático*, 2019)

Estos son algunos ejemplos de muchos que están aplicándose o desarrollándose. Ahora aplicados a Supply Chain los más relevantes que encontramos son:

Mercedes Benz usará Blockchain para rastrear las emisiones de carbono en la cadena de suministro de cobalto

El importante fabricante de automóviles Mercedes Benz y la startup de cadenas de bloques, Circulor, están desarrollando conjuntamente un piloto destinado a rastrear las emisiones de carbono en la cadena de suministro de cobalto.

El proyecto de Mercedes y Circulor²⁸ forma parte de la iniciativa Startup Autobahn, destinada a identificar la próxima generación de automóviles. Las compañías desplegarán blockchain para rastrear las emisiones de gases relevantes para el clima y la cantidad de materiales reciclados a lo largo de las complejas cadenas de suministro de los fabricantes de celdas de baterías.

Mercedes tiene la intención de utilizar los datos recogidos durante este piloto para desarrollar su nueva flota de coches de pasajeros de carbono neutral.

Pero primero, el cobalto

El proyecto centrará inicialmente en los suministros de cobalto, que recientemente han planteado cuestiones relacionadas con la procedencia y la ética. El cobalto es un mineral clave para la fabricación de baterías de iones de litio, y la mayor parte de la producción de cobalto proviene de la República Democrática del Congo, una región criticada por sus condiciones poco éticas de extracción de cobalto. En 2017, las Naciones Unidas estimaron que 168 millones de niños estaban en condiciones de explotación laboral en todo el mundo, con alrededor de 40,000 niños en las minas de cobalto en la RDC. Eso significa que es especialmente importante para las empresas saber de dónde provienen los materiales de sus productos.

²⁸ Circulor: Empresa dedicada a brindar servicios de trazabilidad mediante Blockchain
<https://www.circulor.com/about>

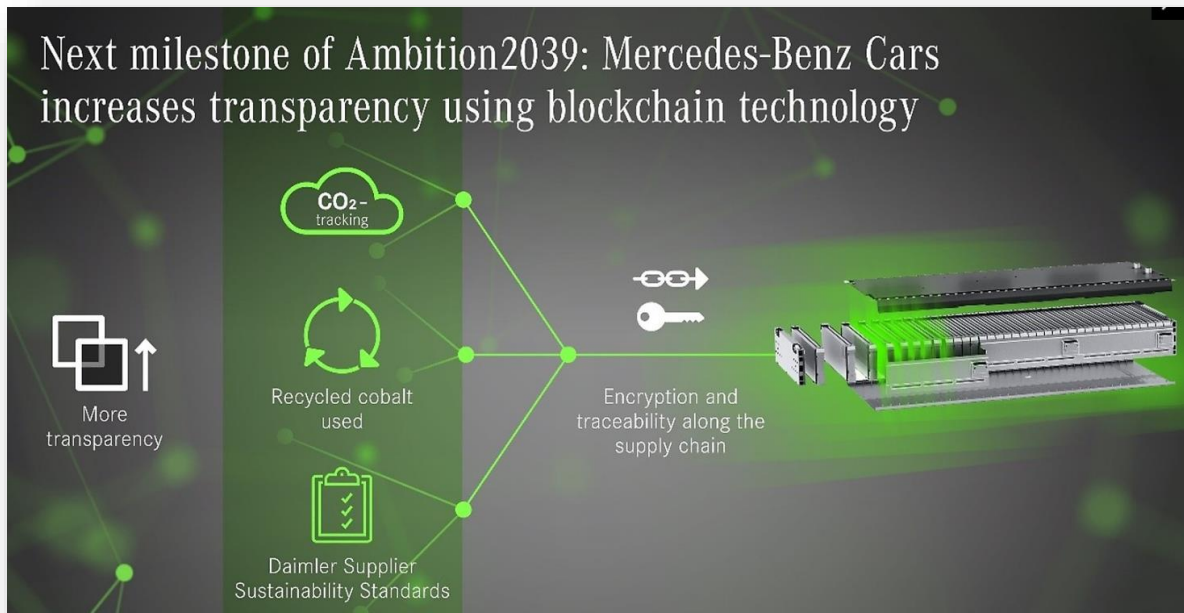


Figura 17 - Mercedes Benz Project

Un programa piloto basado en cadenas de bloques trazará un mapa del flujo de producción de estos materiales y de sus emisiones de carbono asociadas, así como registrará la cantidad de material reciclado que es utilizado en la cadena de suministro.

Esto supuestamente ayudará a Mercedes a determinar si sus empresas asociadas cumplen con sus requisitos de sostenibilidad, especialmente en lo referente a los derechos humanos.

(Benz, 2019) (Benz, Blockchain pilot project provides transparency on CO2 emissions, 2020)

Conectividad y trazabilidad

Daimler (Mercedes Benz) está trabajando también para un registro completo de sus vehículos a través de la tecnología Blockchain, esta misma iniciativa que consta de tener un registro completo de sus autos lo están comenzando a implementar en otras marcas reconocidas. Básicamente se trata de un historial del auto, imposible de adulterar, la investigación indica que solo en Alemania el 33% de los odómetros de los autos son adulterados, esta manipulación podría evitarse con un registro completo a través de la cadena

(Daimler, 2019)

Maersk

Maersk, el gigante danés del transporte marítimo, ha realizado con éxito proyectos pilotos en los que ha aplicado el modelo blockchain en el transporte internacional de mercancías.

El objetivo marcado es mejorar la administración y trazabilidad de contenedores marítimos mediante la digitalización extremo a extremo de la cadena de suministro, con lo que se pretende incrementar la transparencia y conseguir un intercambio seguro y confiable de información entre los socios comerciales. El resultado esperado; contar con una plataforma de gestión que pueda implantarse a gran escala, con un importante ahorro potencial de costos. *(Maersk, 2019)*

SmartLog

En la región báltica, la compañía Kouvola Innovation dependiente de la administración municipal de la ciudad de Kouvola (Finlandia), está realizando una prueba de concepto del uso de blockchain e IoT en colaboración con compañías logísticas locales.

El proyecto, denominado SmartLog, está centrado en la aplicación de blockchain para la transferencia de datos operacionales de las empresas logísticas y la consiguiente mejora en los flujos de información, haciendo uso de Hyperledger Fabric como plataforma blockchain. Con el objetivo de probar las mejoras obtenidas a través de la aplicación de blockchain, durante el piloto se medirán los tiempos de tránsito de las mercancías a lo largo de dos corredores de la red principal europea TEN-T en la región báltica (ScanMed y Mar del Norte–Báltico). La prueba es realizada extremo a extremo, involucrando a entidades y compañías de Finlandia, Suecia, Letonia y Estonia. Como resultado del proyecto se espera obtener una solución abierta y de aplicación en el sector. *(smartlog, 2018)*

Blocklab

En los Países Bajos, la iniciativa Blocklab desarrolla casos de uso blockchain en el ámbito de la logística. Con base en el Puerto de Rotterdam, Blocklab trabaja junto con administraciones, organizaciones, desarrolladores y usuarios finales, explorando la aplicación conjunta de blockchain, IoT y Bigdata.

Uno de los casos de uso en desarrollo gira en torno a la financiación de inventarios, liderado por un consorcio formado por Exact, ABN-AMRO Commercial Finance, Innopay y NBK.

El objetivo es proporcionar crédito adicional a los expedidores en función del inventario que almacenen en un proveedor de servicios logísticos. En este escenario blockchain presenta un gran potencial si la cadena de suministro tiene un gran número de participantes y ninguno de ellos tiene una posición claramente dominante, de modo que el problema pueda abordarse con un enfoque descentralizado. En este caso, la solución está basada en la plataforma blockchain Ethereum.

Otro proyecto desarrollado en el ámbito de Blocklab involucra a ABN-AMRO, las Autoridades Portuarias de Rotterdam, Flora Holland y Transfollow. En este caso, se trata de vincular el recibo físico de la carga por el receptor con los datos de una hoja de ruta digital (o CMR), y activa la financiación de la factura del proveedor de servicios logísticos. (Wolfpack, 2016) <https://www.blocklab.nl/media/uploads/2017/09/A-lead-via-Blockchain-Technology.pdf>

T-Mining

Por su parte, T-Mining, empresa radicada en Bélgica, está desarrollando aplicaciones basadas en blockchain para logística y transporte de contenedores, con el objetivo de crear una plataforma de smart contracts que ayude a incrementar la seguridad en el traspaso de contenedores en los puertos marítimos y aumente la eficiencia y la confiabilidad en el intercambio de información entre las partes, reduciendo los costos operacionales y administrativos. Actualmente están llevando a cabo una prueba de concepto de en el puerto de Amberes, involucrando al operador del puerto, transportistas, transitarios etc. (*t-mining, s.f.*)

A2B Direct

A2B Direct se posiciona como una compañía del norte de Europa al estilo Uber Freight, donde transportistas con licencia fiscal pueden darse de alta y recibir pedidos directamente de los clientes finales. Ofrecen servicios de gestión de la identidad de los transportistas, así como rankings basados en datos registrados en blockchain y opiniones de los clientes (*a2b.direct, s.f.*)

PassLfix

PassLfix plantea el transporte de objetos de forma descentralizada y segura utilizando blockchain junto con IoT. Con el uso de blockchain en conjunción con capacidades de sensorización y control físico de objetos, puede probarse la transmisión de activos sin necesidad de un tercero de confianza.

La utilización de smart contracts permite la gestión de flujos financieros de acuerdo con términos contractuales definidos y firmados, y la creación de aplicaciones para organizaciones distribuidas. Con estos ingredientes, PassLfix propone una nueva forma de transferir bienes, usando smart contracts para gestionar las entregas, y activos digitales para el pago de tasas y depósitos. (*PassLfix, s.f.*)

Provenance

Una referencia notable en este ámbito es Provenance, que está desarrollando un sistema de trazabilidad para materiales y productos utilizando blockchain, con el objetivo de garantizar que la información sea almacenada de manera segura, auditable, inmutable y accesible.

Los productos pueden incorporarse al sistema de trazabilidad a través de etiquetado, smart tags o código en un sitio de comercio electrónico y la plataforma blockchain (basada en tecnología Ethereum) actúa como un sistema descentralizado del que pueden ser parte todos los intervinientes en la cadena de suministro.

Ya han sido realizados pilotos para la trazabilidad en la cadena de producción y suministro de alimentos con blockchain, en mercados como Japón, Estados Unidos y Reino Unido. (*Provenance, s.f.*)

Resulta asombroso como la empresa Tiffany & Co. Junto a Provenance desarrollaron la trazabilidad completa de sus diamantes (*Co, s.f.*)

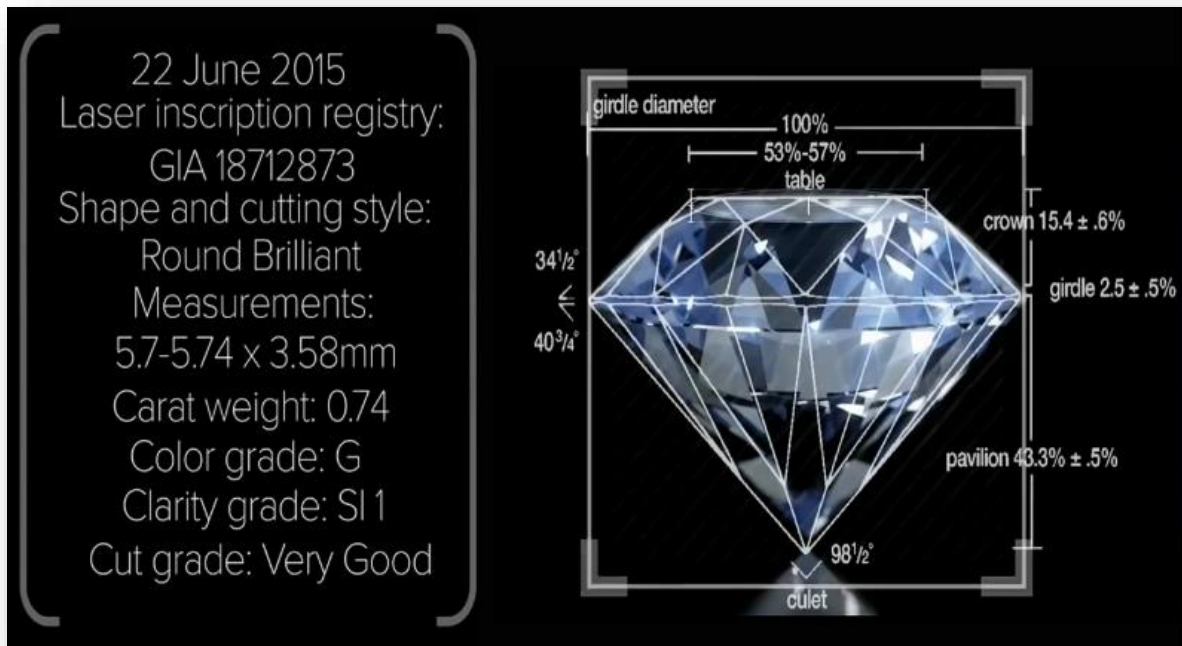


Figura 18 - Trazabilidad de diamantes

(Altoros, 2015)

Ripe.io

Ripe.io, por su parte, aspira a constituir la “blockchain de los alimentos” y transformar la cadena de suministro de alimentos frescos. Para ello, habilita un nuevo nivel de transparencia en cuanto al origen de los mismos y su viaje hasta el consumidor final.

La conjunción de blockchain e IoT incrementará la recogida de datos en los procesos y la visibilidad de los mismos, permitiendo nuevas analíticas, mayor automatización y diferentes modelos de negocio. (Ripe.io, s.f.)

Smart AgriFood

En Italia, Smart AgriFood aplica blockchain al sector de los productos agrícolas a través de su sistema AgriOpenData.

Utilizando un código de seguridad, accesible mediante la lectura de un código QR, se registra paso a paso la historia de un producto agrícola a lo largo de todo el proceso productivo, desde

la siembra hasta la llegada a los puntos de venta finales, pasando por toda la transformación, para garantizar una calidad certificada a los consumidores. (*smartagrifood, s.f.*)

Medicamentos

También muchos actores del sector farmacéutico están considerando blockchain para la mejora de la seguridad y la trazabilidad en la cadena de suministro de los medicamentos, la cual ha crecido en complejidad y enfrenta a retos de gestión y optimización de los procesos. La transferencia de custodia de los medicamentos, así como la garantía de autenticidad de los mismos son dos aspectos en los que blockchain puede aportar beneficios. La participación de los distintos actores de la cadena (fabricantes, envasadores, distribuidores, farmacias y hospitales etc.) en una plataforma blockchain dotaría de integridad, transparencia y trazabilidad a todo el proceso extremo a extremo a lo largo de la cadena. Existen varias iniciativas que están explorando las capacidades de blockchain para la trazabilidad en la cadena de suministro de medicinas, como Blockverify (<http://www.blockverify.io/>) o BlockRx (<https://www.blockrx.com/>). Además de la trazabilidad y autenticidad de producto, blockchain puede contribuir a solucionar problemas de índole financiera que afectan especialmente a los operadores más pequeños de la cadena de suministro. La cadena de bloques puede proporcionar registros fiables y confianza para agilizar los créditos. En China, EasySight Supply Chain Management han desarrollado una plataforma blockchain que involucra a retailers farmacéuticos, hospitales y bancos. Mediante el seguimiento de los medicamentos a través de la cadena de suministro y el registro cifrado de registros comerciales, se reduce el riesgo crediticio percibido por las entidades financieras y pueden acortarse los periodos de pago. Una mayor integración de la información permite que los bancos estén más informados y consigue ciclos de financiación más rápidos en el ecosistema.

Walmart

Desde su posición dominante como retailer en la parte final de la cadena de suministro, Walmart está aplicando blockchain en el desarrollo de nuevos sistemas de gestión de entregas. En concreto; los desarrollos del líder en retail están orientados a la automatización de la logística en procesos de entrega de paquetes con drones y a las capacidades de

blockchain para gestionar la identificación de los drones al aproximarse a los puntos de reparto. (*hyperledger, s.f.*)

FreshTurf

También en relación al reparto de paquetería, FreshTurf está desarrollando en Singapur, un sistema para mejorar la entrega de envíos en lockers utilizando blockchain. La solución se ha diseñado para gestionar todas las transacciones entre comerciantes, operadores logísticos, compañías dedicadas a la colocación y mantenimiento de lockers de recogida y consumidores finales. Se persigue la creación de un Marketplace desintermediado en el que los puntos de recogida (espacio en lockers) puedan proporcionarse a cualquiera que los quiera alquilar. (*FreshTurf, s.f.*)

Servicios postales

Asimismo, servicios postales de diversos países, como EE. UU, Canadá o Australia, están explorando las capacidades de blockchain para distintos usos, que van desde la prestación de servicios de verificación de identidad digital, al tracking de los envíos, pasando por servicios financieros como giros postales o envíos internacionales de dinero, en los que blockchain puede incrementar la eficiencia. (*efintechshow, 2018*) (*DÍAZ, 2019*)

Sin dudas día a día irán incorporándose nuevas plataformas

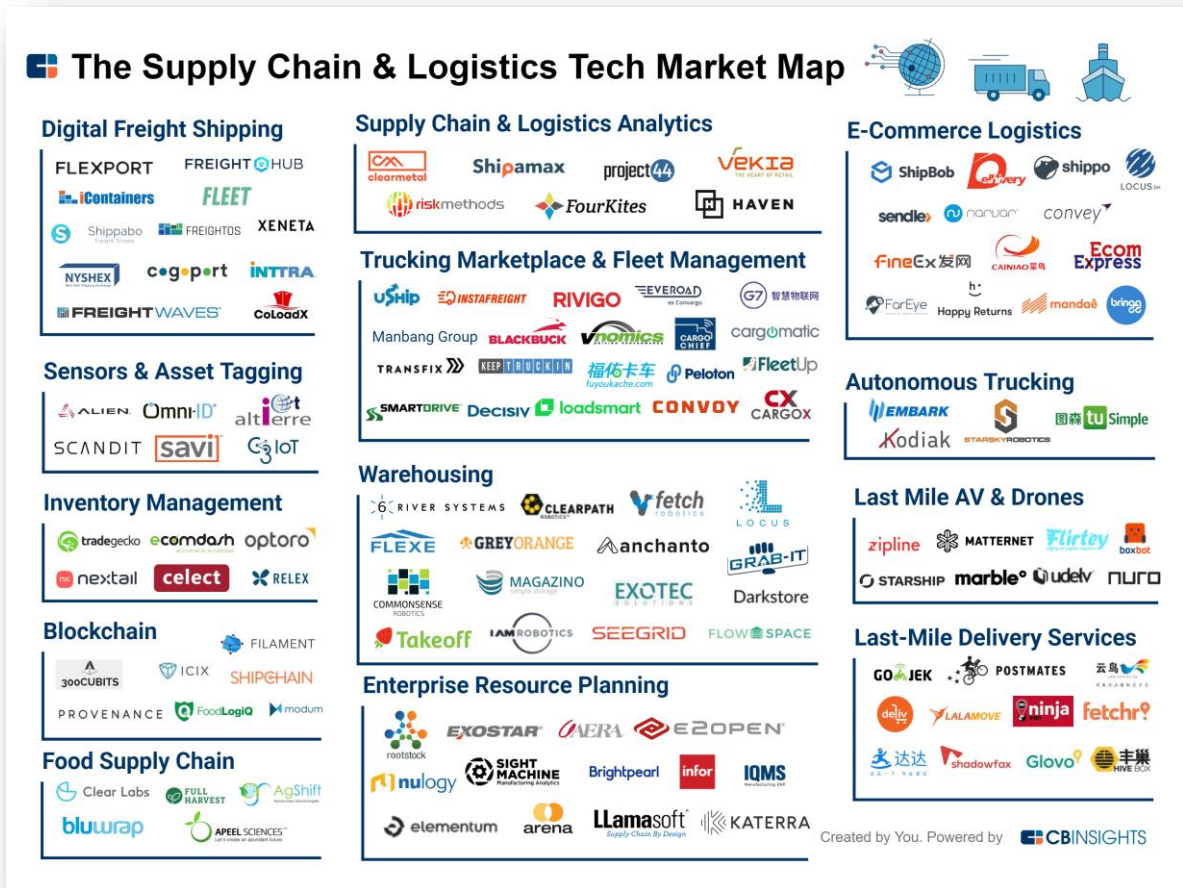


Figura 19 - Proyectos Blockchain

11) DESARROLLO DE BLOCKCHAIN EN LOGISTICA / SUPPLY CHAIN

Para el desarrollo del trabajo voy a ir de mayor a menor, en principio un flujo normal del Supply Chain consta de las siguientes etapas:

Planificación Estratégica (Strategic Planning)	En esta etapa se define la estrategia de toda la cadena de abastecimiento, como de donde se abastecerá, transportes a utilizar, ubicaciones del / los almacenes, etc.
Planificación de Demanda (Demand Planning)	En esta instancia se incluyen las previsiones de ventas, ciclo de vida de los productos, promociones
Planificación de Abastecimiento (Supply Planning)	Se definirán los parámetros de stock, niveles de inventario, stocks de seguridad, lotes óptimos de compra, como se interactúa con los proveedores y con los clientes
Compras (Procurement)	Gestión completa de las compras, desde la negociación con proveedores, confirmación de recepción de orden de compra, verificación de facturación
Fabricación (Manufacturing)	Dentro de Fabricación se incluye la planificación de producción, costos de producción, tiempos
Almacenamiento (Warehousing)	El almacenamiento incluye las etapas de recepción, despacho, realización de inventario
Gestión de Ordenes de venta y facturación (Order Fulfillment)	Dentro de esta etapa se encuentra el procesamiento de las ordenes de venta y el proceso de facturación
Transportes (Transportation)	Transportes incluye a planificación de transportes nacionales, internacionales, medios de transportes, tarifas

Figura 20 - Etapas de Supply Chain

Debería ser en la etapa de Planificación Estratégica donde se define si será utilizado Blockchain en alguno de los procesos, por supuesto que esto puede implementarse posteriormente; pero al definirlo desde esta instancia temprana puede determinarse de manera más prolija que tipo de Blockchain es conveniente (Pública, Privada o Permissionada, Híbrida o Federada), en que etapas será implementado y como se desarrollará.

En Planificación de Demanda la tecnología mayormente empleada es Big Data y Machine Learning, Blockchain conjuntamente con otras tecnologías trabaja para dar información ya que sería el libro de Blockchain una de las fuentes donde quedaría almacenada la información utilizable posteriormente para el análisis de Big Data y Machine Learning ofrece la inteligencia de interpretar acontecimientos, por ejemplo:

un retailer que opera en aeropuertos ofreciendo productos frescos. Su demanda fluctúa no solo de un día para otro, sino que también lo hace a lo largo del día, dependiendo del número de personas que transita por el aeropuerto. La entrada manual de este tipo de datos consumiría muchísimo tiempo, sin mencionar que; casi seguro, garantizaría un pronóstico sin errores.

Un algoritmo de machine learning con acceso a los datos del aeropuerto podría, automáticamente, reconocer los patrones de tránsito y aplicar estas tendencias a la previsión de la demanda del retailer, sin necesidad de programación.

Machine Learning no es determinista, sino que aprende de los datos

Machine Learning le da al sistema la capacidad de aprender y mejorar automáticamente a partir de los datos, sin necesidad de programar. El sistema se alimenta de datos como por ejemplo, experiencias directas o instrucciones, en los que buscar patrones. Aún más, puede usar los patrones que identifica en los datos para tomar mejores decisiones. En resumen, el algoritmo de aprendizaje elimina la necesidad de programación al generar automáticamente un programa/modelo basado en los datos que son proporcionados.

El principal beneficio del machine learning es que el sistema puede procesar grandes cantidades de datos de varias fuentes sin la intervención de las personas. El valor obtenido del machine learning dependerá de la calidad y cantidad de los datos.

Ejemplos prácticos del Machine Learning en Retail

En el escenario del retailer de aeropuerto, el machine learning es utilizado para identificar la relación entre un factor externo (afluencia) y una demanda local por tienda y producto. Pero el machine learning puede tomar en consideración una variedad de factores externos en el entorno de retail.

Meteorología

La meteorología, por ejemplo, también es una fuente importante de fluctuaciones en la demanda de los consumidores. Aunque predecir el tiempo que va a hacer puede ser difícil, en realidad es bastante sencillo crear reglas o modelos basados en la relación entre la demanda para un producto y factores meteorológicos como la lluvia, horas de sol, temperaturas, etc.

Pero, al contemplar nuestro surtido completo, esta sencilla tarea se convierte en algo bastante laborioso. Es necesaria una metodología automatizada para procesar los datos en tan grandes cantidades, esto es especialmente cierto cuando nos damos cuenta que el proceso debe mirar tanto al futuro, como al pasado. Un pronóstico robusto y preciso también filtrará el efecto meteorológico de los datos de ventas históricos.

Cuando estos procesos están automatizados, los retailers pueden planear de forma proactiva los aumentos o disminuciones en la demanda local, asumiendo que tienen una disponibilidad de productos suficiente. En el retail de alimentación, tener en cuenta los factores meteorológicos puede reducir los errores de pronóstico entre un 5% y un 15% para los productos sensibles al clima y hasta un 40% en el ámbito de categoría y tienda. Un supermercado de Gran Bretaña utilizó las correcciones de meteorología durante un verano inusualmente frío y lluvioso, pudiendo aumentar la precisión del pronóstico para sus productos sensibles a los factores climáticos a más del 90%.

Canibalización

Mientras que la meteorología puede tener un efecto variable, la promoción de productos siempre tiene un impacto positivo directo en el volumen de ventas de los productos promocionados. Sin embargo, demasiado a menudo, los retailers no tienen en cuenta el impacto que la promoción de un producto puede tener en el volumen de ventas de otros productos no promocionados. Cuando la mayor demanda de un producto se traduce en una menor demanda de otro, se le llama canibalización. La canibalización puede darse, por ejemplo, entre dos tipos de carne picada: cuando una está en promoción, el consumidor prefiere llevársela, lo que resulta una disminución de la demanda de la carne picada que no está en promoción. Tener en cuenta este tipo de relaciones mejora significativamente la precisión del pronóstico durante las promociones que tienen efecto canibalización, lo que disminuye el riesgo de mermas de los productos canibalizados.

Puede parecer fácil predecir como las promociones de ventas afectan el comportamiento de compra; pero ¿qué pasa cuando manejamos miles de productos? ¿Como reconocemos las relaciones importantes entre millones de posibilidades? La solución más práctica sería utilizar técnicas del machine learning que automáticamente reconocen estas relaciones basadas en ventas históricas y datos de promoción.

En el resto de las etapas es donde entiendo existe potencialidad para la implementación y por lo tanto serán ampliadas a continuación:

11.1) Compras Locales

En la mayoría de las empresas, el departamento o sector de compras pertenece a Supply Chain y no a logística; pero en el caso particular que estamos analizando, logística tiene la responsabilidad sobre las compras de su sector (transportes, insumos, almacenamiento en terceros, etc.).

El proceso de esta compañía para la gestión de un transporte para llevar mercadería local desde la fábrica hasta el cliente es el que se muestra a continuación:

Logística comparada entre método tradicional y la aplicación de la tecnología Blockchain

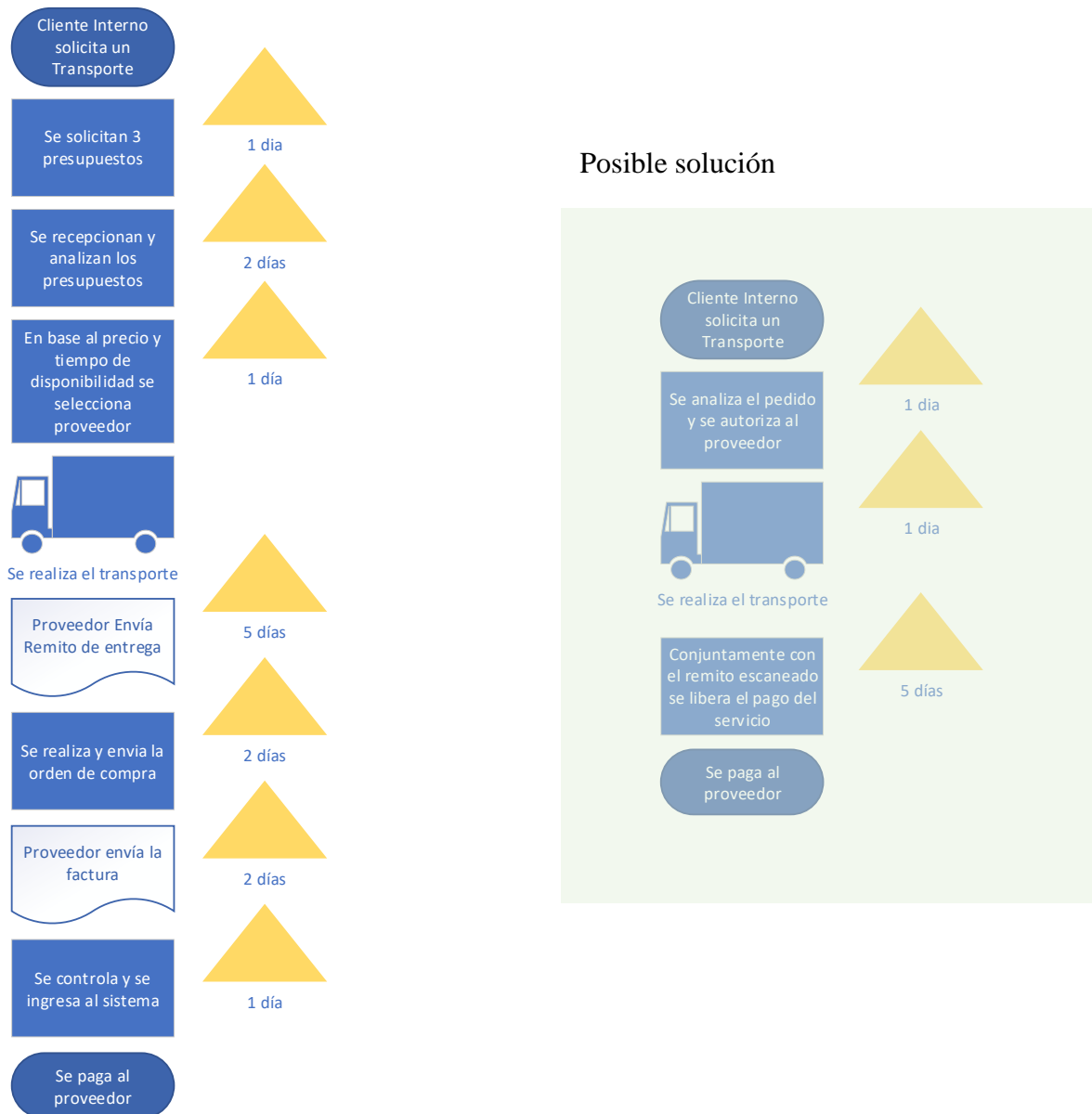


Figura 21 - Proceso de Pedido de Transporte

La posible solución que aplicada en este ejemplo de un caso real es:

- Negociar con los proveedores costo por kilómetro en lugar de realizar una cotización por cada solicitud de servicio. De esta forma se estandariza el costo y no es requisito negociar cada servicio ya que conociendo la cantidad de kilómetros, puede estimarse el valor final que tendrá el flete.
- Mediante la aplicación de un Smart contract se reciben las solicitudes de pedido, se revisan, se envían al proveedor, el primer proveedor que la acepta es el asignado y

mediante la digitalización del remito se cierra el ciclo del pedido para que el proveedor pueda cobrar de acuerdo a los tiempos de pago que hayan sido negociado previamente.

Esta posible aplicación reduciría la intervención humana en el tratamiento del pedido, mejoraría los tiempos que demora el proceso, evitaría el exceso de comunicación ya que la misma información estaría disponible al mismo tiempo para todos los que tengan acceso. Por supuesto que se puede ser mucho más exigente y buscar además saber en todo momento la posición del transporte y de la mercadería, además de tener una base de datos de los kilómetros utilizados, los tiempos de demora, los destinos, etc. Pero esto fue solo un ejemplo de un caso real y como la tecnología podría mejorar las ineficiencias existentes. Simplemente se trata de lograr la desintermediación que agrega tiempos y costos a la operatoria y Blockchain parece ser la tecnología que lo hace posible.

11.2) Compras al exterior

Esto es aún más complejo y es una de las ramas de supply chain donde más apuestan las grandes compañías a obtener ventajas mediante la aplicación de Blockchain.

Las importaciones en Argentina están gravadas con derechos de importación AD VALOREM, que van desde el 0%, 8%, 14%, 16%, 18%, 20%, 25% y 35%. Su variación depende del tipo de mercancía que se vaya a importar. Cabe destacar que también existen otros derechos gravables como, Anti Dumping, Compensatorios, Específicos, etc.

Para calcular los costos de importación en Argentina es importante saber que la alícuota que es aplicada a la mercancía va a depender de su posición arancelaria y, a parte de esa alícuota, debe considerarse la tasa de estadística que pudiese ser de 0,5% o del 0%. Además de estos derechos de importación, también deben tomarse en cuenta otros impuestos a pagar tales como:

IVA tasa general del 21% o 10,5% si la importación se refiere a bienes de capital, informática o de telecomunicaciones. (Artículo 1° de la Ley 23.3449 inc. y Decreto 2407/86 Artículo 2°).

IVA Adicional del 20% (Resolución General AFIP 3373/2012).

Impuesto a las ganancias del 6% (Resolución General AFIP 3373/2012).

Ingresos Brutos si corresponden del 3% (Resolución General AFIP 3373/2012).

Tasa de Oficialización de Aduana de US\$10,00 aplicable a todos los casos.

Tasa de Digitalización de Aduana de US\$28,00 aplicable a todos los casos.

Tasa de SENASA Madera de US\$18 + IVA. Solo si la mercancía posee embalaje de madera.
(Resolución SENASA 614/5).

Valor de mercadería	7500,00	USD
---------------------	---------	-----

Costo de Flete	800,00	USD
----------------	--------	-----

Valor CIF

Los Derechos de aduana y la tasa de estadística determinados según el valor CIF de la mercancía, el cual está compuesto por el Valor FOB + Flete + Seguro estadístico del 1% del valor CFR:

Valor FOB	7500,00	USD
-----------	---------	-----

Valor Flete	800,00	USD
-------------	--------	-----

Valor CFR	8300,00	USD
-----------	---------	-----

Valor Seguro	83,00	USD	Corresponde al 1% del valor CFR
--------------	-------	-----	---------------------------------

Valor CIF	8383,00	USD
-----------	---------	-----

Derechos de Importación

Una vez obtenido el valor CIF (costo, seguro y flete) procederemos a realizar el cálculo de los derechos de importación. Tomaremos el peor escenario con un impuesto de 35% y una tasa de estadística del 0,5%, el cálculo quedaría así:

Valor CIF	8383,00	USD
-----------	---------	-----

Derechos de Importación	2850,22	USD
-------------------------	---------	-----

Tasa de Estadística	41,92	USD
---------------------	-------	-----

Base IVA

Ahora vamos a establecer la BASE IVA, para poder calcular las alícuotas para los impuestos IVA, IVA Adicional, Impuesto a las Ganancias e Ingresos Brutos:

BASE IVA= BASE IMPONIBLE + DERECHOS + TASA ESTADISTICA

Base Imponible	8383,00	USD
Derechos de Importación	2934,05	USD
Tasa de Estadística	41,92	USD
Base IVA	11358,97	USD

Alícuotas generales

Conociendo la BASE IVA procedemos entonces a calcular las alícuotas generales de: IVA: 21%, IVA Adicional: 20%, Impuesto a las Ganancias: 6% e Ingresos Brutos: 3%.

Base Imponible	8383,00	USD	
Derechos de Importación	2934,05	USD	
Tasa de Estadística	41,92	USD	
Base Imponible IVA	11358,97	USD	
IVA	2385,38	USD	21%
IVA Adicional	2271,79	USD	20%
Impuesto a las Ganancias	340,769	USD	3%
Ingresos Brutos	340,769	USD	3%
			Costo
Tasa de Oficialización de Aduana	10	USD	Fijo
			Costo
Tasa de Digitalización de Aduana	28	USD	Fijo

Pago a la Aduana

Derechos de Importación	2934,05	USD
-------------------------	---------	-----

Tasa de Estadística	41,92	USD
IVA	2385,38	USD
IVA Adicional	2271,79	USD
Impuesto a las Ganancias	340,77	USD
Ingresos Brutos	340,77	USD
Tasa de Oficialización de Aduana	10,00	USD
Tasa de Digitalización de Aduana	28,00	USD
Total a pagar en Aduana	8352,68	USD

Tabla 1 - Costos de Importación

En definitiva, en este ejemplo, se paga el doble aproximadamente por nacionalizar un producto; pero a los efectos de lo que podría evitarse utilizando Blockchain, se evidencia que solo podrían ser los 38 USD en los conceptos Tasa de Oficialización de Aduana y Tasa de Digitalización de Aduana, el resto son todos gravámenes. Pero ahora bien, estos son únicamente los costos directos y que pueden ser fácilmente calculados ya que están preestablecidos; pero existen muchos servicios que son parte de la operativa de comercio exterior que no están nombrados en la tabla como ser:

Gastos de transferencia de Fondos al Exterior y Liquidación de Divisas: debido al control de cambio establecido en Argentina, los pagos al proveedor deben ser realizados a través de un banco autorizado. Por lo tanto, se generarán comisiones por la emisión de la transferencia y por la liquidación de divisas.

Además de las transferencias, existen los diferentes medios de pago internacional, cada una asociada a la confianza que se tiene respecto a la contraparte. Por supuesto que a menor confianza, mayor serán los organismos intervinientes, avales y en consecuencia, el costo.

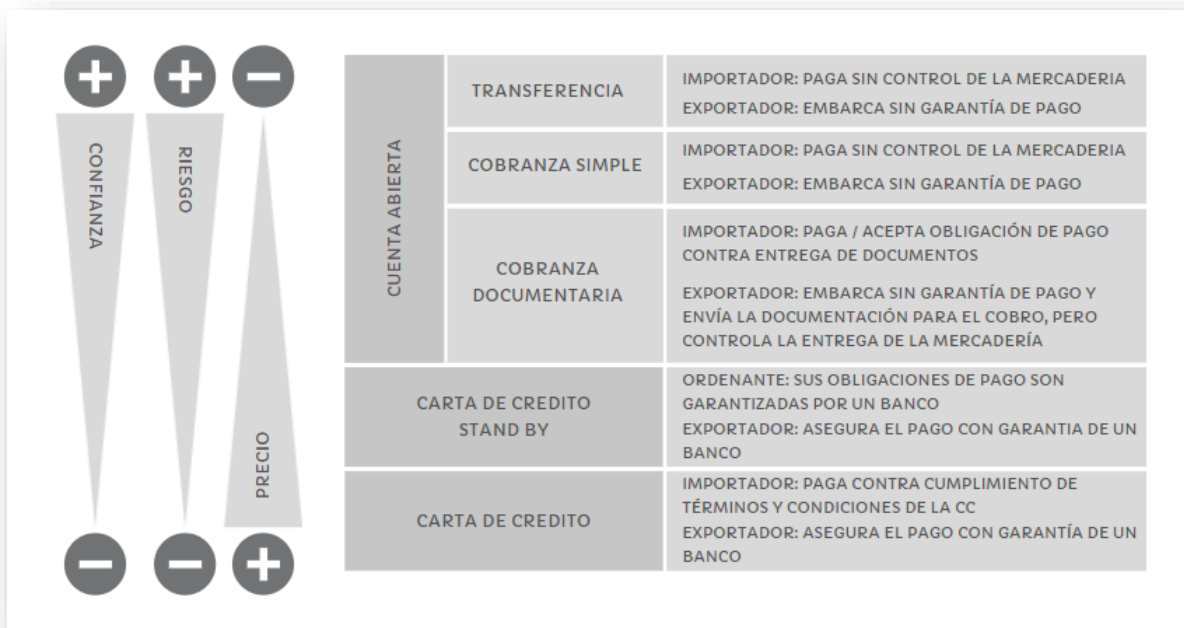


Figura 22 - Medios de Pago Internacional

En el ejemplo del medio de pago más costoso (Carta de crédito), además del tiempo que requiere semejante intervención de intermediarios, cada uno de ellos le agrega costo a la operación, este costo se calcula entre un 3% y 4% sobre el valor total, de acuerdo al país y muchas otras variables. Justamente Blockchain brindaría la confianza que no existe al tomar este tipo de opción. Si bien se han realizado operaciones de este tipo con criptomonedas, aún no existen las regulaciones necesarias para que esta metodología pueda ser realizada completamente mediante smart contracts.

(Ehuletche, 2019)

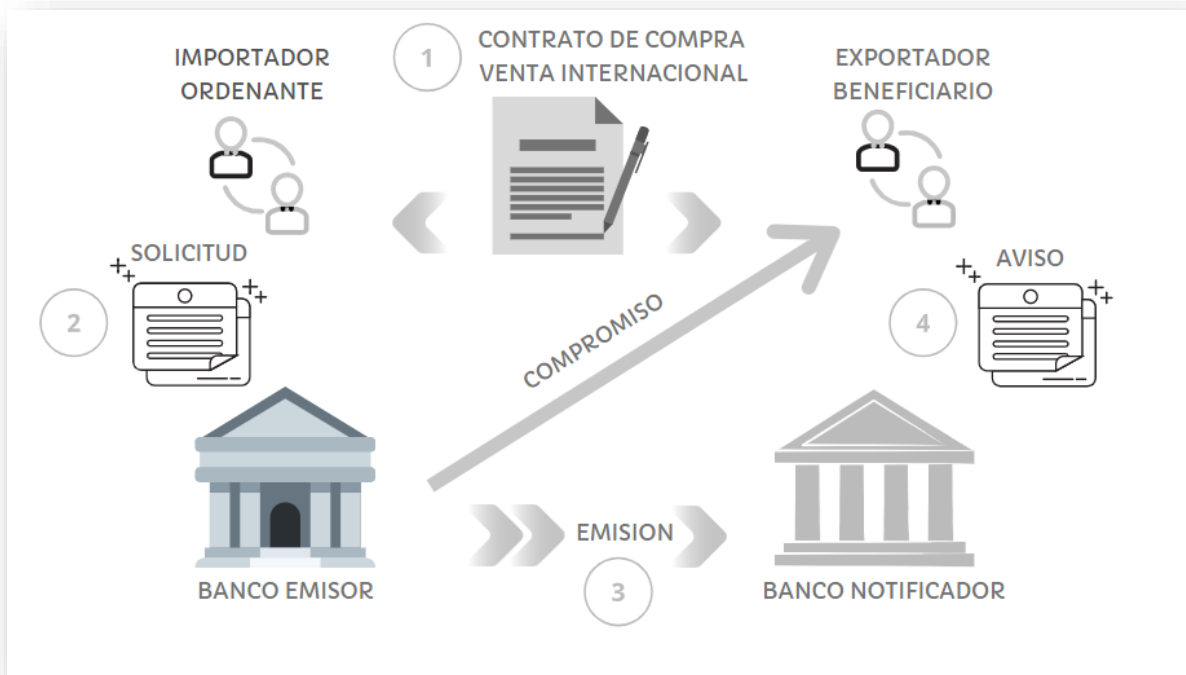


Figura 23 - Carta de Crédito Internacional

Además de los potenciales ahorros de tiempo y económicos, hay un gasto no menor que se incurre en toda la operativa de comercio exterior, y es la excesiva cantidad de papel que es requerido para documentar las instancias. (Gonzalez).

Ante un comercio exterior en el que uno de cada cinco dólares del costo logístico se gasta en papeleo, los analistas advierten que evitándolo podrían reducirse drásticamente los tiempos y que la actividad podría incrementarse en un 15% anual en todo el mundo.

Entre esos estudios, la Comisión Económica para Asia y el Pacífico de las Naciones Unidas (Cespap/Unescap) dio a conocer que en operaciones de comercio exterior sin papeles las exportaciones podrían incrementarse anualmente en el mundo en 257.000 millones de dólares, en tanto el tiempo promedio para exportar se reduciría entre un 24% y un 44%, y los costos para embarcar de un 17% a un 31%.

En cuanto al escenario en la Argentina, en un informe del Banco Mundial que mide la performance logística se indicó que una exportación promedio demora 51 horas (4 días), tiempo que lleva cargar la documentación y cumplir con los trámites aduaneros, con un costo aproximado de 210 dólares. Acerca de las importaciones, se mostró que la demora en

documentaciones y procedimientos insumen 252 horas (10 días) y redundan en un costo que trepa a los 1400 dólares. *(Lozano, 2018)*

(IBM, s.f.)

11.3) Producción

En el caso de la manufactura, Blockchain genera potenciales ahorros directos en su proceso a través de la trazabilidad y transparencia que puede obtenerse. Resulta muy complejo determinar el valor de este ahorro, porque estos podrían producirse únicamente si se detecta un problema cuando el producto llega al mercado, en el caso de la compañía de estudio, la falla de un producto en un cliente puede ser potencialmente peligroso para las vidas humanas y en caso que eso sucediera, el costo y daño de imagen de la empresa sería imposible de cuantificar. *(Columbus, 2018)*. Entonces, Blockchain, junto a IoT tienen un potencial enorme para asegurar la trazabilidad y transparencia y es sobre estos campos específicos donde los expertos aseguran que está la mayor aplicabilidad de la tecnología. Ahora bien, como aclaré anteriormente, un producto de los que comercializa la compañía de estudio puede provocar daños fatales en caso de un desperfecto mayor, justamente por este mismo motivo que las empresas más importantes de automóviles, alimentos o salud están investigando y desarrollando Blockchain. En los automóviles para evitar los famosos “recall” que implica que tengan que ir a revisión lotes de autos por posibles fallas y en alimentos o salud no es necesario imaginar el peligro que supondría una adulteración que llegue a consumo.

(Deloitte, 2017) (DHL, 2018)

11.4) Almacenamiento

Similarmente con lo que sucede en Manufactura, en almacenamiento Blockchain junto con IoT brindan trazabilidad y transparencia al proceso, puede quitar ineficiencias propias del proceso, y toda quita de ineficiencias se traduce en mejora de servicios y ahorros. La información es valor, y lograr obtener información sobre la fecha exacta de ingreso de mercadería permite optimizar el espacio en almacenamiento y los movimientos dentro del mismo, distribuir eficientemente los recursos, anticipar posibles cuellos de botella, etc.

11.5) Transportes

En este caso nos remitimos al ejemplo de compras locales en la empresa en estudio, este caso se estima que a nivel mundial esto representa 140 billones de dólares en disputas por pagos

en la industria del transporte. Se estima también que el costo de la excesiva documentación por la dependencia de transacciones en papel implica un 20% del costo general de los transportes. (*winnnesota, 2018*).

El mayor potencial de la cadena de bloques dentro de transportes sin dudas esta dado en transporte marítimo, por lo explicado anteriormente, la complejidad del comercio internacional hace que sea el foco natural de una tecnología que busca eliminar ineficiencias. En este caso el proyecto actual más ambicioso es TradeLens, una plataforma industrial abierta y neutral respaldada por la tecnología Blockchain, con la colaboración de los principales actores de la industria logística. Utiliza la tecnología IBM Blockchain como la base de las cadenas de suministro digitales, permitiendo a múltiples socios comerciales colaborar mediante el establecimiento de una única vista compartida de una transacción sin comprometer los detalles, la privacidad o la confidencialidad. De esta iniciativa forman parte 94 organizaciones que participan activamente o han aceptado unirse a la plataforma. Cuentan con 20 operadores de puertos y terminales en todo el mundo.

Las autoridades aduaneras de los Países Bajos, Arabia Saudita, Singapur, Australia y Perú participan, junto con los agentes de aduanas Ransa y Güler & Dinamik. Empresas de transporte y logística, como Agility, CEVA Logistics, DAMCO, Kotahi, PLH Trucking Company, Ancotrans y WorldWide Alliance también están en ella.

En transporte terrestre la mayor aplicabilidad que está estudiándose es una especie de modelo Uber; pero sin intermediación para la contratación de transportes directamente, esto permitiría optimizar la logística terrestre ya que posibilitaría a los dadores de carga contratar con precios más competitivos y a los transportistas optimizar los recursos. Actualmente Argentina convive con un problema de distribución de cargas, es común llevar camiones cargados al sur del país; pero resulta complejo conseguir mercadería para que el transporte regrese con carga y optimizar su costo.

11.6) Trazabilidad

La mayor fortaleza en la aplicación de Blockchain en Logística, parece ser sin dudas la trazabilidad que brinda. Un completo sistema de registros inalterables que permiten conocer la historia completa de un producto desde el origen de la materia prima hasta la entrega final al cliente. Lograr este nivel de trazabilidad no solo produce ahorros económicos, sino que garantiza que la imagen de una compañía no se vea seriamente dañada. Solo imaginarse el

peligro potencial que generaría que un producto comestible o farmacológico adulterado que llegue al consumo humano. Un ejemplo de esto: En el año 2006 hubo un gran problema en los EE. UU. Un brote de E-Coli comenzó a extenderse y el culpable fue la espinaca. Además, afectó a 199 personas, y entre ellos, había 22 niños menores de 5 años. Además, 31 de esas personas desarrollaron algún tipo de problema renal, y 3 de ellos murieron.

Entonces, la comercialización de espinaca se detuvo completamente. Al final, le tomó a la FDA²⁹ un total de 2 semanas seguidas encontrar la fuente, y durante estas dos semanas, toda la industria se mantuvo cerrada. La fuente provino de un solo proveedor y un lote. Durante esta investigación todo el sistema se detuvo y muchos productores se quedaron sin dinero.

Es por eso que el sistema necesita una transparencia total. Por lo tanto, es fácil descubrir la fuente del problema antes que todo lo demás se vea afectado.

Un mecanismo de seguimiento adecuado recorrería un largo camino en la cadena de suministro.

En nuestro caso no es un producto de este tipo; pero una falla de una materia prima que compone un tablero eléctrico o una simple termomagnética o disyuntor puede ser también muy peligroso con consecuencias económicas difícilmente posibles de prever. Podemos atenuar problemas de calidad trabajando mediante herramientas lean como puede ser Poka-Yoke³⁰; pero este tipo de herramientas difícilmente pueden detectar una falla o adulteración

²⁹ FDA: La FDA es la agencia del gobierno de los Estados Unidos responsable de la regulación de alimentos, medicamentos, cosméticos, aparatos médicos, productos biológicos y derivados sanguíneos

³⁰ Poka-Yoke Un *poka-yoke* (en japonés, ポカヨケ; literalmente, «a prueba de errores») es una técnica de calidad que se aplica con el fin de evitar errores en la operación de un sistema. Por ejemplo, el conector de un USB es un *poka-yoke*, puesto que no permite conectarlo al revés.¹ Algunos autores manejan el *poka-yoke* como un «sistema a prueba de tontos» (*baka-yoke*, en japonés) que garantiza la seguridad de la maquinaria ante los usuarios y procesos y la calidad del producto final. De esta manera, se evitan accidentes de cualquier tipo. Estos dispositivos los introdujo el ingeniero Shigeo Shingo en la empresa Toyota en la década de 1960, dentro de lo que se conoce como sistema de producción Toyota. Aunque con anterioridad ya existían *poka-yokes*, no fue sino hasta su introducción en esa empresa cuando se convirtieron en una técnica común para el control de calidad.

Shingo afirmaba que la causa de los errores estaba en los trabajadores y que los defectos en las piezas fabricadas se producían porque no se corregían. Consecuente con tal premisa, cabían dos posibilidades u objetivos a lograr con el *poka-yoke*:

de una materia prima a excepción que la misma sea lo suficientemente evidente. Es imposible evitar que se vendan productos sustraídos por otros medios de ventas que impiden garantizar la calidad final del producto. En un proceso de manufactura como el caso de estudio, estos costos que se incurren para la detección y contención son los denominados costos de la calidad, estos pueden clasificarse:

COSTOS DE CONFORMIDAD

Costos de prevención

Costos de evaluación

COSTOS DE NO CONFORMIDAD

Costos de falla interna

Costos de falla externa

Y dentro de estos podemos discriminarlos de acuerdo a la siguiente tabla:

-
- Imposibilitar de algún modo el error humano; por ejemplo, los cables para la recarga de baterías de teléfonos móviles y dispositivos de corriente continua solo pueden conectarse con la polaridad correcta, siendo imposible invertirla, ya que los pines de conexión son de distinto tamaño o forma.
 - Resaltar el error cometido de tal manera que sea obvio para quien lo ha cometido. Shingo cita el siguiente ejemplo: un trabajador ha de montar dos pulsadores en un dispositivo colocando debajo de ellos un muelle; para evitar la falta de este último en alguno de los pulsadores, se hizo que el trabajador cogiera antes de cada montaje dos muelles de la caja donde se almacenaban todos y los depositase en una bandeja o plato; una vez finalizado el montaje, el trabajador se podía percatar de inmediato del olvido con un simple vistazo a la bandeja, algo que resulta imposible si se observa la caja donde se apilaban montones de muelles.

Este sistema radica en lo sencillo y en lo simple. Hace énfasis en la realización de cosas obvias en las que detecta errores o evitan que se cometan. El objetivo final es concretar un proceso o terminar un producto sin la posibilidad que exista un defecto.

COSTOS DE CONFORMIDAD	
Costos de prevención	Costos de evaluación
Planificación e ingeniería de la calidad	Inspección y ensayo de productos, materiales y servicios consumidos
Revisión de nuevos productos	Calibración de los equipos de prueba
Ingeniería de diseño de productos y procesos	Auditorías
Control de procesos	Control de la documentación
Entrenamiento	Control de artes
Adquisición y análisis de datos para la calidad	Inspección final
Estudios de capacidad	Inspección de IPC
Mantenimiento preventivo	Control analítico
Desarrollo y puesta a punto de técnicas	Evaluación rutinaria del personal
Inventario de mercadería	Inspección de prototipos
Pronósticos	Inspección de recepción (incluye muestreo)
Descripción de tareas	Inspección de despacho
Análisis de mercado	Inspección y test de ensayos
Documentación	Tests en equipos de mantenimiento
Ensayos con prototipos	Informes de inspección
Capacitación en GMP	
Ingeniería de materiales	
Encuestas	
Estudios de movimientos y tiempos	
Evaluación y selección de proveedores	
Incentivos para la calidad	
COSTOS DE NO CONFORMIDAD	
Costos de falla interna	Costos de falla externa
<i>Scrap</i> y su aceptación	Respuesta a las quejas
Trabajos repetidos	Productos y materiales devueltos
Ensayos repetidos	Costo de la garantía
Análisis de fallas	Costos de la responsabilidad legal
Disminución de rendimientos	Costos indirectos
Accidentes	Falta de satisfacción del paciente
Corrección de errores contables	Notas de crédito hacia el cliente (Droguería)
Rotación del personal	Equipo adquirido por el cliente fuera de uso
Cambios desde Ingeniería	Costos de instalación no previstos en el contrato de compra (equipos hospitalarios)
Paradas de máquina	Sobrestock por falta del producto en el mercado farmacéutico
Sobrestock	Gastos de traslado (Medicación trasladada al Interior del país)
Sobreconsumo por manejo del material	Revisión por fallas en el uso por el paciente
Obsolescencia debida a cambios de diseño	Reparación posventa
Horas extras (sobresueldos)	Costos de distribución de productos devueltos
Rediseño	Pérdidas por ventas menores (Calidad - Precio)
Reparaciones	Ejecución de la responsabilidad sanitaria
Repetición de controles	Pérdida de <i>market share</i>
Selección de entidades conformes	Obsolescencia del producto por mejoras en el diseño (o forma farmacéutica)
Reprogramación	Sobrefacturación al cliente
Repetición de análisis	Concesiones de precio
Margen de contribución perdido por mala calidad	Errores en la facturación
Repetición de mecanografiado de documentos por fallas	<i>Recalls</i>
Ficheros de entradas tardías	Las 5 R
Cambios de diseño por fallas anteriores	Visitas por reclamos de clientes
	Entrenamiento postservice por reclamos

Figura 24 - Costos de Calidad

Se trabaja normalmente con modelos económicos de calidad:

EL MODELO TRADICIONAL DE LOS COSTOS DE LA CALIDAD

El modelo tradicional de los CC supone un compromiso entre dos categorías de costos:

Mientras que los costos de fallas internas y externas (la primera categoría) disminuyen con el incremento del porcentaje de conformidad de los productos, los costos de evaluación y prevención (la segunda categoría) aumentan cuando se busca lograr un porcentaje de conformidad mayor. Estas relaciones se presentan gráficamente en la siguiente figura:

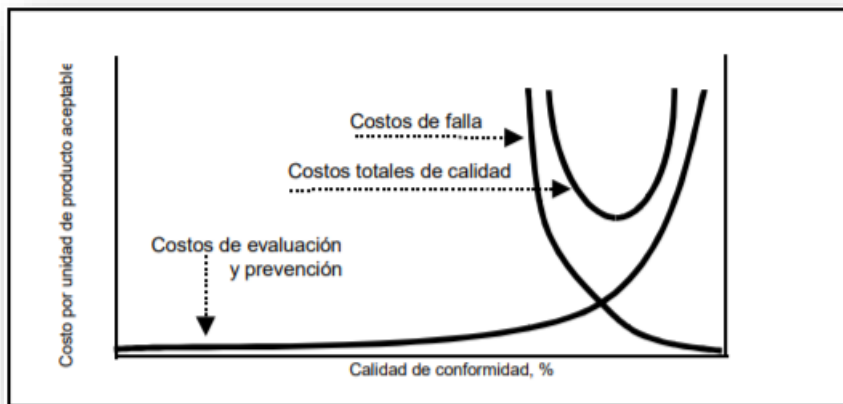


Figura 25 - El modelo tradicional de los CC. Fuente: Rao et al. (1996)

Se observa en la figura que existe un punto mínimo para los costos totales de la calidad. Ese extremo se verifica para algún valor de la calidad de conformidad menor que el 100%. Para valores bajos de calidad de conformidad, ésta se puede incrementar significativamente con pequeñas inversiones en prevención y evaluación. Sin embargo, al acercarse la conformidad al 100%, los costos de prevención y evaluación tienden a infinito. Por el contrario, los costos de falla disminuyen gradualmente, hasta alcanzar un valor nulo, cuando la conformidad se acerca al 100%.

El modelo sugiere que la excesiva perfección es demasiado cara, y que el gerente debe buscar el nivel de calidad en el cual los costos de prevención y evaluación igualen a los costos de fallas externas e internas. En el área de acondicionamiento del laboratorio, el modelo tradicional se utilizó en las primeras reuniones de capacitación para inducir al personal a pensar en términos de compromiso entre distintos tipos de costos. La dificultad principal del modelo, en términos de su utilización con el personal operativo, es su relativo nivel de

abstracción.

EL MODELO EMERGENTE

El "modelo emergente de los CC" es una derivación del modelo tradicional y, al igual que éste, presta atención exclusiva a los costos de conformidad y no conformidad; es decir, a los estándares. El modelo emergente, esquematizado en la siguiente figura, responde mejor a las tendencias de gestión actuales y busca superar algunas de las limitaciones del modelo tradicional

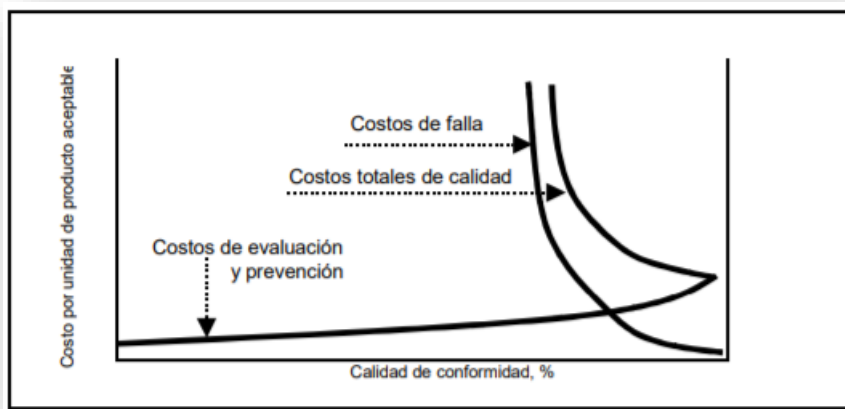


Figura 26 - El modelo emergente de los CC. Fuente: Rao et al.(1996)

Se destacan los siguientes aspectos:

1. Se presta mayor interés a la prevención y evaluación, de modo de poder realizarlas aún cerca del 100% de conformidad;
2. Los costos de prevención y evaluación son relativamente proporcionales al nivel de conformidad y no se disparan cuando éste se aproxima al 100%.
3. La caída en los costos de falla interna y externa también es menos abrupta que en caso del modelo tradicional, debido a un aumento en la fiabilidad de los nuevos materiales y procesos de fabricación.
4. El menor costo de la calidad se obtiene cuando la conformidad se acerca al 100%.

Existe un término utilizado para identificar a los problemas de calidad, este es “fábrica oculta”, ”, contrapuesta a “la fábrica visible”. Esta última es la fábrica productiva, eficiente, mientras que la primera es el derroche de recursos debido a problemas de calidad. La fábrica oculta siempre existe; aunque su magnitud varía según la industria y las categorías de costos consideradas, como se muestra en la siguiente tabla . Los porcentajes indicados son representativos de numerosas industrias.

Categoría de los costos de calidad	Porcentaje del total
Prevenición	0-5
Evaluación	10-50
Fallas internas	20-40
Fallas externas	20-40

Tabla 2 - Magnitudes relativas de los CC según sus diversas categorías

Se observa que en general los costos de prevención son menores que los de otras categorías, y que existe una amplia gama en la inversión en actividades de evaluación. Por otra parte, las fallas ocasionan una importante carga a la empresa. Una primera observación consiste en recomendar el incremento de los costos de prevención. En cuanto a las demás categorías de costos, su reducción se dará como consecuencia de las mejoras de los sistemas derivadas de la inversión en prevención. Particularmente si no se ha realizado ningún esfuerzo sistemático de control y mejora, es posible reducir los CC en un 50 % o más a través de un proceso de control de CC acompañado de un programa de mejora.

La gestión de los CC no es, entonces, un fin en sí mismo ni busca generar simples registros contables, sino que debe orientarse a detectar y aprovechar oportunidades de mejora en los procedimientos utilizados. Detrás de cada falla hay unas pocas causas raíces, en principio evitables, que deben encontrarse y resolverse, dado que la prevención tiene un gran poder de apalancamiento.

Para que los programas de control de CC no fracasen, la experiencia sugiere tener en cuenta las siguientes recomendaciones:

- Atacar directamente los fallos internos, fijándose como objetivo el “cero defecto”.

- Recordar la importancia del apalancamiento de las actividades de prevención y destinarles toda la importancia posible, en tiempo y dinero.
- Evaluar continuamente los sistemas utilizados y sus resultados, y reorientar los esfuerzos de prevención para conseguir más mejoras.
- A medida que la prevención va mostrando resultados positivos, ir reduciendo gradualmente los costos de evaluación.
- Tratar a los CC como una herramienta de control de gestión, que permita detectar oportunidades de mejora, y no como un elemento del sistema contable; se debe evitar la búsqueda de la perfección en la precisión de los datos.

Blockchain, conjuntamente con IoT, brindan una herramienta única para mejorar los CC ya que toma el proceso como uno solo, independientemente de los proveedores, intermediarios y demás que puedan intervenir en este. Más allá de las funciones logísticas más “tradicionales” como un control automatizado de stock incluyendo los almacenes de tránsito, una vez la mercancía sea recepcionada será posible conocer, por ejemplo, si ha sufrido oscilaciones de temperatura, humedad, sacudidas o cualquier alteración en su manipulación que supere las especificaciones de calidad vinculadas al producto.

Un ejemplo gráfico de esta trazabilidad, sería el siguiente:

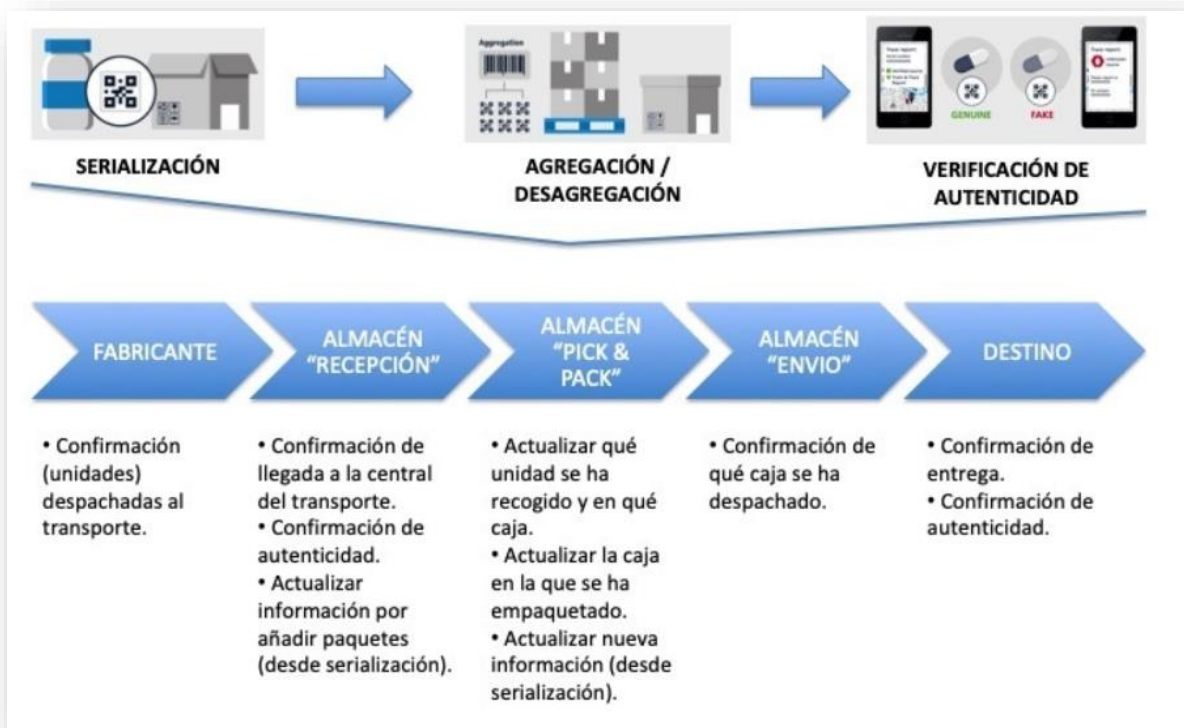


Figura 27 - Trazabilidad con Blockchain

11.7) Resumen

Se puede determinar que existen características de Blockchain que son de gran utilidad en Logística, a saber:

1.- Reducciones de Inventario y Almacenamiento

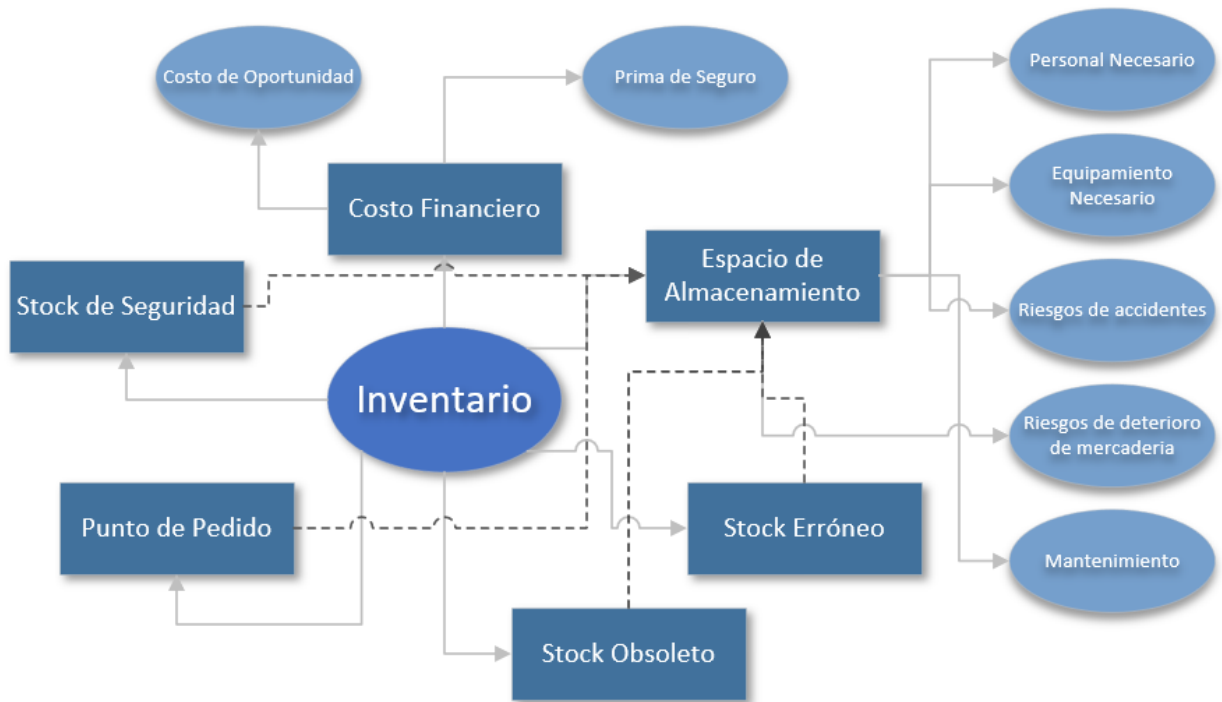


Figura 28 - Inventario

Inventario

Los inventarios representan recursos monetarios inmovilizados, ya que para producirlos o adquirirlos es necesario incurrir en costos de materiales, mano de obra y otros insumos y servicios que representan dinero, este costo representa entre 1,5 y 2% anual por inmovilización de fondos.

Por otra parte, los inventarios llevan implícito un costo de oportunidad, debido a que los fondos utilizados en los mismos, no deben destinarse a corto plazo a otros requerimientos financieros de las empresas.

Es por ello que deben administrarse eficientemente a fin de que la inversión en los mismos no llegue a niveles que sean excesivos, ni tampoco que sean reducidos a tal grado que ponga a las empresas en peligro de reducir los volúmenes de producción y venta o en el peor de los casos suspender la actividad productiva en su totalidad.

El buen manejo de dos posiciones totalmente opuestas, el exceso de recursos inmovilizados versus el riesgo que representan inventarios reducidos, se logra mediante una administración técnica de las existencias.

En todas las empresas se necesita por una parte, de la inversión en inventarios para poder realizar el proceso productivo con flexibilidad, y por la otra, lograr satisfacer adecuadamente la demanda. Es por ello, se debe tratar de lograr una eficiente Gestión de Stock, que permita el equilibrio entre la inmovilización de recursos y el riesgo de paralizar la producción y venta.

Dentro de los parámetros que conforman el inventario se pueden destacar ahorros en los siguientes:

Stock de Seguridad

El stock de seguridad es uno de los componentes del inventario total que más impacto tiene en el caso de estudio ya que por la distancia con los fabricantes (mayormente provenientes de China y Europa), la incertidumbre aduanera y la necesidad de asegurar un excelente nivel de servicio al cliente genera que los niveles sean altos.

En el caso de estudio la composición del inventario total es de 80% materia prima importada y solo el 20% materia prima local, de este último porcentaje, solo un 5% es de fabricación netamente nacional. Esto explica la poca flexibilidad existente y el alto nivel de inventario. La decisión sobre el mix de productos nacionales o importados no es de cada filial, sino que existe obligación de abastecerse con productos propios y muy excepcionalmente estos pueden reemplazarse por productos de origen nacional.

No existe una política universal sobre la administración del inventario, dependerá de la estrategia de cada empresa.

La fórmula utilizada por la compañía en estudio es $SS = (k * v * \sqrt{D} * FDU) + x * FDU$

SS = Stock de Seguridad

k = coeficiente basado en la experiencia del operador

v = coeficiente que depende del nivel del servicio requerido

x = coeficiente basado en la performance del proveedor

FDU = previsión diaria de utilización

D = Tiempo de entrega del proveedor

Un ejercicio realizado con datos reales del caso de estudio es una simulación sobre el Stock de Seguridad. El mismo está establecido en 700.000 USD, si solo modificamos la variable k y mantenemos las restantes ceteris paribus, la sola reducción de la variable k a la mitad, representa una reducción del 43% del valor total del stock de seguridad; es decir, 301.000 USD. Pero esta no sería la única variable que podría considerarse, ya que la mejora en la eficiencia podría inducir una reducción de las variables v , x y FDU. Estas últimas variables, no podrían cuantificarse con precisión actualmente, pero solo tomando un valor teórico de una reducción del 20% en cada una de las variables, el Stock de Seguridad se podría reducir un 58%, es decir; 406.000 USD.

Punto de Pedido

El punto de pedido ayuda a determinar un punto en el que tiene suficiente inventario para poder responder a la demanda mientras se espera la llegada del próximo envío. Para poder calcularlo es necesario conocer:

La demanda de tiempo de entrega: se obtiene al multiplicar el tiempo de entrega por las ventas diarias promedio

El stock de seguridad: es la diferencia entre la demanda máxima de tiempo de entrega y la demanda promedio de tiempo de entrega

Una vez se hallan estos dos factores, la suma de ambos da como resultado el dato que desvelará la clave de una gestión de compras óptima, el punto de pedido.

Punto de pedido = demanda de tiempo de entrega + stock de seguridad

Para ser competitivo hay que ser capaz de ofrecer un nivel constante de producto y servicio a los clientes y para eso hay que conseguir el equilibrio entre el exceso de existencias y el desabastecimiento. El cálculo del punto de pedido ayuda a lograrlo, aunque hay que tener en

cuenta que, como sucede con las variables de las que depende, puede cambiar a lo largo del tiempo, por lo que se recomienda actualizarlo con frecuencia.

El grafico típico de punto de pedido es:

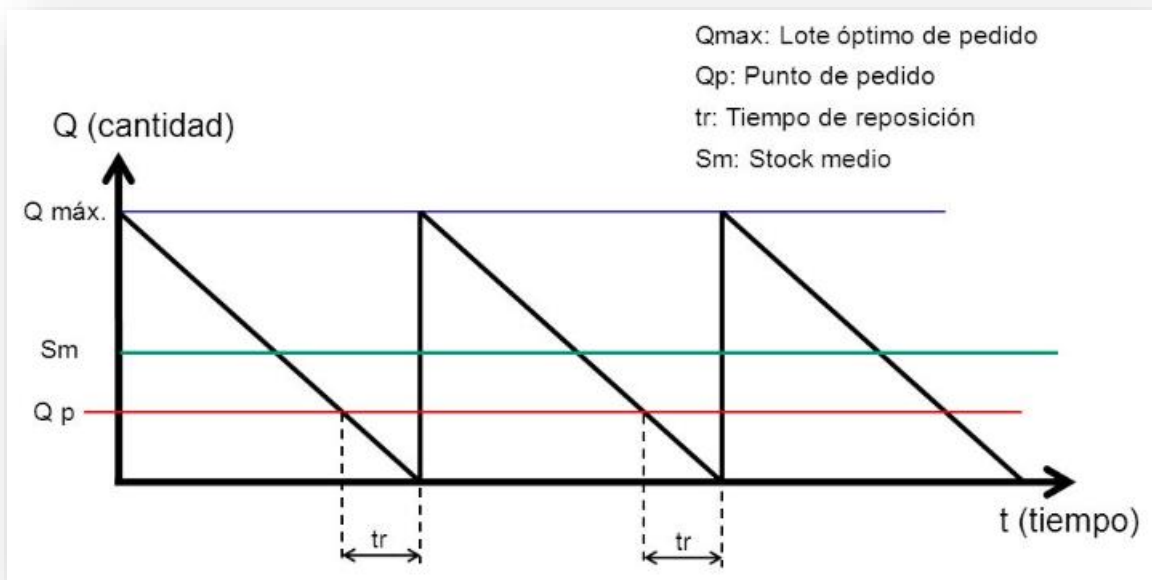


Figura 29 - Punto de Pedido

Por lo tanto; la intención al aplicar la tecnología es lograr reducir el serrucho que está representado a la mínima expresión posible sin afectar el servicio al cliente.

Reducción del Costo Financiero por Tenencia del Stock

Solo por la tenencia de stock en almacén se incurren en costos evitables, el más representativo es sin dudas el costo del capital inmovilizado que podría destinarse a otras inversiones y asociado a la simple tenencia. A menudo se considera que equivalen al 25% del valor anual del producto, aunque hay autores que afirman que pueden oscilar entre 12% y 34%. Esto incluye los gastos financieros, seguros, alquileres, otros gastos variables y lo que se denomina costos del riesgo (obsolescencia por ejemplo).

Reducción de Stock Obsoleto

Otra posibilidad que podría evaluarse es la reducción de la obsolescencia, esta representa actualmente un 8% del stock total, pero solo suponiendo que se podría mejorar un 2%, la reducción podría ser de 130.000 USD al año.

Reducción de Stock Erróneo

También se puede inferir una reducción del 5% del valor del stock que se adquiere por error. Denominamos error a la simple equivocación del operador por datos erróneamente cargados en el sistema o también porque el stock que se ha adquirido para un proyecto puntual, ya no es necesario cuando el mismo ingresa (por caída del proyecto o modificaciones en el alcance). El total promedio mensual del stock es de 6.500.000 USD, la reducción podría ser de 325.000 USD al año.

Reducción del Stock Total

La precisión en la información y trazabilidad brindarían la oportunidad de reducir inventarios debido a que se podrían mejorar los plazos de entrega de los proveedores y se evitarían excesos de stock a causa del tiempo que el mismo permanece en depósito hasta su consumo. Tomando una reducción de solo 10% del stock total por la mejora de todos los procesos asociados a la implementación de Blockchain, obtendremos una reducción de 561.000 USD durante el año.

Reducción de espacio de almacenamiento

Tener stock obsoleto, exceso de stock o materia prima con baja rotación, además de generar un costo financiero genera una necesidad de mayor volumen de espacio requerido, a veces este puede conseguirse internamente y el costo es absorbido por el costo total de las instalaciones, pero a veces el espacio interno no es suficiente y se requiere tercerización logística. Esto implica no solo el costo de mudar la materia prima, sino también el costo de transporte para movilarla.

En el caso de estudio, el costo por esta tercerización logística, incluidos todos los costos de almacenamiento, ingreso y egreso de mercadería y transportes necesarios para llevarla o retirarla, representa un costo anual de 140.000 USD anuales. Además; el exceso de stock

provoca sobrecostos varios, ya sea por la necesidad de mover los mismos, realización de inventario o aumento de roturas de los productos. Siempre existen costos denominados “ocultos” en la logística con operadores tercerizados, son estos costos que no se identifican con claridad porque exceden la normal operación (ej. Ir a buscar un solo material de manera urgente).

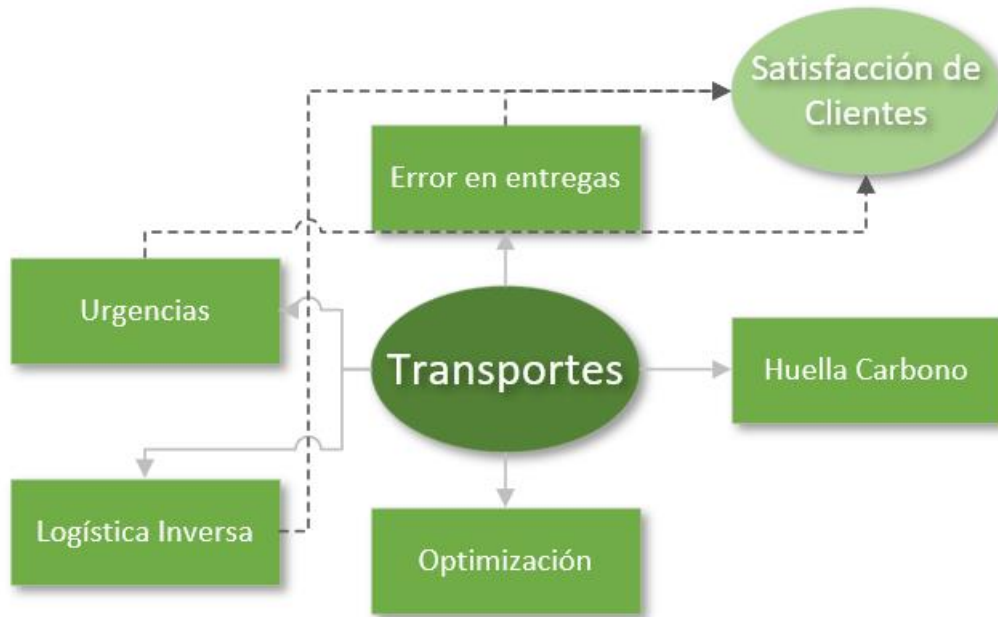


Figura 30 - Transportes

Reducción en Transportes por error en entrega / devoluciones

La logística inversa que se requiere para solucionar errores de entregas o devoluciones por temas de calidad en el producto es una de las más costosas en el transporte, ya que no siempre puede optimizarse y aprovecharse los recorridos habituales.

En la compañía de estudio, esto representa el 12% del total de costos de fletes en el cual se incurre, resultando en un costo anual de 15500 USD.

Esto es solo por movilizar los transportes, no se puede calcular con precisión el costo por mala calidad de servicio.

Reducción en Transportes por necesidades urgentes de fabrica

Otro de los sobrecostos en los cuales podrían obtenerse reducciones es por las compras realizadas para solucionar problemas de rupturas de stock o cambios en el programa de producción. Esto requiere que se deban conseguir transportes que retiren mercaderías de proveedores no habituales, a su vez, estos proveedores no tienen acuerdos de precios; por lo tanto resultan en mayores costos de adquisición y generan que el precio promedio del inventario se eleve cuando entran en el cálculo los nuevos valores.

El costo de fletes que se utiliza para esto es de 6500 USD al año

Base estadística de Transportes

Mediante el uso de la tecnología se podría tener un registro del histórico de los destinos, volumen de mercadería transportada, tiempos de esperas, falsos fletes y toda la información inherente al movimiento de los transportes. Con esta base de información sería factible una mejor negociación de contratos a futuro además de la optimización del transporte y mejora en el problema de la capilaridad existente para eficientizar lo que se denomina el problema de la última milla.

Huella de Carbono

Tal vez aun no sea un motivo representativo en nuestro país actualmente, pero la necesidad de reducir gases de efecto invernadero está cobrando cada vez más importancia en el mundo, y más temprano que tarde, será condición sine qua non para poder ser proveedor de grandes compañías. La reducción de las emisiones en el transporte no solo puede ser a través de motores más modernos, sino también con la optimización de los transportes y cargas. (Telam, 2018)

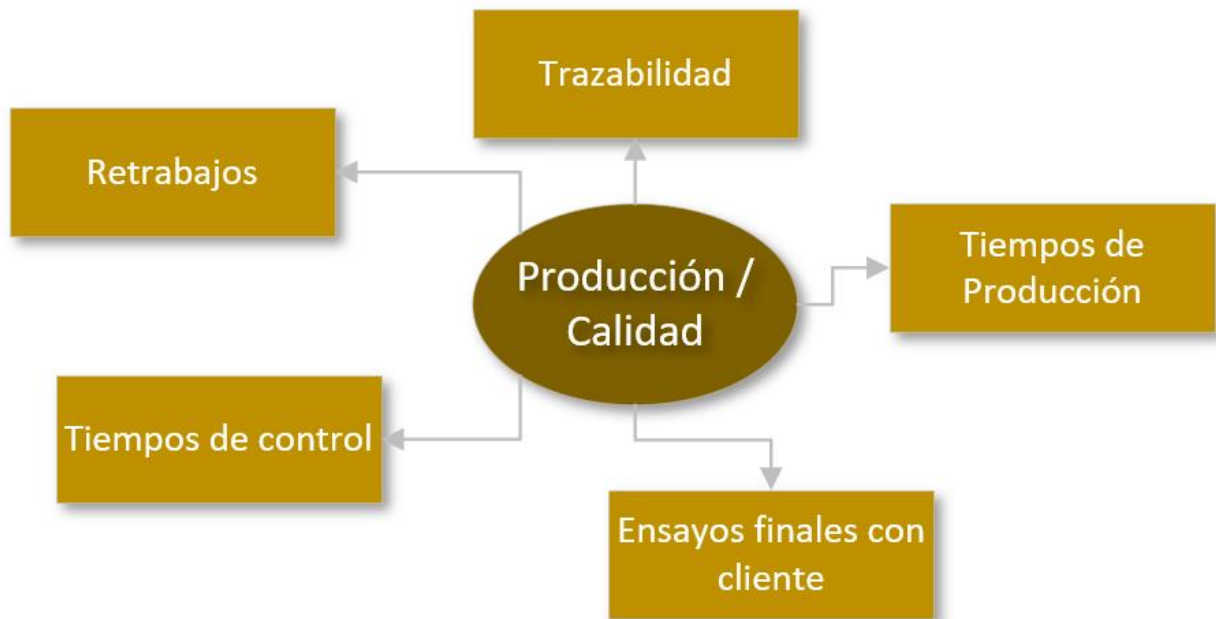


Figura 31 - Producción - Calidad

Mejora en la productividad y en la calidad

Al existir trazabilidad absoluta, los posibles fallos por calidad pueden detectarse en instancias muy tempranas, incluso antes de ingresar el producto al almacén. Esto implica que todo el costo de calidad en el proceso y control de calidad final serían mínimos. En el caso de estudio, este costo implica utilización de personal para control de recepción de mercaderías, personal de control de calidad durante el proceso y personal de control de calidad final del producto. Además de una reducción de los días del ciclo productivo se evitarían los retrabajos innecesarios, mermas y rechazos de productos semi elaborados.

Este costo está separado en diferentes instancias:

Personal directamente afectado a la calidad: 160.000 USD al año

Reducción de 5 días en el proceso productivo, trasladable a una mejora en los plazos de entrega a los clientes

Reducción de rechazos o retrabajos: En este caso tomaremos que se reduce un 70% el costo de mano de obra y materia prima que se destina a estos procesos. Actualmente el total de horas utilizadas para esto es proporcional a la de 5 personas por año, representando un ahorro anual estimado de 70.000 USD

Pérdida de clientes por demoras en entrega o entregas con problemas de calidad

Existe un costo difícil de evaluar pero existente, el costo que tiene la pérdida de clientes por incumplimiento del contrato, sea este por demoras en la entrega o por mala calidad del producto entregado. En compañías de la envergadura del estudio de caso, no son clientes “simples”, sino que son los distribuidores de energía más importantes del país, grandes petroleras, etc. Para ganar estos clientes no solo es necesario el respaldo de la marca y la calidad, sino que se requiere en muchos casos un trabajo muy fuerte de prescripción.

En este, una estimación conservadora podría ser que esta pérdida representa el 2% de la facturación anual, la cual asciende a 120.000.000 USD; es decir, 2.400.000 USD. Generalmente un cliente que se pierde, es difícilmente recuperable por mucho tiempo, y este a su vez genera un efecto replicador sobre la reputación de la marca.

Total de reducciones estimadas:

Concepto	Monto (en USD)
Reducción del Stock de Seguridad	406.000
Reducción de Stock Erróneo	325.000
Reducción de Stock Obsoleto	130.000
Reducción del Stock Total	561.000
Reducción en Transportes por error en entrega / devoluciones	15.500
Reducción en Transportes por necesidades urgentes de fábrica	6.500
Reducción de espacio de almacenamiento	140.000
Pérdida de clientes por demoras en entrega o entregas con problemas de calidad	2.400.000
Mejora en la productividad y en la calidad	230.000

Total ahorros Posibles

4.214.000

Otros beneficios

Cliente / Proveedores

La trazabilidad; tanto para la mejora en la calidad del producto como para la mejora logística genera que la cadena de abastecimiento, conocida como supply chain pueda contar con proveedores más fiables en cuanto a calidad y servicio, esta mejora y estandarización de la calidad mejora la posibilidad de homologar proveedores en nuestro país que sirvan al propósito de la compañía a nivel global, ya que el principal obstáculo que existe actualmente es el aseguramiento de la calidad de los mismos.

Con proveedores locales fiables y eficientes lograr una exitosa implementación de Just In Time (JIT) es posible, esta mejora de los procesos permite trabajar con muy poco stock propio logrando ahorros en todos los aspectos logísticos. Esto sería posible a través de implementaciones diferenciadas de cadenas de bloques o conteniendo a los proveedores en una cadena de bloques propia. JIT sumado a Blockchain acercaría posiciones de interés entre las partes mejorando la calidad, trazabilidad, velocidad como así también la liberación de pagos una vez que se cumplan los hitos declarados en el contrato inteligente. Actualmente este tipo de proceso es casi exclusivo de grandes automotrices que logran este cometido acercando en muchos casos al proveedor a la propia planta del fabricante (Alonso, 2019). Blockchain, conjuntamente con otras tecnologías asociadas podría mejorar los procesos “lean manufacturing” tal como los conocemos ya que se reemplazarían muchas de las ejecuciones manuales que se realizan actualmente por automatizaciones.

Pero para que funcione esta sinergia el beneficio no puede ser unilateral, y es por ello que la relación cliente / proveedor está en continuo proceso de mejora relacional. Los clientes comenzaron a entender que no se puede tener una compañía exitosa con proveedores que no lo son. Sin dudas el caso más representativo en Argentina es el de Toyota con la integración de sus proveedores en la nueva plataforma de la Toyota Hilux. Toyota entendió que para lograr un JIT que funcione y que además tenga los estándares más altos de calidad, debía no solo contratar proveedores, sino además capacitarlos y facilitarles todo lo necesario para que

sea una relación donde ambas partes ganen. Los sistemas informáticos colaboran cada vez más en que la relación sea aún más estrecha, actualmente los clientes pueden enviar previsiones, ciclos de vida de los productos y mucha más información directamente a sus proveedores a través de un sistema ERP posibilitando a los proveedores administrar de forma más eficiente su capacidad y calidad.

Blockchain podría ir un paso más allá en la integración cliente / proveedor garantizando la inmutabilidad de la información entre las partes, reduciendo tiempos de gestión de la información a través de la automatización lograda con Smart Contracts. En definitiva, lograr proveedores más eficientes es garantizar que los costos sean los acordados al proceso y no se agreguen las improductividades al costo y la calidad esté garantizada continuamente, pudiendo delegar la calidad al proveedor y reducir costos de control de recepción en el cliente.

Reducción de riesgos

La automatización en la gestión de inventarios a través de Blockchain permitirá minimizar errores típicos en la gestión a saber:

- **Comunicación:** Sin dudas es el mayor problema que genera excesos de inventario o rupturas de los mismos (efecto látigo). Normalmente hay un divorcio comunicativo entre ventas, logística y compras. Si bien para mejorar esto es necesario que los objetivos estratégicos sean transversales y no diferenciados por sector, la calidad de la información y la comunicación de la misma mediante blockchain será indiscutible.
- **Cuellos de botella:** La administración eficiente de recursos requiere que la información sea fiable. Conocer cuando y cuanta mercadería recibiremos o debemos despachar, permitirá que se puedan tomar las acciones necesarias para mejorar la elasticidad.
- **Demanda:** Uno de los grandes errores que se cometen es desconocer estacionalidad o ser poco reactivo ante un cambio de la demanda. Las nuevas tecnologías trabajando en conjunto nos permite asociar información de varias fuentes para predecir y actuar rápidamente ante estos cambios.

- **Información:** Sin información es imposible mejorar, la posibilidad de centralizar información para tener indicadores que sean funcionales es otra de las ventajas que podremos obtener.

2.- Garantía de calidad y evitar falsificaciones

Cuanto más se puede anticipar el problema, menores serán los costos en los cuales habrá que incurrir para solucionarlos.

La tecnología blockchain permite que la información sea veraz. De hecho, es prácticamente imposible manipularla debido a su registro en diferentes bloques de información descentralizados. La logística se beneficia de este punto, puesto que así garantiza la calidad de sus servicios y productos.

Además, la capacidad del blockchain de controlar los stocks promueve que no se distribuyan productos falsos. Y, de ser así, poder identificarlos fácilmente.

3.- Ethical sourcing

Gracias al blockchain la empresa es capaz de certificar cuáles son sus proveedores y cuál es el origen de los materiales que éstos utilizan. De esta forma, la empresa puede demostrar, de cara al cliente, que utiliza fuentes de origen éticas y no, por ejemplo, producciones bajo condiciones extremas en países en vías de desarrollo. Este tema tomo real dimensionamiento cuando en 2013 un edificio donde funcionaban talleres textiles para las compañías más importantes del mundo se derrumbó y comenzó a evidenciarse las condiciones laborales a la que estaban expuestos los trabajadores. (*Mundo, 2013*)

4.- Ahorro de costes con smart contracts (reducción de personal, automatización, mayor agilidad y eficiencia)

El concepto de smart contracts es el de una herramienta de software, un código ejecutable, que se implementa en cada uno de los bloques de la cadena. Por la arquitectura propia del blockchain se verifica al momento, sin la necesidad de más agentes implicados y con la reducción de coste que ello supone.

De forma más concreta, un smart contract es un software que se ejecuta en cada uno de los nodos de una red blockchain, de modo que, debido a las características del blockchain, el

contrato se verifica dentro de un modelo de confianza distribuida, sin la necesidad de un tercero. Ethereum, es la red de referencia que soporta smart contracts en su plataforma basada en blockchains.

Un ejemplo de smart contract en el mundo de la logística sería uno aplicado a la recepción de mercancías. Cuando se procede a verificar que toda la mercancía recibida está en buen estado y es la correcta, el smart contract, de forma automática, se ejecuta, liberando así el importe al distribuidor.

5.- Sistema de Registro Transparente

Blockchain en la cadena de suministro ayuda a ofrecer un acceso más transparente en cada operación en la cadena de suministro. Además, cada vez que un producto va del punto A al punto B, se guardará en el registro. Entonces, en resumen, crearía un camino desde donde el precorte llegó del punto A al punto B. Además, las empresas pueden usar esto en caso de un reclamo.

Por otro lado, al usar esto, los clientes sabrán exactamente dónde llegó el producto y, finalmente, será una plataforma transparente. También ayudará a que otras personas sean responsables de cualquier error que puedan haber cometido en el registro.

6.- Seguimiento en Tiempo Real

Con la transparencia viene la opción de seguimiento en tiempo real. Sí, con blockchain para la gestión de la cadena de suministro, puedes hacer un seguimiento de tus productos en tiempo real. Además, también puedes saber en qué condiciones se encuentran, e identificar exactamente su ubicación mientras se desplazan.

Por ejemplo, imagina que solicitaste materiales al proveedor, cuando el proveedor adjunta los chips RFID a los productos, sabrás exactamente en qué condición o ubicación se encuentran.

La administración de la cadena de suministro puede rastrearlo desde su PC utilizando los ejemplos de la cadena de suministro de blockchain. Además, con eso, pueden estimar cuánto tiempo les tomará a los materiales llegar a la fábrica.

Una vez que están aquí, pueden realizar un seguimiento del proceso de producción y verificar el estado del inventario cuando lo deseen. Por lo tanto, ni siquiera tendrán que intervenir

personas para saber qué sucede exactamente en la línea de producción utilizando los ejemplos de la cadena de suministro de blockchain.

7.- Transacciones Más Rápidas

Otro gran beneficio de la blockchain para el esquema de la cadena de suministro. En realidad, hay que esperar mucho para obtener el pago en diferentes niveles de la cadena de suministro. Pero con blockchain para el esquema de la cadena de suministro, sería sumamente sencillo y ágil.

Los ejemplos de la cadena de suministro de Blockchain tienen el potencial de romper el registro de transacciones de Visa cada segundo, que es de 10,547. La velocidad es una de las características lucrativas de todos los sistemas de pago y con los ejemplos de la cadena de suministro de blockchain, estás obteniendo todo en un solo lugar.

En realidad, cuanto más rápida sea la blockchain para la plataforma de la cadena de suministro, mejor podrá procesar todas las transacciones. Entonces, en resumen, blockchain en la cadena de suministro tiene el mayor potencial para escalar que el sistema Web 2.0 típico.

Otro gran dato sobre blockchain en la gestión de la cadena de suministro son las opciones de micropago. Por lo tanto, no solo estás enviando grandes cantidades, sino también cantidades más pequeñas en solo segundos.

8.- Cadena Sin Confianza

Luego viene el beneficio sin confianza de la blockchain para la gestión de la cadena de suministro. En realidad, la administración de la cadena de suministro debe confiar en que el producto sería auténtico y se entregaría en un plazo determinado. Sin embargo, con blockchain en el sistema de la cadena de suministro, puedes saberlo con seguridad.

Por lo tanto, no hay necesidad de poner tu confianza ciega en ninguna de las partes. Además, en caso de pago, muchas empresas permanecen en total incertidumbre que podrían obtener el pago. Sin embargo, blockchain en el sistema de la cadena de suministro viene con la integración de contrato inteligente. El contrato inteligente automatizará el proceso de pago una vez que se realice la entrega.

Por lo tanto, las empresas pueden simplemente tomar un respiro de toda la incertidumbre de una vez por todas.

Este proceso puede integrarse en diferentes niveles de la cadena de suministro. Por ejemplo, los proveedores pueden usarlo para pagar a los fabricantes, y los consumidores pueden usarlo para pagar al proveedor.

9.- Certificación de Producto

La certificación del producto es una necesidad cuando se trata de la cadena de suministro. ¿De qué otra manera puede los fabricantes probar que el producto es auténtico y no es una falsificación? Aquí es donde interviene blockchain para la gestión de la cadena de suministro. Los empleados pueden utilizar los ejemplos de la cadena de suministro de blockchain para certificar todos los productos en cada industria. Además, puede ayudar a saber si el producto fue reemplazado con una falsificación o no. Además, el consumidor puede verificar fácilmente la blockchain en la plataforma de la cadena de suministro y saber con certeza que el producto es auténtico.

Cada año se desperdician millones de dólares debido a actividades fraudulentas y productos falsificados. Sin embargo, con blockchain para la gestión de la cadena de suministro, finalmente eso terminaría.

10.- Mayor Seguridad

La cadena de suministro debe ser segura. Con la ayuda de blockchain para la gestión de la cadena de suministro, ahora puede ser extremadamente seguro. Como el registro es inmutable, nadie puede manipular los datos. Además, sus protocolos de seguridad de múltiples capas en la cadena de suministro y la blockchain mantienen a piratas informáticos más alejados que con los sistemas tradicionales.

Como resultado, no hay un único punto de entrada. Si un hacker quiere atacar la blockchain en el sistema de la cadena de suministro, tendría que atacar la red con varios dispositivos a la vez, lo cual es casi imposible. En realidad, eso requiere más recursos de los que realmente ganará, así que no vale la pena.

11.- Menor Huella de Carbono

Con la fabricación de productos llega el agregado de emisiones de carbono. Sin embargo, con la ayuda de blockchain en el sistema de la cadena de suministro, la necesidad de un retorno desaparecería o se reduciría drásticamente. Esto es básicamente por la mejora en la calidad durante el proceso que se podría lograr.

Se pueden producir entonces resultados de alta calidad de manera consistente. Por lo tanto, el proceso de devolución o reciclaje de la cadena de suministro se reduciría drásticamente. Y no solo aumentaría los ingresos, sino que también eliminaría el proceso adicional de creación de productos. En consecuencia; menos huella de carbono.

Juan Manuel Martínez Mourín, que conduce dos de los mayores proyectos españoles de esta tecnología, dio razones y datos. “El recorte de tiempo y de papel al realizar las transacciones por un sistema blockchain ahorra el 89% de los costos, y aumenta el 57% de los ingresos de las empresas. Mejora la trazabilidad y la transparencia en el entorno del 80%. Reduce los riesgos a la mitad. Crea un 44% de nuevas oportunidades de negocio”.

Junto a tan aplastantes razones, Martínez Mourín eliminó obstáculos. Habló del camino hacia la estandarización de la tecnología blockchain, que “ayudará a eliminar dudas en la industria y en los consumidores”. La disyuntiva entre qué tipo de blockchain elegir lo dejará de ser porque “la estandarización permitirá que las blockchain hablen entre sí, y que la tecnología se vuelva transparente para el usuario”. (BLÁZQUEZ, 2020)

12) REGULACION

La incertidumbre regulatoria a nivel global podría afectar la innovación blockchain y su adopción.

Esta es la preocupación constante y creciente de los actores que forman parte del ecosistema de la cadena de bloques. Si bien favorecen el establecimiento de normas básicas simples y claras, temen que la regulación afecte el desarrollo de sus proyectos.

En este sentido, no podemos negar que las autoridades —en su afán casi compulsivo de regular absolutamente todas las actividades que realizamos— afectan negativamente la innovación al generar regulaciones prematuras que, en los casos más extremos, podrían terminar por completo con una industria.

Por ejemplo, la Cámara de Comercio Digital de Estados Unidos ha publicado un llamado a la acción pidiendo a los hacedores de políticas federales que aborden y resuelvan el problema de la «falta de un entorno legal predecible» que está obstaculizando la experimentación e innovación de la cadena de bloques.

(Bolaños, 2019)

Como se indica, existe un tironeo entre los gobiernos y Blockchain, en gran medida por la presión que ejercen algunos sectores que podrían verse afectados por la implementación e incluso sería como pretender que el gobierno avale transacciones financieras fuera del sistema financiero tradicional y altamente regulado. Actualmente existe una puja entre las empresas que necesitan que se generen las regulaciones necesarias para continuar invirtiendo en esta tecnología y las empresas que pueden ser afectadas y los propios gobiernos que son reticentes (mayormente por el desconocimiento), sobre el riesgo que esta tecnología puede acarrear. *(Orcutt, 2019)*

- Es evidente que aún se continúa necesitando un consenso que permita la utilización de Blockchain; pero para que esto suceda se requiere:
- Creación de un marco legal nacional e internacional
- Entrenamiento de legisladores, reguladores y cortes
- Cuestiones jurisdiccionales y de derecho aplicable.
- Creación del estatuto jurídico de las DAO como entidades que esencialmente actuaran como entidades de software autónomo que se dedicaran a facilitar el comercio
- La aplicabilidad legal de los contratos inteligentes

Adicionalmente, el potencial para el anonimato en algunos libros de contabilidad en línea puede complicar el cumplimiento de la legislación contra el lavado de dinero, regulación fiscal, mientras que las leyes de protección del consumidor deben ser revisados tal como fueron en su momento inventadas ante el aumento del comercio electrónico.

- Empresas protegidas (Protect Cell Companies) - Documentación comúnmente utilizado para establecimiento de resguardos en mano las compañías de seguros,
- Carta de Crédito (LOC) - Protección a las Cartas de Crédito (LOC) que los bancos, aseguren que un vendedor recibirá un pago, hasta el monto de El LOC

- Regulación a la desconfianza de la tecnología relacionada con Bitcoin debido a connotaciones criminales
- Marco regulatorio a la privacidad y seguridad de datos en bloqueos públicos
- Problemas de compatibilidad de software

Existen algunas regulaciones que ya han comenzado a desarrollarse en algunos países; pero aún son muy pocas para la necesidad completa (Zigurat, 2020) (Yafimava, 2019)

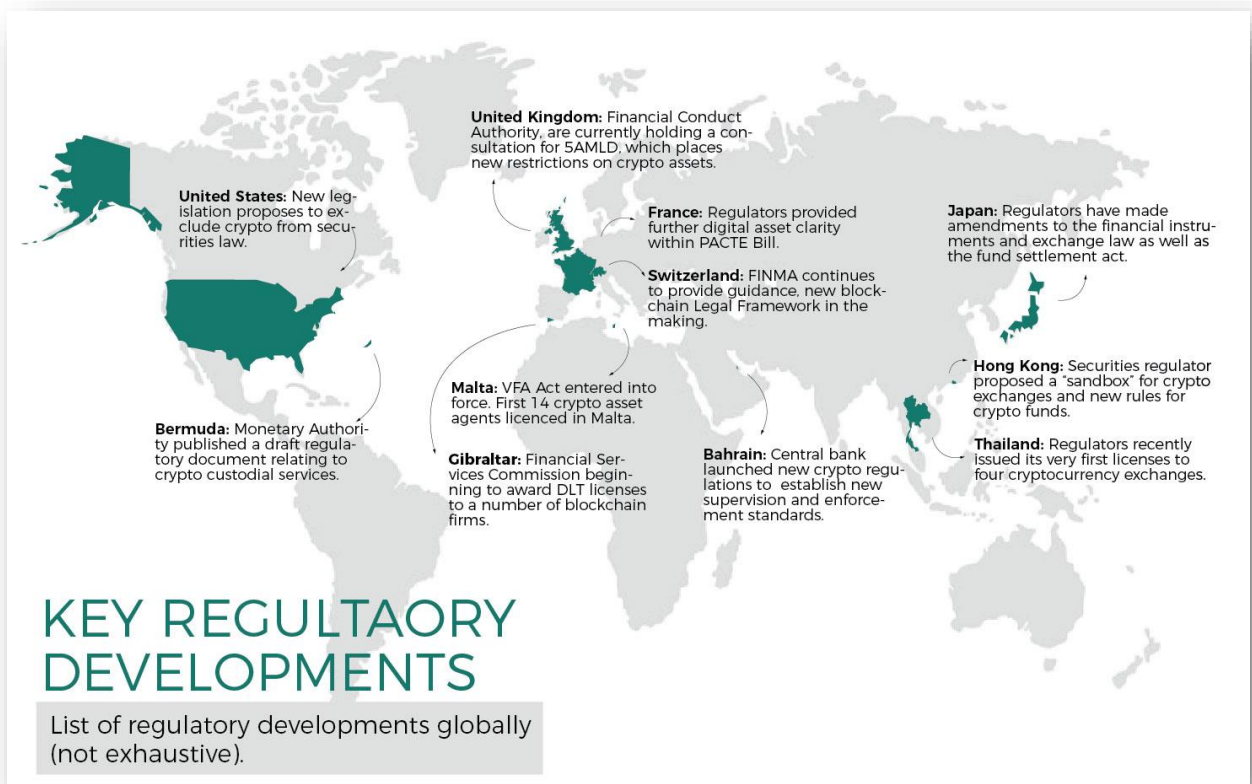


Figura 32 - Regulaciones desarrollándose

Tenemos que ser conscientes que la tecnología aún es muy nueva, BiTA (Blockchain In Transport Alliance), estima que la madurez de Blockchain se dará a partir del año 2026, donde actualmente atravesamos un ciclo de aprendizaje y adopción temprana sobre algunos casos de estudios, y a medida que esto sucede se van generando las regulaciones que permitan un completo desarrollo de la tecnología.

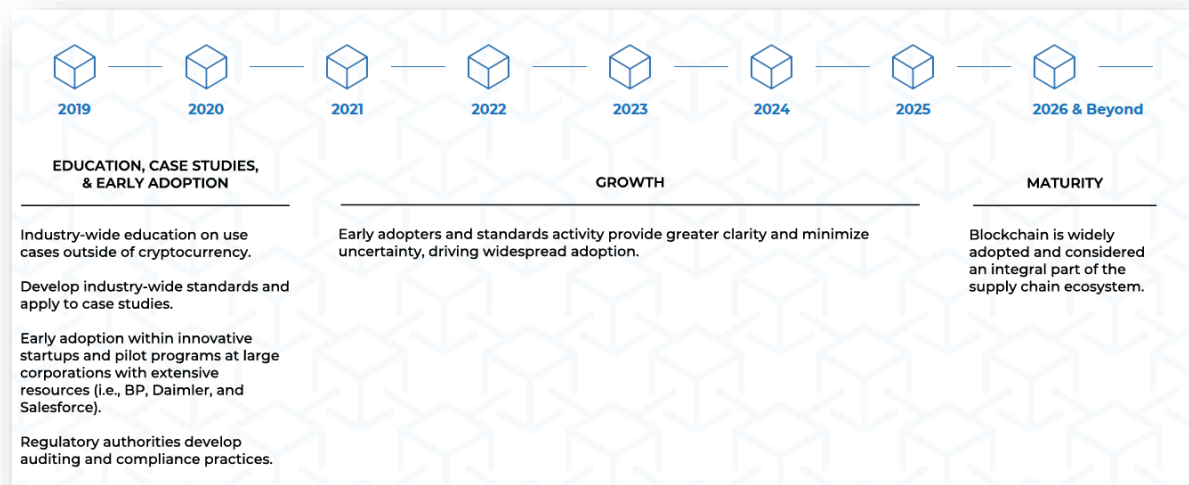


Figura 33 - Adopción Estimada de Blockchain

13) GLOSARIO

Altcoin. Toda criptomoneda que no sea el Bitcoin. Las altcoins más importantes son el Ether, Ripple, Litecoin, Monero, Zcash y Dai.

Bitcoin. La primera criptomoneda basada en tecnología blockchain. El paper fue publicado bajo el seudónimo de Satoshi Nakamoto el 31 de octubre de 2008. La red entró en funcionamiento el 3 de enero de 2009.

Blockchain. Registro compartido entre múltiples computadoras donde las transacciones se registran en bloques unidos con una cadena criptográfica.

Bloque. Paquete de datos que contiene transacciones que se registran en el blockchain.

Comisión de Transacción. Comisión que es pagada a los mineros para procesar una transacción con criptomoneda.

Confirmación. Acto realizado por los mineros que verifica una transacción y la agrega al blockchain.

Consenso. Ocurre cuando todos los participantes de la red se ponen de acuerdo en una cadena de transacciones, lo que asegura que todos los nodos tienen una copia exacta del mismo registro.

Contrato inteligente (Smart contract). Instrucciones escritas en forma de código en una red descentralizada, que es ejecutada tras la ocurrencia de cierto evento.

Criptografía. Del griego *kryptós* (secreto) y *graphein* (escritura), es una disciplina que se ocupa de la construcción de protocolos para garantizar la confidencialidad, la integridad y la autenticidad de los datos.

Criptomoneda. Activo digital construida con tecnología criptográfica.

DAO. Una organización autónoma descentralizada equivaldría a una corporación que corre sin intervención humana y que opera a través de una serie de reglas de negocio imposibles de modificar por una sola persona.

Dapp. Una aplicación descentralizada es una aplicación open source que opera de manera autónoma y tiene sus datos almacenados en el blockchain. Son muy importantes dentro del blockchain de Ethereum.

Derechos Ad Valorem: son los tributos que gravan la importación de mercancías y que son fijados en un porcentaje sobre el valor aduanero.

Derechos Antidumping: Por regla general, la medida antidumping consiste en aplicar un derecho de importación adicional a un producto determinado de un país exportador determinado para lograr que el precio de dicho producto pueda aproximarse al “valor normal” o para suprimir el daño causado a la rama de producción nacional en el país importador

Derechos Compensatorios: Elevación de los "derechos aduaneros" para combatir y neutralizar los subsidios eventualmente otorgados por países extranjeros, a sus exportadores, tornándolas más competitivas y perjudicando de ese modo, a una rama de producción nacional de un producto nacional.

Derechos Específicos: Impuesto que grava las Importaciones o Exportaciones y que es aplicado sobre la base de alguna característica física de los Bienes y servicios, tales como su peso, medida y unidad.

Desintermediación. Proceso de reducción del uso o necesidad de intermediarios. En el contexto del blockchain, refiere a la reducción de la necesidad de terceras partes intermediarias para la validación y facilitación de transacciones.

Dirección pública. Conjunto de caracteres alfanuméricos utilizado para enviar y recibir fondos en las transacciones de una red de criptomoneda.

Doble gasto. Ocurre cuando un activo digital es gastado más de una vez.

Explorador de Bloques. Herramienta online que sirve para visualizar transacciones en el blockchain.

Firma Digital. Código digital generado por encriptación pública que se adhiere a un documento transmitido electrónicamente para verificar su contenido y la identidad del que lo envía.

Fork: Un blockchain fork, o separación de cadenas (chain split o chain fork en inglés), es la creación de una nueva cadena de bloques a partir de un bloque de una cadena principal

Función de hash criptográfica. Produce un valor de hash de tamaño fijo de un input de tamaño variable. El algoritmo SHA-256, utilizado por la red de Bitcoin, es un ejemplo de hash criptográfico.

ICO. ICO es un acrónimo que significa Initial Coin Offering; es decir, oferta inicial de moneda. El acrónimo ICO se parece bastante al de IPO, Initial Public Offering (que en castellano se denomina OPV, oferta pública de venta) término que se utiliza cuando una empresa sale a bolsa y quiere ofrecer las acciones a los posibles inversores a cambio de dinero. Y es que el ICO tiene que ver con la financiación de un proyecto empresarial.

Llave privada. Código alfanumérico que permite controlar los fondos de un monedero de criptomoneda.

Llave pública. Clave que se utiliza para cifrar una transacción en la red de blockchain.

Mineros. Computadoras encargadas de validar transacciones en un blockchain. Los mineros agrupan transacciones individuales en bloques y los difunden al resto de la red para que

formen parte del registro compartido. Por su contribución, reciben comisiones de transacción y pagos en criptomoneda.

Multisig. Dirección de una cuenta de criptomoneda en la que se requiere más de una firma para mover los fondos.

Nodo. Computadora que forma parte de una red de blockchain.

Posición Arancelaria: La clasificación arancelaria es un proceso que consiste en asignar un código numérico creado por la Organización Mundial de Aduanas (WCO por sus siglas en inglés) a las mercancías. Armonizar la descripción, clasificación y codificación de mercancías. Ayudar a definir aranceles aduaneros

Recompensa de Bloque. Pago en Bitcoin que la red otorga a un minero que calculó exitosamente el hash de un bloque.

Red Distribuida. Tipo de red donde el poder de cómputo y los datos están repartidos en nodos en lugar de en un agente centralizado.

Registro Centralizado. Registro mantenido por un agente central.

Registro Distribuido. Registro donde los datos están almacenados en una red de nodos descentralizados.

RFID: RFID o identificación por radiofrecuencia es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, tarjetas o transpondedores RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto mediante ondas de radio

SHA-256. Algoritmo criptográfico utilizado por criptomonedas como el Bitcoin.

SMART TAG. Las etiquetas inteligentes son una función de búsqueda temprana basada en la selección, que se encuentra en versiones posteriores de Microsoft Word y versiones beta del navegador web Internet Explorer 6, mediante el cual la aplicación reconoce ciertas palabras o tipos de datos y los convierte en un hipervínculo.

Token: Un 'token' (en inglés, ficha, como por ejemplo las que son utilizadas en las máquinas recreativas o los coches de coche) en realidad no es otra cosa que un nuevo término para una

unidad de valor emitida por una entidad privada. Un 'token' tiene semejanzas con 'bitcoin' (tiene un valor aceptado por una comunidad y se fundamenta en blockchain); pero a la vez es un concepto más amplio. Es más que una moneda, ya que tiene más usos. Además, casi todos los 'tokens' son asentado sobre el protocolo (de blockchain) Ethereum, más completo, según los expertos, que la blockchain de bitcoin.

Wallet. Software que permite realizar transacciones en el blockchain, como enviar/recibir pagos y consultar el saldo.

WEB 2.0. El término 'Web 2.0' o 'Web social' comprende aquellos sitios web que facilitan compartir información, la interoperabilidad, el diseño centrado en el usuario y la colaboración en la World Wide Web. Web 2.0 permite a los usuarios interactuar y colaborar entre sí, como creadores de contenido.

14) CONCLUSIONES

Aún parece prematuro establecer el alcance de Blockchain; pero sin dudas cada vez más la seguridad informática, la privacidad de la información personal y como la misma fue y es utilizada para causas de las cuales ni siquiera estamos enterados, pone en cuestionamiento la centralización cada vez más monopólica de la información, lo que alguna vez era un manifiesto ciberpunk, ahora con la abundancia de información circulando en las redes parece ser más una necesidad de eliminar; o al menos acotar un poco el poder que muy pocas empresas tienen sobre nuestra información.

En cuanto a la aplicación de la tecnología en Supply Chain se evidencia que tiene una potencialidad enorme en muchos aspectos, y por la envergadura de los participantes que están en el juego, pareciera que cuando la tecnología alcance su madurez, será inevitable que las regulaciones actuales puedan limitar su expansión.

En el caso de estudio, la potencialidad de su aplicación está totalmente limitada a las regulaciones locales e internacionales, no podría reemplazar actualmente una orden de compra por un smart contract porque no está ni siquiera en estudio que la AFIP implemente la tecnología (*Hernandez, 2018*), por tal motivo un registro blockchain no es prueba de facturación. Tampoco se encuentra habilitado el formato de pago que propone un smart contract y mucho menos desplegada la automatización del COT (Código de Operación de Transporte), que habilita el movimiento de mercadería en territorio argentino.

En el caso de estudio, la potencialidad de ahorro está dada principalmente en todas las posibilidades que brinda la trazabilidad, con todas las ramificaciones que hemos visto anteriormente, cubriendo desde la planificación de demanda, manufactura, calidad, almacenamiento y transporte.

Blockchain: entre el crecimiento y las dudas

Según una encuesta global de PwC, las tres principales barreras para la adopción de tecnología blockchain son: incertidumbre regulatoria (48%), falta de confianza entre los usuarios (45%) y la capacidad de unir distintas redes (44%). El 84% de las empresas ya se involucraron en el uso de la tecnología; aunque más de la mitad (52%) se encuentran aún en

la etapa de investigación y desarrollo, según los resultados de la encuesta efectuada por PwC, Global Blockchain Survey. A pesar de los avances, las organizaciones siguen cuestionando la confiabilidad de esta tecnología.

“El blockchain se ha convertido en la tecnología que, al parecer, revolucionará el entorno de los negocios y la forma en la que depositamos confianza en las transacciones digitales”, comenta Alejandro Rosa, socio de PwC Argentina de la práctica de Gobierno Corporativo, sobre el concepto que, en una primera etapa, parecía secundario dentro del mundo de las Bitcoins. Sin embargo, esta tecnología disruptiva del entorno de los negocios no ha despejado todavía las dudas sobre la confiabilidad de los procesos, un tema que acapara la atención de las compañías y gana espacio en sus agendas.

Las empresas están preocupadas por la confiabilidad, velocidad, seguridad y escalabilidad de esta tecnología; pero sobre todo por la falta de regulación/estandarización y, de algún modo consecuencia de lo anterior, los potenciales problemas de compatibilidad e interacción entre cadenas de bloques desarrollados por entidades diversas. Según la encuesta de PwC, las tres principales barreras para su adopción son: incertidumbre regulatoria (48%), falta de confianza entre los usuarios (45%) y la capacidad de unir distintas redes (44%).

A pesar de la incertidumbre, algunos de los beneficios de una cadena de bloques bien diseñada son: reducción de costos, mayor alcance y velocidad en las operaciones, más transparencia y trazabilidad.

Si bien la industria de servicios financieros es actualmente líder en cuanto a su utilización, esta tecnología está expandiéndose en otros sectores como la salud, la consultoría y los productos industriales.

¿Qué deberían saber las empresas sobre blockchain? A continuación, algunos conceptos básicos que surgen de la encuesta realizada por PwC a 600 ejecutivos de empresas de 15 países.

Las empresas deben, en primer lugar, entender la tecnología, considerando sus oportunidades y riesgos. Preguntarse si podrían adaptarla a su estrategia y modelo de negocio, analizar a la competencia y contemplar los riesgos de seguridad y privacidad. Existen ciertos temas que podrían afectar significativamente el negocio de las organizaciones y que conllevan cierta complejidad técnica. En ese sentido siempre es recomendable contar con el soporte de

especialistas externos que ayuden no solo a entender la temática, sino fundamentalmente a prever impacto y riesgos que puedan generar para el negocio de la empresa.

(Rosa, 2019)

15) BIBLIOGRAFIA

- a2b.direct. (s.f.). *A2B Direct*. Obtenido de A2B Direct: <https://www.a2b.direct/#/home>
- Alonso, H. (10 de 4 de 2019). *Ambito*. Obtenido de El "método Toyota" que hizo a la Hilux el modelo más vendido: <https://www.ambito.com/edicion-impres/toyota/el-metodo-que-hizo-la-hilux-el-modelo-mas-vendido-n5025529>
- Altors. (2015). *A Close Look at Everledger—How Blockchain Secures Luxury Goods*. Obtenido de A Close Look at Everledger—How Blockchain Secures Luxury Goods: <https://www.altors.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods/>
- Amr, M. (2018). *Logistics 4.0: Definition and Historical Background*. Giza: Faculty of computers and artificial intelligence, Cairo University Giza, Egypt.
- Anderson, J., Narus, J., Narayandas, D., & Seshadri, D. (2011). *Business Market Management (B2B)*. Nodras: Pearson.
- ANNA. (28 de 6 de 2019). *Inventory management using drones*. Obtenido de Inventory management using drones: <https://roboticsandautomationnews.com/2019/06/28/inventory-management-using-drones/23992/>
- As.Kirtchev, C. (s.f.). *UN MANIFIESTO CYBERPUNK*. Obtenido de http://project.cyberpunk.ru/idb/manifiesto_es.html
- Ast, F. (17 de 10 de 2017). *medium*. Obtenido de Breve Historia del Bitcoin: <https://medium.com/astec/breve-historia-del-bitcoin-3cd9942debef>
- Ast, F. (17 de 2 de 2019). *El Blockchain en la Lucha contra el Cambio Climático*. Obtenido de Medium: <https://medium.com/astec/el-blockchain-en-la-lucha-contra-el-cambio-clim%C3%A1tico-59c228e3250f>
- Bashir, I. (2018). *Mastering Blockchain*. Birmingham: Packt Publishing Ltd.
- Bastardo, J. (26 de 1 de 2019). *Bitcoin y el sueño cypherpunk*. Obtenido de CriptoNoticias: <https://www.criptonoticias.com/opinion/bitcoin-sueno-cypherpunk/>
- Bendapudi, N., & Berry, L. (1997). Customers' Motivation for Maintaining Relationships with Service Providers. *Journal of Retailing*, 73 (1), 15-37.
- Benz, M. (24 de 2 de 2019). *Mercedes-Benz Cars develops Blockchain-prototype for sustainable supply chains for the first time*. Obtenido de Mercedes-Benz Cars develops Blockchain-prototype for sustainable supply chains for the first time: <https://media.mercedes-benz.com/article/c48af76e-e285-4020-b3d2-327f61aac23f>
- Benz, M. (13 de 2 de 2020). *Blockchain pilot project provides transparency on CO2 emissions*. Obtenido de Blockchain pilot project provides transparency on CO2 emissions: <https://www.daimler.com/sustainability/resources/blockchain-pilot-project-supply-chain.html>

- Berry, L., & Parasuraman, A. (1991). *Marketing Services: Competing Through Quality*. New York: The Free Press.
- Bikramaditya Singhal, G. D. (2018). *Beginning Blockchain*. New York: apress.
- Bikramaditya Singhal, Gautam Dhameja, P. S. (2018). *Beginning Blockchain*. Bangalore: Apress.
- binance. (s.f.). *Encriptación Simétrica vs. Asimétrica*. Obtenido de Encriptación Simétrica vs. Asimétrica: <https://www.binance.vision/es/security/symmetric-vs-asymmetric-encryption>
- BLÁZQUEZ, S. (21 de 2 de 2020). *Blockchain Economía*. Obtenido de blockchain economía: <https://www.blockchaineconomia.es/blockchain-ahorra-costes-en-transporte-logistica/>
- Bolaños, J. F. (18 de 3 de 2019). *Cuáles son las regulaciones que blockchain necesita*. Obtenido de <https://www.academiablockchain.com/2019/03/18/regulaciones-que-blockchain-necesita/>
- Brooks, D. (2019). *Qué es el "problema de los generales bizantinos" y por qué explica el origen del bitcoin*. Obtenido de Qué es el "problema de los generales bizantinos" y por qué explica el origen del bitcoin: <https://www.lanacion.com.ar/tecnologia/que-es-problema-generales-bizantinos-que-explica-nid2333912>
- Carpenter, G., Glazer, R., & Nakamoto, K. (1994). Meaningful Brands for Meaningless Differentiation: The Dependence on Irrelevant attributes. *Journal of Marketing Research*, 339 - 350.
- Chaum, D. (s.f.). *Blind Signatures for Untraceable Payments*. Obtenido de Blind Signatures for Untraceable Payments: https://link.springer.com/chapter/10.1007/978-1-4757-0602-4_18
- Chen, C., & Wang, J. (2016). Customer Participation, Customer Co-creation and Customer Loyalty - A Case of Airline On-line Check-in System. *Computers in Human Behavior*, 62, 346 - 352.
- Co, T. &. (s.f.). *The Leader in Diamond Traceability*. Obtenido de The Leader in Diamond Traceability: <https://www.tiffany.com/engagement/diamond-provenance/>
- Collins, D. (25 de diciembre de 2018). *www.wordreference.com*. Obtenido de <http://www.wordreference.com/definition/commodity>
- Columbus, L. (28 de 10 de 2018). *How Blockchain Can Improve Manufacturing In 2019*. Obtenido de FORBES: <https://www.forbes.com/sites/louiscolombus/2018/10/28/how-blockchain-can-improve-manufacturing-in-2019/#4cd16c585db6>
- Corey, E. (1975). *Key Options in Marketing Selection and Product Planning*. Boston: Harvard Business Review.
- Cortés, J. (19 de 12 de 2019). *Nike patenta unas zapatillas basadas en 'blockchain'*. Obtenido de Nike patenta unas zapatillas basadas en 'blockchain': https://retina.elpais.com/retina/2019/12/17/innovacion/1576572302_779289.html
- Cossio Silva, F., Revilla Camacho, M., Vega Vázquez, M., & Palacios Florencio, B. (2016). Value Co-creation and Customer Loyalty. *Journal of Business Research*, 60 - 1621-1625.
- Coughlan, A., Anderson, E., Stern, L., & El-Ansary, A. (2001). *Marketing Channels*. New Jersey: Prentice Hall.

- Daimler. (2 de 10 de 2019). *BLOCKCHAIN IS A RADICAL REVERSAL*. Obtenido de INTERVIEW WITH DR. HARRY BEHRENS: <https://www.daimler-mobility.com/en/company/news/interview-harry-behrens/>
- Deloitte. (2017). *Continuos Interconnected supply chain*. Luxembourg: Deloitte.
- DHL, A. /. (2018). *BLOCKCHAIN IN LOGISTICS - Perspectives on the upcoming impact of blockchain technology and use cases for the logistics industry*. Troisdorf, Germany: DHL Customer Solutions & Innovation.
- DÍAZ, A. (28 de 4 de 2019). *CRIPTO TENDENCIA*. Obtenido de FedEx quiere que se haga obligatorio el uso de Blockchain para los envíos: <https://criptotendencia.com/2019/04/28/fedex-quiere-que-se-haga-obligatorio-el-uso-de-blockchain-para-los-envios/>
- Economipedia. (26 de diciembre de 2018). *www.economipedia.com*. Obtenido de <https://economipedia.com/definiciones/competencia-monopolistica.html>
- efintechshow. (14 de 3 de 2018). *DHL and Accenture Unlock the Power of Blockchain in Logistics*. Obtenido de DHL and Accenture Unlock the Power of Blockchain in Logistics: <https://efintechshow.com/news/dhl-and-accenture-unlock-the-power-of-blockchain-in-logistics/>
- Ehuletche, A. B. (2019). Bitcoin: la criptomoneda hace su aparición en operaciones de comercio exterior. *La Nación*, 4.
- Fernandez, M. (5 de 1 de 2019). Para que no haya más títulos apócrifos, cobra fuerza blockchain y una universidad argentina ya lo aplica. *Infobae*, pág. 2.
- Forbis, J. L., & T, M. N. (1981). Value-Based Strategies for Industrial Products. *Business Horizons*, 24, 32-42.
- FreshTurf. (s.f.). *Deliver more*. Obtenido de Deliver more: <https://www.freshturf.io/>
- Friedman, M. (s.f.). Milton Friedman predicts the rise of Bitcoin in 1999. (<https://www.youtube.com/watch?v=6MnQJFEVY7s>, Entrevistador)
- Gates, M. (2017). *Blockchain_ Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money*. Wise Fox Publishing and Mark Gates.
- Gómez Herrera, G. (2009). La innovación como estrategia y solución empresarial para impulsar la competitividad y un crecimiento sostenido a largo plazo. *Ciencia y Mar*, 38. 51- 60.
- Gómez Roldán, I. (2006). Gestión del Conocimiento, Innovación y Competencia. *Revista Escuela de Administración de Negocios Bogotá*, 58, 107 - 134.
- González Fernández, A. (2017). La Diferenciación de Commodities Más Allá del Precio y el Servicio. *II Congreso Internacional Virtual Sobre Desafíos de las Empresas del Siglo XXI*.
- Gonzalez, A. (s.f.). *Cómo Importar en Argentina*. Obtenido de Cómo Importar en Argentina: <https://www.comoimportarenargentina.com.ar/blockchain-en-el-comercio-exterior/>
- Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2006). *Metodología de la Investigación*. Ciudad de México: McGraw Hill.

- Hernandez, I. (25 de 10 de 2018). *Blockchain: El fin de las agencias Tributarias?* Obtenido de El Cronista: <https://www.cronista.com/columnistas/Blockchain-fin-de-las-agencias-tributarias-20181024-0080.html>
- hyperledger. (s.f.). *Tracking food for better safety*. Obtenido de Tracking food for better safety: <https://www.hyperledger.org/resources/publications/walmart-case-study>
- Iacobucci, D., & Hibbard, J. (1999). Toward an Encompassing Theory of Business Marketing Relationships (BMR's) and Interpersonal Commercial Relationships (ICR's): An Empirical Examination. *Journal of Interactive Marketing*, Vol 13, No 3, 13 - 33.
- IBM. (2018). *IBM Food Trust. Una nueva era para la cadena de suministro de alimentos del mundo*. Obtenido de IBM Food Trust. Una nueva era para la cadena de suministro de alimentos del mundo: <https://www.ibm.com/ar-es/blockchain/solutions/food-trust>
- IBM. (s.f.). *Maersk and IBM Introduce TradeLens Blockchain Shipping Solution*. Obtenido de Maersk and IBM Introduce TradeLens Blockchain Shipping Solution: <https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution>
- Jones, M., Mothersbaugh, D., & Beatty, S. (2002). Why Customers Stays: Measuring the Underlying Dimensions of Services Switching Cost and Managing Their Differential Strategic Outcomes. *Journal of Business Research*, 55, 441-450.
- Keller, K., Stenthal, B., & Tybout, A. (2002). Three Questions You Need To Ask About Your Brand. *Harvard Business Review*, Vol 80, Sept, 80 - 89.
- Keysuk, K. (1999, mencionado por González Fernandez, 2017). *On Determinants of Joint Actions in Industrial Distributor - Supplier*.
- Killing, P., Malnight, T., & Keys, T. (2006). *Must-Win Battles*. Upper Saddle River, NJ: Pearson Education Inc - Prentice Hall.
- Kotler, P. (2006). *Dirección de Marketing*. Madrid: Pearson Educación.
- Kotler, P., & Armstrong, G. (2012). *Principles of Marketing*. Upper Saddle River, NJ: Pearson Prentice Hall.
- Levitt, T. (1980). *Marketing Success Through Differentiation of Anything*. Boston: Harvard Business Review.
- López Villegas, L. I., & Mora Arteaga, A. (2012). Estrategias de Marketing en las Empresas del Sector Manufacturero de Caldas, Quindío y Risaralda. *Novum*, 49 - 64.
- López, M. A. (28 de 6 de 2018). *¿Pública, federada o privada? Explora los distintos tipos de blockchain*. Obtenido de ¿Pública, federada o privada? Explora los distintos tipos de blockchain: <https://blogs.iadb.org/conocimiento-abierto/es/tipos-de-blockchain/>
- Lozano, N. G. (2018). Blockchain: una autopista más eficiente para el comercio exterior. *La Nación*, 4.
- Macedo, B. (2005). *El Concepto de Sostenibilidad*. Santiago de Chile: Oficina Regional UNESCO.

- MacMillan, I., & MacGrafth, R. (1997). Discovering New Points of Differentiation. *Harvard Business School*, 133 - 145.
- Maersk. (2 de 7 de 2019). *TradeLens blockchain-enabled digital shipping platform continues expansion with addition of major ocean carriers Hapag-Lloyd and Ocean Network Express*. Obtenido de TradeLens blockchain-enabled digital shipping platform continues expansion with addition of major ocean carriers Hapag-Lloyd and Ocean Network Express: <https://www.maersk.com/news/articles/2019/07/02/hapag-lloyd-and-ocean-network-express-join-tradelens>
- Mainelli, M. (19 de 4 de 2017). '*Blockchain*': el gran carnet de identidad que nos trae el mundo digital. Obtenido de 'Blockchain': el gran carnet de identidad que nos trae el mundo digital: <http://igomeze.blogspot.com/2017/04/blockchain-el-gran-carnet-de-identidad.html>
- Marco, J. A. (s.f.). *El Internet de las Cosas (IOT) aplicada a la Logística 4.0*. Obtenido de El Internet de las Cosas (IOT) aplicada a la Logística 4.0: <https://blogs.imf-formacion.com/blog/logistica/logistica/internet-cosas-iot-aplicada-logistica/>
- Marqués, M. P. (2015). *BIG DATA Tecnicas, herramientas y aplicaciones*. Mexico: Alfaomega Grupo Editorial.
- Marr, B. (2018). Why Blockchain Could Kill Uber. *Forbes*, 3.
- Michael Casey, R. G. (9 de 6 de 2018). Combining IoT and Blockchain Toward New Levels of Trust. (M. T. Insights, Entrevistador)
- Mundo, D. E. (26 de 4 de 2013). *La tragedia en Bangladesh destapa 'los talleres de la miseria'*. Obtenido de elmundo.es: <https://www.elmundo.es/elmundo/2013/04/25/internacional/1366885756.html>
- Najafi, F. (25 de 9 de 2017). *Solar Power Word*. Obtenido de Solar Power Word: <https://www.solarpowerworldonline.com/2017/09/virtual-power-plant/>
- Nakamoto, S. (s.f.). *Bitcoin*. Obtenido de Bitcoin.org: <https://bitcoin.org/bitcoin.pdf>
- Orcutt, M. (8 de 3 de 2019). *Blockchain boosters warn that regulatory uncertainty is harming innovation*. Obtenido de MIT Technology Review: <https://www.technologyreview.com/2019/03/08/136720/blockchain-boosters-warn-that-regulatory-uncertainty-is-harming-innovation/>
- PassLfix. (s.f.). *Smart contract ethereum based parcel delivery*. Obtenido de Smart contract ethereum based parcel delivery: <https://tokenmarket.net/blockchain/ethereum/assets/passlfix/>
- Pauw, C. (4 de 12 de 2018). *cointelegraph*. Obtenido de cointelegraph: <https://cointelegraph.com/news/how-significant-is-blockchain-in-internet-of-things>
- Porter, M. (1982). *Estrategia Competitiva*. Boston: Patria Editorial.
- Porter, M. (1987). *Ventaja Competitiva*. Buenos Aires: Pirámide.
- Provenance. (s.f.). *Every product has a story*. Obtenido de Every product has a story: <https://www.provenance.org/>

- Quench, J. (2007). *How to Avoid the Commodity Trap*. Boston: Harvard Business Review.
- Rangan, V., & Bowman, G. (1992). *Beating the Commodity Magnet*.
- Ries, A., & Trout, J. (2001). *Positioning: The Battle For Your Mind*. New York: McGraw - Hill.
- Ripe.io. (s.f.). *Blockchain for food*. Obtenido de Blockchain for food: <https://www.ripe.io/>
- Rosa, A. (2019). Blockchain: entre el crecimiento y las dudas. *Enfasis Logística*, 1.
- Sampieri, R. H. (2016). *Metodología de la Investigación*.
- Samuelson, P., & Nordhaus, W. (2010). *Economía*. México D.F.: McGraw - Hill.
- Sánchez Sumelzo, N. (2016). *Importancia de los Distintos Grupos de Interés en el Proceso de Cambio*. Barcelona: Universitat Politècnica de Catalunya.
- Sanchís Palacio, J. (27 de Diciembre de 2018). *Diccionario Empresarial Wolterskluwer*. Obtenido de http://diccionarioempresarial.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAEAMtMsBf1jTAAASNjMzNTtbLUouLM_DxblwMDS0NDA7BAZlqIS35ySGVBqm1aYk5xKgCV229FNQAAAA==WKE
- Santandreu i García, P. (2016). *El EVA (Economic Value Added)*. Recuperado de <http://www.centrem.cat/ecomu/upfiles/publications/el%20eva.htm>.
- Schiller, B. (2018). On This Blockchain-Based Version Of Airbnb, There's No Middleman. *Fast Company*, 3.
- Schneider, S. (3 de 3 de 2019). *State of Enterprise Blockchain Study Report*. Obtenido de Provide: <https://provide.services/state-of-enterprise-blockchain-study-report/>
- School, E. B. (20 de 4 de 2018). *EAE Business School*. Obtenido de EAE Business School: <https://retos-operaciones-logistica.eae.es/machine-learning-en-las-empresas-de-logistica/>
- School, I. B. (s.f.). *IMF Business School*. Obtenido de <https://blogs.imf-formation.com/blog/logistica/logistica/logistica-4-0/>
- Schumpeter, J. (1971). *Historia del Análisis Económico*. Barcelona: Editorial Ariel.
- Sethuraman, R., Anderson, J., Narus, & J. (1988). Partnership Advantage and Its Determinants in Distributor and Manufacturer Working Relationships. *Journal of Business Research*, Vol 17, No 4, 327 - 347.
- Siguaw, J., Simpson, P., & Baker, T. (1998). Effects of Supplier Market Orientation on Distribution Market Orientation an the channel Relationship: The Distributor Perspective. *Journal of Marketing*, 99 - 111.
- smartagrifood. (s.f.). *SmartAgriFood*. Obtenido de SmartAgriFood: <http://smartagrifood.com/>
- smartlog. (29 de 3 de 2018). *BLOCKCHAIN PLATFORM FOR LOGISTICS*. Obtenido de BLOCKCHAIN PLATFORM FOR LOGISTICS: <https://smartlog.kinno.fi/articles>
- Swan, M. (2015). *Blockchain BLUEPRINT FOR A NEW ECONOMY*. CA: O'Reilly Media.
- Telam, A. (20 de 3 de 2018). *Por primera vez, vinos argentinos recibieron certificaciones de huella ecológica*. Obtenido de Por primera vez, vinos argentinos recibieron certificaciones de

huella ecológica: <https://www.telam.com.ar/notas/201803/262074-por-primera-vez-vinos-argentinos-recibieron-certificaciones-de-huella-ecologica.html>

- Tirole, J. (1990). *Teoría de la Organización Industrial*. Barcelona: Talleres Gráficos Duplex.
- t-mining. (s.f.). *blockchain use-cases*. Obtenido de blockchain use-cases: <https://t-mining.be/>
- Tybout, A., & Sternthal, B. (2005). *Brand Positioning*. New York: John Wiley & Sons Inc.
- Valinsky, J. (1 de 8 de 2019). *7 de los mayores hackeos de la historia*. Obtenido de 7 de los mayores hackeos de la historia: <https://cnnespanol.cnn.com/2019/08/01/7-de-los-mayores-hackeos-de-la-historia/>
- Vargas, G., & Rodríguez, C. (2013). Un análisis microeconómico de los efectos de la innovación en el desarrollo y el bienestar social. *Economía Informa*, 383, 64 - 76.
- Vikram Dhillon, D. M. (2017). *Blockchain Enabled Applications*. Orlando, Florida: Apress.
- Warburg, B. (s.f.). How the blockchain will radically transform the economy.
- winnesota. (2018). *HOW BLOCKCHAIN IS REVOLUTIONIZING THE WORLD OF TRANSPORTATION AND LOGISTICS*. Obtenido de HOW BLOCKCHAIN IS REVOLUTIONIZING THE WORLD OF TRANSPORTATION AND LOGISTICS: <https://www.winnnesota.com/blockchain>
- Wolfpack, A. B.-B.-S. (2016). *A lead via Blockchain technology - Position paper on a digital Port of Rotterdam*. Rotterdam: blocklab.
- Yafimava, D. (17 de 1 de 2019). *Blockchain And The Law: Regulations Around the World*. Obtenido de Blockchain And The Law: Regulations Around the World: <https://openledger.info/insights/blockchain-law-regulations/>
- Zigurat. (18 de 1 de 2020). *Blockchain Regulations: Recent Key Developments*. Obtenido de Zigurat: <https://www.e-zigurat.com/innovation-school/blog/blockchain-regulations-recent-key-developments/>