Escuela Politécnica Superior de Jaén

Grado en Ingeniería Mecánica

UNIVERSIDAD DE JAÉN
ESCUELA POLITÉCNICA SUPERIOR DE JAÉN

Trabajo Fin de Grado

BLOCKCHAIN Y SU APLICACIÓN EN LA CADENA DE SUMINISTRO

Alumno: Alberto Elósegui Horno

Tutor: Prof. D. Jose Antonio La Cal Herrera

Dpto: Organización de Empresas

Universidad de Jaén
Escuela Politécnica Superior de Jaén
Departamento de Informática

D. José Antonio La Cal Herrera, tutor del Proyecto Fin de Carrera titulado: "**Blockchain y su aplicación en la cadena de suministro"**, que presenta **Alberto Elósegui Horno**, autoriza su presentación para defensa y evaluación en la Escuela Politécnica Superior de Jaén.

Jaén, Julio de 2021

El alumno: El tutor:

Alberto Elósegui Horno José Antonio La Cal Herrera

Índice

1. Introducción

1.1. Justificación del tema elegido

El hecho que ha determinado la elección del tema del Trabajo de fin de grado ha sido la novedad e importancia que lleva consigo la tecnología *Blockchain* a nivel mundial, y el gran interés que suscita en diferentes campos profesionales.

Con anterioridad al inicio de mi trabajo de investigación, mi conocimiento sobre *Blockchain* era particularmente pobre, con la única salvedad de las criptomonedas, y en concreto del *Bitcoin*. Es por este motivo que consideré una buena oportunidad para investigar y seguir aprendiendo sobre él, y sobre su utilidad en la cadena de suministro. Lo que hizo, en suma, decantarme por este tema, que resulta tan cautivador como interesante para trabajar.

1.2. Problema y finalidad del trabajo

La tecnología *blockchain* ha aparecido de forma repentina en el escenario empresarial, generando muchas expectativas. La sociedad de hoy en día, generalmente, espera que tenga un efecto disruptivo y que provoque la aparición de nuevos tipos de empresas.

Es por ello, que a lo largo de esta tesis abordaremos no solo lo que es el funcionamiento de la tecnología *Blockchain*, o cadena de bloques, sino también, la criptografía, el concepto de minería, y cómo irá gobernando dicha tecnología la cadena de suministro de grandes empresas.

1.3. Objetivos

El principal objetivo de este proyecto es analizar con profundidad el funcionamiento de la tecnología *blockchain*, para así poder comprender qué puede aportar a la cadena de suministro.

Estudiaremos también su aplicación en la sociedad actual, en diferentes sectores y las consecuencias que pueden desencadenar la llegada de esta tecnología a la cadena de suministro. Así profundizaremos sobre algunos ejemplos de casos reales donde se ha aplicado dicha tecnología.

El objetivo subyacente a lo largo de este proyecto es dar al lector una visión amplia de la importancia de las nuevas tecnologías en un campo bastante tradicional como es la cadena de suministro.

2. Tecnología *Blockchain (Descentralized Ledger Tecnology)*

2.1. Los orígenes del *blockchain*

La tecnología *blockchain* o cadena de bloques es una de las innovaciones tecnológicas más presente en la sociedad actual. Principalmente, comenzó a desarrollarse a principios de la década de 1990 cuando los ingenieros empezaron a germinar elementos de monedas virtuales modernas. En 1998, el ingeniero Wei Dai desarrolló la idea de '*'B-Money*'', como un concepto de un sistema de pago descentralizado, precedente al *bitcoin*. Más tarde, ese mismo año, un desarrollador llamado Nick Szabo, matizó dicho concepto, debido a la preocupación que le generaba tanta inseguridad en la red, mediante la creación del *Bit Gold*, una moneda que realmente no llegó a existir, pero llevaba aparejada algunas de las principales características de las criptomonedas como lo son la descentralización, la privacidad, y lo que se conoce como "*proof of work"* (PoW) o prueba de trabajo. Este concepto utiliza el poder de la computadora de los participantes para resolver ecuaciones criptográficas asignadas por el sistema.

El origen de la *Blockchain* se retrotrae al nacimiento del Bitcoin, creado a finales del 2008, por una persona anónima cuyo pseudónimo es Satoshi Nakamoto. En plena crisis financiera[1], las autoridades se valían de los recursos de los particulares con el fin de poder salvar a las entidades financieras. En este contexto de fragilidad y

[1] La crisis financiera de 2008 se produjo por la quiebra de uno de los principales bancos de inversiones de Estados Unidos, Lehman Brothers, lo que provocó una gran recesión económica a nivel mundial, con la consecuente desconfianza en las entidades financieras y bancos centrales.

desconfianza financiera, Nakamoto propuso el Bitcoin como una moneda virtual libre de cualquier autoridad, un sistema que no dependiese de ningún banco central, y que facilitara transacciones inmediatas sin que fuesen éstas limitadas por terceros (Ionov, 2018). Fue entonces cuando nació la tecnología *Blockchain*, con el propósito de que se utilizase como una base de datos descentralizada, asentada sobre la base de la arquitectura tecnológica del *Peer To Peer* (P2P), o red de pares, la cual posibilita una comunicación entre aplicaciones y permite el intercambio de información sin necesidad de un servidor central ni de terceros, sino que lo hace mediante unos nodos[2] que conforman la cadena de bloques en que trabaja la *Blockchain* (Catchlove, 2017).

Así, la red *Blockchain* se compone de un grupo de bloques conectados entre sí, identificados de forma individual mediante una huella digital o hash, una señal de tiempo en que se crean, y el hash del nodo anterior, pudiendo identificar así, cada uno de los bloques, dentro de cada cadena de bloques.

En este sentido, Nakamoto describió su idea de un nuevo tipo de moneda digital, la cual permitiría a las personas enviar dinero directamente entre sí a través del sistema P2P, sin necesidad de intermediario alguno, por lo que los bancos no tendrían control sobre el sistema, ni tampoco lo harían los gobiernos. El *Bitcoin* sería una especie de dinero puro, completamente democrático, con costes de transacción mínimos, sin intermediarios y completamente digital.

2.2. Principios esenciales del *Blockchain*.

2.2.1. Integridad y transparencia en la red

Definimos la integridad como la protección frente a una posible modificación, o incluso, destrucción de la información contenida en los nodos que conforman la Blockchain, asegurando y autenticando dicha información.

Por lo tanto, dicha protección de la información está descentralizada en cada fase del proceso, es decir, no depende de cada uno de los participantes de forma individual. Así, dicha integridad va asociada a un proceso de

[2] Un nodo es un punto individual en una red que, en relación con otros nodos, valida los datos antes de agregarlos a la cadena de bloques. Traducción libre. Versión original: “A node is an individual point in a network which, in relationship to other nodes, validates data before adding it to the blockchain”

codificación, por lo que un comportamiento que carezca de integridad, es prácticamente imposible.

Cuando se utilizan transacciones en línea para la gestión de inversiones y activos por diferentes intermediarios, no sólo aumentan los costes de transacción, sino que también conlleva el riesgo de falsificar los certificados. Por lo tanto, el sistema debe garantizar dicha integridad en las transacciones, con el fin de evitar que las transacciones sean manipuladas. Es por ello que Nakamoto quería eliminar la intervención de las autoridades, o de cualquier tercero, no solo por el incremento del coste, sino también por la posible manipulación que podía haber.

Nakamoto, se dió cuenta de que, al estar el dinero descentralizado, existía de que una moneda digital podía ser publicada y usada en ocasiones diferentes. Esto es lo que él denominó como problema del doble gasto (*double-spend problem*). Ese problema fue solucionado por el mismo que lo descubrió, creando un mecanismo de consenso, en el que se registra la primera transacción que hace un usuario con una moneda concreta, y rechaza las transacciones siguientes donde vaya a ser utilizada la misma moneda (Tapscott, 2017).

Hoy en día, podemos comprobar, que la falta de transparencia en la información es un problema existente, y la tecnología *Blockchain* viene a garantizar una red totalmente cristalina. Es por ello que, todos los usuarios de las redes, pueden acceder al libro de registros, es decir, que todos los miembros que pertenecen al grupo tienen acceso a todas las transacciones que se efectúan por el mismo. Pero esa transparencia no quiere decir que cualquier persona pueda saber quién hace esas transacciones. Estas son visibles, pero están vinculadas a un código. (Porxas & Conejo, 2018)

2.2.2. Poder Distributivo

La distribución del poder implica, que todos los usuarios ven lo que está pasando en cada momento y en cada bloque. Esto garantiza, en primer lugar, que no haya cambios malintencionados, es decir, si una persona quiere modificar un registro de forma ilícita, debido a que los cambios ocurren en todos los registros de forma inminente, cualquier persona puede darse cuenta.

En segundo lugar, implica que haya una verificación de los registros por parte de los nodos, y si una persona quiere añadir un bloque, este tendrá que ser verificado por otra persona. Esto conlleva a una participación justa por parte de los usuarios.

En tercer lugar, conlleva a que nadie tiene más beneficios respecto a otros. Debido a la transparencia de la red, todos los cambios se ven rápidamente, por lo que todo el mundo tiene que pasar por los canales habituales, es decir, no existen favoritismos de unos sobre otros.

Y, por último, supone que las respuestas son rápidas debido a la supresión de intermediarios, podemos hablar de minutos, y a veces de segundos.

2.2.3. El valor como incentivo

"La primera transacción en un bloque es una transacción especial que inicia una nueva moneda de propiedad por el creador del bloque. Esto agrega un incentivo para que los nodos respalden la red y proporciona una forma de distribuir inicialmente las monedas en circulación, ya que no existe una autoridad central para emitirlas'' (Nakamoto).

A lo que se refiere Nakamoto, mencionado en el párrafo anterior, es que el proceso de minado, del que posteriormente hablaremos, requiere mucho esfuerzo, y es por ello que los mineros al terminar dicho proceso, reciben una cantidad de *Bitcoin* como recompensa. Esos nuevos *bitcoins* son añadidos a la red, generando así más *bitcoins* en movimiento por la red.

2.2.4. Privacidad

Satoshi Nakamoto, veló por la salvaguarda de la privacidad de los usuarios, como derecho humano fundamental, a la hora de utilizar una plataforma asentada sobre las bases de la tecnología *Blockchain*, con el fin de operar con *Bitcoins*; lo que garantiza el derecho de los usuarios a la privacidad, sin que sea necesario introducir ningún dato sensible de carácter personal, brindándoles a éstos la oportunidad de decidir sobre la publicidad de su identidad.

En la mayoría de los movimientos en línea, los usuarios desean tener la mínima divulgación de sus transacciones e información de cuenta en un comercio en línea.

La divulgación mínima incluye lo siguiente:

1. A la información de transacciones de los usuarios no puede acceder cualquier usuario no autorizado.
2. El administrador del sistema o el participante de la red no puede revelar la información de ningún usuario a otros sin su permiso.
3. Los datos de todos los usuarios deben almacenarse y acceder a ellos de manera consistente y segura, incluso bajo fallos inesperados o ciberataques.

El usuario debe estar al tanto de exigir que las transacciones relacionadas con ellos mismos no se puedan vincular. Este se debe a que una vez que se pueden vincular todas las transacciones relevantes para un usuario, es fácil inferir otra información sobre el usuario, como el saldo de la cuenta y el tipo y la frecuencia de sus transacciones. Usando esos datos estadísticos sobre transacciones, junto con algunos conocimientos previos acerca de un usuario, las partes curiosas o adversarias pueden adivinar la verdadera identidad del usuario con alta confianza.

2.2.5. Seguridad

Todo usuario que quiera hacer uso de la red, debe usar datos criptográficos, de lo contrario, las consecuencias serán sufridas por el usuario que tenga un mal comportamiento. El uso de la cadena de bloques, permite a aquellas personas a poder plasmar sus datos en la red con seguridad y confianza, ya que dicha tecnología es, teóricamente, a prueba de ser manipulada debido al uso de un Hash o huella digital para cada bloque y a un protocolo de consenso, mediante el cual los nodos de la red acuerdan un historial compartido.

La red *Blockchain* se compone de un grupo de bloques conectados entre sí, identificados de forma individual mediante una huella digital o hash, una señal de tiempo en que se crean, y el hash del nodo anterior, pudiendo identificar así, cada uno de los bloques, dentro de cada cadena de bloques. lo

explican Primavera de Filippi y Aaron Wright: “mientras que un libro depende de la numeración de las paginas para ordenar su contenido interno – haciendo posible que cualquier persona pueda articular un libro en su orden apropiado – la Blockchain (cadena de bloques) del Bitcoin, depende de la información almacenada en el encabezamiento de cada bloque para organizar la base de datos compartida, que incluye el hash (identificación) del bloque anterior, y un sello del tiempo, creando así una cadena organizada secuencialmente’’ (de Filippi & Wright, 2019).

En 2014, uno de los mejores bancos de Hong Kong, fue defraudado, perdiendo así una cantidad de unos 200 millones de dólares[3]. Debido a ese fraude, incluyendo el robo de facturas duplicadas, el banco, junto con una agencia del gobierno de Singapur, implantaron la tecnología *Blockchain*, desarrollando un hash criptográfico para cada factura, de tal forma que cada factura era única.

2.2.6. Derechos preservados

El derecho a la propiedad es un derecho fundamental. A modo de ejemplo, analizamos el caso de los artistas, con su respectivo derecho de propiedad, e Internet. Aquellos, han utilizado Internet como una herramienta que han implantado en su vida cotidiana, con el fin de darse a conocer y seguir creciendo profesionalmente.

Sin embargo, los intermediarios han obstaculizado el esfuerzo de los artistas beneficiándose de forma indirecta de parte de la obra de los mismos. Así, en numerosas ocasiones el porcentaje de beneficio acordado por los intermediarios es muy elevado; y es entonces, cuando se ve vulnerado el derecho de propiedad del artista.

Yuxtaponiendo dicha situación a la tecnología *Blockchain*, ésta no solo regula el problema del doble gasto, sino que confirma la propiedad de cada una de las criptomonedas que circulan a lo largo de la red, y, por ello, cada operación es inmutable e irreversible. Por lo que, la propiedad de cada usuario se ve respetada en cada momento.

[3] Ver en https://av.sc.com/hk/content/docs/hk-news-media-140707.pdf

2.2.7. Inclusión.

Es evidente que el desarrollo de la economía mundial crece de forma exponencial cuando más Estados engloba, por lo que resulta de gran importancia crear vínculos, tales como lo son las plataformas sobre las que se asienta la tecnología *Blockchain*, que faciliten la participación de dichos Estados, en el crecimiento y desarrollo de la economía global.

Sin embargo, a pesar de que la irrupción de Internet ha sido de gran ayuda, y ha facilitado esta labor, hemos de recalcar que no cualquier persona tiene acceso a esta red, de hecho, en 2015 había alrededor de dos mil millones de personas sin acceso al sistema financiero[4].

Es por esto que, Satoshi Nakamoto, desarrolló un sistema para que funcionase de forma independiente, sin que estuviese supeditado al acceso a Internet. Este imaginó que una persona podría utilizar las cadenas de bloques a través de lo que él denominó ‘’verificación de pago simplificado’’ (SPV, por sus siglas en inglés), es decir, que, con cualquier dispositivo, cualquier persona podría ser partícipe, como consumidor o como productor en la economía, sin que resulte preceptivo certificar una cuenta bancaria, o un certificado de ciudadanía, entre otros, para usar la tecnología *blockchain*.

2.3. Tipos de redes

Dentro de la red *blockchain*, podemos diferenciar tres tipos de redes:

1. Red pública. Una cadena de bloques pública no requiere un permiso para su acceso. Cualquiera puede unirse a la red y leer, escribir o participar dentro de la cadena de bloques. Está descentralizada y no tiene una sola entidad que controle la red. Los datos en una cadena de bloques pública son seguros, ya que no es posible modificar o alterar los datos una vez que se han validado en la cadena de bloques. *Bitcoin* y *Ethereum* son ejemplos bien conocidos de una cadena de bloques pública.

[4] Banco Mundial, 2 de septiembre de 2015: https://www.worldbank.org/en/news/press-release/2015/04/15/massive-drop-in-number-of-unbanked-says-new-report

2. Red privada. Se trata de una cadena de bloques autorizada. Las cadenas de bloques privadas funcionan en base a controles de acceso que restringen a las personas que pueden participar en la red. Hay una o más entidades que controlan la red y esto lleva a depender de terceros para realizar transacciones. En una cadena de bloques privada, solo las entidades que participan en una transacción tendrán conocimiento sobre ella, mientras que las demás no podrán acceder a ella. *Hyperledger* Fabric de la Fundación Linux es un ejemplo perfecto de una cadena de bloques privada.
3. Red híbrida: La cadena de bloques híbrida se define como la cadena de bloques que intenta utilizar la mejor parte de las soluciones de cadenas de bloques públicas y privadas. En un mundo ideal, una cadena de bloques híbrida significará acceso controlado y libertad al mismo tiempo. La arquitectura híbrida de *blockchain* se distingue del hecho de que no está abierta a todos, pero aún ofrece características de *blockchain* como integridad, transparencia y seguridad.

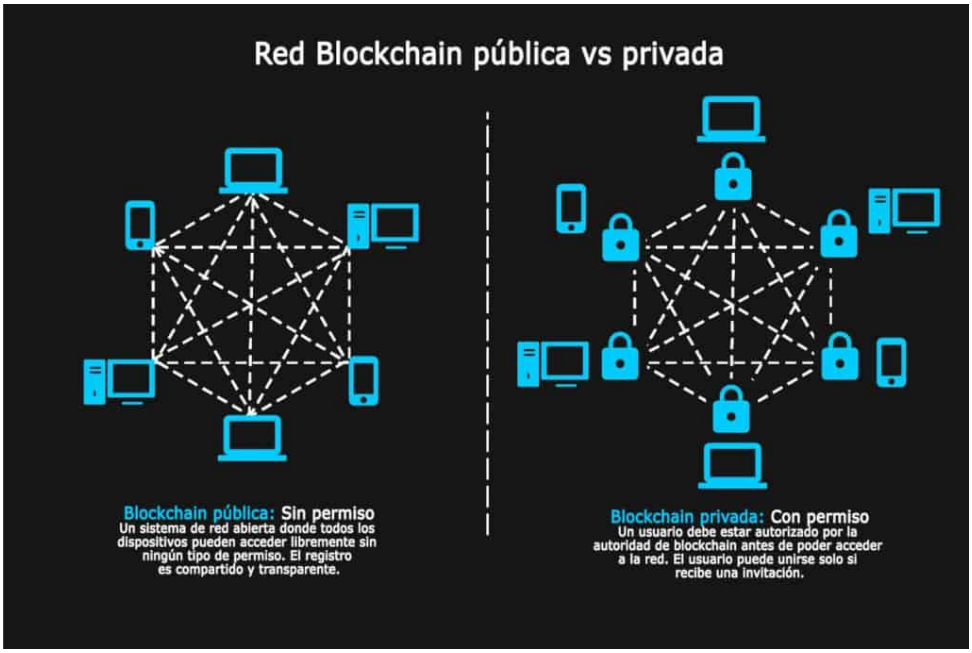

Figura 1: Diferencia entre red pública y privada

3. Funcionamiento y marco técnico del *Blockchain*.

3.1. *Hash* criptográfico

Para poder entender correctamente la tecnología de la cadena de bloques, es importante entender el funcionamiento del *hash* criptográfico, ya que todo gira alrededor del mismo.

3.1.1. Función *Hash*

El término *hash* proviene de la analogía del significado del vocablo anglosajón, traducido como “picar y mezclar”. El término *hash* no tiene una traducción literal al español, por lo que se usan directamente “*hash*” y “*hashing*”.

En el mundo de la criptografía han recibido este nombre debido a que este tipo de funciones y algoritmos realizan “picadillos” y “mezclas” con los *bits* de los mensajes.

Una función *hash*, es la encargada sintetizar una gran cantidad de datos, contenidos en la cadena de bloques; lo que hace que también se conozca como función resumen, y cuya finalidad es proteger los datos mediante la generación de claves, denominadas “llaves”.

Para la construcción de un *hash*, es preciso el uso de procedimientos matemáticos complejos, siendo, entre otras, las funciones modulares las que garantizan la característica principal de unidireccionalidad. Una explicación más sencilla es la siguiente: las funciones modulares crean el remanente de una división (Pérez, s.f.). Por ejemplo, 11 md 2 = 1, porque la división 11 entre 2, es 5 más un remanente de 1.

Como hemos dicho anteriormente, para construir un *hash* necesitamos una llave (Y) md 7 = 2. Al ser una llave privada, solo el usuario conocerá el valor de Y. En este caso, a modo de ejemplo, suponemos que, Y es 37, ya que 37 entre 7 es 5 más el remanente de 2. Suponemos, también, que 7 es el dato de una transacción realizada, y que 2 es el *hash* de esa transacción. Sabiendo que los datos son públicos, es imposible adivinar que la llave privada es 37, ya que si resolvemos esa ecuación con 2 y 7 obtenemos infinitas soluciones.

3.1.2. Características de una función *hash.*

Las características principales de las funciones hash son las siguientes:

- **Unidireccionalidad:** entendemos la unidireccionalidad, desde un punto de vista matemático, como la posibilidad de resolver una ecuación de forma simple, resultando imposible realizar la operación inversa para obtener la ecuación inicial. Lo mismo debe ocurrir en una función *hash*, pues debe ser computacionalmente imposible encontrar el mensaje a partir del cual se ha formado el *hash*.

Mensaje	Hash SHA-256
Hola	5AEABDFF63D243EDE0CF64001A9AE5396E12F02EEB78A6E5DA2FF54CEB9D7A6B
Que	73C130BB62CA66815BDD028F5923337AA8065CCD1428D0AEC0B357E5A4B6ACFE
Tal	0DA10BCDCA1967CE9AD378F4B59A9F5ACF2CF38A1733CBF2661F43550A296DF2[5]

Como podemos ver, es imposible obtener el mensaje a partir del *hash*.

- **Compresión:** realiza una reducción del tamaño de *bits* del archivo generando un resumen y un identificativo único del mismo.
- **Inmutabilidad:** los algoritmos deben asegurar que, ante cualquier modificación del dato del archivo original, éstos generarán un *hash* distinto del primero.

Mensaje	Hash SHA-256
Hola	5AEABDFF63D243EDE0CF64001A9AE5396E12F02EEB78A6E5DA2FF54CEB9D7A6B
hola	133EE989293F92736301280C6F14C89D521200C17DCDCECCA30CD20705332D44
ola	55A9F4F8994B1BBF2058EA38C8EFB6C459000814D5F39C087002571639E6230E

- **Únicos:** nunca pueden existir dos mensajes cuyos *hashes* sean idénticos, siempre y cuando utilicen el mismo algoritmo.

3.1.3. Sobre tipos de *hash*.

[5] Dichos Hashes han sido generados por el algoritmo SHA 256 en: https://passwordsgenerator.net/sha256-hash-generator/

Existen una gran variedad de tipos de funciones *hash*, pero cada una funciona de manera diferente, ofreciendo distintos grados de seguridad, aunque quizás, los más conocidos sean los SHA (*Secure Hash Algorithm*).

Los *Hashes SHA* fueron diseñados por la Agencia Nacional de Seguridad (NSA) estadounidense. Dentro de los SHA, el más conocido y usado en criptografía es el SHA-256 pues fue el escogido por Satoshi Nakamoto para hacer funcionar la cadena de bloques de *Bitcoin*. Consiste en un algoritmo en el que no importa los datos que tenga dentro, y devolverá una cadena de 256 bits, y eso es lo que llamamos huella digital. Lo que sale parece que sea aleatorio, pero, sin embargo, está determinado. Como hemos mencionado anteriormente, si el usuario modifica cualquier dato de lo que contenga ese *hash*, automáticamente, el algoritmo nos facilitará otro *hash* totalmente diferente.

En la siguiente tabla se muestran los diferentes algoritmos *SHA* y su tamaño de salida:

Algoritmo y variante		Tamaño de salida (bits).
MD5 (como referencia)		128
SHA-0		160
SHA-1		160
SHA-2	*SHA-224*	224
	SHA-256	256
	SHA-384	384
	SHA-512	512
	SHA-512/224	224
	SHA-512/256	256
SHA-3		224/256/384/512

Tabla 1: Algoritmos SHA

3.1.4. Árbol de Merkle

La cadena de bloques va almacenando una multitud de datos, y, con ello, el tamaño de los bloques va aumentando progresivamente con el tiempo pues siempre se va incorporando información. Por este motivo, surge la necesidad de acceder a la cadena de forma eficaz, permitiendo realizar

consultas sin tener que disponer de toda esa información almacenada. Así, en *Bitcoin* se decide utilizar lo que se conoce como *hash* de Merkle (Merkle, 1987).

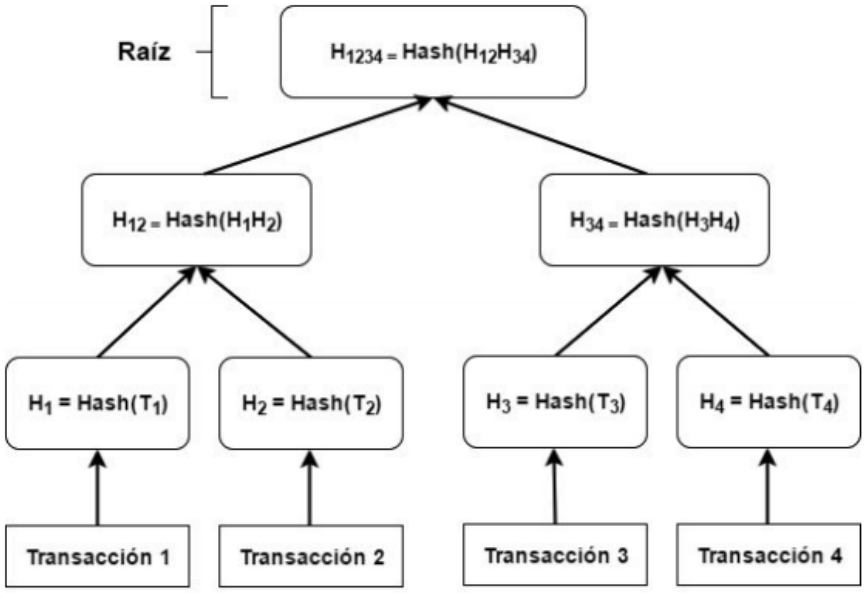

Figura 2: Árbol de Merkle[6]

Como podemos ver en la imagen anterior, dicho árbol de *hashes* posibilita el almacenamiento de diversos módulos de información independiente, que, en el caso de *Bitcoin*, se corresponden con transacciones.

El uso de esta estructura hace que los datos permanezcan seguros e imposibilita alteraciones en los mismos. De igual modo, hacen más rápida la búsqueda autenticada de los datos, sin tener que disponer de toda la información almacenada en el árbol. Así, "*en particular, se puede consultar de forma autenticada cualquier contenido del árbol con una cantidad de valores hash proporcional al logaritmo de números de nodos del árbol*" (Dolader Retamal, Bel Roig, & Muñoz Tapia).

3.2. Firmas Digitales

[6] (Dolader Retamal, Bel Roig, & Muñoz Tapia)

Una firma digital, es un esquema matemático, utilizado para verificar la autenticidad de mensajes o documentos digitales. Una firma digital válida, garantiza la integridad de la información (utilizando un algoritmo *hash*) para asegurar la inmutabilidad del mensaje, que ha sido previamente creado por el remitente (autenticación) y éste no puede negar haber enviado el mensaje (no repudio). La firma digital tiene que ser auténtica, infalsificable, no reutilizable, inalterable e irrevocable.

En cuanto a las firmas digitales se trata, hemos de hacer mención a la "criptografía asimétrica" o "de llave pública", ya que se configura como una parte indispensable del funcionamiento de la misma. Es un sistema criptográfico que utiliza pares de claves: claves públicas, que pueden ser conocidas por otros; y, claves privadas que puede que nunca serán conocidas por nadie excepto por el propietario. La generación de tales pares de claves depende de algoritmos criptográficos basados en problemas matemáticos denominados funciones unidireccionales. La seguridad efectiva requiere mantener privada la clave privada y la clave pública se puede distribuir abiertamente sin comprometer la seguridad (Das & Veni Madhavan, 2009).

3.2.1. Desarrollo de una firma digital.

En el ejemplo que se muestra a continuación, se muestra cómo se crea una firma digital y su recorrido.

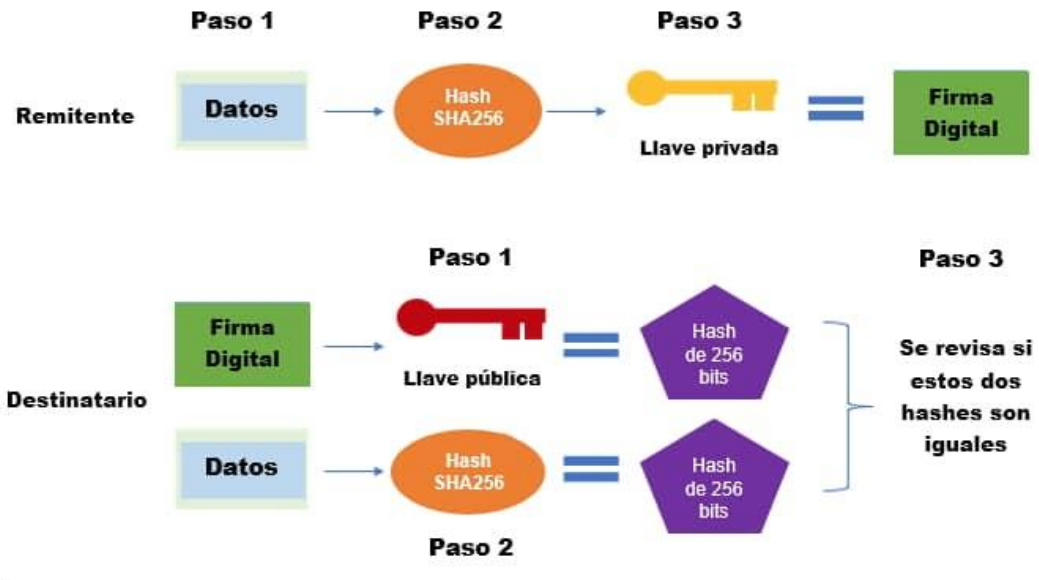

Figura 3: : Proceso de una firma digital[7]

Suponemos que un usuario A, de una cadena de bloques, le quiere transferir un *Bitcoin* (BTC) a un usuario B de la red. Previamente, ambos usuarios necesitarán obtener las claves criptográficas para poder transar las operaciones y, deberán crearse un monedero digital (*wallet*).

De esta forma, para que sea válida dicha transacción, ésta debe ser firmada por A con su llave privada y B debería verificar la autenticidad de esa firma.

Los pasos que sigue dicha transacción son los siguientes:

1. Se toman los datos de la transacción de A y al ser *Bitcoin*, se emplea el algoritmo SHA-256 cifrando los mismos con un *hash* de 64 caracteres.
2. Dicho *hash* se firma con la llave privada de A. Debido al algoritmo usado en *Bitcoin* (se explicará en el siguiente epígrafe), como resultado de esa firma, aparecen dos números X e Y con 71, 72 o 73 *bits* de longitud (CRYPTOGRAPHY, s.f.). Eso es lo que conocemos como firma digital.
3. Al usuario B se le envían los datos de dicha transacción, la firma digital y la clave pública de A.
4. Con la llave pública de A, B puede obtener la firma digital, pero sin saber la clave privada de A, consiguiendo así el *hash* de 64 caracteres que hacen referencia a los datos de la transacción.
5. Los datos son recibidos por B, y el sistema realiza el mismo proceso de cifrarlos con SHA-256 para obtener el *hash* correspondiente.
6. Los *hashes* del paso 4 y del 5 deben ser exactamente idénticos. Si esto no ocurre, quiere decir que los datos han sido modificados, o no hay coincidencia entre la clave pública y

[7] https://www.criptonoticias.com/criptopedia/blockchain-bloques-transacciones-firmas-digitales-hashes/#Sobre_los_tipos_de_hash

privada de A. Por lo que la transacción no se llevaría a cabo en cuanto existe la posibilidad de que haya sido alterada.

3.2.2. Características de una firma digital segura.

La ECDSA (*Elliptical Curve Digital Signature Algorithm*) en español, algoritmo de firma digital de curva elíptica, es la criptografía detrás de las claves públicas y privadas utilizadas en *Bitcoin*. Consiste en combinar las matemáticas detrás de campos finitos y curvas elípticas para crear ecuaciones unidireccionales, lo que significa que puede elegir su clave privada (algún número) y calcular fácilmente su clave pública (algún otro número). Sin embargo, no puedo tomar mi clave pública (ni la de nadie más) y calcular fácilmente su clave privada. De hecho, para *Bitcoin* se necesitarían billones de dispositivos, billones de años de trabajo de averiguación continua de diferentes claves privadas, para descubrir cuál crea una determinada clave pública (Marshall, 2018).

Hemos mencionado uno de los muchos algoritmos que hay para crear claves. Sin embargo, las características comunes que han de tener los algoritmos son las siguientes:

- **Autenticación:** la firma debe garantizar al destinatario, que el documento, o transacción, proviene de un usuario concreto, y que, a través de la misma, se pueda verificar la identidad del remitente.
- **Integridad:** esta propiedad garantiza que los datos lleguen al destinatario sin haber sido modificados. Los datos pueden llegar a ser vistos y modificados por algún *hacker,* pero al ser modificados, la firma cambiaría, y por lo tanto no sería válida.
- **No repudio:** dicha propiedad es un concepto legal, e implica que un usuario al realizar una transacción o una operación, jamás podrá negar lo que haya podido hacer.

3.3. Minería.

Como hemos visto, con la creación de cada nuevo bloque se ha de producir un *hash*, que, mediante un protocolo matemático, identifica una función criptográfica, cuyo objetivo primordial es el de encriptar toda la información contenida en el bloque. Este proceso de asociación de *hashes* a los bloques se materializa bajo el denominado proceso de "minería" o "*mining*", configurado como un procedimiento por el cual los "mineros" confirman y transmiten, mediante dicho protocolo matemático, las transacciones que están a la espera de ser incluidas en una determinada cadena de bloques, conforme a la verificación de demás mineros, imposibilitando la posterior mutabilidad de los bloques anteriores (Padilla Sánchez, 2020).

Por este motivo, el *mining*, es un proceso informático P2P. La minería en *Blockchain* se utiliza para asegurar y verificar las transacciones de *bitcoin*. Esta involucra a los mineros de *Blockchain,* que agregan datos de transacciones de *Bitcoin* al libro mayor público de *Bitcoin*. Así, una de las funciones principales de los mineros es la de asegurar los bloques, y conectarlos entre sí, de tal forma que surge la cadena de bloques, quedando registro de todo ello en los libros de contabilidad. A diferencia de los sistemas tradicionales de servicios financieros, *Bitcoin* no tiene sistema central, sino que las transacciones que se realicen en el marco de *Bitcoin* se verifican mediante sistemas descentralizados en los que actúan como colaboradores los usuarios que aportan recursos informáticos, con el fin de verificarlas.

Esencialmente, el término 'minería de *Blockchain*' se utiliza para describir el proceso de adición registros de transacciones a la cadena de bloques de *Bitcoin*. En definitiva, el procesamiento de las transacciones y la seguridad en el movimiento de dinero de forma segura en *Bitcoin,* se completa mediante el procedimiento de adición de bloques a la cadena.

Cualquier persona puede optar a convertirse en minero de *Blockchain*. Estos mineros de *Blockchain* instalan y ejecutan un software especial de minería de *Blockchain* que permite a sus dispositivos conumicarse de forma segura entre sí. Una vez que dicho software ha sido instalado, se une a la red

y comienza a extraer *bitcoins*, se convierte en lo que se llama un 'nodo'. Juntos, todos estos nodos se comunican entre sí y procesan transacciones para agregar nuevos bloques a la cadena de bloques, formando de esta forma la red *bitcoin*, la cual nunca está inactiva (Abdullah Aljabr, Sharma, & Kumar, 2019).

3.3.1. Etapas del proceso de minado.

3.3.1.1. Envío de la transacción.

Con esta primera etapa se inicia el proceso de minado, que ocurre cuando un usuario de la cadena de bloques desea enviar un *bitcoin* a otro usuario de la misma cadena. Para ello, el usuario emisor debe hacer uso de su cartera digital (*wallet*) y, una vez que su transacción haya sido realizada y confirmada, ésta podrá ser minada e incluida en un bloque.

3.3.1.2. Agrupación.

En esta segunda etapa, los nodos mineros son los encargados de agrupar todas esas transacciones pendientes en la red, y, una vez minado dicho bloque, se confirmará la transacción.

3.3.1.3. Formación de un nuevo bloque.

Los mineros deben elegir qué transacciones van a incluir, para así poder formar su bloque. Puede ocurrir que el minero incluya transacciones que ya están validadas en su bloque, por lo que dichas transacciones validadas serán eliminadas del mismo.

Una vez generado el bloque, éste deberá someterse a una prueba de trabajo (PoW) para poder ser validado, mientras tanto, se le denomina bloque candidato.

3.3.1.4. PoW.

Una vez que el minero haya generado su bloque con las transacciones correspondientes, éste debe someterse a una prueba de trabajo con el fin de encontrar una firma válida.

Esta prueba de trabajo, o *proof of work* (PoW) consiste en que cada minero debe llevar a cabo un procedimiento matemático, único para cada bloque que haya formado. Dicho proceso se repite para cada bloque que sea creado, y es idéntico para todos, siendo su resultado único para cada bloque.

La solución que deben encontrar los mineros con ese proceso es lo que hemos llamado *hash*, ya comentado anteriormente. Para encontrar dicho *hash*, los mineros deben hacer cálculos matemáticos de forma reiterada a través de un *nonce*, entendiendo por *nonce* un número aleatorio utilizado y cambiado continuamente hasta encontrar un *hash* de salida que sea válido. Es imposible predecir qué *nonce* va a poder resolver dicho problema, por ello, se deben utilizar tantos como se necesiten, implicando el uso de millones de *nonces*.

3.3.1.5. Transmisión.

En esta quinta etapa, el minero se supone que ya ha encontrado un *hash* de salida válido para cada bloque, por lo tanto, éste transmite el bloque con la firma a los demás nodos de la *blockchain* para estos puedan validar el mismo.

Después del proceso de minado, el minero recibe su recompensa, poniendo así nuevos *bitcoins* en movimiento.

3.3.1.6. Verificación

En esta etapa, como su nombre indica, se verifican varias cosas. La primera es que el bloque y el hash cumplan con las condiciones del sistema. En segundo lugar, se verifica la *PoW*, garantizándole al minero que puede hacer uso de *bitcoins* que ha obtenido gracias a la resolución del proceso de minado.

3.3.1.7. Confirmación

Cuando un bloque se ha añadido a la cadena de bloques, los bloques que sean añadidos posteriormente, se usarán también como una prueba de validez, ya que como su nombre indica, al ser una cadena, un bloque va enlazado con otro, dentro de la misma cadena. Esto es, que en el momento en que el minero consiga un *hash* válido, durante ese proceso se han podido minar nuevos bloques, por lo que el *hash* de salida del bloque que se está minando, puede no coincidir con el *hash* del bloque que le precede, por lo tanto, ese *hash* será rechazado.

3.3.2. Estructura de un bloque

Una vez adquiridos los conocimientos de cómo se forma un bloque, podemos comprender cómo se forma la cabecera del mismo. Esta incluye 6 datos principales:

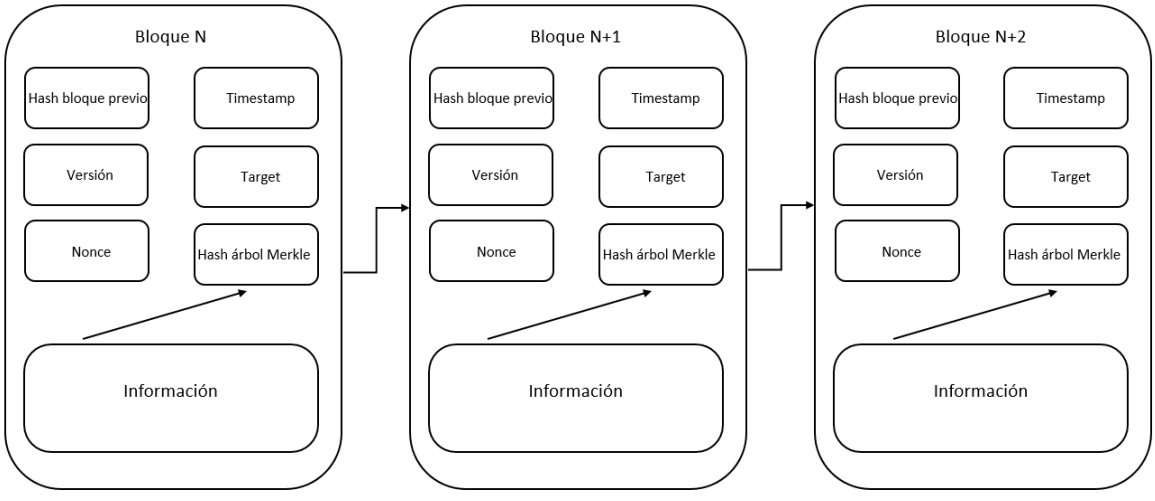

Figura 4: Ilustración cabecera de bloque (Elaboración propia)

- Versión: En un software, la versión va cambiando dependiendo del número de actualizaciones de la misma. Pues en la cadena de bloques ocurre lo mismo, y se muestra la versión del software en el momento que fue minado dicho bloque. El software de bitcoin, por ejemplo, ha tenido en 2019 unas 56 versiones. (Pérez, s.f.)
- *Hash* del bloque anterior: Es un valor alfanumérico de 64 bits en el caso del *bitcoin*, y hace que los bloques queden vinculados de forma secuencial formando la cadena de bloques.
- Raíz de Merkle: Este valor permite que se pueda hacer referencia a todos los datos de un bloque. Esto es importante a la hora de hacer consultas sobre de la información contenida en un bloque, puedes acceder a ella de forma segura y eficiente. (Dolader Retamal, Bel Roig, & Muñoz Tapia)
- Marca de tiempo (*Timestamp*): Como bien indica su nombre, indica el momento exacto en el que fue minado el bloque.
- Objetivo (*Target*): Es un numero de 256 bits que se les facilita a los mineros, indicando cual puede ser el *hash* correcto.
- *Nonce*: Es un número al azar que los mineros han utilizado para encontrar el *hash* valido para el bloque.
- Información: Dicha información hace referencia a los datos de la transacción.

3.3.3. Características de un bloque

Los bloques que hayan sido minados dentro de la red de *Bitcoin*, para que sean válidos, deben cumplir unas condiciones. Veamos cuales son:

- El hash que aparece en la cabecera de cada bloque tiene que ser menor que el target. De lo contrario, no será válido.
- El tamaño de cada bloque minado tiene límites. En *Bitcoin*, un bloque debe tener un tamaño máximo de 2 MB.

- El *Timestamp* del bloque debe ser inferior a dos horas en el futuro. Todas las transacciones añadidas al bloque son válidas.

4. ¿Para qué se usa realmente la tecnología *blockchain*?

Hoy en día, la *blockchain* tiene una gran variedad de casos de uso potenciales, además de servir como combustible detrás del *bitcoin*. Hablaremos de tres grandes grupos:

1. En banca y finanzas
2. Aplicaciones en los negocios
3. Aplicaciones gubernamentales
4. Aplicaciones en otras industrias

4.1. Casos de uso de la *blockchain* en banca y finanzas

4.1.1. Pagos internacionales

Blockchain proporciona una forma de crear de manera segura y eficiente un registro de actividad sensible a prueba de manipulaciones. Esto lo hace excelente para pagos internacionales y transferencias de dinero.

Por ejemplo, en abril de 2018, Banco Santander lanzó el primer servicio de transferencia de dinero basado en *blockchain* del mundo. Conocido como "Santander One Pay FX" (Santander Corporate Comunications, 2018)

Al automatizar todo el proceso en la cadena de bloques, Santander ha reducido la cantidad de intermediarios que normalmente se requieren en estas transacciones, lo que hace que el proceso sea más eficiente.

4.1.2. Los mercados capitales

Los sistemas basados en *blockchain* también tienen el potencial de mejorar los mercados de capitales. Un informe de McKinsey identifica los beneficios que las soluciones *blockchain* ofrecen a los mercados de capital, algunos de los cuales incluyen: (McKinsey & Company, 2015)

- Compensación y liquidación más rápidas
- Auditorías consolidadas
- Mejoras operativas

4.1.3. Financiamiento comercial

Los métodos históricos de financiación del comercio han sido un problema importante para las empresas porque los procesos lentos a menudo interrumpen el negocio y hacen de la liquidez difícil de manejar. El comercio transfronterizo involucra una gran cantidad de variables al comunicar información, como el país de origen y los detalles del producto, y las transacciones generan grandes volúmenes de documentación.

Blockchain tiene la capacidad de agilizar los acuerdos de financiamiento comercial y simplificar el proceso transfronterizo. Permite a las empresas realizar transacciones entre sí más fácilmente más allá de los límites regionales o geográficos.

4.1.4. Protección contra blanqueo de capitales

Una vez más, el cifrado que es tan integral en *blockchain* lo hace sumamente útil para combatir el lavado de dinero. La tecnología subyacente permite el mantenimiento de registros, lo que respalda "Conozca a su cliente", del inglés, *Know your customer* (NYK), el proceso mediante el cual una empresa identifica y verifica las identidades de sus clientes.

4.1.5. Transacciones de igual a igual (peer-to-peer)

Los servicios de pago P2P tienen límites. Algunos servicios restringen las transacciones según la geografía. Otros cobran una tarifa por su uso. Y

muchos son vulnerables a los piratas informáticos, lo que no resulta atractivo para los clientes que divulgan su información financiera personal. La tecnología *Blockchain*, con todos sus beneficios antes mencionados, podría solucionar estos obstáculos.

4.1.6. Seguros

Podría decirse que la mayor aplicación de *blockchain* para seguros es a través de contratos inteligentes (*smart contracts*). Estos contratos permiten a los clientes y aseguradoras gestionar las reclamaciones de forma transparente y segura. Todos los contratos y reclamaciones pueden registrarse en la cadena de bloques y validarse por la red, lo que eliminaría las reclamaciones no válidas, ya que la cadena de bloques rechazaría múltiples reclamaciones en el mismo accidente.

4.2. Aplicaciones de la *blockchain* en el mundo de los negocios

4.2.1. Gestión de la cadena de suministro

El libro de contabilidad inmutable de *Blockchain* lo hace muy adecuado para tareas como el seguimiento en tiempo real de los bienes a medida que se mueven y cambian de manos a lo largo de la cadena de suministro. El uso de una cadena de bloques abre varias opciones para las empresas que transportan estos productos. Las entradas en una cadena de bloques se pueden usar para poner en cola eventos con una cadena de suministro, por ejemplo, asignar mercancías recién llegadas a un puerto a diferentes contenedores de envío. *Blockchain* proporciona un medio nuevo y dinámico para organizar los datos de seguimiento y ponerlos en práctica.

4.2.2. Historial clínico

Los datos de salud que son adecuados para *blockchain* incluyen información general como la edad, el sexo y datos del historial médico potencialmente básico, como el historial de inmunizaciones o los signos

vitales. Por sí sola, ninguna de esta información podría identificar específicamente a ningún paciente en particular, que es lo que permite que se almacene en una cadena de bloques compartida a la que puedan acceder numerosas personas sin preocupaciones de privacidad indebidas.

4.2.3. Transacciones de suministro de energía

La tecnología *Blockchain* podría usarse para ejecutar transacciones de suministro de energía, pero también para proporcionar la base para los procesos de medición, facturación y compensación (PWC). Otras aplicaciones potenciales incluyen documentación de propiedad, gestión de activos, garantías de origen, derechos de emisión y certificados de energía renovable.

4.2.4. Medios de comunicación

Las empresas de medios ya han comenzado a adoptar la tecnología *blockchain* para eliminar el fraude, reducir los costos e incluso proteger los derechos de propiedad intelectual (IP) del contenido, como los registros de música.

4.3. Uso de la tecnología *blockchain* dentro del gobierno

4.3.1. Gestión de registros

Los gobiernos nacionales, estatales y locales son responsables de mantener los registros de las personas, como fechas de nacimiento y defunción, estado civil o transferencias de propiedad. Sin embargo, administrar estos datos puede ser difícil y, hasta el día de hoy, algunos de estos registros solo existen en papel. Y, a veces, los ciudadanos tienen que acudir físicamente a las oficinas del gobierno local para realizar cambios, lo que requiere mucho tiempo, es innecesario y frustrante. La tecnología *Blockchain* podría simplificar este mantenimiento de registros y hacer que los datos sean mucho más seguros.

4.3.2. Votación

La tecnología *Blockchain* tiene la capacidad de hacer que el proceso de votación sea más accesible al tiempo que mejora la seguridad. Los piratas informáticos no serían rivales para la tecnología *blockchain*, porque incluso si alguien tuviera acceso a la terminal, no podrían afectar a otros nodos. Cada voto se atribuiría a una identificación y, dado que la capacidad de crear una identificación falsa es imposible, los funcionarios del gobierno podrían contar los votos de manera más eficiente y efectiva.

4.3.3. Impuestos

La tecnología *blockchain* podría hacer que el engorroso proceso de presentación de impuestos, que es propenso a errores humanos, sea mucho más eficiente con suficiente información almacenada en *blockchain*.

4.4. Aplicaciones en otras industrias

4.4.1. Ciberseguridad

La mayor ventaja de *blockchain* en ciberseguridad es que elimina el riesgo de un solo punto de falla. La tecnología *Blockchain* también proporciona cifrado y privacidad de un extremo a otro.

4.4.2. Big Data

La naturaleza inmutable de *blockchain*, y el hecho de que cada computadora en la red verifica continuamente la información almacenada en

ella, hace que *blockchain* sea una excelente herramienta para almacenar *big data.*

5. Aplicación de *Blockchain* en la cadena de suministro

Una vez entendido el funcionamiento de dicha tecnología, yo podemos hablar del tema principal sobre el que se desarrolla dicho trabajo de investigación.

Hoy en día, la gestión de las cadenas de suministro, es algo que se ha ido convirtiendo en una tarea cada vez más complicada. Esto ha ocurrido gracias a que cada vez se distribuyen más productos, a diferentes ubicaciones geográficas, llevando a cabo un sinfín de facturas, pagos, cobros, cada uno de ellos perteneciente de diferentes partes del mundo. Esto conlleva que, para la organización y el desarrollo de la misma, es necesario contar con un gran número de personas físicas y jurídicas que se hagan cargo de diferentes tareas. Es por ello que la complejidad y la falta de transparencia, han obligado a explorar acerca de la posibilidad de usar blockchain en la cadena de suministro.

En este apartado iremos viendo que dicha tecnología ha nacido para satisfacer las necesidades y resolver los problemas que la cadena de suministro tiene. Al final de este epígrafe, podremos decir que uno de los ámbitos dónde más ventajas ha aportado dicha tecnología es en la cadena de suministro.

5.1. ¿Qué es la gestión de la cadena de suministro?

Como sabemos, cuando nosotros compramos un producto, antes de llegar a estar a la venta, este pasa por muchos procesos e intermediarios. Por lo tanto, este sistema de empresas, personas, actividades y recursos involucrados en el traslado de un producto del proveedor al cliente, se denomina cadena de suministro. Esta incluye tanto la planificación como la ejecución de diferentes procesos dentro de la misma. Entre estos procesos se incluyen: El flujo de materiales, el flujo de información y el flujo de capital financiero.

¿Por qué es necesaria una buena gestión de la cadena de suministro? Una buena gestión nos proporcionará una gran cantidad de beneficios de los cuales no solo serán económicos. Entre ellos destacaran:

- Aumento de ventas.
- Reducción de fraudes y gastos generales.
- Mejora la calidad.
- Mayor velocidad en la producción y en la distribución.
- Reducir costos durante el proceso de fabricación.

Todo esto es muy importante conocerlo, pero, ahora bien, si un proceso de fabricación cada vez va siendo más complejo, inevitablemente, la cadena de suministro se vuelve complicada, llegando a ser ineficiente en algunos casos. Es por ello que hoy en día, el proceso de gestión de la cadena de suministro tradicional se está quedando prácticamente obsoleto, necesitando una nueva forma de gestión como por ejemplo está siendo el Blockchain.

5.2. Problemas de la cadena de suministro tradicional

5.2.1. Dificultad para localizar

A la hora de fabricar un móvil, necesitamos muchos componentes de los cuales cada uno puede fabricarte en una parte del mundo diferente. Por eso uno de los mayores problemas existentes es la falta de transparencia. Si por ejemplo un componente sale defectuoso de su teléfono, será casi imposible determinar exactamente de dónde vino esa pieza defectuosa y, por tanto, quienes fueron las personas responsables.

A lo largo del año 2006, podemos ver un ejemplo claro de lo mencionado anteriormente. Varios estados de Estados Unidos, se vieron infectados por un brote de una enfernedad. Pero, ¿Quién fue el culpable? Una mala cosecha de espinacas. Como resultado de lo sucedido, la industria perteneciente a la alimentación, entró en caos. Se intentó rastrear de donde pertenecían las espinacas infectadas. Todos los proveedores de espinacas dejaron de vender. Finalmente, se encontró de donde provenían, pero al cabo de 2 o 3 semanas

de búsqueda constante. Las consecuencias fueron desastrosas. Todo se podía haber solucionado si hubiera una mejor manera de rastrear, para así poder dar con el lote defectuoso de forma inmediata.

5.2.2. Corrupción

Uno de los mayores problemas de una cadena de suministro compleja es que debe existir un grado de confianza extremo por parte de la dirección hacia las personas implicadas en ella, para que realmente hagan su trabajo. Pero muchas veces, las personas nos podemos equivocar, y orientarnos hacia un camino que no es el más adecuado, y no solo comprometemos la calidad de los productos y de la empresa en general, sino que los mayores implicados somos nosotros, nos vamos corrompiendo poco a poco. Y, además, esa confianza que nos habíamos ganado la perdemos, y hacemos que otras personas la pierdan.

Podemos poner varios ejemplos sobre lo expuesto anteriormente. Imaginemos que una empresa necesita un nuevo material para un nuevo producto. Sin embargo, ese material es un bien escaso y solo un proveedor puede proporcionarlo. Conociendo su monopolio, el proveedor puede estafarlo.

Otro ejemplo puede ser: En algún lugar de la cadena de suministro, alguien insiste en obtener un producto de un proveedor específico, sin mirar otras ofertas. Cuando se enfrentan, insisten en que solo ese proveedor puede cumplir con ciertas especificaciones, que pueden ser ciertas o no.

Así podemos encontrar infinidad de casos. Es por ello que también se quiere hacer uso de la cadena de bloques, para garantizar la seguridad dentro de la cadena de suministro.

5.2.3. Costes

Principalmente, dentro de la cadena de suministro nos podemos encontrar cuatro factores que hacen que los costes de la misma sean excesivos:

- Costes de adquisiciones
- Costes de transporte
- Costes de inventario

- Costes de calidad

5.2.3.1. Costes de adquisiciones

El coste de adquisiciones es básicamente el pago de los productos a lo largo de la cadena de suministro. En el caso de tener una empresa grande, el director de la misma, obviamente, no se será el encargado de ir a los proveedores y comprar los materiales y componentes necesarios. Es por eso que una persona o varias se tendrán que dedicar a realizar dicha tarea.

Por lo tanto, el coste de adquisición no será únicamente el coste de los productos o materiales, sino también será el salario y bonificaciones de la persona dedicadas a dicha labor.

5.2.3.2. Costes de transporte

Al hablar de los costes de transporte, nos enfrentamos a otro problema: tenemos que valorar que nos conviene, si velocidad o mayores gastos. Generalmente, las opciones de transporte de alta velocidad cuestan mucho dinero. Por otro lado, optar por una opción más económica puede comprometer en gran medida el tiempo, que es casi tan importante o más.

5.2.3.3. Costes de inventario

Los almacenes son lugares donde almacena los productos. Por lo tanto, llenar ese inventario de productos costará mucho dinero. Para eso, muchas empresas no tienen liquidez, y es por eso, que terminan pidiendo préstamos a los bancos para pagar los inventarios. Por lo tanto, no solo deben ocuparse del préstamo, sino también del interés del mismo.

Además, tener un inventario sin vigilancia que está lleno de sus cosas tiene mucho riesgo. No solo necesita contratar personas que puedan cuidar y catalogar sus productos, sino que también necesitará

personal de seguridad. A pesar de todos sus esfuerzos, aun así, muchos de sus productos podrían perderse, dañarse, ser robados, caducados o quedar obsoletos.

5.2.3.4. Costes de calidad

Después de todo, obtener productos defectuosos generará problemas más adelante en la cadena. Sin embargo, para realizar estos controles de calidad, deberá contratar a expertos debidamente capacitados. Además, también tenga en cuenta que una gran parte de sus productos se eliminará a la vez.

5.2.4. Globalización

La globalización es el proceso mediante el cual una empresa se vuelve lo suficientemente grande como para tener influencia internacional o comienza a operar a escala internacional. Dicha globalización presenta varios desafíos para la gestión de la cadena de suministro.

Muchas empresas necesitan ejecutar su cadena de suministro a través de varios países para adquirir diferentes partes de sus productos. Sin embargo, esto trae muchas complicaciones. Por ejemplo, los proveedores se pueden encontar en ubicaciones geográficas muy diferentes, lo que dificulta la coordinación y la colaboración. En otras palabras, es muy difícil saber si realmente están haciendo su trabajo o no.

5.2.5. Conclusión

Entonces, hay dos cosas que hemos aprendido hasta ahora:

- Las cadenas de suministro son absolutamente críticas para el bienestar general de un negocio.

- El sistema actual de cadenas de suministro está desactualizado y requiere un reinicio significativo. Por eso se necesita una cadena de suministro gobernada por la cadena de bloques.

5.3. ¿Cómo entrará la tecnología blockchain en la cadena de suministro?

Entonces, por lo que hemos conocido hasta ahora, la tecnología blockchain tiene propiedades de descentralización, transparencia e inmutabilidad. Como tal, es la herramienta perfecta a utilizar para la interrupción de la industria de gestión de la cadena de suministro.

Cada vez que un producto cambia de manos, la transacción podría documentarse en la cadena de bloques, creando un historial permanente de un producto, desde la fabricación hasta la venta, consiguiendo una trazabilidad del producto perfecta. Con esto se reducen los retrasos de tiempo, el error humano y algunos costos agregados.

5.4. Mejoras que se consiguen con la tecnología blockchain.

Algunos de los beneficios que la cadena de bloques puede aportar al sistema son los siguientes:

- La transparencia de Blockchain ayuda en la documentación cuidadosa del viaje de un producto desde su punto de origen hasta todos sus proveedores. Esto aumenta la confianza entre las distintas partes de la cadena de suministro porque todos los datos están visibles para que todos los vean.
- La red blockchain puede acoger a todos y cada uno de los participantes de la red de la cadena de suministro. Además, independientemente de su ubicación geográfica, todos podrán conectarse con la cadena de bloques.
- La inmutabilidad de Blockchain asegurará que todos los registros de la cadena sean honestos y libres de corrupción. Además, la sólida seguridad de su criptografía innata eliminará auditorías innecesarias, ahorrando una gran cantidad de tiempo y dinero.

- La utilización de blockchain también abre las puertas a la innovación futura.

6. Casos de aplicación del blockchain a la gestión de la cadena de suministro

6.1. Walmart

En la descripción del problema de trazabilidad, hablábamos sobre un problema que surgió en 2006 acerca de una cepa mortal de E. coli en espinacas contaminadas, en la que murieron varias personas, y enfermaron muchas otras. El brote representa lo que puede suceder cuando el abastecimiento de alimentos y el rastreo de contaminaciones sale terriblemente mal.

Los consumidores, en general, dejaron de comer espinacas. Los restaurantes las sacaron del menú. Si se pudiera rastrear de dónde vino el problema más rápido, todo se podría haber solucionado rápidamente, garantizando la confianza del consumidor.

Walmart[8], una empresa norteamericana, se unió con IBM, para explorar cómo aplicar la tecnología blockchain, a sus cadenas de suministro de alimentos. Usando blockchain, los empleados de Walmart pueden rastrear algunos productos hasta sus raíces, literalmente. Después de escanear mangos o un par de docenas de otros productos con la aplicación de la tienda, los empleados pueden ver de dónde proviene la fruta y dónde está almacenada en la trastienda. La tecnología podría ayudar a los clientes a comprender de dónde provienen sus alimentos y podría agilizar el proceso de reabastecimiento. En definitiva, las empresas quieren garantizar la trazabilidad del producto, desde el primer momento hasta su consumo final.

Uno de los titulares más llamativos es que Walmart e IBM se unieron para poner carne de cerdo china en una cadena de bloques.

Walmart planea utilizar tecnología desarrollada en la cadena de bloques, haciendo uso de una base de datos privada desarrollada conjuntamente por IBM. Dicha base de datos está diseñada para proporcionar al minorista una forma de

[8] https://fortune.com/company/walmart/

registrar de manera indeleble una lista de transacciones que indique cómo la carne fluyó a través de una red comercial, desde los productores hasta los procesadores, los distribuidores y finalmente, a los consumidores.

Los consumidores de hoy quieren más transparencia sobre dónde y cómo surgió un producto, ya que eso trasmite confianza y no pone en juego la integridad de la empresa que comercializa.

La información que se almacenará en la cadena de bloques, donde el fraude y las inexactitudes son mucho más difíciles de salirse con la suya, incluye detalles relacionados con el origen de la granja, datos de fábrica, fechas de vencimiento, temperaturas de almacenamiento y envío.

6.2. Starbucks: “Desde la siembra a la taza”

La franquicia multinacional Starbucks utilizará una red en la que se analizará el producto “desde la siembra a la taza”.

Starbucks está trabajando para facilitar un seguimiento del producto en tiempo real a lo largo de toda la cadena de suministro. La franquicia cuenta con la colaboración del servicio Blockchain de Microsoft, donde quedarán registrados todos los movimientos a lo largo del trayecto del café en un libro de contabilidad, otorgando a los usuarios una vista completa de toda la cadena de suministro.

El mayor problema que tiene dicha multinacional es que en 2018, se hizo un estudio acerca de la procedencia del café, en el cual, se vio que dichos granos de café venían de unas 380,000 fincas aproximadamente, de diferentes países como pueden ser Costa Rica, Ruanda o Colombia. Es por eso que decidieron sumergirse en una blockchain. Además, se ha observado que, para el amante del café, conocer el lugar de origen del grano de café que va a consumir, es un dato de gran interés. (Blanco, 2019)

¿Cómo lo ha hecho Starbucks? Principalmente creando una aplicación móvil en la que todos los consumidores podrán ver toda la información acerca del origen, tostado del café, sabores, esencias, etc. En definitiva, una aplicación primordial para la persona amante del café.

Michelle Burns, vicepresidenta senior de Starbucks, comentaba que "Este tipo de transparencia ofrece a los clientes la oportunidad de ver que el café que disfrutan, es el resultado de que muchas personas se preocupan".

6.3. Maersk

En el año 2018, IBM y Maersk finalizaron su prueba piloto de cadena de suministro digitalizada de extremo a extremo utilizando tecnología blockchain. Al terminar dicha pruaba piloto, IBM estimó, que pasar a la tecnología completamente digital podría ahorrarles a los transportistas alrededor de $ 38 mil millones cada año[9]. Con la unión de IBM y Maersk nació una plataforma que se llama Tradelens, que es la encargada de los "contenedores tecnológicos"

Como resultado del uso de la plataforma TradeLens durante la prueba piloto, se pudo observar que las ventajas fueron notables:

- Se redujo el costo del papeleo. Por ejemplo, cuando se envían aguacates de Mombasa a Rotterdam, los costos representan $ 300 o entre el 15 y el 20% del costo de envío. TradeLens redujo estos costos en un 70-90% dependiendo de la cadena de suministro específica y su lista de participantes[10].
- Los tiempos de envío reducidos. En el marco de Estados Unidos, el transporte de mercancías disminuyó un 40%. Principalmente por la reducción de colas y la agilización del flujo de trabajo. En cadenas de suministro largas, la ganancia de tiempo es menor.
- Reducir la cantidad de pasos que se toman para responder preguntas operativas básicas, como "¿dónde está mi contenedor?".

6.4. British Airways

[9] https://supplychaindigital.com/technology-4/maersk-and-ibm-are-bringing-blockchain-tech-shipping-industry
[10] https://merehead.com/blog/maersk-blockchain-use-case/

La firma de tecnología de SITA ha construido un sistema de cadena de bloques con permiso privado llamado FlightChain, que almacena información de vuelo y utiliza contratos inteligentes para juzgar información potencialmente conflictiva. El ingeniero principal de SITA explica cómo blockchain podría crear una única 'fuente de verdad' para los datos de vuelo.

La compañía creó una cadena de bloques con permiso privado para los participantes en el proyecto, British Airways, el aeropuerto de Ginebra, Heathrow y el aeropuerto internacional de Miami. Estos proporcionaron datos de vuelo que se fusionaron y almacenaron en la cadena de bloques. Durante este proyecto, el contrato inteligente procesó más de dos millones de cambios de vuelo y los almacenó en FlightChain.

El objetivo de FlightChain era descubrir cómo blockchain podía crear una única 'fuente de verdad' para varios datos utilizados por diferentes partes interesadas en la industria de la aviación.

El problema es que no existe una fuente única de la verdad sobre los datos de vuelo, y no todas las partes acceden fácilmente a los datos que existen. Si bien hay muchos casos de aerolíneas y aeropuertos que colaboran para compartir datos de vuelos, estos datos aún residen en silos separados. Cuando hay retrasos en los vuelos, esto da como resultado diferencias entre las aplicaciones para pasajeros, los sistemas de visualización de información de vuelo del aeropuerto y los agentes de las aerolíneas y los aeropuertos. Puede resultar difícil para los pasajeros y otras partes interesadas saber cuál es la información correcta.

SITA también está estudiando el uso de blockchain para la identidad soberana en los viajes aéreos. La identidad soberana permitirá a los pasajeros tener un mejor control sobre sus propios datos y con quién se comparten. Al mismo tiempo, puede permitir a los gobiernos tener una mayor confianza en la calidad de los datos que reciben sobre los pasajeros en el punto de llegada a un país.

7. Conclusión

La tecnología Blockchain está emergiendo de sus primeras implementaciones en y ahora está teniendo un impacto significativo en casi todas las industrias. Como una piedra tirada a un lago, las ondas de esta tecnología están comenzando a expandirse hacia afuera en todas las direcciones, incluyendo la industria de la logística, donde blockchain promete hacer procesos de negocio más eficientes y facilitan la innovación nuevos servicios y modelos de negocio.

Ya hay muchos proyectos en marcha para aplicar blockchain a la logística global, agregando valor al garantizar transparencia de la cadena de suministro y automatización administrativa de operaciones. Además, la tecnología blockchain se está cruzando con otras innovaciones para amplificar impacto, como pueden ser la inteligencia artificial, robótica, drones, etc, con lo que aún se puede desarrollar mucho más.

Parece que la tecnología blockchain y los sistemas de gestión de la cadena de suministro se crearon el uno para el otro. De hecho, como hemos visto, todas las inconvenientes de las cadenas de suministro actuales se pueden mitigar fácilmente mediante el uso de la tecnología blockchain. Creemos que esta es una de las industrias más importantes que la cadena de bloques puede interrumpir y cambiar para mejor. Realmente, lo sistemas de gestión de la cadena de suministro basados en blockchain pueden ser la norma en el futuro.

Bibliografía

1. Abdullah Aljabr, A., Sharma, A., & Kumar, K. (2019). Mining Process in Cryptocurrency Using Blockchain Technology: Bitcoin as a Case Study. *Journal of Computational and Theoretical Nanoscience*.
2. Amos K., K., Demeke G, B., & Rosanna A, E. (2019). Blockchain: It's Structure, Principles, Applications and Foreseen Issues. 13.
3. B. d. (2020). Blockchain e integridad: aplicaciones de política pública. *Innovacion digital*.
4. Blanco, L. Q. (2019). El Café de Starbucks ofrece Trazabilidad Blockchain a través de Microsoft.

5. Catchlove, P. (1 de Diciembre de 2017). Smart Contracts: A New Era of Contract Use.

6. CATCHLOVE, P. (2017). Smart Contracts: A New Era of Contract Use. Independent Research Project.

7. *CRYPTOGRAPHY*. (s.f.). Obtenido de https://crypto.stackexchange.com/questions/75996/probability-of-an-ecdsa-signature/75997#75997

8. Das, A., & Veni Madhavan. (2009). *Public-Key Cryptography: Theory and practice.* Pearson.

9. DE FILIPPI, P., & WRIGHT, A. (2018). Blockchain and the Law: The Rule of Code. Harvard University Press.

10. de Filippi, P., & Wright, A. (2019). *Blockchain and the Law: The Rule of Code.*

11. DEL CASTILLO IONOV, R. (2018). Las Initial Coin Offerings (ICOS) y la tockenización de la economía. Pamplona: Editorial Aranzadi.

12. Department of Finance. (2018). Virtual Currencies and Blockchain Technology. Obtenido de www.finance.gov.ie

13. DHL Customer Solutions & Innovation. (2018). *Blockchain in Logistics.*

14. Dolader Retamal, C., Bel Roig, J., & Muñoz Tapia, J. M. (s.f.). La Blockchain: Fundamentos, aplicaciones y relacion con otras tecnologias disruptivas.

15. Geroni, D. (28 de Enero de 2021). *101 Blockchains*. Obtenido de https://101blockchains.com/hybrid-blockchain/

16. Hero, F. (s.f.). Industry 4.0: A key enabler of resilient Supply Chains. *Forbes*.

17. Ionov, R. d. (2018). *Las initial coin offerings (ICOS) y la tokenización de la economía.* Pamplona, España: Aranzadi.

18. Jani, S. (2020). Smart Contracts: Building Blocks for Digital Transformation. 14.

19. Lecuit, J. A. (s.f.). *Real Instituto Elcano*. Obtenido de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciberseguridad/ari106-2019-alonsolecuit-seguridad-y-privacidad-del-blockchain-mas-alla-de-tecnologia-y-criptomoneda#:~:text=El%20blockchain%2

20. Magnuson, W. (2020). *Blockchain Democracy: Technology, law and the rule of the crowd.* Nueva York, Estados Unidos: Cambridge University Press.

21. Marshall, B. (2018). How does ECDSA work in Bitcoin. Obtenido de https://medium.com/@blairlmarshall/how-does-ecdsa-work-in-bitcoin-7819d201a3ec

22. Mattilda, J. (2016). *The Blockchain Phenomenon.*

23. McKinsey & Company. (2015). *Beyond the hype: Blockchains in capital markets.*

24. Merkle, R. (Agosto de 1987). A digital signature based on a conventional encryption function. 369-378.

25. Nakamoto, S. (s.f.). Bitcoin: A Peer-to-Peer Electronic Cash System. Obtenido de www.bitcoin.org

26. Orcutt, M. (25 de abril de 2018). *MIT Technology Review*. Obtenido de https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/

27. Padilla Sánchez, J. (2020). Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos. (39), 175-201.

28. Pérez, I. (s.f.). *Criptonoticias*. Obtenido de https://www.criptonoticias.com/criptopedia/blockchain-bloques-transacciones-firmas-digitales-hashes/#Propiedades_de_una_funcion_hash_segura

29. Piscini, E. (8 de Marzo de 2019). The Future of Blockchain Within Supply Chain. (M. D. Castillo, Entrevistador) Obtenido de https://www.forbes.com/video/6011370420001/the-future-of-blockchain-within-supply-chain/?sh=6d39d8797a77

30. Porxas, N., & Conejo, M. (2018). Tecnología Blockchain: Funcionamiento, aplicaciones y retos jurídicos relacionados. *Actualidad jurídica Uría Menéndez*.

31. PWC. (s.f.). *Blockchain – an opportunity for energy producers and customers?*

32. Rodriguez, N. (s.f.). *101 Blockchains*. Obtenido de https://101blockchains.com/es/caracteristicas-tecnologia-blockchain/

33. Santander Corporate Comunications. (2018). *Santander launches the first blockchain-based international money transfer service across four countries.*

34. SHARMA, T. K. (s.f.). *Blockchain Council*. Obtenido de https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/

35. Shoukry, A. (2020). The Intersection Of Blockchain And Supply Chain. *Forbes*.

36. Smith, S. S. (s.f.). Blockchain Based Smart Contracts; Considerations For Implementation. *Forbes*.

37. Sunyer, R. (2018). Blockchain y las posibilidades que ofrece para una nueva economía urbana. 20.

38. Tapscott, A. (2017). *La Revolucion Blockchain.* Barcelona: Deusto S.A. ediciones.