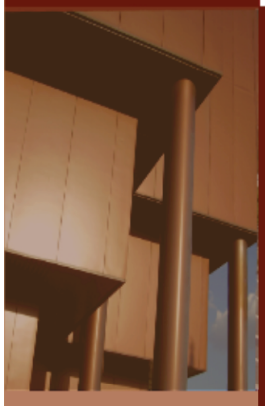
Trabajo de Fin de Grado
Grado en Ingeniería de Tecnologías Industriales

Blockchain aplicado a la Cadena de Suministros

Autor: África Aguayo López
Tutor: Alejandro Escudero Santana



Dpto. de Organización Industrial y Gestión de Empresas II

Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2019

Trabajo Fin de Grado

Grado en Ingeniería de Tecnologías Industriales

Blockchain aplicado a la Cadena de Suministros

Autor:

África Aguayo López

Tutor:

Alejandro Escudero Santana

Profesor Contratado Doctor

Dpto. de Organización Industrial y Gestión de Empresas II

Escuela Técnica Superior de Ingeniería

Universidad de Sevilla

Sevilla, 2019

Índice

1. Introducción

1.1. Objeto del proyecto

El objeto de este proyecto es dar a conocer en detalle la tecnología blockchain para poder entender así su potencial en el sector logístico y, más en concreto, en la cadena de suministros.

Esta incipiente tecnología se presenta como solución a muchos de los problemas actuales, cuyas soluciones no se habían encontrado hasta ahora. El sector financiero es el que ha tomado ventaja en la aplicación de esta tecnología, pero seguido por el sector logístico muy de cerca.

Las principales características que trae implícitas el blockchain son la integridad, la seguridad y la descentralización. Gracias a un gran sistema criptográfico, inmutable, abierto a todos y sin necesidad de ser controlado o verificado por ninguna entidad central, esto es posible. No cabe duda de que puede suponer una revolución que beneficiaría a todos.

También se hablarán de la tecnología IoT y del uso de drones en la cadena de suministros. Su compatibilidad con el blockchain ayuda a vislumbrar una mejor solución aún de muchos de los puntos de mejora actuales, tales como el flujo de información o la trazabilidad.

Es un cambio integral que parte de un cambio en el modelo de negocio, lo que lo convierte en una gran apuesta. Si se apuesta definitivamente por él, puede salir bien. En caso contrario, puede llegar a no despegar. Una concienciación del cambio, una predisposición positiva ante nuevos acontecimientos y estar abiertos a responder a preguntas, como las mostradas a continuación, ayudará a ese despegue.

¿Cómo aceptar una tecnología tan disruptiva y con un potencial tan grande como para alterar a directivos, políticos, sectores y, en definitiva, a todos? ¿Cómo es posible que en tan poco tiempo algo genere un cambio tan grande en tantas áreas de la vida cotidiana? ¿Cómo puede esta tecnología solucionar algunos de los problemas más relevantes de hoy en día? ¿Cómo afrontar este cambio?

1.2. Estructura del proyecto

Para poder transmitir en qué consiste el blockchain y cómo, ayudado por la tecnología IoT y el uso de drones, puede impactar en el sector logístico, en la cadena de suministros y en la última milla; el trabajo se ha estructurado según los siguientes capítulos.

Tecnología blockchain: explicación conceptual

En este capítulo se introduce la tecnología blockchain. Se explica las reglas e ideas principales sobre las que se sustenta, así como los beneficios que se obtienen con su aplicación frente a los sistemas actuales de almacenamiento y transferencia de información.

Tecnología blockchain: explicación técnica

En este capítulo se explica el funcionamiento de la tecnología blockchain desde un punto de vista más técnico. Se presenta el sistema criptográfico que otorga tanta seguridad a la red. También se detalla el protocolo de consenso que ayuda a su crecimiento. Y, por último, se alerta del impacto medioambiental que se puede genera por el gran número de recursos empleados.

Otras tecnologías disruptivas

En este capítulo se presentan dos tecnologías innovadoras que están suponiendo ya un cambio social importantes. Éstas son 'Internet of Things' y la tecnología que hace posible la existencia de drones. Estos dos avances pueden complementar muy bien al blockchain en el sector logístico.

Cadena de suministros y la última milla

En este capítulo se explica el funcionamiento de la cadena de suministros con especial foco en la última milla. El objetivo es poder entender bien esta área para, a continuación, entender cómo la tecnología blockchain puede ayudar a mejorar este sector.

Aplicación de blockchain en la cadena de suministros

En este capítulo se presentan los puntos flojos de la cadena de suministros donde la tecnología blockchain puede jugar un papel importante y cómo juega ese papel. Se añaden ejemplos de aplicaciones reales y pilotos que ya se están desarrollando. También se comenta cómo la tecnología IoT y el uso de drones pueden ayudar a este sector a mejorar y evolucionar junto a blockchain.

Encuestas

En este capítulo se muestran los resultados de una encuesta realizada a una muestra muy grande y variable de personas con el objetivo de que los resultados estuviesen sustentados en opiniones sólidas y fundamentadas.

Cómo promover el desarrollo de blockchain

En este último capítulo se indican algunos pasos que podrían ayudar a las empresas a impulsar este cambio y revolución. Son ellas las que deben dar ejemplo con proyectos respaldados por blockchain, que vayan dando el resultado que se espera.

2. Tecnología blockchain: explicación conceptual

¿Girará el sistema económico y sociocultural entorno al **blockchain** en unos años? Desde hace un tiempo se habla constantemente de esta **nueva tecnología**.

Es difícil encontrar quien no haya escuchado o leído sobre ella aún. Parece que va a jugar un **papel** muy importante en muchas **industrias**, como en la industria de las aseguradoras, en la de las telecomunicaciones, en la de la energía, en la industria 4.0, en la de la salud o en la financiera.

El desarrollo de esta tecnología incipiente empezó en el año **2008**. Inicialmente, la evolución del blockchain se realizó en base a una moneda, el **bitcoin,** pero a lo largo de los años se ha extendido mucho más allá de esta moneda virtual y del sector financiero que la rodea (Tascot, 2017). Para explicar el funcionamiento técnico del blockchain se tendrá en cuenta esta relación.

No se sabe si a raíz de la crisis global que hubo en el 2007, pero fue en el 2008 cuando **Satoshi Nakamoto**, una persona o grupo de personas bajo este pseudónimo, desarrollaron un protocolo para un nuevo sistema de pago electrónico, directo y entre iguales (**peer-to-peer o P2P**), soportándose en una criptomoneda, el **bitcoin**.

La principal diferencia entre la **criptomoneda** y lo que se entiende actualmente por *dinero* (monedas y billetes) es que la criptomoneda no se crea, ni se regula, ni se controla por ningún país, gobierno o entidad.

En referencia al **protocolo** desarrollado por Nakamoto, se puede definir como un conjunto de códigos inteligentes que garantizan la integridad y confidencialidad de información intercambiada entre los diferentes usuarios que constituyen la red y sin necesidad de **intermediarios**. Hasta la fecha sin precedentes.

Esta idea, fácil de entender conceptualmente, pero difícil de creer (hoy en día no es habitual tal tipo de transacción) ha **atraído** considerablemente a muchos negocios, artistas, medios de comunicación, incluso a gobiernos.

2.1. El protocolo

El protocolo se fundamenta en una serie de **registros distribuidos** por todo el mundo, llamados ***cadena de bloques****.* De todos los protocolos con esta idea, el más conocido es el ***protocolo blockchain****.* Estas cadenas de bloques permiten guardar transacciones varias de manera segura y sin la necesidad de un intermediario (entidad bancaria, Paypal, gobierno…).

Estas transacciones quedan estructuradas cronológicamente y reflejadas abiertamente. Es un **código de fuente libre,** es decir, todo el mundo se lo puede descargar, ejecutar y usar.

Actualmente numerosas instituciones, como bancos o gobiernos, están incorporando algún tipo de blockchain a su sistema de trabajo mediante blockchain privada con el objetivo de almacenar mejor la información y tener un buen seguimiento de la misma. Por este motivo, entre otros, cada día hay más tipos de blockchains, pero las más reconocidas siguen siendo las que se fundamentan en el **modelo de Satoshi**. Este modelo está reflejado en detalle en el paper ***'Bitcoin: A Peer-to-Peer Electronic Cash* System'** (Nakamoto, 2008)**.**

A lo largo del paper Nakamoto presenta su estudio acerca de este nuevo concepto sustentándolo además con cálculos matemáticos.

¿Cómo funciona este **modelo**? El bitcoin u otra criptomoneda no se guarda en una carpeta que está en un lugar concreto, sino que está representado por transacciones que quedan registradas en una cadena de bloques. Entiéndase cadena de bloques como un tipo de hoja de cálculo o registro que usa todos los recursos posibles para poder verificar y aprobar todas las transacciones realizadas.

Todas las cadenas de bloques, como la de bitcoin, están **distribuidas**, es decir, se ejecutan por todo el mundo por parte de personas totalmente independientes entre sí. El blockchain, en concreto, también es **pública,** es decir, la puede ver quien quiera, está en la red. No hay ninguna institución que se encargue de regularla y llevar un control y registro de las transacciones. Y, además, está **encriptada.** Usa una encriptación a partir de claves públicas y privadas que proporcionan una **seguridad** absoluta. Ello permite poder despreocuparse del tipo de información (confidencial, personal, corporativa…) que se guarde en ella.

De media cada **10 minutos** todas las transacciones llevadas a cabo se comprueban, se clasifican y se almacenan en un bloque. Éste bloque tiene que estar relacionado con el anterior para su validación y posterior incorporación a la cadena, favoreciendo a su crecimiento. Este esquema de bloques, que se enlazan al anterior, permite un registro del momento en el que se hizo la transacción y un almacenamiento con imposible alteración. Entiéndase como una pila en la que se va poniendo un folio encima de otro y es imposibles quitar uno, una vez que ya se ha puesto otro encima.

2.2. Tipos de redes: públicas y privadas

La **red pública** se caracteriza principalmente por no presentar ningún tipo de limitación para que nuevos nodos se sumen a ella. Las características principales de la red pública son (Victor Sánchez Horreo, 2017):

- Globales y permanentes
- Constituidas por una gran cantidad de nodos
- Actúan como un registro común, ayudando a la creación de servicios de valor añadido
- Potencian la transparencia y la confianza

Sin embargo, en entornos de negocio las **redes privadas o permisionadas** se ajustan más las necesidades de privacidad y rendimiento que se requieren.

Estas redes sin perder la esencia del blockchain, permiten configurar redes entre diferentes partes de un mismo entorno de manera que la participación esté controlada y no sea posible que cualquier se añada a ella. Las características principales son:

- Alto rendimiento
- Alta confidencialidad
- Enfocadas al intercambio de información y a la colaboración entre dos en ámbitos complejos
- Mayor seguimiento sobre el comportamiento en la red

En este caso, se atenta contra una de las propiedades principales del blockchain, la descentralización. Pero se consiguen otras propiedades importantes de la red como la verificabilidad, la inmutabilidad o la ejecución de Smart contracts.

Actualmente el número de redes públicas es mayor al de redes privadas.

2.3. La integridad

Hoy en día existe una **falta de transparencia** de la información importante.

Las empresas tienen una tendencia a ocultar sus datos o no exponer su usabilidad. En los acuerdos, relaciones o contratos se intenta beneficiarse en la medida de lo posible de los términos no especificados en detalle o incluso cambiarlos. La circulación de los datos se desconoce.

Esto no hace más que aumentar la **desconfianza**. La confianza en los negocios y en las instituciones alcanza sus niveles más bajos desde el comienzo de la crisis en 2007. Incluso en el sector tecnológico, anteriormente considerado como uno de los que mayor

confianza generaba, ha sufrido caídas en muchos países. El uso de los datos personales utilizados por algunas empresas en su propio beneficio es un motivo importante de ello.

Con el uso del blockchain este problema se erradica. Para que alguien pueda modificar los datos de alguna transacción, el **51%** de la red tiene que estar de acuerdo con el cambio. De esta manera, suponiendo que haya una mayoría honesta no se podría validar la transacción en la que se pretende alterar algún registro previo.

La analogía informática de esto es que los principios de la compromiso y **honestidad** están **codificados**, de manera tal que actuar sin integridad no es solo inútil, sino que no rentable también.

El **problema** que puede generar esta falta de honestidad en blockchain es el **doble gasto del dinero**. El dinero tiene una gran diferencia respecto a otros bienes: en el caso de un documento de texto, el **mismo** documento se puede enviar a varios destinatarios a la vez; con el dinero se sabe que no se puede hacer lo propio.

Cuando al hacer una transacción el dinero sale de una cuenta corriente, puede ir únicamente a otra cuenta y no puede estar en dos sitios a la vez. Sin embargo, en blockchain al tratar con monedas virtuales existe el peligro del doble gasto (**double-spend-problem)**. Este problema afecta directamente a quien recibe el dinero *falso* y a la reputación del defraudador.

Con la moneda actual, problema se resuelve mediante **terceros**, como Visa (compañía de tarjeta de crédito) o Paypal (plataforma de pago online). Se encargan de validar las operaciones una vez confirmado que el uso del dinero está siendo único. El problema de la intervención de estos terceros para la validación de la operación, es el **tiempo** (días y hasta semanas) y el **coste** de la operación.

Lo que hace blockchain es **registrar** en la red el **momento** en el que se gastó la unidad monetaria y rechazar las siguientes transacciones que gasten esa misma unidad monetaria. Así se consigue evitar el doble gasto.

Los responsables de registrar las transacciones son los **mineros**. Se encargan de reunir muchas transacciones, almacenarlas en forma de bloque y añadir el bloque a la cadena, referenciándolo siempre al bloque anterior. Gracias al protocolo cada uno de los **nodos** de la red tiene una **copia c**ompleta de toda la cadena de bloques.

De esta manera, Nakamoto encontraba no solo la manera de prescindir de terceros, sino de eliminar cualquier duda de fraude o conflicto por transacciones sospechosas. Cada una de las transacciones no dependen de uno solo, sino de todos. La red se

encarga de buscar consenso y una vez alcanzado por una mayoría de los usuarios de la red, se valida la transacción y se incorpora a la red.

Para lograr este consenso la red utiliza la ***prueba de trabajo*** (PoW, proof of work). Consiste en crear un acertijo muy difícil de resolver (se requieren muchos recursos, principalmente un hardware muy potente y mucha electricidad), pero que, sin embargo, es fácil de verificar (todo el mundo puede hacerlo). El primero que resuelva el acertijo será el que podrá incorporar su bloque a la red.

La solución del acertijo es un **hash**, una especie de huella dactilar única de cada documento. Como recompensa de haber resuelto el acertijo se le **retribuye** al minero con **bitcoins**.

Así se garantiza la **integridad** de las operaciones sin necesidad de tener que confiar en el buen hacer de algunos, pero sí suponiendo que el 51% de la cadena actúen correctamente.

2.4. El incentivo a un buen comportamiento

Para que los usuarios de la red se **comporten correctamente** hay que compensarles. Para ello Satoshi configuró el sistema de tal manera que, se **premiase** a aquellos que trabajasen en su crecimiento y expansión.

La revolución de internet ocasionó, entre otras cosas, que grandes empresas y bancos hicieran un mal uso de esta tecnología con motivo de una explotación indebida de los datos de sus clientes.

Uno de los motivos fue un **mal incentivo** por el uso correcto de la herramienta. A cambio de datos de clientes, había empresas que ofrecían servicios gratuitos. Este intercambio beneficiaba a la empresa a partir de un manejo de **datos ajenos** que usaban **sin consentimiento** real de sus propietarios y sin penalización alguna tampoco, como sí ocurría con los hackers.

Para acabar con este problema, Nakamoto desarrolló un software pensando en que cada uno actuaría bajo su **propio interés**. Hasta entonces, la protección de las redes existentes distribuidas era baja, habían recibido varios ataques Sybil (un ataque Sybil ocurre cuando un sistema distribuido es corrompido por una misma entidad que controla distintas identidades de dicha red).

Para solucionar estos puntos flojos programó un código en que por muy egoísta que se fuese, las acciones de cada uno beneficiarían a toda la red y a la reputación de uno mismo, convirtiéndose los ataques Sybil en económicamente inviables.

La energía que cuesta llegar a un consenso para llevar a cabo un ataque, genera un mayor coste que lo que se gana por generar un nuevo bloque. Esto fuerza a un comportamiento correcto e **incentiva económicamente** por su esfuerzo al primero que complete un bloque.

Satoshi reflejó lo siguiente en su paper: *La primera transacción de un bloque es una transacción especial que da comienzo a una nueva moneda que pertenece al creador del bloque. Esto constituye un incentivo para que los nodos sostengan la red.* (Nakamoto, 2008)

El valor de la política monetaria también fue tomado en cuenta por Satoshi, **evitando** uno de los mayores problemas de la historia con el dinero, la **devaluación**. Satoshi puso límite al total de bitcoins, **21 millones**, que se emitirían a lo largo del tiempo para evitar, efectivamente, una inflación. Esta cantidad total está estimada que para el **2140** ya esté en circulación.

Hace unos años nada de esto era imaginable. Actualmente, se dispone de una plataforma que exige portarse bien para recibir incentivo y que hacer lo contrario no interesa. Una consecuencia real de este buen comportamiento puede ser la retribución inmediata para los propietarios de una red de placas solares o un proyecto de código abierto donde se compense a los que hagan contribuciones importantes.

2.5. La seguridad

Blockchain presenta gran **seguridad** y garantiza la **autenticidad**, **confidencialidad** y el **acceso** a todas las operaciones.

Actualmente existen gran número de **robos de identidad, de información, fraudes, pirateo, programas con virus**, etc. Lo que inicialmente (principio de Internet) parecía que iba a aumentar la seguridad, no ha hecho más que disminuirla. Un caso claro de ello son las débiles contraseñas que protegen muchos datos, pudiendo ser pirateadas fácilmente.

El año que Nakamoto publicó su paper el número de fraude en entidades financieras supuso un 50% del total. En el 2014 descendieron los **delitos financieros**, pero en detrimento de los sanitarios que aumentaron en más de un 40%. El coste medio de un robo de identidad es de 13.000 dólares en el sector financiero. Este posible error del sistema no se puede asumir.

Nakamoto ofreció una solución a partir de las **claves públicas** (PKI, Public Key Infraestructure) para poder tener una plataforma segura.

Esta forma de **criptografía** concede al usuario dos claves con funciones diferentes: una es para encriptar y la otra para desencriptar.

Los sistemas antiguos que utilizaron PKIs fracasaron, porque no había incentivos y, además, los usuarios no se planteaban poder preservar su identidad o la posibilidad de poder mantener seguros sus datos personales.

De esta manera toda la información se encuentra en la red y un **fallo criptográfico** puede convertirse en un **robo inmediato** de un coche aun estando en la otra parte del mundo. Es un riesgo y que aumenta al haber cada vez más plataformas. No obstante, la seguridad que ofrece la criptografía de blockchain es muy elevada. Se verá más en detalle en el siguiente capítulo.

2.6. La distribución del poder

En la red de blockchain **no existe** ningún **centro de control** que regule el sistema, sino que el poder está distribuido por toda la red. Una parte de la red no puede apagar el sistema por sí sola o actuar de manera independiente.

En la actualidad, la información reside en entidades u organizaciones que la gestionan según su criterio. Se conoce algunos casos de los últimos años en los que se ha hecho evidente el uso de **información personal** de algunas empresas, consiguiendo **manipular** a la sociedad en un sentido u otro. Un ejemplo son las elecciones americanas o la votación del Brexit mediante Facebook.

En blockchain **no** existe esta **centralización** de la información, es decir, el control de la red por parte de una única institución no es posible. En caso de que alguien quisiese atentar con la red, tal y como se comentó anteriormente, los costes de uso de recursos (software y electricidad) superarían a los ingresos (recompensa con bitcoin).

El protocolo bitcoin puede descargárselo cualquiera de forma gratuito, incluso en un dispositivo móvil. De esta manera, la red alcanza a tener una base de datos presente en miles de ordenadores distribuidos por todo el mundo. Los **usuarios** son los que tienen el **poder** sobre sus datos, propiedades y nivel de participación.

Esto **protege** a la red del **control del Estado**, lo cual puede ser malo o bueno en función de la situación del país. En el caso de un disidente de un país totalitario, que lucha por la igualdad entre hombres y mujeres, sería beneficioso. Sin embargo, sería perjudicial en el caso de un delincuente de un país democrático.

2.7. La privacidad

Las personas tienen que ser las únicas **dueñas de sus propios datos e identidad**, y decisores de cómo, cuándo y en qué medida compartirla con quién.

Si se elimina la obligación de tener que confiar en el segundo actor de la transacción porque el sistema sea fiable, no sería necesario conocer la identidad del otro. Bajo esta idea desarrolló Satoshi su protocolo.

En la Segunda Guerra Mundial Alemania disponía de una máquina llamada **Enigma**, que servía para cifrar y descifrar mensajes. Fue patentada en 1918 por la empresa alemana Scherbius & Ritter.

La privacidad de la que disponían al poder comunicarse entre ellos sin el riesgo de que el bando contrario interceptase sus mensajes les hacía *libres.* Libres de que las consecuencias de la Guerra no se viesen alteradas por las comunicaciones que se cruzaban.

Como funciona Enigma es cogiendo la información, troceándola y repartiéndola por los diferentes nodos de la red de manera aleatoria. La privacidad que ofrecía esta máquina hace ya 70 años es la que hoy en día se busca y cada vez con más urgencia. El mundo está actualmente muy interconectado y un flujo de información en direcciones equívocas no hace más que perjudicar a la sociedad.

En un mundo libre como el de hoy la **privacidad** debe considerarse un **derecho humano** imprescindible y no ha sido así en los últimos tiempos. La recopilación, el almacenamiento y el manejo de la información personal sin conciencia, ni consentimiento del propietario ha sido constante. Como también lo ha sido el uso de esta información para **estudiar** a individuos y manipular su **comportamiento** a base del conocimiento extraído de ellos.

Esto es un **atentado a la privacidad** y por partida doble. Por un lado, por la recopilación de los datos y, por otro lado, por no proteger dicha información de los piratas informáticos.

La posesión de información confidencial de clientes se está convirtiendo en un problema para muchas empresas, expuestas a un posible robo informático por una parte y a una multa por ‘ofrecer’ información confidencial, por otra. La información de cliente se puede convertir en un **activo muy perjudicial**.

La reciente **aplicación de la GDPR** europea cambia el panorama en cuanto a la seguridad y privacidad de los datos personales (Pérez, 2018). Este reglamento enumera los requisitos detallados, que cualquier institución que procese datos de los 28 países

pertenecientes debería cumplir, sin importar la localización de dicha empresa. GDPR aumenta los derechos de los ciudadanos y pone techo al poder de plataformas de software que hacen uso de información almacenándola, analizándola y usándola. Sin embargo, también cuenta con **modelos centralizados** de almacenamiento y transferencia de información.

Ante este problema, blockchain puede ser la solución a un uso correcto de la información. En esta plataforma no existe ningún campo obligatorio de rellenar en la capa de red, es decir, nadie está obligado a tener que proporcionar una información concreta (nombre, dirección, correo electrónico o cualquier otro tipo de información personal).

A la hora de realizar cualquier transacción (comercializar un producto, realizar una transferencia…), la red no tiene por qué saber la identidad del que la realiza. Las **capas** de **verificación e identificación** están **separadas** de la de la transacción. Esto favorece a una mejor administración de la información personal y del entorno, así como un aumento en la confianza de los diferentes actores de cualquier transacción de la red.

Blockchain permite cortar el camino hacia una sociedad vigilada cada vez más. Hace 20 años del comienzo de Internet y la **información recopilada** en las bases de datos a día de hoy es **incalculable**. La tecnología avanza cada vez más rápido y las herramientas con las que trabajar la información también. A este paso, pronto se podrá obtener información de cualquier aspecto personal de alguien: su condición física, información médica, alimentación, etc. Podrá haber millones de avatares analizando cada paso. Blockchain puede permitir que **cada uno** posea su **propio avatar**.

2.8. Los derechos de propiedad

Los **derechos de propiedad** deben ser **legítimos y transparentes**.

Internet se percibió inicialmente como un buen medio para ayudar a los **artistas** (pintores, músicos, escritores, etc.) a darse a conocer, lanzar propaganda y, en definitiva, ganar el dinero que ellos pensaban que merecían por su esfuerzo y resultados.

Sin embargo, la existencia de **intermediarios** ha impedido que el negocio de los artistas se desarrolle tal y como se deseaba. Los intermediarios (discográficas, plataformas virtuales…) se acaban beneficiando indirectamente de parte de la obra del artista. En ocasiones, entran en conflicto con ellos por el porcentaje acordado, hay desacuerdo en el valor añadido generado por cada uno en el resultado final, incluso acaba habiendo

casos de fraude. De esta manera los **derechos legítimos del artista** acaban viéndose **pisoteados** junto a los derechos de privacidad y seguridad.

Como se ha explicado antes, el protocolo hace que se registre el momento en el que se realiza cualquier transacción, de modo que sólo se autoriza la primera vez que se gasta una moneda, impidiendo así el **doble gasto**. Además, las KPIs consiguen que se confirme la propiedad de todas las monedas de la red.

Entendiendo esta sistemática con la moneda virtual, se puede extender esta idea a cualquier otra **propiedad real**, intelectual o derecho de la persona. No se puede negociar con lo que no es de la propiedad de uno. Este sistema demuestra qué es propiedad de quién y posee un registro y verificación de ello.

En el caso de que se realice alguna operación que implique muchas transacciones o muchas partes, se opta por contratos inteligentes, ***Smart contracts*.** Son unos códigos que ejecutan instrucciones en blockchain, una combinación absoluta entre el derecho y la informática.

Un uso útil de un contrato inteligente es el creado por un compositor para recoger en él, los derechos de uso a otro músico, la duración de la concesión, el dinero que le va a cobrar, la cláusula de rescisión, etc. Otra aplicación de contrato inteligente puede ser el que recoja las condiciones para la creación de una sociedad a partir de varios activos, incluyéndose en él los derechos de la agencia, los derechos de los propietarios, etc.

Esta idea innovadora para el derecho y las finanzas proporciona un importante grado de certidumbre **sobre** el **cumplimiento de un contrato**, que puede desencadenar un **sistema de gestión de los derechos** en su conjunto.

2.9. La inserción social

El mundo funciona mejor cuando la **economía es global** y no excluye a nadie. Para acercarse a esta economía, ayudaría crear plataformas favorables y quitar los obstáculos que impiden tal integración.

La aparición de Internet ayudó a que esta desigualdad aumentase. Hoy en día un 43% de la población sigue sin acceso a Internet, un 66% no tiene cuenta bancaria y otras muchas solo tienen su dispositivo móvil, como herramienta de conexión al exterior.

Satoshi desarrolló su protocolo, teniendo en cuenta que muchos países subdesarrollados no tendrían acceso a Internet. Se podría pertenecer a la red aún sin tener conexión, a través de lo que Nakamoto denominó **SPV, Simplified Payment Verification**.

Permitiría acceder a una parte de la cadena desde cualquier móvil, sin necesidad de descargarse una copia de la cadena entera. Este acceso a la cadena a personas con una situación desfavorable las ayudaría a su inserción en el mundo. Trámites burocráticos, como abrir una cuenta bancaria o recibir un crédito, se agilizarían. La participación en transacciones extranjeras sería mucho más común y sencilla.

Blockchain puede ayudar a alcanzar esta **hegemonía social, económica y política**. Y que las decisiones no se tomen en base a la relación de unos con otros, al pasado de uno, a la raza o al lugar de origen.

2.10.El impacto actual

Está creciendo el número de **instituciones** que se unen a investigar los posibles casos de uso de esta tecnología con el objetivo de mejorar la estructura y el funcionamiento de la sociedad actual.

No solo en el ámbito tecnológico, sino también **personalidades** de diferentes sectores han mostrado su interés en este nuevo paradigma.

"Es interesante porque muestra lo barato que puede ser. Es mejor porque no tiene que estar físicamente en el lugar, y por supuesto, para grandes transacciones la moneda [física] puede ser bastante incómoda". Bill Gate, cofundador de Microsoft y portador del título de *el hombre más rico del mundo* por varios años.

"El sistema blockchain es a la confianza lo que internet a la información. Igual que el internet original, las cadenas de bloques tienen la capacidad de transformarlo todo".

Joichi Ito, director del MIT Media Lab.

"Existen muchos proyectos en el mundo con monedas digitales, pero sin duda la más notable es Bitcoin. Esto va a cambiar el mundo del dinero desde un punto de vista transaccional (…) para todo el mundo". Akon, cantante de Hip Hop y R&R, también hombre de negocios.

"Las Blockchains son todo.", "la tecnología en la que se basa el bitcoin para cambiar el funcionamiento de la economía", "el mejor modo de estar seguro de las cosas" y otras muchas más, son parte de las reflexiones de personas o revistas tan importantes como la exdirectora financiera de JP Morgan, Blythe Master; Bloomberg Markets o The Economist.

No solo hay opiniones ante esta idea "abstracta", sino que existen aplicaciones reales que se mostrarán más adelante, así como **ejemplos de posibles aplicaciones**. Se están creando ya bases de datos sustentadas en esta tecnología preparadas para

decidir a la hora a la que hay que levantarse, pagar el agua caliente de la ducha que se gasta, garantizar la seguridad de los dispositivos conectados a la red mediante Internet of Things, decidir cuándo arreglar el jardín o para identificar a alguien con el coche para llevarle al trabajo.

Numerosas empresas están incorporando esta tecnología a su modelo de negocio con la transformación empresarial que ello implica. Empresas tan reconocidas como **Maersk** con el transporte de contenedores, o **Barclays**, con las transacciones y fraude financiero.

3. Tecnología blockchain: explicación técnica

Gran parte del potencial de blockchain reside en la **criptografía**. Es la función hash criptográfica la que posibilita el desarrollo de la cadena y que se vayan añadiendo bloques a ellas cada diez minutos de media.

3.1. La criptografía

Actualmente, el mundo se mueve en torno al dinero. Por ello es tan importante una buena gestión del mismo, así como un buen sistema de seguridad, que evite el fraude y la falsificación entre otros.

La criptografía es una disciplina de investigación profunda que utiliza técnicas y avances matemáticos para **cifrar un contenido**, arte difícil de entender. El Bitcoin, en cuya arquitectura se sostiene el blockchain, depende solo en cierta parte de la criptografía.

3.1.1. Función hash

Una **función hash** (en español *moler, picar* o *digerir*), también llamada en ocasiones *transformación de claves*, convierte un gran volumen de datos en un resumen de los mismos. Ello lo hace manteniendo la integridad y la confiabilidad de los datos iniciales. Así se consigue aumentar la eficiencia en la verificación de una gran cantidad de datos.

En definitiva, lo que hace una función hash es convertir un dato de entrada de longitud variables en un dato de salida de longitud fija. (Función hash: concepto y aplicación en Bitcoin, s.f.).

El uso de funciones hash posibilita poder determinar en todo momento el estado de una cadena de bloques. Tanto las transacciones que ya han sido registradas, como las incorporadas recientemente se consideran valores de entrada de la función y dan lugar a una ***imagen criptográfica*** de toda la red hasta ese punto.

Si se produce el más mínimo cambio en el conjunto de datos de entrada, se debe obtener un hash totalmente diferente. Esto quiere decir que es **imposible modificar registros en un bloque**, sin alterar los hashes derivados. Y para validar todos los hashes derivados, tendría que hacerlo también al menos un 51% de todos los nodos de la red. Y esto en un sistema descentralizado, como blockchain, es prácticamente imposible.

Se puede, entonces, concluir que una función criptográfica, conocida usualmente como 'hash', es un algoritmo matemática que convierte todo bloque con un contenido de datos en una serie de caracteres con una longitud fija.

Se habla de **3 propiedades** básicas de las funciones hash:

- La **entrada** puede ser de **cualquier longitud,** como el contenido completo de cualquier bloque.
- La **salida** tiene una longitud **fija**, independiente de la entrada.
- Es **computable,** es decir**,** para un valor de entrada determinado se puede calcular en una cantidad razonable de tiempo la salida correspondiente. Explicado matemáticamente, significa que para una función hash de tamaño n-bit, se necesitaría una cantidad de tiempo de O(n).

Además, para que una función hash criptográficamente se considere segura, debe tener estos 3 atributos adicionales:

a) Libre de colisiones
b) Ocultamiento
c) Puzzle friendly

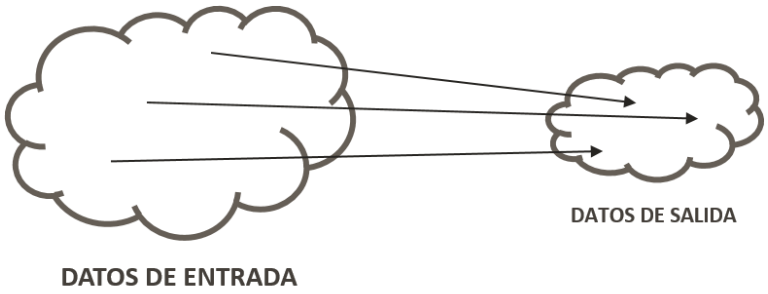
A continuación, se explican estas tres propiedades. (Blogchainers, 2017)

a) Libre de colisiones

La propiedad 'libre de colisiones' es la principal de la función hash. Se dice que una colisión ocurre cuando dos entradas de datos diferentes dan lugar a la misma salida. Si nadie es capaz de encontrar una colisión en la función hash, se puede afirmar que la función H(.) está libre de colisiones.

– Matemáticamente, se puede explicar cómo que, una función hash, H(.) está libre de colisiones si es imposible encontrar dos valores X e Y, tal que siendo X ≠ Y, H(X) = H(Y).–

Que una función esté 'libre de colisiones' no significa que no tenga colisiones, sino que nadie puede encontrarlas. Realmente, se sabe que sí existe una colisión en dicha función y más de una. Es fácil de comprender. Se ha explicado anteriormente que el espacio de datos de entrada es mucho más grande que el espacio de datos de salida, puesto que la entrada puede ser de cualquier longitud, mientras que la salida es de longitud fija. De esta manera resulta evidente que, debe haber varias entradas diferentes que correspondan a una misma salida.



Además, no es que parezca evidente la existencia de una colisión, sino que hay varios métodos que garantizan una colisión entre dos valores de entrada diferentes. El hecho de que se pueda hallar una colisión examinando tan solo la raíz cuadrada de todas las salidas posibles, se sustenta en un fenómeno conocido como *la* ***paradoja del cumpleaños****.*

<< El problema del cumpleaños, también llamado paradoja del cumpleaños, establece que, de un conjunto de 23 personas hay una probabilidad del 50,7% de que al menos dos personas de ellas cumplan años el mismo día. Para 57 o más personas la probabilidad es mayor del 99,666% >>.

El punto clave, sin embargo, está en que encontrar dicha colisión llevaría mucho, mucho tiempo. Estableciendo una similitud con la expresión 'mucho, mucho tiempo', se puede decir que incluso si todos los ordenadores creados en toda la historia de la humanidad estuviesen trabajando desde su inicio hasta el día de hoy, la probabilidad de encontrar dicha colisión sería infinitesimalmente baja.

Existe un algoritmo para hallar una colisión con cualquier función hash, pero no es práctico. Y es por ello, basándonos en que nadie ha demostrado todavía lo contrario, se considera que la **función hash está libre de colisiones**.

¿Y qué utilidad puede tener que una función esté libre de colisiones? Si se conocen dos valores de entradas X e Y que son diferentes, se puede asumir que al estar la función hash, H(.), libre de colisiones, H(X) será diferente a H(Y).

Existen muchas **aplicaciones** gracias a dicha asunción. Considérese un servicio de almacenaje de archivos en la nube en el que los usuarios suben documentos y que asegura la integridad de los mismos. Si Carolina sube un documento de gran tamaño y luego quiere ser capaz de comprobar la integridad del documento y que no haya sido alterado, necesitaría descargárselo de la nube y compararlo con el que subió, aún almacenado localmente, y confirmar que son los mismos. En este caso, no tiene sentido la subida inicial a la nube, si tiene que mantener una copia local con la que luego comparar la descarga.

La función hash, libre de colisiones, ofrece una solución a este problema. Carolina solo necesitaría recordar el hash del documento original. Cuando después se descargase el documento, calcularía hash del documento descargado y lo compararía con el inicial. En caso de que fuese diferente, sabría automáticamente que el documento ha sido manipulado. De esta manera, no sería necesario comparar un documento con Gigas de información, sino que con una cadena de caracteres de 256-bits sería suficiente.

b) Ocultamiento

Se puede afirmar sobre la función que tenga la propiedad de ocultamiento, que conocida una salida de la función hash, Y = H(X), no hay ninguna manera de saber qué X era la entrada.

Considérese el experimento en el que se lanza una moneda al aire. Si sale 'cara', se considerará que el hash es *cara*. Si sale 'cruz', se considerará que el hash es *cruz.* A continuación, se le pregunta a alguien que no vio lanzarse esta moneda, qué había al principio (cara o cruz) que desencadenó el resultado. No podrá tener garantía absoluta al primer intento de que vaya a acertar, pero sí la tendrá en tan solo dos pasos.

El interrogado podrá averiguar fácilmente el 'dato de entrada', puesto que solo había dos valores de X, 'cara' y 'cruz'. Para que este experimento tuviese la propiedad de *Ocultamiento*, no podría haber ningún valor de X que fuese probable. Para ello X tendría que pertenecer a un conjunto de valores muy amplio. Tan amplio que, cogiendo valores al azar de este conjunto, sería improbable dar con el valor correcto de X.

Se podría incluso ocultar una entrada que no perteneciese a este conjunto tan amplio de valores, concatenándola con otra entrada que sí lo hiciera.

– Matemáticamente, una función hash, H(.), está oculta si elegido un valor 'r' de una distribución de probabilidad y dado H (r || X) es imposible averiguar X. –

Un **esquema** del **algoritmo** que seguiría esta propiedad sería el siguiente:

- Convertir (msj, nonce) = Conv. La función *convertir* coge como valor de entrada un mensaje y un valor secreto y aleatorio, conocido como *nonce.* Y devuelve *Conv*.
- Verificar (conv, msj, nonce) = true/false. La función, *verificar,* coge como entrada *conv, nonce* y *mensaje.* Como salida devuelve *true* si *convertir* == *conv* (msj, nonce) y *false*, si no lo es.

De seguir este algoritmo y resultar *true,* se puede afirmar que la función hash tiene las siguientes propiedades:

- Ocultamiento: dado *Conv*, es imposible averiguar *msj*.
- Imposible hallar dos parejas (msj, nonce) y (msj', nonce'), tales que, siendo msj ≠ msj', *convertir* (msj, nonce) == *convertir* (msj', nonce').

De esta manera, si se coge un valor aleatorio *nonce (*cambiar de nonce cada vez que se utilice la función *convertir)*, la propiedad *Ocultamiento* dice que, si aplicamos la función hash al valor *nonce* y a *mensaje*, es imposible saber el valor mensaje a través de la salida de la función hash. Esta propiedad lleva implícita la propiedad *libre de colisiones*, es decir, es inviable encontrar dos valores distintos, msj y msj', de manera que H (nonce || msj) = H (nonce' || msj'), puesto que en ese caso sí existiría una colisión.

Se puede confirmar pues que, si H es una función hash **libre de colisiones** y con la propiedad de **Ocultamiento**, el esquema presentado funcionará y se cumplirá los **requerimientos de seguridad**.

c) Puzzle-friendly

Se dice que una función hash, H(.), es puzzle-friendly si para todos los posibles valores de salida de n-bit, Y; siendo k un número aleatorio elegido entre una muestra de alta incertidumbre, llamada Puzzle-Id; es imposible encontrar X, tal que H (k || x) = Y en un tiempo menos a 2n computaciones, ya que no hay manera de recorrer el espacio más que de forma aleatoria.

La diferencia respecto a la propiedad de Ocultamiento es que la 'k' en este caso es dada, dan el valor 'id', al que se le llama puzzle-ID. Además, se menciona un rango de valores Y, es decir, que puede haber más de 'y' resultados que se den como correctos dependiendo de lo que se haya considerado en ese momento rango válido.

Entiéndase que, para resolver el puzzle se debe hallar una 'x' que dé lugar a una 'y' que caiga en el intervalo Y. Si hay más resultados posibles de 'y', hay más posibles soluciones de 'x', de manera que la probabilidad de encontrar una solución es mayor. Es decir, que la dificultad del puzzle depende directamente del tamaño que tiene el rango Y. Si como se explica hay más de una solución de 'x', parece que no está la función libre de colisiones, pero esta propiedad se refiere a que hay un valor de 'x' por cada valor de 'y', de manera que se mantiene la propiedad, solo que hay más número de resultados 'y'.

Es imprescindible que el puzzle-id provenga de una muestra de alta incertidumbre.

Se puede asemejar ese rango, Y, al aro de una canasta de baloncesto que puede variar su diámetro. Cuanto más grande sea el diámetro, más fácil será encestar la pelota y, cuanto más pequeño, más difícil. Esto significa, que hay más valores de 'x' que pueden encestar en el aro, varias pelotas de distintos diámetros o varios lanzamientos. Así que, cuanto más grande sea el intervalo, Y, más diferentes 'x' habrá y menos tiempo necesitaremos para encontrarla. NO hay que olvidar que el rango de posibles resultados de 'x' es muchísimo mayor que el rango de 'y'.

Matemáticamente se puede definir el puzzle matemático como:

- Una función hash, H
- Un valor id, puzzle-ID, elegido de una muestra de alta incertidumbre
- Un rango Y, como objetivo

De esta manera, una solución a este puzzle sería:

$$H(id \parallel x) \in Y$$

Se puede concluir que para resolver este puzzle matemático, lo que se requiere es probar grandes cantidades de números aleatoriamente hasta dar con el valor de entrada 'x' que, concatenado con puzzle-ID, resulte en un hash que pertenezca al rango de dificultad propuesto de Y. No hay opción mejor.

Mostradas las **tres propiedades de las funciones hash** y algunas de sus aplicaciones, recalcar que hay muchas funciones hash. Pero Bitcoin no usa cualquiera, principalmente usa una función hash llamada **SHA-256**. SHA-256 utiliza una función de comprensión que coge una entrada de 768-bit y produce una salida de 256-bit. El tamaño del bloque es de 512 bits.

Hay que recordar que se requiere una función hash que trabaje con valores de entrada de una longitud arbitraria. Afortunadamente, hay un método que convierte una función

hash que trabaja con un valor de entrada de tamaño fijo en una que trabaja con un valor de entrada de valor variable. Este método es el conocido como el **método de construcción Merkle-Damgard** y usado por la función hash, SHA-256.

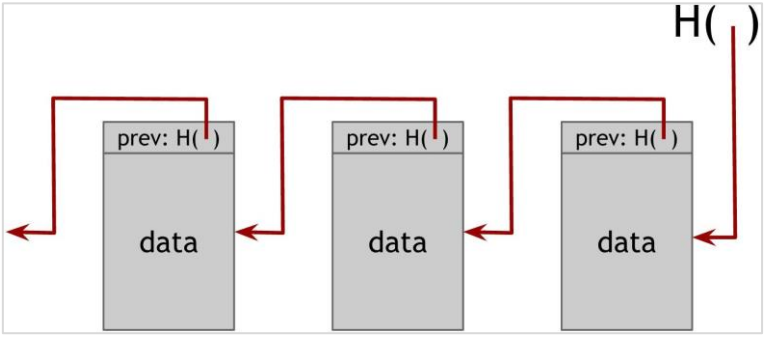
3.1.2. Punteros hash

Se ha explicado ya lo que es una función hash y en detalle algunas de sus propiedades. Ahora se va a hablar de los punteros hash. (Arvind Narayanan, 2016)

Un **puntero hash** es un puntero a un lugar donde hay almacenada información protegida criptográficamente con un hash. Mientras que el puntero ordinario permite alcanzar la manera de obtener datos de información, el puntero hash también te permite **verificar** que la **información no** haya **cambiado**.

Blockchain se trata de una serie de punteros hash conectados. En una cadena corriente de varios bloques, cada bloque almacena tanto una información determinada, como un puntero al bloque anterior.

De esta manera cada bloque nos dice el valor del bloque anterior y también un resumen del bloque, que permite verificar que el contenido del bloque no haya cambiado. El puntero hash que apunta al bloque de datos más reciente, se almacena en la cabecera.



Un **caso de uso** de blockchain sería un registro de **manipulación indebida**. Es decir, se requiere construir un registro con gran volumen de información almacenada. Y se permite siempre actualizar la información, pero únicamente añadiendo ésta a continuación de la última incorporada. En caso de que alguien quiera manipular alguna información previa, añadiendo datos en mitad de la información almacenada, con blockchain se detectaría inmediatamente.

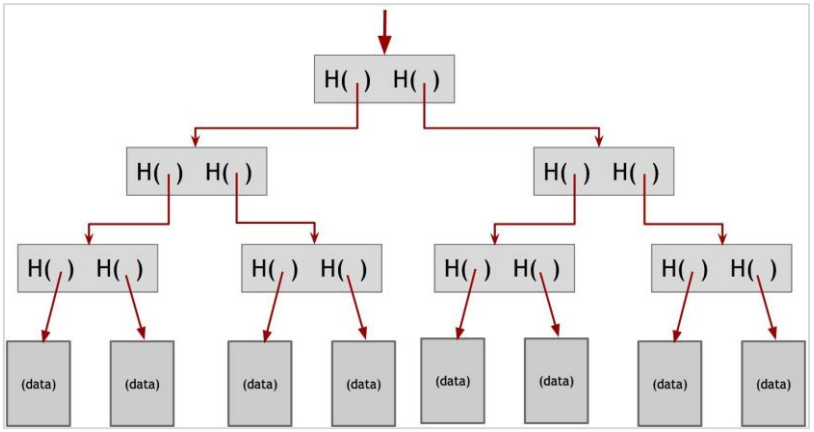
Se va a proceder a explicar cómo blockchain **detecta este intento de alteración** en mitad de la cadena. Alguien modifica la información de un bloque, k. En el momento que este bloque se modifica, genera un nuevo hash, de manera que el bloque siguiente, k + 1, no va a aceptar el cambio, puesto que su puntero hash apuntaba al anterior hash. El que ha querido modificar el bloque, puede intentar modificar el contenido del bloque

siguiente, de manera que cambie el hash del bloque siguiente y haga match con el bloque k, pero igualmente el problema persistirá con el bloque k + 2.

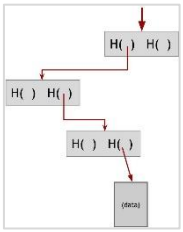
Puede seguir modificando los bloques sucesivos, pero errará cuando llegue a la cabeza de la cadena. Cuando se alcanza la cabecera, el adversario no será capaz de modificar el puntero hash, H(.), y será descubierto en su intento fallido de intentar alterar la cadena de bloques.

Así pues, de esta manera podemos crear una cadena de bloque tan larga como queramos. Si vamos hacia detrás, llegamos al primer bloque que se creó, el **bloque génesis**.

Otra manera útil de estructurar los datos es la conocida como **Merkle Tree**, un árbol binario con punteros hash. Supóngase que se tiene un número de bloques con información, que se agrupan por parejas. Para cada pareja se construye una estructura de datos que tiene dos hashes punteros, cada uno apunta a cada uno de los bloques que constituyen la pareja. Esta estructura de datos, estaría a un nivel más elevado que los bloques de información. A su vez, esta estructura de datos forma una pareja con otra estructura de datos y tienen en un nivel superior a dos punteros hash que apuntan a cada una de las dos estructuras. Y así, hasta llega a un único bloque, la raíz del árbol.



Esta disposición de la información, permite también **detectar cualquier alteración** en cualquiera de los bloques que constituyen el Merkle Tree. Si se intenta modificar un bloque del final, se podrá ir modificando los hashes que están por encima. Pero cuando se llegue a la cabecera, de la misma manera que pasa con la cadena de blockchain, no se podrá modificar el hash y el intento de alteración será detectado. Es decir, cualquier modificación de cualquier bloque, se propaga hasta el último bloque.



Por otro lado, y a diferencia de la cadena de bloques en modo lista o secuencial, esta estructura de árbol permite **comprobar** de una manera mucho **más rápida**, si un bloque de datos pertenece al Merkle Tree. Mientras que en la lista de bloques hay que comprobar todos los bloques uno a uno, en esta estructura solo es necesario recorrer la ruta 'vertical' existente desde el bloque en cuestión hasta la cabecera.

Se ha visto ya el uso de punteros hash tanto en una estructura de datos en modo lista y en modo árbol binario. Ambas funcionan y son viables, así como cualquier otra que permita validar todos los hashes. Una estructura cíclica no sería viable.

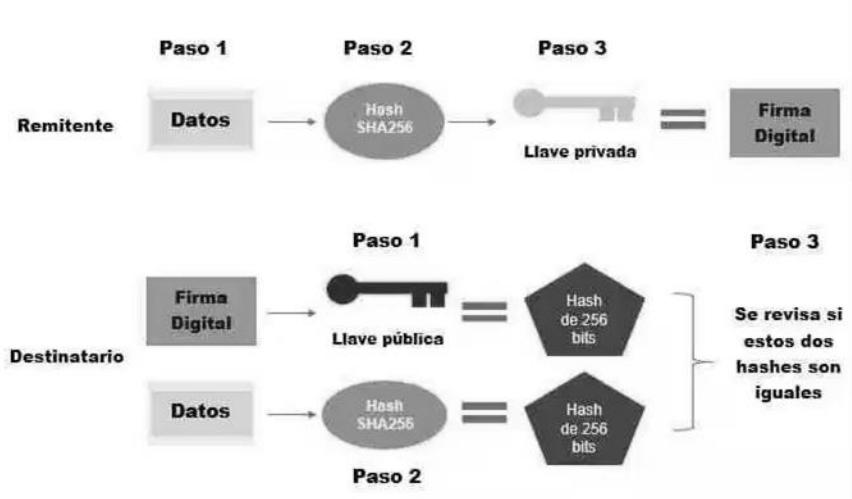
3.1.3. Firma digital

Para entender el funcionamiento de una ***Firma Digital*** se va a establecer un símil con una Firma Tradicional en Papel.

Hay **dos propiedades** que comparten estos dos tipos de firmas:

- Únicamente el **propietario** de una firma pude realizarla
- Una firma está atada a un documento y **no** se puede **reutilizar** para mostrar el acuerdo o conformación de otro contrato o documento. Si así fuere, sería como poder recortar la firma tradicional de hoy en día de un papel y tener autoridad para pegarla en otro documento manteniéndose válida.

¿Cómo se puede crear esta firma digital para que sea útil criptográficamente hablando?



Esquema para la creación de una firma digital:

1. A partir de un método que se le da como **entrada** el tamaño de la clave '**keysize'**, se obtiene como **salida** dos claves. La **clave secreta**, **sk**, que tiene que ser guardada de manera privada y que se utilizará para firmar mensaje; y la **clave pública**, **pk**, que es la que se dará al receptor del mensaje y con la que pueda verificar la firma.

   GeneradorClave(keysize) = (sk, pk)

2. A partir de un método que se le da como **entrada** un '**mensaje'** y la clave secreta, **sk**; se obtiene como **salida** una firma, ***firm***.

   Firmar (sk, mensaje) =firm

3. A partir de un método que recibe como **entrada** el **mensaje**, la **firma** y la clave pública, **pk**; devuelve **true** si firm es una firma válida y **false** en caso contrario.

   Comprobar (pk, mensaje, firm) = true/false

Estos son los métodos que se siguen para el uso correcto de una firma digital y presentan dos propiedades:

- El método *Comprobar* debe devolver true: si el propietario de la firma digital firma un mensaje con su clave secreta, sk, y luego alguien intenta validar la firma sobre el mensaje usando la clave pública, pk.
- Las firmas son infalsificables: si alguien conoce la clave pública de alguien que envía un mensaje y ve también la firma, *firm*, de ese documento; no puede igualmente falsificar la firma, esa firma no vale para otro documento.

3.1.4. Claves públicas

La idea es **asemejar** en un sistema la **identidad** de una **persona** a una **clave pública**. Si se recibe un mensaje con una firma que se verificar correctamente bajo la clave pública, pk, se puede entender que esa clave pública nos está diciendo el mensaje recibido. (Anderson, 2011) No olvidar que para mandar un mensaje a alguien bajo la identidad pk, no se puede olvidar la clave secreta correspondiente, sk.

Una ventaja de trabajar con claves públicas como identidades es que se puede generar tantas claves públicas como se quiera. Como se vio antes en el esquema para generar

una firma válida, a partir del método *GeneradorClave* se pueden generar la pareja de claves, pk y sk. Pk, es la nueva identidad pública, y sk es la correspondiente nueva clave secreta, que solo el propietario debe conocer y que le permitirá hablar en nombre de la clave pública, pk.

Crear una nueva **clave pública**, quizás no sea tan necesario, como lo es actualmente. Hoy en día en numerosas situaciones se desearía poder crear una clave pública para evitar que, por la situación o contexto de uno no se pueda alcanzar aquello que se quiere. Mediante blockchain y la generación de claves no hay una manera directa de vincular una clave pública a una persona física con DNI XXX. La clave pública se genera **aleatoriamente**.

Esto implica una **descentralización** de la **gestión de identidades**. Deja de tener sentido una autoridad central a la que haya que informar del registro en un sistema o de la realización de alguna operación, pasando a depender únicamente del actor de la acción. Tampoco se necesita un nombre de usuario o particular para realizar una transacción. Si alguien requiere una nueva identidad, solo tiene que generarla. Podrá crear tantas identidades como quiera y utilizar cada una para el tipo de acción que quiera.

Queda claro la descentralización de control y gestión de identidades que esto implica. Esto supone una de las propiedades más diferenciadas del blockchain.

Resulta atractivo esta capacidad para preservar el anonimato y la privacidad de uno mismo. Pero este anonimato puede ser destapado. Una persona que utiliza su identidad para realizar un conjunto de operaciones, puede definir sin querer un patrón de comportamiento. Y otra persona que observe las diferentes acciones realizadas por una identidad concreta, identificar ese patrón de comportamiento y vincularlo a una identidad concreta.

Esto quiere decir, que no es necesario registrarse en el sistema o revelar la identidad del mundo real, pero si no se quiere ser identificado hay que intentar no definir un patrón de actuación en base a los movimientos que se realicen.

3.2. La descentralización

La manera en la que se alcanza la descentralización en Blockchain es una combinación entre métodos técnicos e incentivos a los actores que participan en ella y ayudan a su mantenimiento y crecimiento.

3.2.1. Centralización vs. Descentralización

Para empezar a hablar de la 'Centralización vs. Descentralización' se comentarán algunos sistemas consideradas históricamente como descentralizados.

Internet ha sido históricamente el sistema 'descentralizado' por excelencia. Ha tenido competidores a lo largo de su vida, pero siempre ha conseguido imponerse a ellos.

También se puede hablar del **email**, un sistema basado en el servidor Simple Mail Transfer Protocol (SMPT). Nadie puede manejar este servidor según sus intereses, pero sí existen proveedores de Webmail, como Gmail, Outlook o AOL Mail, que son empresas privada que ofrecen ese servicio y, además, abarcan casi la totalidad del sector.

En cuanto a la **mensajería instantánea**, sistema liderado por empresas como Facebook, se puede hablar de un híbrido entre centralización y descentralización. Es difícil hallar una descentralización pura.

Esta batalla entre los diferentes sistemas de comunicación no es actual, lleva existiendo desde el descubrimiento del teléfono, la radio y el cine.

3.2.2. Consenso distribuido

A continuación, se va a analizar la descentralización desde un punto de vista más técnico, para ello se hablará de consenso o **consenso distribuido**.

Para entender cómo funciona este consenso distribuido, se va a explicar cómo se realiza una transacción, recordando el **sistema peer-to-peer**.

Si Carolina quiere realizar una transacción a Roberto, lo que hace realmente es emitir la transacción a todos los nodos de la red. ¿Qué pasa si Roberto no está conectado a la red en ese momento? No hay ningún problema, Roberto no tiene por qué estar conectado, si hay consenso para que esa transacción se realice, la propia red se encargará de que Roberto reciba la transacción una vez que se conecte.

¿Cómo se alcanza ese consenso para que la transacción de Carolina sea validada y la pueda recibir Roberto? En la red se están emitiendo constantemente numerosas transacciones y son los nodos los que tienen que llegar a un acuerdo para ver qué transacciones son válidas para añadirlas a la red y que se puedan ejecutar.

Cada nodo capaz de crear bloques, es decir, los **mineros** tienen un **pool de transacciones pendientes**. Este pool no es igual para todos por imperfecciones de la red P2P. Cada uno tendrá un pool en función de las transacciones pendientes que les hayan llegado antes. De este pool coge el minero las transacciones que más les

interesen, las incorpora al bloque y si averigua el acertijo, será este bloque el añadido a la red. Todas estas transacciones validadas e incorporadas a la red dentro de bloques conforman un gran **registro global** de todos los movimientos.

¿Cómo se alcanza exactamente ese consenso sobre un bloque? Aproximadamente cada 10 minutos de media un minero del sistema presenta su selección de transacciones del pool para conformar el siguiente bloque de la cadena. Con la propuesta de varios bloques, se ejecuta el protocolo de consenso cuya entrada de cada minero es el bloque propuesto y la salida es el bloque que se añadirá a la cadena.

Si hubiese alguien que quisiese atentar contra la red y propusiese un **bloque malicioso**, si se confía en que la mayoría de nodos sean honestos, no se añadirá a la cadena. Respecto a los bloques que han sido validados, pero no se han podido añadir a la cadena de bloques, no hay problemas, podrán añadirse más adelante.

Como se ha comentado hay algunos puntos débiles de esta red que no hay que olvidar. Por una parte, la **imperfección de la red P2P** que hace que no todas las parejas de nodos estén conectadas al resto. Esto es debido principalmente a una pobre conexión a Internet, sobre la que se sustenta toda la red blockchain.

Por otra parte, la intervención de **nodos maliciosos** que intenten añadir bloques con transacciones no válidas a la red o trastocarla. Se ha confiado en la honestidad de la mayoría de los nodos. Pero, ¿y si no es así? Se verá más adelante.

Otro factor perjudicial de la red es el no poder tener una **noción global del tiempo**. Es imposible que todos los nodos estén de acuerdo en el orden en el que se sucedieron las transacciones. Por ello el protocolo de consenso no se puede utilizar como criterio para añadir a la red el orden con el que se realizaron las transacciones.

Teniendo estos obstáculos en cuenta, hay muchos protocolos que no se podrían desarrollar en esta red. Un ejemplo de ello es el *Problema de los generales bizantinos* (Sirer, 2013):

Supóngase un escenario de guerra en el que se tiene un grupo de m generales bizantinos que están asediando una ciudad desde distintos lugares y tienen que ponerse de acuerdo para atacar o retirarse de forma coordinada. Entre los generales hay solo uno que puede cursar la orden por ser el comandante. El resto se dice que son tenientes.

Los generales se comunican a través de mensajeros y las dos posibles órdenes del comandante son "atacar" y "retirarse".

Uno o más de los generales puede ser un traidor (al resto se les llama leales), por lo que su objetivo es conseguir que todos los generales leales no se pongan de acuerdo. Para ello pueden ofrecer información errónea. Por ejemplo, si el comandante es el traidor, podría mandar órdenes contradictorias a los distintos tenientes. Si el teniente es un traidor podría indicarles a otros tenientes, con el fin de confundirlos y que creyeran que el traidor es el comandante.

Se ha probado que es imposible resolver el problema si una tercera parte o más de los generales son traidores. Esto mismo pasa con otros protocolos.

3.2.3. Posibles ataques

Como se ha visto anteriormente la red blockchain no ofrece la identidad de los usuarios que participan en ella gracias al sistema P2P que no dispone de una autoridad central que otorgue identidades a los participantes. Una consecuencia negativa de ello son los Sybil attack.

Un **Sybil attack** consiste en una copia de nodos que crea un mismo actor para parecer que hay varios participantes, cuando realmente todas las identidades están controladas por la misma persona.

Si se recuerda el algoritmo de consenso, los pasos que se seguían al emitir una transacción eran los siguientes:

1. Se emite una transacción a todos los nodos
2. Los mineros que 'hayan escuchado' la transacción y la elijan, la incorporan en un bloque
3. Se permite que un nodo aleatorio sea el que pueda añadir su bloque a la cadena
4. Otros nodos aceptan el bloque, únicamente si consideran que todas las transacciones dentro de él son válidas
5. Los nodos muestran su aceptación del bloque incluyendo su hash en el siguiente bloque que se cree.

¿Cómo se puede conseguir que funcione sin ser alterado por nodos maliciosos? Se van a presentar varios casos y explicar los posibles desenlaces. Carolina será el nodo malicioso y Roberto el nodo al que Carolina quiere perjudicar:

- ¿Puede Carolina robar bitcoins que pertenecen a otro usuario con una address (identidad) que ella no controla?

  No. Para hacerlo Carolina debería de hacer una transacción con esa moneda que quiere robar. Y para ello, Carolina necesitaría falsificar la firma digital del

verdadero propietario, imposible como se comentó en la explicación de *Firma Digital*.

- Si Alicia quiere perjudicar a Roberto, ¿puede decidir no poner en el bloque que ella proponga para la cadena ninguna transacción que le pertenezca?

  Sí lo puede hacer, pero no perjudicará gravemente a Roberto. El próximo nodo que proponga un bloque, confiando en su honestidad, sí incluirá las transacciones de Roberto, así que será solo una cuestión de tiempo.

- ¿Es posible un ataque en el que se gasta una cantidad monetaria por partida doble, es decir, un ataque de **doble gasto**?

  Sí, supóngase que Roberto tiene un negocio a partir de una website en el que vende softwares. Y Carolina para comprar uno le hace una transacción a Roberto. En el momento en el que esa transacción ha sido añadida a un bloque por un nodo honesto y el bloque ha sido validado e incorporado a la cadena de bloques, Roberto considera que la transacción es válida y le permite a Carolina que se descargue el software de la web.

  Sin embargo, supóngase que, el próximo bloque validado y que se va a añadir a la cadena de bloques está controlado por Carolina y al añadirlo, ignora el último bloque incorporado, que recoge su transacción a Roberto, y su puntero apunta al hash del bloque anterior. Además, en el bloque que presenta Carolina incluye una transacción en la que envía a una identidad, suya también, las monedas que le envío a Roberto. Esto sería un patrón claro de doble gasto: dos transacciones han gastado las mismas monedas.

¿Y cómo se puede saber si un intento de **doble gasto** ha resultado **exitoso** o no? Que el intento de doble gasto resulta exitoso dependerá de la rama que acabe siendo la más larga, aquélla en la que está la transacción a Roberto o en la que está la transacción a la otra identidad de Carolina.

¿Y en base a qué el siguiente bloque será añadido a una rama u otra? Como política de consenso, se debe añadir el bloque validado a la **rama más larga**, pero en este punto ambas cadenas son igual de largas. Además, para otro minero no hay manera de saber cuál de las dos transacciones que están en los dos bloques por partida doble es la válida. Y al no haber una noción global del tiempo, tampoco se puede comprobar cuál se realizó primero. Por ello, dependerá exclusivamente de lo que decida el que incorpore el nuevo bloque.

En caso de que, por algún motivo (también se debe contemplar un posible soborno de Carolina al que vaya añadir el bloque) el bloque se acabe añadiendo a continuación de aquél que contiene la transacción de Carolina a otra identidad propia, esta rama pasará a ser la más larga y se consolidará como tal. De esta manera, se habrá llevado a cabo el doble gasto y el bloque que se quedó con la transferencia de Carolina a Roberto no tendrá validez. A este tipo de bloques se les considera **orphan block.**

Para evitarlo, Roberto debería esperar a recibir al menos una confirmación antes de permitir a Carolina descargarse el software. Recibir una confirmación, significa que se haya añadido un bloque a continuación de aquel que contiene la transacción que se espera recibir. Cuantas más confirmaciones se reciba, más garantía habrá de que el bloque se consolide dentro de la red. La probabilidad de doble gasto disminuye exponencialmente con el número de confirmaciones. Se dice que lo razonablemente seguro es esperar **seis confirmaciones**.

En este último caso la **evolución** de la **cadena** no **depende** de la criptografía, sino simplemente del **consenso**.

3.3. Minería

En el punto anterior se ha visto cómo se añade un bloque a la cadena de bloques gracias al consenso. En este apartado se va a tratar quiénes son los mineros, cómo consiguen generar esos bloques o qué impacto medioambiental tiene esta actividad. (Antonopoulos, 2017)

3.3.1. Incentivos

Como se ha visto anteriormente, en el caso de un ataque de doble gasto, cuando se crea un bloque con la transacción no legítima, ignorando el último bloque y apuntando al anterior, es difícil detectar por otro minero cuál es el bloque legítimo. Pero, incluso en el caso de ser detectado algún tipo de violación, es difícil castigar al nodo malicioso; no tiene identidad. De la misma manera, es difícil premiar a alguien que cree un bloque legítimo y se consolide dentro de la rama más larga; no hay una dirección de domicilio o un correo electrónico al que poder mandarle un cheque o una recompensa vinculado al usuario.

Sin embargo, hay otras opciones, distintas a las conocidas hoy en día, de premiar a los nodos que se comporten honestamente: usando el **bitcoin como incentivo**. (Paula, 2018) Hay dos maneras:

- La primera es con un **incentivo** al nodo que incorpore un **bloque nuevo** a la cadena. Se hará mediante una transacción especial en la que se crea monedas y el nodo elige el receptor de esa cantidad de monedas mediante la address. Normalmente, el creador del bloque pone una address que pertenece a él mismo. Se puede entender como una manera de pagar por los servicios prestados al crear un bloque.

  La recompensa por bloque comenzó siendo de 50 bitcoins y se determinó que, **cada 210.000 bloques** el valor de la **recompensa se dividiese a la mitad**. **Actualmente**, se está en el segundo periodo, en el que se recibe **12,5 bitcoins** por bloque creado. De esta manera se puede fácilmente deducir, que llegará un momento en el que no habrá bitcoins como recompensa por bloque creados.

  Ésta es la única manera de crear bitcoins y si todo sigue como hasta ahora, en **2140** habrá llegado el momento en el que esos **21 millones de bitcoins** estén **en circulación**. Llegado ese momento, será cuando tomará protagonismo la segunda manera de incentivar un comportamiento honesto: las tarifas por transacción.

- Las **tarifas por transacción** consisten en que el propietario de una transacción elige el valor de salida de la misma, que tiene que ser inferior al valor de entrada. Esa diferencia entre el valor de salida y el de entrada es lo que se considera la tarifa de transacción. Un nodo que genere un bloque con 200 transacciones, recibirá una suma de las tarifas de las 200 transacciones como recompensa por su servicio, y lo hará igualmente a la address que el creador del bloque elija y así refleje en la cabecera del bloque.

  No solo hay que contemplar el trabajo extra que ha tenido que realizar el nodo para meter una transacción en su bloque, sino que cuanto más grande sea el bloque, más probabilidad tiene de quedarse huérfano. En caso de que otro bloque se cree simultáneamente, el **proceso de verificación** será más lento para el bloque de mayor tamaño.

  Esta tarifa es totalmente voluntaria, pero hay que tener en cuenta que conforme mayor sea la tarifa, más interés despertará esa transacción en el minero con respecto a otras y antes se añadirá probablemente a la red.

De momento no es imprescindible ponerles tarifas a las transacciones, puesto que el creador de un bloque ya recibe incentivo por la creación, pero conforme la recompensa por bloque vaya decreciendo, irá tomando cada vez más peso esta segunda manera de incentivo.

No se sabe exactamente cómo va a evolucionar el sistema en este sentido, depende mucho de la Teoría de Juego, y éste es un área aún por explorar.

3.3.2. Prueba de trabajo

El incentivo por bloque generado lo desencadena la **prueba de trabajo** (**Proof of Work, PoW**, en inglés). La idea principal de prueba de trabajo es que se haga a los nodos competir, es decir, conseguir ganar una recompensa en función a la cantidad de energía consumida para calcular el problema matemático que les permitirá optar a añadir su bloque a la red.

Este problema matemático está formado por un **puzle de hashes**. Para proponer un bloque, primero ha tenido que dar el minero con un número llamado **nonce**. A continuación, hay que **concatenar** este nonce, con el hash del bloque previo y con la lista de todas las transacciones que conforman el bloque. Y calcular el **hash** resultante de esta **concatenación** y que esté dentro del espacio objetivo.

Este **espacio objetivo** es mucho menor que el espacio objetivo de todos los hashes posibles resultantes del hash de la cadena. Esto quiere decir que:

- H (nonce || prev_hash || tx || tx || ... || tx) < target -

Y la única manera de hallar ese nonce, es probando uno a uno aleatoriamente hasta dar con aquel que cumpla esta condición. Averiguado ese nonce, el nodo podrá proponer el bloque a la cadena.

¿Qué es exactamente un nonce?, ¿cómo se halla?, ¿cómo se convierte un bloque en válido? La **cabecera de un bloque** la constituyen el hash del bloque, el nonce, el hash de todas las transacciones del bloque y el puntero al bloque anterior. El campo reservado para el nonce tiene 32 bits y ayudará a la validación del bloque cuando se dé con el nonce correcto que haga que el hash de la concatenación, comentada anteriormente, esté por debajo del objetivo.

El **nonce** es un número arbitrario que solo se utiliza una vez. Cuando se pide que un hash comience con una cantidad de ceros, realmente se está pidiendo que sea cualquier número por debajo del número ya presentado, *target*. De manera que, cuanto menor sea el target, mayor será la dificultad para dar con el hash correcto.

Una vez que se hubiesen intentado todas las posibles soluciones dentro de los 32 bits del nonce, se debería haber dado con el hash válido, sin embargo, esto no ocurre. Puede haber más cambios que sean necesarios para dar con el hash válido. Dentro del bloque se tiene el árbol Merkle de transacciones y cada bloque tiene también su nonce Si se modifica el nonce del bloque que está en la parte más baja del árbol, el árbol entero

cambiará. El cambio del nonce en la base se propaga hacia arriba, cambiando el árbol entero. Por ello, los mineros tienden a invertir su tiempo y recursos en calcular las diferentes opciones del nonce de la cabecera, porque cambiar el nonce del bloque más bajo cuesta mucho más trabajo, en lo que a tiempo y recursos se refiere.

La gran mayoría de nonces no funcionarán, pero si se persiste en diferentes nonces de los bloques más bajos, antes o después, se acaba dando con el nonce de la cabecera correcto que genera un hash por debajo del target.

¿Pueden estar dos mineros intentando validar el mismo bloque? Cuando se ha comentado "una vez probados todos los posibles nonces de la cabecera, ir modificando el nonce de uno de los bloques más bajos" se sobre entiende que se hace aumentando el valor del nonce uno a uno, para así seguir un orden y no perder una posible combinación. Así que, si todo el mundo actuase así, pudiera ser que se estuviese intentando resolver el mismo puzzle. Y ganaría el minero más rápido, es decir, el que tuviese más recursos. Pero es muy difícil que se dé esta situación.

Por una parte, se tiene que dar la coincidencia de que dos mineros diferentes estuviesen intentando hashear un bloque con exactamente las mismas transacciones.

Y, además, la dirección que el minero pone en la cabecera del bloque para recibir la compensación en caso de hallar el acertijo, debería ser la misma. Esta address desencadena cambios en todo el árbol Merkle. En caso de que dos mineros pertenezcan a un grupo (**pool de mineros**) que comparten una misma address, sí se podría dar.

Un ejemplo de target, debajo del cual tiene que estar el hash que valide el bloque es:

0000000000000265GC0000000000000000000000000000000000000000

Como se ha dicho antes, cuanto más bajo sea el target, más difícil será encontrar la solución. Esto es lo que se regula para que la media de hallazgo de bloques se mantenga en 10 minutos. Si la dificultad del problema fuese siempre la misma, la dificultad disminuiría. Cada vez hay equipos mejor preparados para este problema, por lo que se devaluaría la moneda y se llegaría más rápido al total de emisión de bitcoins. Para evitarlo se aumenta cada vez más la dificultad del problema, en base al tiempo que se haya tardado en validar los 2016 bloques anteriores.

- ***(Dificultad_próxima) = (Dificulta_previa * 2016 bloques * 10 minutos) / (tiempo tardado en minar los 2016 bloques)*** -

Cuanto más mineros estén minando, antes se encontrará un hardware más eficiente, antes se minará y más se tendrá que aumentar la dificultad.

Por norma general el **número de bloques** que encuentra un nodo son una **fracción** del total de **energía consumida**. Es decir, que si Carolina ha utilizado en calcular hashes un 0.1 % de la energía total consumido por todos los mineros, encontrará alrededor de 1.000 bloques. Realmente cada intento se considera un **intento de Bernoulli**: válido o no válido.

Otra característica importante de esta prueba de trabajo es la **verificación**. Cualquier nodo puede verificar la validez del boque, observando el contenido del mismo y verificando que el valor de salida es menor que el objetivo, condición indispensable ya comentada.

Se puede ver que no se trata de un sistema centralizado. No se necesita ninguna autoridad central que tenga que verificar y controlar la generación de bloques, ni el gasto de energía.

3.3.3. Costes de minado

Sea computar muy difícil o no, lo que realmente importa es que el beneficio que se obtenga por hacerlo sea mayor que lo que cuesta. La recompensa que se puede obtener, si se encuentra un bloque, es la 'recompensa por bloque' y las tarifas de las transacciones. Y lo que nos cuesta minar es el coste del material (hardware) y el coste de energía, principalmente coste de electricidad y de enfriar los equipos. Condición:

Recompensa de minar < Coste de minar

(Recompensa bloque + tarifas de transacciones) < (Hardware + (Elect, enfriar…))

El problema de esta inecuación está en que **no todos** estos **costes** son **fijos** o calculables. El coste del **hardware** sí es **fijo**, sin embargo, el coste de la **electricidad** depende del tiempo que se esté mimando y no solo de la potencia del hardware.

Por otro lado, está el tema de la **moneda**. Mientras que el gasto se hace en la moneda del país en el que se reside (euro, dólar, libra…), el beneficio se obtiene en bitcoins. Puede que no importe, pero puede que donde se quiera gastar el beneficio obtenido no sea en bitcoins.

Es por todo ello que la decisión de minar no es fácil. No se puede predecir si será rentable o no.

Equipos de minado

¿Cuáles son esos hardware que ayudan a computar?

La principal dificultad de minar reside en el cálculo de la función hash. Aunque hay

muchas funciones hash criptográficas, la más segura es la **SHA-256**, la utilizada en la red Bitcoin. No se sabe si seguirá siendo segura durante todo el ciclo de vida del Bitcoin, pero de momento sí. Fue desarrollada por la NSA (US National Security Agency).

Para resolver esta función se requieren unos **equipos muy potentes**. La competitividad en el minado es muy alta y la velocidad con la que se mine es crucial para conseguir el objetivo.

En los inicios del blockchain se empezó a computar con los **PC's de escritorio**. Con estos equipos se alcanzaba a computar alrededor de 15 millones de hashes por segundo (MH/s). Esto se traduce en una media de varios cientos de miles de años para encontrar un bloque válido. Por ello, los mineros pronto vieron el PC's como un recurso inviable para el hallazgo de bloques.

Se sustituyeron por el **GPU** (**graphics processin unit**), un coprocesador dedicado al procesamiento de gráficos u operaciones de coma flotante para aligerar la carga de trabajo del procesador central en aplicaciones como los videojuegos o aplicaciones 3D interactivas.

Al empezar a utilizarse este recurso, necesario para los jugadores de videojuegos, empezaron a escasear las unidades de GPU en el mercado. Muchos jugadores, resultaron perjudicados y explorando el motivo, se convirtieron en mineros. Con este procesador la media para encontrar un bloque válido era de unos 300 años aproximadamente.

A continuación, aparecieron el **FPGA** (field-programmable gate array), un dispositivo programable que contiene bloques de lógica cuya interconexión y funcionalidad puede ser configurada en el momento, mediante un lenguaje de descripción especializado. Estos dispositivos mejoran la velocidad de hallazgo de hashes por segundo, pasando a 1.000 millones de hashes por segundo (GH/s), es decir, encontrar un bloque cada 50 años de media. Como siempre, referido a la dificultad actual.

La última incorporación fue el microprocesador, **ASIC**, diseñado exclusivamente para el minado de bitcoins. No se esperaba el diseño de un procesador tan específico y potente tan rápido.

Con este procesador tan avanzado y de uso exclusivo para el hallazgo de bloques, blockchain se ha convertido en una tecnología que ha despertado el interés ya no solo a nivel particular, sino empresarial. Y lo que, inicialmente, era un equipo particular, se ha convertido en muchos casos en grandes **centros de minado**.

Estos grandes puntos de minado suponen, sin embargo, ir en contra del principio de Satoshi Nakamoto; favorecen a la desigualdad y a la centralización. Es fácil entender que, con estos grandes centros de minado, no sean competitivos muchos individuos,

que no tienen recursos para realizar un despliegue como éste. Para evitarlo una solución pasaría por que solo fuese posible minar con CPU's.

3.3.4. Piscinas de mineros

Esta desigualdad que sufren los mineros individuales no es ya solo por la diferencia de potencia respecto a un centro de minado, sino también debido a la **variabilidad** a la que se enfrentan.

Esta variabilidad implica que un minero pueda tardar 16 meses en encontrar un bloque. Prorrateado puede ser que no sea una cantidad despreciable, pero no da ninguna estabilidad económica.

Para solucionar esta desigualdad por falta de recursos y por enfrentamientos a dicha variabilidad no sostenible, se crearon las **piscinas de minado**.

Un pool de minería se trata de un protocolo para que un grupo de mineros trabajen conjuntamente en el minado de un bloque con una addresses preacordadas para recibir el dinero. La persona que reciba el dinero, se le denomina el **gestor de la piscina**. Una vez hallado el bloque, se encargará de distribuir proporcionalmente el dinero a cada uno de los mineros de la piscina en función de la cantidad de trabajo realizado.

El problema que presentan las piscinas de minado es alcanzar ese 51 % de minado de la red total. Esto también iría en contra de la descentralización que busca el blockchain. Pero, por otro lado, ayuda a mineros solitarios a participar de la red y tener una recompensa fija cada un tiempo determinado.

Los mineros son libres de abandonar un **pool de mineros**, si ven que se está alcanzando mucho poder, pero es algo que no es obligatorio, por lo que el desarrollo y avance de los pools dejan otro **frente abierto** en esta tecnología.

3.3.5. Comportamiento estándar

La actuación de los mineros ayuda al crecimiento y consolidación de la red blockchain. Su intervención sigue una conducta concreta con consecuencias positivas tanto para el propio minero, como para la red en general. Se va a presentar los pasos que dan para cada una de estas dos causas.

Pasos que dan para ayudar al mantenimiento y consolidación de la red

1. **Observar transacciones.** Cuando se ven nuevas transacciones que interesan, se validan comprobando que la firma es la correcta y que no existe ningún caso de doble-gasto.

2. **Mantener la red y registrar nuevos bloques**. Teniendo que estar conectado a todos los nodos de la red, se le pregunta por el registro de todos los bloques que ya pertenecían a la red antes de ingresar. A continuación, se empieza a ver cómo nuevos bloques son propuestos para añadirse a la red, se comprueba las transacciones de su interior, así como el nonce, y se validan.
3. **Formar un bloque candidato para la red.** Una vez que ya se tiene una copia entera de la red, se puede empezar a montar un bloque propio. Con las transacciones observadas previamente, se agrupan y se añaden a un bloque asegurándose de que sean válidas.

Pasos para incentivar al minero a formar parte de la red y a participar en ella

1. **Encontrar un nonce que haga el bloque válido.** Este es el paso que más trabajo cuesta en ambos sentidos (de tiempo y económico).
2. **Esperar a que el bloque sea aceptado.** Aunque ya se haya encontrado un bloque con todas sus transacciones válidas y con su nonce también, no es seguro que pase a formar parte del consenso de la red. Influye la suerte. Si alguien encuentra un bloque más o menos al mismo tiempo y el resto de nodos, por consenso, deciden seguir por encima del otro bloque, el otro no será validado.
3. **Obtener beneficio.** Cuando el resto de mineros aceptan un bloque, el minero que lo propuso habrá ganado una recompensa por el bloque (actualmente de 12.5 bitcoins, que es igual a 65.000€ aproximadamente), aparte de las tarifas de las transacciones.

Estos pasos que se han definido de los mineros, es suponiendo que siguen un comportamiento estándar. Pero este comportamiento es subjetivo, es decir, no hay nada definido respecto a la forma de **minar** o a la **estrategia** que seguir, cada nodo es libre de actuar como quiera, aunque ello desencadena un bloque huérfano o un doble gasto.

La estrategia de **minado estándar** suele ser la siguiente:

- Respecto a las transacciones qué incluir, los mineros suelen elegir las transacciones con tarifas más altas.
- Respecto al bloque sobre el cual añadir el de uno mismo, se suele optar por aquel que pertenezca a la cadena más larga.
- En caso de tener dos bloques que proceden de dos cadenas igual de largas, se debe optar por poner el de uno delante de aquel sobre el que se escuchó primero.
- Sobre cuándo anunciar un nuevo bloque, se suele hacer en cuanto se tiene. Pero una alternativa, puede ser querer anunciar dos bloques a la vez, uno encima de

otro, dando lugar a un posible bloque 'huérfano' que antes pertenecía a la cadena más larga, pero que después no al ser incluidos dos bloques simultáneamente por otra rama.

Pero como se ha dicho esto es lo que se suele hacer. En cada punto, cada decisión que se tome determinará el desarrollo de la red en un sentido u otro. Al no ser nada fijo, aquí se abre otro punto de **incertidumbre** de la red.

3.3.6. Impacto medioambiental

En los puntos anteriores se ha hablado del gran esfuerzo económico que cuesta minar tanto por los equipos tan potentes que se requieren, como por la energía que se necesita para su funcionamiento. Pero, ¿qué **impacto medioambiental** tiene este consumo?

Inicialmente el minado lo realizaban varios individuos, actualmente ya existen numerosos centros con miles de equipos dedicados exclusivamente a ello. Para realizar la labor de minado, se **consume energía** por partida triple:

- La primera, en la **construcción** del equipo **ASIC**. El equipo está compuesto por muchos materiales, que hay que ensamblar. Una vez el equipo está montado, hay que gastar más energía en el envío al particular/empresa de destino.
- La segunda manera en la que se consume energía es en la **electricidad**. Durante el minado, todos los equipos están conectados a la red eléctrica.
- Y la tercera, en el **proceso de enfriamiento** de los equipos. Durante el minado, el tiempo de conexión de los equipos, a veces, es casi ilimitado. Y durante su funcionamiento los equipos disipan la energía en forma de calor. Este calor concentrado en la habitación donde se sitúen los equipos, puede sobrecalentar en exceso el hábitat y perjudicar al funcionamiento de los mismos. Para ello se desarrollan unos procesos de enfriamiento.

En el caso de la energía empleada para el equipamiento y la electricidad, ésta disminuye con el minado de escala. Es decir, es más barato fabricar 1000 ASIC seguidos, que construir 5. Y, en cuanto a la energía, lo mismo. Si los equipos para la generación de bloques están concentrados, habrá menos fuentes de suministro de energía. Sin embargo, con la energía de enfriamiento, ésta aumenta más de lo proporcional conforme aumenten los equipos de minado.

Se estima que, aproximadamente, el consumo actual de **energía** que genera la red de **blockchain** se corresponda con el **10 %** de lo que puede consumir una **gran central**

eléctrica. Muchos comentan que es un **desperdicio** el consumo de energía para este fin, pues solo tiene como objetivo la creación de bitcoins.

Pero si se tiene en cuenta toda la energía empleada en la elaboración del dinero actual, también se podría hablar de un desperdicio para mantener el sistema actual monetario. También se emplea mucha energía en la fabricación de los billetes y las moneda, en el empaquetamiento para el transporte, en el propio transporte, en el almacenamiento, etc.

Un problema del uso de esta energía para la generación de bloques lo tienen algunos países que subvencionan electricidad para captar a empresas. Pero si estas empresas tienen como objetivo la creación de bitcoins, se trataría de convertir energía en algo cuyo uso no es para el propio país. El uso de **energía renovable**, es un campo de investigación pendiente del blockchain.

3.4. Incertidumbre sobre la evolución de blockchain

Hasta ahora se ha visto cómo funciona esta nueva tecnología de una forma más técnica y algunos ejemplos de cómo puede impactar en la sociedad actual y futura.

Pero también se ha ido viendo algunos puntos que no ayudan a tener una visión clara de la evolución del blockchain.

Uno de los principales **problemas** reside en la **debilidad** de la **red P2P**. El propósito de esta red es propagar todas las transacciones y nuevos bloques por todos los nodos, sin embargo, debido a las imperfecciones de la red, la garantía no es absoluta.

Por otra parte, está la política de añadir los bloques a la rama más larga. Como se ha dicho, es una política de consenso, pero no es obligatorio actuar así. Y que algún nodo no siga un **comportamiento estándar**, puede traducirse en bloques huérfanos.

También se puede contemplar la **desigualdad** que se puede generar entre diferentes nodos al **minar** por la capacidad de computar que tenga el **hardware** que utilizan. Los costes que tienen son mayores por el hardware de mayor potencia, por lo que parece lógico que necesiten menos tiempo para minar. Pero, por otro lado, blockchain busca la descentralización, la igualdad y la no dependencia económica para evolucionar.

Y, como se ha presentado anteriormente, no se debe olvidar el **impacto medioambiental** que esta revolución está generando y puede genera.

A pesar de estos puntos débiles, si se quiere hacer crecer a esta nueva tecnología, hay que conseguir que se confíe en ella y que se ayude en su desarrollo. Un comportamiento honesto es lo que más puede favorecer a ello.

4. Otras tecnologías disruptivas

La sociedad está desde hace varios años expuesta a una gran evolución y cada vez mayor, especialmente en el ámbito tecnológico. Acompañando a blockchain, hay otras muchas tecnologías que están impactando hasta tal punto que las empresas tienen que renovarse y renovar su proceder diario casi cada temporada. Algunas de esas tecnologías son Internet of Things o la tecnología que posibilita la existencia de drones.

4.1. Internet of Things

Internet de las cosas (Internet of Things, **IoT**, en inglés) es un concepto que hace referencia a la interconexión digital de objetos con Internet.

Consiste en la **equipación** con **microcontroladores, transceptores** para la comunicación digital y **pilas** de algunos de los **objetos** cotidianos del día a día, como electrodomésticos, cámaras de vigilancia, sensores monitorizados, pantallas, vehículos, etc. (Yousaf Bin Zikria, 2018) Esta equipación posibilita la comunicación entre objetos y usuarios, convirtiéndose así IoT en una parte integral de Internet.

Los dispositivos se conectan entre sí utilizando diferentes tecnologías, entre las cuales destacan (Guru 99, s.f.):

- Conexión inalámbrica (ej.: Bluetooth, Wifi, RFID)
- Red en malla
- Red de área amplia o Wide Área Network (ej.: 3G, LTE, 4G)
- Conexión por cable

Se ha predicho que en el **2020** alrededor de **26.000 millones de dispositivos** pertenecerán a IoT. Una cifra muy significativa a tener en cuenta. Hay que aprovechar esta tendencia positiva que está mostrando para mejorar aquellas áreas que se puedan.

Se espera que esta conexión entre dispositivos de lugar a la generación de nuevos datos. IoT ayudará a numerosos negocios a mejorar su eficiencia, mejorar su operativa y aumentar la satisfacción de sus clientes.

Un punto a mejorar de esta nueva tecnología es la variedad de todos estos dispositivos que forman y formarán parte de este nuevo sistema de intercomunicación. Todos los dispositivos intervinientes procederán de **diferentes proveedores** de todo el mundo, por lo que será **difícil** integrar todos estos dispositivos en **un único software**.

En IoT los dispositivos tienen **sensores** conectados a una plataforma. Esta plataforma recoge datos de los diferentes dispositivos y aplica estudios analíticos para explotar al

máximo la información que se recoge. Las plataformas IoT pueden detectar exactamente qué información es útil y cuál se puede desechar. En este aspecto, el uso de Data Analytics o Big Data es muy interesante. Garantiza un mejor uso de la información.

4.2. Vehículo aéreo no tripulado

Un **vehículo aéreo no tripulado** (Unmanned Aerial Vehicle, UAV) o comúnmente conocido como dron es una aeronave que vuela sin tripulación. Este artículo novedoso se ha desarrollado bastante en las últimas décadas gracias principalmente a **aplicaciones militares**. Su evolución en este ámbito ha hecho que acabase encontrando un hueco en el ámbito civil. (Francois Laurent, 2016)

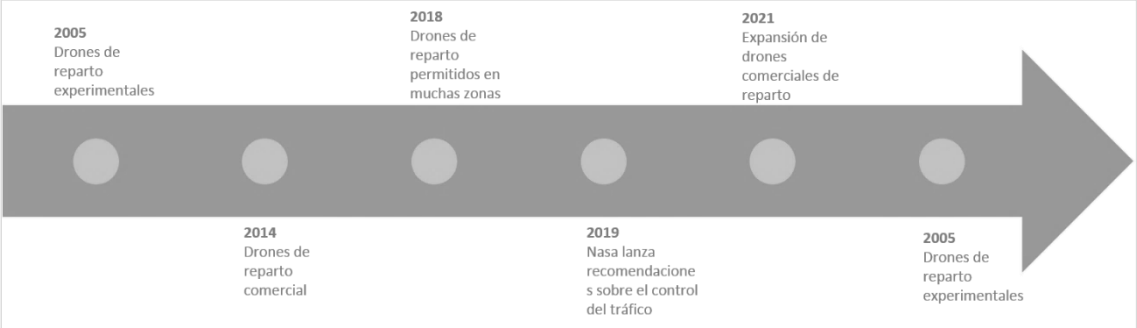
Actualmente el uso más conocido que se le da al dron es el de realizar fotos, vídeos o recreaciones. Pero su gran potencial, más allá de tener la función de cámara voladora, ya ha despertado el interés de muchas empresas.

Algunos **ejemplos de usos** o **empresas** que ya comercializan con drones son:

- Entrega de medicamento y comida en países subdesarrollados con apenas regulación aérea
- Salvamento marítimo
- DHL con PaketKopter
- Axdron para salvamento marítimo
- Google con Project Wing

Actualmente ya existen los drones híbridos con una mayor duración de vuelos y equipados con hélices y alas, que les permite planear, despegar y aterrizar igual que un avión o un helicóptero. Estas características posibilitan a los drones tener una funcionalidad de transporte.

Esta posibilidad de **distribución** de los drones ha atraído a muchos sectores y empresas, a pesar de las **limitaciones** actuales que tienen en gran medida por **regulación aérea**.



En esta imagen se muestran los puntos más importantes en la **evolución de los drones**.

En el **2005**, empresas como DHL, UPS, Google o Amazon empezaron a probar con drones prototipos. Inicialmente no estaban muy desarrollados tecnológicamente, pero en **2014** la evolución fue tal, como para que DHL lanzase su primer dron comercial a la isla alemana de Juist. En **2015** Amazon recibió la aprobación de la FAA (Administración Federal de Aviación de EEUU) para poder investigar y desarrollar drones de reparto. Actualmente ya alrededor de 8.000 drones comerciales han obtenido el permiso para operar.

La NASA ya ha lanzado sus recomendaciones sobre la **regulación de tráfico aéreo** y se estima que para el **2021** la entrega a partir de drones ya esté muy extendida y estandarizada.

El CEO de Amazon, Jeff Bezos, ya dijo: “Pronto ver drones de Amazon será tan común como ver vehículos de reparto”.

5. Cadena de suministros y la última milla

En este capítulo se va a presentar el punto de aplicación del blockchain en este trabajo. Ya se debe tener una idea clara de cómo funciona el blockchain y en dónde puede desencadenar una mejora significativa.

Así que, en este capítulo se va a explicar el funcionamiento del sector logístico con especial enfoque en la cadena de suministros y última milla.

5.1. Logística

Se denomina *logística* a la función de la empresa responsable de entregar el producto correcto, en las condiciones de cantidad y calidad correctas, en el lugar y en el momento correcto y con los costes mínimos.

Se puede hablar de tres objetivos básicos que se persiguen en la logística:

- **Servicio de mercado**, es decir, la rapidez con la que se realizan las entregas y la variedad de productos que se ofrecen.
- **Eficiencia en el uso de recursos**, es decir, hacer un buen uso de los recursos, de manera que sirvan para dar un valor añadido al producto.
- **Mínimos costes,** siendo uno de los costes principales el **coste de stock**. Un aumento en el nivel de stock, implicaría un aumento también del coste de stock, por lo que hay que saber qué cantidad de stock se debe tener para conseguir abastecer siempre al cliente.

El problema de perseguir estos tres objetivos es que no son complementarios, por lo que alcanzar el **punto de equilibrio óptimo** no es fácil.

Por ejemplo, si el gerente de una empresa quiere aumentar la rapidez de sus entregas, tendría que aumentar los niveles de stocks para no quedarse nunca sin productos. Esto mejoraría el servicio de mercado, pero no ayudaría a una reducción de costes. Otro ejemplo sería el caso en el que un gerente quisiese ampliar la variedad de productos ofertados a sus clientes. Ayudaría de nuevo al servicio de mercado, pero no a la eficiencia en el uso de recursos.

Se puede concluir pues, que alcanzar un rendimiento máximo en esta transformación económica resulta una tarea difícil. En ello reside el objetivo de toda empresa: alcanzar ese equilibrio que dé un mayor beneficio y que te diferencie de tus competidores.

5.2. Cadena de Suministros

Cadena de Suministros implica **control y seguimiento** de las operaciones desarrolladas sobre el producto, desde la disponibilidad de las materias primas hasta la entrega del producto final al cliente.

Hay muchos tipos de cadenas de suministros; algunas que son sencillas, requieren pocas etapas de transformación y una gestión fácil, y otras más complicadas: las cadenas de suministros desarrolladas en los últimos años. Su exigencia crece cada vez más debido en gran medida al **comercio electrónico**.

La gestión de la cadena de suministros (**SCM**, por sus siglas en inglés de *Supply Chain Management*) requiere un buen flujo de materiales y de información. Uno de los principales objetivos que se persiguen es que, todos los intervinientes de la cadena de suministros (fabricantes, intermediarios, mayoristas, minoristas o distribuidores) puedan acceder a cualquier **información** de la cadena, que le ayude a tomar decisiones útiles para alcanzar sus objetivos.

En cuanto al **flujo de material** se puede decir que, cuando existe una sincronización entre las necesidades y los suministros todos los intervinientes de la cadena ganan: los fabricantes usan mejor su capacidad, los mayoristas y minoristas venden el producto exacto que tienen almacenado, los clientes reciben su pedido antes y, en general, los costes disminuyen y la satisfacción de todos aumenta.

Conocer las necesidades del cliente lo antes posible es clave hoy en día, para ello el flujo de información tiene que ser bueno para poder actuar lo antes posible. De lo contrario el nivel de servicio empeorará y las empresas perderán clientes.

Para que la **información** disponible en la cadena de suministros resulte **eficaz**, es necesario que se satisfagan los siguientes puntos:

- **Actualización de la información dinámica**. Cualquier dato repercute de una manera u otra sobre los diferentes agentes de la cadena. La falta de propagación de un dato a lo largo de ésta favorece a la ralentización de los procesos. Esto se traduce en un retraso en la entrega al cliente y su consecuente insatisfacción, así como aumento de costes.
  En caso de que existan eventos importantes y de gran impacto, se deben notificar de inmediato para disminuir el tiempo de reacción.
- **Visibilidad de la información**. Qué tipo de información puede ver qué agente de la cadena de suministros. La información puede ser:

  - **Información horizontal**: información disponible para un mismo nivel de la cadena, por ejemplo, compartir cualquier información acerca de un producto determinado.
  - **Información vertical**: información que procede de diferentes niveles de la cadena, por ejemplo, un mayorista que desea conocer en qué parte de la cadena se halla su pedido.
- **Procedimientos de aprobación**. Es normal que exista cierta limitación en cuanto a la disponibilidad de datos e información. No cualquier actor de la cadena puede acceder al máximo detalle de información de cualquier otro. Debe existir cierta privacidad, siempre que no afecte al resto de la cadena. Para ello es aconsejable determinar unos procedimientos que establezcan **acuerdos entre** los diferentes **agentes** de la cadena.

De todas formas, sea cual sea la actualización o visibilidad de información o los procedimientos de aprobación, parece evidente pensar que cada vez más este tipo de colaboración será más estrecha debido a los avaneces tecnológicos, así como a las exigencias de mercado.

En cuanto a la medición **general** de la **eficiencia y funcionamiento** de la cadena de suministros, existen una serie de **parámetros** que ayudan a evaluarla. Algunos de los más importantes son los siguientes:

- **Calidad de entrega**. Se evalúa en función del número de envíos entregados con la calidad esperada por el cliente.
- **Plazo de entrega del pedido completo**. Para medir este tiempo medio se calcula la media y la desviación típica del tiempo que transcurre entre el que el cliente realiza el pedido hasta que lo recibe.
- **Cobertura de stock.** Esto indica el número de días que puede seguir abasteciendo una cadena ante una parada de producción o de las fuentes de suministro. En una buena gestión, esta cobertura debería ser baja. Una cobertura alta implicaría un gran stock y los altos costes correspondientes.
- **Tiempo de respuesta de la cadena de suministros.** Evalúa la adaptabilidad que presenta la cadena ante un cambio del cliente en cuanto al producto o a la cantidad. Esto se calcula con la media y la desviación típica del tiempo necesario desde que el cliente realiza el pedido hasta que se terminar de preparar todo el proceso de preparación del producto.

- **Eficiencia en los medios de transportes.** Se calcula a partir de la cantidad de horas que se utilizan los medios de transporte frente a las horas de trabajo.

De esta manera ya se conocen los principales factores que pueden influir en una buena cadena de suministros, que se gestione bien y que satisfaga a los diferentes actores que intervienen en ella, destacando entre ellos al **consumidor final**.

5.3. La Última Milla

La última milla es un término utilizado en la gestión de la cadena de suministros, SCM, para describir el **movimiento** de **personas** y **mercancías** desde un centro de distribución **hasta** el **punto final**: hogar, punto de recogida, taquillas, etc.

El Comité de Profesionales de la Gestión de la Cadena de Suministro estima que hasta un **28% del coste de entrega** proviene de la **última milla.**

El objetivo de la última milla es entregar la mercancía lo antes y en las mejores condiciones posibles. Actualmente el consumidor final quiere los productos de manera inmediata y está dispuesto a pagar por ello.

Según un estudio de McKinsey (Martin Joerss, 2016), una parte significante de las personas estarían dispuestas a pagar hasta un **25% más por recibir el producto el mismo día** del pedido o al día siguiente. Esto se ha traducido en una nueva era en la que cualquier tipo de producto se **compra online** en pocos minutos y sin necesidad de desplazarse a ningún sitio.

El tiempo de entrega es actualmente uno de los puntos diferenciales y los drones pueden jugar aquí un punto muy importante.

El estudio de **McKinsery** también añade que los **drones** serán los que realicen las entregas en las zonas rurales y que por ello se necesita que sean más baratos y que la regulación cambie. No solo harán las entregas en las zonas rurales, sino que realizarán un **80% del total de los paquetes**. Además, se estima que el **20-25%** de todas las **entregas** se realicen el **mismo día** o al día **siguiente**.

Vista la importancia de realizar una buena entrega al cliente final, parece que las nuevas tecnologías pueden ayudar a optimizar este sector y satisfacer al cliente. No se puede ignorar las nuevas oportunidades que la evolución tecnológica está brindando.

Características operativas

A continuación, se van a presentar algunas de las **características operativas** de esta última parte de la cadena de suministros con el objetivo de poder entender mejor cómo los avances tecnológicos pueden ayudar a su optimización.

Según el ebook, The Ultimate Guide to Last Mile & White Glove Logistics, publicado por la empresa de gestión de transporte, Cerasis, existen once métricas o KPIs en la última milla recogidas en tres categorías principales: **tiempo, coste y eficiencia**.

Nº	Categoría	Métrica para la Última Milla
1		Entregas a tiempo
2	Time	Número de paradas
3		Tiempo medio de servicio
4	Coste	Coste por producto, por kilómetro y por vehículo
5		Tasa de consumo de gasolina
6		Capacidad del medio de transporte usado Vs. Capacidad disponible
7		Kilometraje planificado Vs. Realizado
8	Eficiencia	Horas del conductor en movimiento Vs. Horas estacionado
9		Quejas del cliente
10		Exactitud de las condiciones del pedido
11		Quejas por daños

Todos estos indicadores mejorarían con una buena aplicación y adaptación entre el sistema actual de entrega y los avances que están aterrizando.

Se puede hablar de **cuatro variables** que juegan un papel importante sobre la última milla y cuyos indicadores mejorarían con las nuevas tecnologías*:* (Terzia, 2011)

- Gestión de las operaciones de distribución
- Punto de intercambio del producto
- Transbordo del producto
- Plazo de entrega

A continuación, se va a presentar algunos ejemplos de diferentes aspectos de la última milla, cuya mejora impactaría directamente sobre los indicadores.

- **Espacio de tiempo**: hace referencia al espacio de tiempo en el que puede tener lugar la **entrega del pedido***.* En este caso, lo que solicita el consumidor se opone a lo que beneficia a la compañía de entrega. El cliente solicita siempre una franja horaria de entrega pequeña. Las entregas más frecuentes son a domicilio, y una franja larga obligaría al cliente a estar en su domicilio durante ese tiempo. Mientras que las compañías tendrán más flexibilidad, cuanto mayor sea esta franja.
  El **momento de entrega** también es importante. Para una compañía que tenga pocos pedidos en un área determinada, quizás no sea posible realizar entregas

más allá de los martes y jueves, lo cual puede suponer una insatisfacción del cliente traducido en un abandono.

En este aspecto el comercio electrónico está intentando avanzar hasta el punto de realizar las entregas el mismo día y ofertando diferentes puntos de recogida. De esta manera indicadores de tiempo y de eficiencia mejorarían de manera significativa.

- **Plan de ruta:** la planificación de ruta de los vehículos para alcanzar un servicio de entrega efectiva es un área crítica de la *última milla.* Mejoras sobre los cálculos de las **rutas óptimas** o maneras para **actualizar** las rutas en base a **cambios** externos, ayudaría a una reducción de costes considerables.

  Sería muy beneficioso que todos los vehículos con mercancía de pedidos pendientes, tuviesen una información lo más actualizada posible del **estado del tráfico** y los puntos de congestión o **atasco**. Esta información les permitiría cambiar su ruta ganando tiempo y dinero. Los valores de esta variable pueden ser:
  - **Estático:** la ruta es previamente definida a partir de una herramienta computacional, pero no admite cambios una vez que la entrega se está realizando.
  - **Dinámico:** la ruta se define también previamente a partir de una herramienta computacional y admite cambios/actualizaciones durante la propia entrega en función de sucesos que estén ocurriendo en el momento.
  - **Ninguno:** no se usa ninguna herramienta computacional para el diseño de rutas.

  Internet of Things podría ayudar en este aspecto consiguiendo una mejoría de la mayoría de indicadores. Una actualización constante de la información permitiría que aproximadamente los kilómetros planificados correspondiesen a los realizados, que las entregas se realizasen a tiempo o que la tasas media de consumo de gasolina disminuyese.

- **Modo de recepción:** es importante evaluar el servicio de entrega proporcionado por la empresa. El servicio de entrega implica el punto de recogida del pedido, en un punto común de recogida, en un lugar con taquillas para pedidos, en tiendas, etc. La **implementación** de estos **servicios** puede reducir el número de envíos a domicilio, siempre que no se requiera una firma por el receptor. Estos puntos de recogida son seguros y requieren menos viajes para los repartidores, ya que las entregas están más concentradas. Esta disminución de kilómetros recorridos lleva una reducción de costes y un menor impacto sobre el medioambiente.

Existen cuatro formas de recepción:

- **Taquillas:** el pedido se deja sobre una taquilla o caja, esperando a ser recogido por el cliente.
- **Tiendas:** la empresa encargada de entregar los pedidos, tendría que llegar a un acuerdo con los distintos puntos de recogida que quiera para sus empleados. Esto implicaría una limitación horaria para el cliente, al tratarse de un supermercado, una tienda u otro establecimiento público, pero mejoraría la franja horaria a la que se acoge uno en a la entrega asistida a domicilio.
- **A domicilio asistido:** los pedidos son entregados en casa a la espera de una firma. Esto implica una menor flexibilidad para el cliente.
- **A domicilio no asistido:** entrega a domicilio, pero sin la necesidad de un recibimiento personal.

Los drones podrían ayudar a que la oferta de puntos de entrega fuese mayor y no dependiese tanto de la ubicación de la zona de entrega.

- **Tiempo de espera**: hace referencia al tiempo transcurrido entre que se realiza el pedido y se produce la entrega. Esta característica está directamente relacionada con la eficiencia de la empresa y su habilidad para responder a un cambio en el mercado.

  Esta variable a su vez está relacionada directamente con otras sub variables relacionadas con el almacén y el lugar de preparación de los pedidos.

  Esta variable relacionada con indicadores de tiempo (tiempo de entrega) o de eficiencia (quejas del cliente) se verían mejoradas con el uso de drones, que harían las entregas más rápido, y de IoT, que agilizaría todos los trámites gracias una mejora en el flujo de información.

De esta manera se podría erradicar con algunos de los **frentes abiertos** actualmente de la última milla:

- **Costes de transporte**. Las exigencias del cliente se traducen en envíos individualizados, en destinos finales muy diversos que no permiten aprovechar una misma ruta para diferentes entregas y en cambios constantes de la ruta planificada.
- **Comercio electrónico**. Hoy en día con el comercio electrónico los consumidores exigen entregas cada vez de más calidad, más rápidas y a coste cero, convirtiéndose en desafiante el reto de los costes de la última milla. Cuanto mejor sea la gestión en las partes previas de la cadena, menor serán los costes en esta

última parte. Parece evidente pues, que es necesario encarar esta parte final del recorrido de un pedido. Más aún, si se tiene en cuenta la **tendencia ascendente** que está adquiriendo el comercio electrónico, que ha aumentado hasta casi un 30% en los últimos cinco años, llegando el año pasado a alcanzar unas ventas de 1.350 M $ (*statista, 2018*). Los principales productos que han favorecido a este aumento han sido los productos de electrónica, de entretenimiento, de salud y bien estar y de comida.

- **Contaminación medioambiental**. Cumplir con la satisfacción plena del cliente implica un aumento de la contaminación medioambiental. El transporte mediante vehículos para realizar todas las entregas genera mucho tráfico y emisión de CO2.
- **Infraestructura**. En las zonas urbanas la infraestructura para los **medios de transporte** ya utiliza su **capacidad total**, generándose con frecuencia tráfico y grandes atascos. Los proveedores luchan a diario contra otros usuarios de las carreteras por el escaso espacio limitado del que se dispone.

La disponibilidad de buenos canales de comunicación y de la calidad de información correspondiente, apoyado por unos medios de distribución más eficientes, está allanando el camino al sector logístico y especialmente a la última milla. El uso de Smartphones es un claro ejemplo de mejora en este aspecto.

¡Que no se desaproveche la ventaja que ofrece cualquier evolución!

6. Aplicación de blockchain en la cadena de suministros

En los primeros capítulos del trabajo se presentó la tecnología blockchain como una tecnología innovadora que está empezando a tener impacto en ciertos sectores y que puede llegar a suponer un cambio del modelo de negocio en general.

A continuación, se van a nombrar algunas de las principales características del blockchain, que ya se comentaron en los capítulos iniciales, para entender mejor su aplicación en la cadena de suministros.

- La **seguridad** e **inmutabilidad**, gracias a su sistema criptográfico.
- La **transparencia**, gracias a la posibilidad de acceso de cualquier usuario a cualquier bloque de la red.
- La fácil **verificación** por parte de cualquier usuario a partir de claves públicas y privadas, que favorece junto a otras propiedades a una **descentralización**.

El sector logístico, precedido por el financiero, es uno de los sectores cuya mejoría gracias al blockchain parece inevitable. En este capítulo se mostrarán los motivos.

6.1. Smart Contracts

Un **Smart contract**, también conocido como cryptocontract, es como un programa informático que controla la transferencia de activos entre diferentes partes y bajo ciertas condiciones (Search compliance, 2018).

La idea de los Smart contracts la desarrolló **Nick Szabo**, un ciudadano estadounidense que empezó a hablar en 1995 sobre este concepto en una web (King, 2019). En aquel momento no despertó mucho interés, pues no existía esa plataforma digital distribuida que lo pudiese sostener. Sin embargo, en **2008** con el nacimiento del blockchain empezaron a cobrar sentido y aplicabilidad los Smart Contracts.

Desde entonces, la popularidad de los Smart contracts ha ido creciendo. Actualmente, muchas transacciones son ejecutadas ya a partir de estos contratos inteligentes.

En un Smart contract, al igual que en un contrato tradicional, se definen tanto las condiciones como las penalizaciones por el no cumplimiento. La diferencia reside en la codificación de cualquier posible desenlace, de forma que la resolución del Smart Contract se ejecute automáticamente.

Este automatismo se definirá de la siguiente manera: se tomará como input una información determinada, se le asignará a cada input un output según las condiciones acordadas y cuando una de esas condiciones se cumplan, automáticamente se ejecutará su output correspondiente programado. Es por ello, que será muy importante definir con exactitud y detalle todas las condiciones del acuerdo.

Los Smart contracts son complejos. Su potencial va más allá de una simple transferencia de activos. Pueden ejecutar una gran variedad de transacciones en diferentes ámbitos (el legal, el financiero, el de seguros, etc.).

Una de las consecuencias del automatismo que ejecutan es la **no** necesidad de **intermediarios** que tengan que verificar el cumplimiento/no cumplimiento de las cláusulas. Las condiciones se ejecutan en tiempo real. Esto se traduce en un **ahorro** de **tiempo** y **dinero**.

¿Por qué el potencial de los Smart Contracts con blockchian?

Blockchain es perfecto para almacenar Smart contracts gracias a la **seguridad** que brinda y a la **imposibilidad de alterar** la información una vez registrada. Además, no se trata de un papel que se pueda perder o un documento que se pueda eliminar; el acceso a él será siempre posible a través de la red.

Otra ventaja que encuentran los Smart contracts en blockchain es la **flexibilidad** que ofrece para poder almacenar en ellos cualquier tipo de información, así como ejecutar cualquier tipo de acción.

Los Smart contracts, respaldados por el blockchain, están ayudando a muchas empresas a optimizar muchos procesos, alcanzando más seguridad, eficiencia y reducción de costes.

¿Cómo se ejecuta un Smart Contract?

Véase con un ejemplo de cambio de propietario de un inmueble:

1. Dos partes, A y B, crean un Smart Contract para hacer un traspaso de un inmueble una vez que se deposite una cantidad de bitcoins en la dirección de B. Para que se ejecute el cambio de propietario, A inicia la transacción.
2. La transacción se almacena junto a otras transacciones pendientes hasta que es incluida en un bloque que se propone como candidato para ser añadido a la red. En ese momento el bloque es enviado a todos los nodos de la red.
3. Los mineros evalúan si la transacción es válida. Cuando se alcance el consenso de al menos el 51% la transacción se considerará válida.

4. Este bloque será identificado con un hash y tendrá un puntero al hash del bloque anterior.
5. Cuando se realicen las confirmaciones acordadas en el Smart Contract, se dará por válida la transacción que A ha realizado a B y automáticamente el propietario del inmueble pasará a ser B. En caso de que A se arrepienta, no habrá opción de cambio. La ejecución será automática.

En referencia a la cadena de suministros una aplicación clara sería en el **envío de un paquete**: en el Smart Contract se codificaría que el pago a la empresa se realizase automáticamente en el momento en el que el consumidor recibiese el paquete. Esto implicaría una reducción de tiempos, de documentación y de control.

Un ejemplo real de Smart Contract lo llevó a cabo la compañía de seguros, Axa, en 2018 en Francia. Estos Smart Contracts compensaban a los clientes de las aerolíneas en caso de que éstas sufriesen algún retraso (Clement, 2018).

6.2. Mejoras en la cadena de suministros gracias al blockchain

En este punto se va a presentar más en detalles algunos de los puntos flojos de la cadena de suministros y cómo el blockchain puede fortalecerlos. A continuación, se mostrará también en qué operativas se puede traducir la mejoría de estos puntos flojos y ejemplos reales de esta aplicación.

6.2.1. Puntos flojos y soluciones

Algunos de los **puntos flojos de la cadena de suministros** y más importantes son los siguientes (Clemente, 2018):

- **La trazabilidad** la capacidad para controlar algunas circunstancias e información relacionadas con el producto. Por ejemplo, saber la localización de un activo en un momento concreto.
- **El cumplimiento**, la seguridad de que se va a llevar a cabo aquello que se haya acordado previamente bajo unas condiciones. Por ejemplo, hacer una devolución de parte del dinero, si el paquete no se ha entregado en el tiempo estimado.

- **La flexibilidad**, la capacidad para adaptarse a nuevos cambios o problemas. Para ello es importante contemplar varios escenarios y sin que suponga un gran incremento de costes de operación. Por ejemplo, una entrega urgente que se va a realizar por medio de transporte y hay un atasco que va a retrasar la entrega varias horas.
- **La gestión de la cadena**, la efectividad en el control de la cadena. Una buena comunicación entre los diferentes actores ayuda a reducir el riesgo y aumentar la confianza entre las diferentes partes.

Expuestos estas áreas de mejora de la cadena de suministros, se va a explicar cómo blockchain podría interceder en cada una de ellas para su mejora:

- Respecto a la **trazabilidad**, blockchain puede ofrecer acerca de cualquier producto de cualquier parte de la cadena una información completa y detallada de éste, como el lugar o el estado en el que se encuentra en cada momento.
- En cuanto al **cumplimiento** de los acordado, blockchain puede ayudar con su propiedad de **inmutabilidad**. Las transacciones que se realizan en blockchain no tienen opción de manipulación, convirtiéndose la red así en una fuente de datos única e íntegra. Esto es muy favorable en la cadena de suministros para que no se pueda modificar la información de un material en un momento determinado una vez registrado en la red, como el origen o el recorrido que hizo hasta su destino.
- Respecto a la **flexibilidad** de adaptación ante el cambio, los **Smart Contracts** ayudarían bastante. Los Smart Contract junto a la tecnología IoT facilitarían un seguimiento en tiempo real de la información relativa a los productos, pudiendo ayudar ésta a redefinir el plan de actuación según nuevos acontecimientos, como un atasco en un punto de la ruta planificada.
- En cuanto a la **gestión de la cadena** de suministros, la desaparición de **intermediarios** que implica el blockchain simplificaría bastante los procesos. También las **firmas digitales**, ahorrarían a la cadena mucho papeleo y procedimientos de verificación y aprobación.

Éstas son las principales áreas de mejora que ofrece blockchain en la cadena de suministros y que favorecería también a un gran ahorro de tiempo y costes.

Actualmente existe un software para Smartphones y ordenadores que ayuda a gestionar la cadena de suministros de una manera más efectiva, **TraceChain** (Hash, 2018). Este prototipo recoge todas las mejoras vistas anteriormente. Permite el seguimiento y rastreo de materiales y productos terminados, brindando a los usuarios un gran nivel de

confianza en cuanto a los datos que almacena. También ofrece datos más enriquecidos y análisis más profundos, casi a tiempo real. Además, permite casi la eliminación al completo de cualquier trámite administrativo, reduciendo ello las equivocaciones, el tiempo de verificación y las falsificaciones.

6.2.2. Operativas mejoradas gracias al Blockchain

A partir de la mejoría de algunos puntos de la cadena de suministros, algunas operativas más generales de la cadena están sufriendo un cambio con gran impacto sobre el modelo general del sector logístico. Algunos de esos cambios se muestra a continuación (Minsait, 2017):

Comercio internacional

En el ámbito del comercio internacional blockchain supone un gran avance. Para un desarrollo óptimo del comercio internacional se requieren grandes operaciones logísticas transnacionales en las que intervienen empresas de todo tipo y de cualquier parte. Además de un buen flujo de información y dinero para cubrir correctamente el gran volumen de movimiento de mercancías existente.
En busca de esta solución, se empezó diseñando una arquitectura de servidor central, se evolucionó a soluciones en la nube y, hasta hoy, cuando blockchain parece ser una gran solución con su aporte de descentralización, confianza y colaboración para potenciar la eficiencia en las operaciones.

Una **buena gestión** del comercio internacional sustentado en el blockchain **conectaría** a las **diferentes partes** que actúan en él: importadores, exportadores, bancos, compañías de seguros, operadores logísticos, auditorías, abogados, etc. Esto ayudaría a agilizar los procesos mediante el uso de Smart Contracts en la gestión de operaciones, implicando ello una operativa más rápida, una reducción de costes, una mayor transparencia, una auditoría mejorada (cuanto más acceso tenga una auditoría a la información financiera correcta, más fácil y de mejor calidad será el resultado) y una disminución de litigios.

Procesamiento de papeleo en el transporte

El transporte internacional conlleva siempre un gran volumen de papeleo asociado. Por ejemplo, el envío de medicamentos de África Occidental a Europa requiere sellos y aprobaciones de alrededor 30 personas y entidades que deben intervenir entre sí hasta en más de 200 ocasiones. Además, muchos de los documentos que se intercambian son objeto de fraude. Se puede afirmar que la gestión de documentos implica un coste

muy elevado, que puede llegar hasta un 50% de los costes del transporte físico (Moller, 2018) .

Para eliminar este tipo de procesos ineficientes y digitalizar registros en papel, **IBM y Maersk** comenzaron en 2015 con un proyecto disruptivo basado en blockchain. El proyecto consistió en la creación de una gran red de blockchain privada que sirviese para conectar la gran red mundial que conforman los transportistas, los puertos y las aduanas.

Con esta nueva plataforma existiría una visión completa del estado de los contenedores casi a tiempo real. En 2018 se alcanzó a controlar uno de cada siete contenedores, lo que significa unos 10 millones de contenedores al año. Esto reduciría significativamente la gestión de papeleo, que no solo existe en este caso concreto, sino que obstaculiza cualquier tipo de flujo comercial.

Identificación de productos falsificados

La procedencia de productos de gran valor suele estar sujeta a certificados que pueden perderse o ser falsificados. Un ejemplo de falsificación mundialmente conocido son los **diamantes**. Para este caso concreto la startup Everledger estudió y definió los 40 datos que identifican a un diamante de manera unívoca. Con esta información registrada en la red blockchain, cualquier comprador de diamantes sabría exactamente qué está comprando y no tendría alguna duda de estar ante un caso de falsificación. Esta empresa planteó en el año 2018 ampliar su red al registro de información de otros productos de gran valor.

Otro sector en el que la falsificación es muy común es en la medicina. Sin embargo, en este caso no solo está en juego el aspecto económico, sino que se pone en riesgo con gran asiduidad la salud y la vida de muchas personas. Blockchain dificultaría también la falsificación sobre la procedencia, composición o estado de un medicamente. Más adelante, se verá este caso en detalle.

Identificación del origen del producto

En caso de existir un brote de una **enfermedad transmitida por los alimentos**, los minoristas presentan una gran dificultad para averiguar de dónde procede el producto intoxicado (Aitken, 2017).

Actualmente puede llevar semanas el rastreo del origen de la contaminación, tiempo suficiente para que un producto se haya extendido demasiado y haya llegado a afectar a la salud de numerosas personas, así como a su confianza.

Para facilitar el seguimiento del origen de los productos alimenticios, la empresa **Walmart** se asoció en 2016 con **IBM**. De la misma manera que hizo IBM con Maersk, encontró en blockchain la manera de rastrear los movimientos de los alimentos, registrando su información en el registro de blockchain.

Esto implicó una gran mejora al servicio que ofrecía anteriormente Walmart, soluciones basada en una base de datos central y que implicaba tener que confiar a ciegas en los diferentes participantes.

En uno de los primeros pilotos, Walmart e IBM rastrearon movimientos domésticos (transporte de carne de cerdo de pequeñas granjas chinas hasta las tiendas de venta) y movimientos internacionales (productos de América del Sur a EEUU). En estos pilotos, los datos como los inicios de la granja, el número de lote, los datos de procesamiento, las fechas de vencimiento o los detalles de envío, se registraban en blockchain y se ponían a disposición de todos los intervinientes de la red, existiendo una trazabilidad completa del producto. Esto permitía a Walmart, **rastrear el origen** del producto en **cuestión de segundo**s y no de semanas.

Otro de los proyectos desarrollados por Walmart a partir del blockchain es **reducir el desperdicio de alimentos**. Para ello utiliza los datos sobre la vida útil de un producto como parámetro para la optimización de la cadena de suministros.

Y, éstas son algunas de las operativas más importantes cuya mejora viene de la mano de blockchain.

6.2.3. Ejemplos reales de aplicación

A continuación, se van a indicar algunos ejemplos reales de iniciativas que se han desarrollados en diferentes áreas del sector logístico:

- Comercio internacional
- Transporte terrestre de mercancías
- Trazabilidad del producto
- Reparto de “última milla”

Comercio internacional

El comercio internacional, y más aún las operativas portuarios, representan un escenario perfecto para la aplicación de blockchain como se ha visto anteriormente, debido a sus operativas complejas y a su gran flujo de información.

- **Maersk**, es el ejemplo más claro, ya comentado.

- **SmartLog**, un proyecto que se está desarrollando en la ciudad finlandesa de Kouvola. La iniciativa se centra en la transferencia de datos operacionales entre las empresas del sector logístico, así como en una mejora del flujo de información. Las mejoras, consecuencia del proyecto, se midieron calculando los tiempos que tardaban en transportar la mercancía de un punto de la ciudad báltica a otro.
- **T-Mining**, empresa belga con una plataforma de Smart Contracts para ayudar a incrementar la seguridad del transporte de los contenedores en el comercio marítimo.
- **Blocklab**, una iniciativa de los Países Bajos con base en el puerto de Rotterdam respaldada por Blockchain, IoT y Big Data. El objetivo es conceder crédito añadido a los expedidores (persona encargada de organizar y ejecutar el transporte de mercancías en nombre de otros) en base al inventario que almacenen en un proveedor de servicios logísticos.

Algunas de las mejoras más significativas de la puesta en marcha de estos proyectos en el ámbito del comercio internacional han sido:

- Automatización de los procesos a partir de Smart Contracts
- Reducción de las gestiones administrativas y de aduana
- Reducción de fraudes
- Disminución los tiempos de transporte

Transporte de mercancías terrestre

En el transporte terrestre de mercancías se persigue una mayor colaboración entre los diferentes actores, así como una mayor transparencia y mejor flujo de información. Algunos ejemplos de empresas que han trabajado con este enfoque son las siguientes:

- **A2B Direct** [1], es una empresa del norte de Europa en la que transportistas pueden recibir pedidos directamente de clientes finales. Respecto a estos transportistas, la empresa gestiona información sobre la identidad de ellos y crea rankings sobre datos registrados en blockchain y encuestas de calidad de los clientes.
- **PassLfix** [2], una empresa que presenta la posibilidad de transportar mercancías de forma descentralizada y segura gracias a blockchain y a IoT. Además, también se apoyan en los Smart Contracts para una mejorar la gestión de acuerdo financieros.

[1] URL: https://www.a2b.direct
[2] URL: https://pacifics.org/

- **Hagglin** [3], una empresa con un enfoque descentralizado, de procesos P2P y sin intermediarios.

En el caso del transporte terrestre de mercancía, las mejoras más notables son las siguientes:

- La eliminación de intermediación de entidades centrales en busca de transparencia, seguridad y confianza.
- La desaparición de situaciones de fraude o de 'no cobro', gracias a la desintermediación y a la inexistencia de desigualdades generadas por el puesto profesional. Los Smart Contracts jugarán un papel importante en este sentido.
- La creación de criptodivisas de uso único en el sector que automaticen pagos para reducir así costes financieros, sobretodo en el comercio internacional.

Trazabilidad

El origen, el estado o las condiciones de transporte son algunos de los aspectos que más quiere conocer el consumidor de un producto, sobretodo en el ámbito de la alimentación, los productos de valor o de los medicamentos. Algunas empresas, que ya están utilizando blockchain con este objetivo son:

- **Provenance** [4]**,** está desarrollando un sistema de trazabilidad para productos y materiales a partir de blockchain. Ya se han realizado varias pruebas en algunos países como Estados Unidos, Reino Unido y Japón.
- **Ripe.io** [5]**,** busca crear una especia de mercado de alimentos frescos a partir de blockchain ofreciendo una información completa y transparente de los mismos, así como análisis en base a su estado, su procedencia o su temperatura.
- **Smart AgriFoo** [6], una empresa italiana que se encarga de recoger todos los pasos por los que pasa un producto agrícola a partir de la información que se lee de un código QR y se almacena en blockchain.

En la línea de la trazabilidad de productos y tras haber estudiado algunas aplicaciones o pruebas piloto las mejoras más significativas gracias a blockchian son:

- La **intervención** de todos los agentes de la cadena en las diferentes partes de ésta, bien para aportar o consultar información de algún producto, siempre inalterable.
- Ayuda a las **marcas** a resaltar su nombre en caso de poseer un buen producto

[3] URL: URL: https://hagglin.com
[4] URL: https://www.provenance.org
[5] URL: http://ripe.io
[6] URL: http://www.smartagrifood.it

- Nuevas maneras más eficientes de **auditoría**
- La generación de una **huella digital** de un producto añadiendo toda la información que queramos del mismo:
    - Identificación, lugar y momento en el que se recogió, camino que siguió hasta el cliente final
    - Información de calidad y certificados
    - Información de seguridad
    - Condiciones de transporte y conversación
    - Estado de conservación

Reparto de "última milla"

Además de los tres enfoques del sector logísticos en los que está habiendo importantes aplicaciones basadas en blockchain, también hay otra línea en la que se está desarrollando bastante, la "última milla". Algunos ejemplos reales son los siguientes:

- **Walmart**, ya comentada.
- **FreshTurf** [7]**,** está desarrollando en Singapur una manera para mejorar la entrega de paquete en taquillas/lockers.
- **Servicios Postales** de varios países están investigando cómo prestar servicios sobre la verificación de identidad, tracking de pedidos o giros postales.
- **Volt**, ofreció un cambio a las compañías DHL, USPS y UPS. Lo que ofrece VOLT es un modelo que ya funciona en el Sur de Corea en donde los pedidos están siendo entregados en un plazo de 1-3 horas, lo que correspondería a 1-3 días para algunas de las empresas anteriores. El nombre de este modelo se llama "**Quick Quick**" (WOLT, s.f.).

  El motivo por el que pueden ofrecer esta gran mejora de este servicio es sencillamente por una mejora del modelo. Los mensajeros locales recogen el paquete en un **sistema P2P**. Hoy en día se enviaría el paquete a un centro logístico de otra región del país para registrar el paquete y luego se enviaría a la dirección del consumidor final, que podría estar en la ciudad origen de la que partió el paquete. Esto muestra una clara ineficiencia en el sistema de entrega actual.

  VOLT evita mediante el sistema P2P este desplazamiento innecesario de un punto a otro del paquete, ahorrando tiempo de envío y costes.

[7] URL: http://freshturf.io

Además, VOLT hace uso de Big Data y Smart Contract para calcular el precio correcto de la entrega, que va variando en función de diferentes parámetros, resultando el cliente final siempre beneficiado.

En esta línea se puede percibir los siguientes cambios importantes:

- Blockchain como opción para intervenir entre los vendedores, operadores logísticos y clientes finales.
- La generación de muchos espacios para que los transportistas depositen los envíos de los consumidores finales con las correspondientes consecuencias:
    - Los proveedores de taquillas cobrarán mayor importancia y tendrán mejores condiciones.
    - Los clientes finales tendrán más flexibilidad en cuanto a la recepción de pedidos
    - Los proveedores logísticos simplificarán sus procesos de la “última milla”.

Y estos son algunos de los muchos ejemplos y consecuencias que la tecnología blockchain está teniendo ya en este sector. Si la evolución sigue está línea, poco a poco irá cambiando el modelo de negocio.

6.3. Aplicación de tecnologías disruptivas

Además de la tecnología blockchain, hay otras tecnologías muy innovadoras que complementado al blockchain pueden ayudar bastante a una mejora de la cadena de suministros. Big Data, Data Analytics o Internet of Things son algunas de ellas. En este caso se va a hablar de Internet of Things y el uso de drones.

6.3.1. Internet of Things

Como se comentó anteriormente, Internet de las Cosas, IoT, implica que, un elemento conectado a la electricidad y equipado con tecnología electrónica, permita un intercambio de información del propio elemento a través de Internet y en todo momento.

Esta tecnología combinada con blockchain, permitiría almacenar casi a tiempo real toda la información de numerosos objetos IoT (medios de transportes, electrodomésticos, envío, etc.), pudiéndose **tomar decisiones** de **inmediato** en base a la información registrada en la red y a posibles cambios.

6.3.1.1. Puntos de mejora gracias a IoT

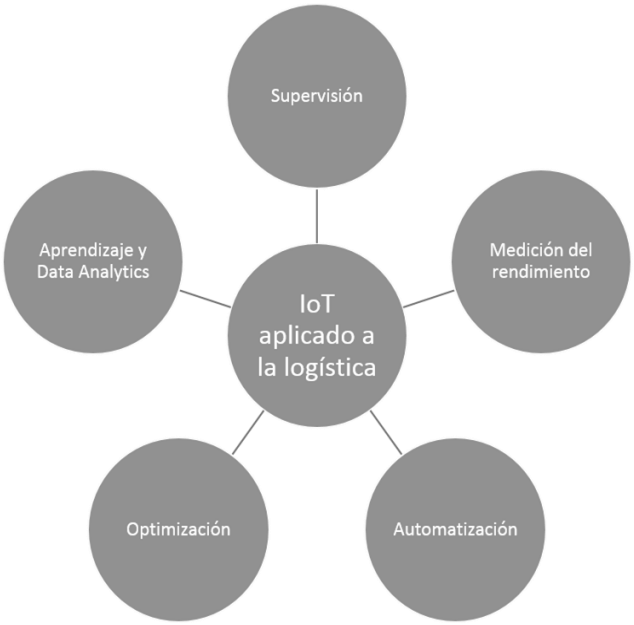
El registro de información tan completa que se alcanza gracias a IoT ofrece un gran abanico de posibilidades para la cadena de suministros. Teniendo en cuenta los puntos

flojos de la cadena de suministros, expuestos anteriormente, se va a nombrar alguna de las principales causas positivas de la aplicación de IoT junto a blockchain.

- **Control:** la aplicación de IoT con sistemas como RFID favorece al control de estado de un activo, así como a una mayor transparencia. Una aplicabilidad se podría encontrar en el transporte de mercancías en puertos o en la dificultad para la expansión del terrorismo a base del transporte de armas en contenedores.
- **Comunicación:** en el caso de la última milla actores como gestores de flotas, conductores, minoristas y clientes, les gustaría ser informados de una manera más rápida ante determinadas situaciones. IoT ayudaría a ello aumentando la eficiencia del plan de acción de hoy en día y aumentando considerablemente la rapidez antes eventos no previstos.
- **Reducción de costes**: la tecnología IoT puede ayudar a ello y abrir nuevas oportunidades para generar otros ingresos. Por ejemplo, los mensajeros pueden utilizar IoT con los vehículos, con el seguimiento de paquetes o con la monitorización del almacén. La disposición de toda la información relacionada, actualizada y en tiempo real puede ayudar a detectar recursos no utilizados por las empresas, así como oportunidades para mejorar el proceso.

Estos tres aspectos principales se traducen en la mejora de varias operativas importantes como (James Macaulay, 2015):

- Supervisar el estado de los activos, paquetes y personas en tiempo real a lo largo de toda la cadena de valor.
- Medir el rendimiento de los activos y cambiar lo que están haciendo en el momento y lo que harán a continuación.
- Automatizar los procesos de negocios para eliminar las intervenciones humanas, mejorar la calidad y la previsibilidad y reducir los costos.
- Optimizar cómo las personas, los sistemas y los activos trabajan juntos y coordinar sus actividades.
- Hacer uso de analíticas en toda la cadena logística para identificar oportunidades y mejores prácticas.



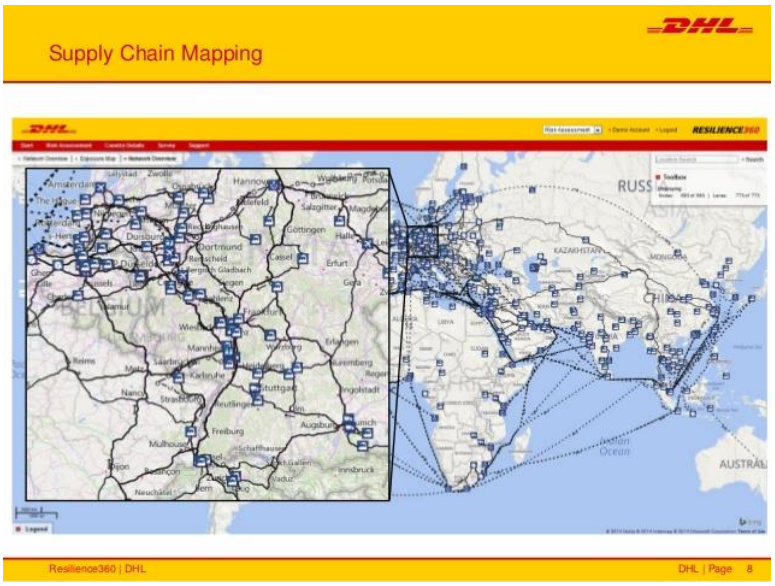
6.3.1.2. Ejemplos de aplicación de IoT

Una vez presentada esta tecnología y algunos de sus puntos flojos de la cadena de suministros sobre los que, de manera conjunta a blockchain, puede interceder para su mejor, se va a mostrar alguna ejemplos reales y pilotos de apliación.

DHL. Plataforma Resilience 360 para la gestión de riesgo de la cadena de suministros.

Un desafío actual de la cadena de suministros es su vulnerabilidad y riesgo consecuente. El área que se encarga de este aspecto es SCRM, por sus siglas en inglés de *Supply Chain Risk Management.* Esta área se encarga de identificar, evaluar, analizar y tratar todos los puntos vulnerables o que suponen un riesgo para el cumplimiento del objetivo de la cadena de suministros.

En esta línea, DHL desarrolló con la tecnología IoT una plataforma llamada “Resilience 360” (Nietzsche, 2015) para gestionar el riesgo de toda la cadena de suministros. Esta nueva plataforma ofrecía una visualización integral de toda la cadena, incluida la última milla.



Esta plataforma con una visualización 360 de la cadena se encarga de actuar, según la estrategia definida, de manera automática ante cualquier tipo de cambio. Cuanta más información se obtenga, más control se tendrá sobre los activos de la empresa, más rápido se podrá detectar un fallo o posibles mejoras y, por lo tanto, actuar en consecuencia. Algunos ejemplos:

- Un camión que transporta una carga urgente y se avería o un invernadero que se inunda tras una tormenta.
- Una huelga aérea que impide transportar un envío aéreo y se pasa a un transporte terrestre.
- Ajustar una ruta por ciudad en función del tráfico o de posibles cierres de calles por accidentes.

Todas estas acciones pueden ser únicamente solventadas con información fiable y a tiempo real. Manejar de manera interrelacionada toda la información sobre huelgas portuarias, cierres de aeropuertos o autovías cortadas lo permite IoT. Esta capacidad analítica no solo permitirá aumentar el índice y velocidad de respuesta, sino también predecir otros sucesos.

Dirección de envío flexible

Uno de los puntos más críticos de la cadena de suministros y, en concreto, de la última milla es la recepción del pedido por el consumidor. La solución a la que se tiende actualmente es a concentrar todos los envíos en unos puntos de recogida, como taquillas o tiendas, y así reducir el número de viajes y la distancia recorrida.

Sin embargo, hay muchos consumidores que quieren recibir su pedido directamente y no recurrir a estos puntos de recogida. Y, ya se sabe, que uno de los requisitos

principales en la última milla son los requerimientos del consumidor final. Además, que muchos experimentos han conducido a la necesidad de ofrecer esta flexibilidad en cuanto a la entrega.

Si los diferentes agentes y activos (paquete, lugar de recepción…) están interconectados, en caso de ser el lugar de recepción elegido por el consumidor, un posible cambio de última hora en la dirección ayudaría.

En caso de que un envío esté planificado para recibirlo en un domicilio y, por cualquier motivo, el receptor no puede estar en el momento acordado allí, un cambio de dirección al vecino o al lugar en el que vaya a estar posibilitaría la entrega. Incluso supondría, en ciertos aspectos, una reducción de costes. El mensajero final no tendría que ir una segunda vez a realizar la entrega.

Respecto al análisis de datos que se consigue con IoT, éste permite predecir sucesos. En caso de que el historial de un consumidor a la hora de recibir paquetes sea negativo, es decir, que nunca esté donde se hubiese acordado; el mensajero podría pedir, gracias a la interconexión, confirmación del lugar y la hora antes de realizar la entrega.

Plataforma AOS

Respecto a la última milla y el IoT, también se puede hablar una posible solución logística. Se trata de la **plataforma usada por AOS** que traslada los datos de los dispositivos al formato blockchain. La plataforma se encarga de filtrar determinados sucesos e información de los dispositivos y enviar únicamente la información requerida para los Smart Contracts.

Actualmente la mayoría de transacciones se llevan a cabo **manualmente** en la cadena de suministros y eso genera grandes retrasos y un riesgo alto en cuanto a la información registrada. Una diferencia entre lo que fue registrado y lo que fue cargado no se puede permitir. Mediante la digitalización del proceso con blockchain e IoT la información más relevante es detectada directamente por los sensores situados en los camiones y registrada al completo en blockchain, dando lugar así a un único y compartido repositorio al que todos los participantes autorizados pueden acceder, y cuyo contenido solo puede ser alterado si existe consenso entre una mayoría de todas las partes.

Las principales **ventajas** que ofrece la solución de **AOS**, proporcionarán:

- Empresas con **una gran tasa de producción gracias** a la capacidad que tendrán de priorizar unos proyectos antes otros por poder conocer exactamente **cuándo** llegarán **qué recursos**. Así se evitará tiempo de espera ineficientes.

- Disponer de información acerca de la procedencia de productos y de los problemas de seguridad relacionados con ellos.
- Evitar el error humano. Aunque la información IoT ya se estuviese registrando en blockchain, los **reportes** y ese filtrado se seguían haciendo manualmente. Con AOS todo está **automatizado** y se evitan posibles cambios en la información por error.
- Geolocalizar a los vehículos.
- **Medir a tiempo real** lo relacionado con el estado de la carga o mantenimiento de la carga.
- Ejecución de **Smart Contracts** cuando sean necesarios con alertas programables, si así se requiriese.

Los usuarios de este tipo de solución pueden ser todos los actores de la cadena de suministros. Esto no significa que haya que implantar IoT con blockchain en cualquier punto de la cadena de suministros. Habría que realizar un **estudio previo** de qué clientes se beneficiarían más de este servicio, qué empresas de transporte son las que querrían brindar esta seguridad a los usuarios finales o qué empresas de producción querrían tener información sobre la procedencia de sus productos.

Sector farmacéutico

Una vez hablado de los principales impactos que va a tener el blockchain y la tecnología IoT sobre el sector logístico y la cadena de suministros, y haber visto algunos casos de aplicación real, se va ver en detalle cómo cambiaría la **cadena de suministros en la industria farmacéutico** con la llegada de ambas tecnologías. El cambio en este sector es un reflejo del cambio revolucionario que esta tecnología va a jugar.

Según World Health Organization se venden anualmente en torno a 200.000 M $ de medicamentos falsificados, siendo el 50% de estas ventas online. Por norma general el punto de la cadena de suministros donde existe mayor falsificación es en el origen, en la producción. En ese punto se aprovecha para meter entre las unidades legítimas productos falsificados. Se sabe que Blockchain puede ser una buena solución a este gran problema.

En la cadena de suministros de productos farmacéuticos lo más importante es disponer de una buena **trazabilidad** de las unidades de medicamentos en cualquier punto del recorrido del camino. Además, de que cualquier interviniente de la cadena con autorización pueda acceder en todo momento a consultar el estado de algún producto en tiempo real.

¿Cómo **funcionaría** exactamente el recorrido del medicamento de manera que se detectase cualquier falsificación o alteración?

La funcionalidad de **Smart Contract** de Blockchain junto con el uso de dispositivos **IoT** ofrecería una capacidad de seguimiento del medicamento eficaz y continua para los interesados. Se podría acceder a la totalidad de la **información** del **medicamento** (procedencia, condiciones, derechos de autoridad, aprobaciones en puntos de control, etc.), mejorando así también la auditoría de cada elemento en la cadena.

En el caso de que algún **medicamento** sufriese alguna **alteración** como un aumento de la temperatura del entorno, el dispositivo IoT lo detectaría, enviaría los datos a blockchain, el Smart Contract detectaría este dato que aplica a las condiciones del contrato y ejecutaría la consecuencia correspondiente de que se cumpla esa condición determinada. De esta manera los **afectados** de la alteración del medicamento serían **notificados** y conocerían el estado real del medicamento, con cuya consecuencia deberían estar de acuerdo. El Smart Contract previamente habría sido codificado para desencadenar una acción determinada en respuesta a las nuevas condiciones del producto.

De esta manera se automatizaría la respuesta en función a determinados sucesos. Por ejemplo, si unas ciertas condiciones de un medicamento previamente definidas no se cumplen, el medicamento podría ser retirado antes de que llegase al mercado. Definiendo especialmente las condiciones que implicarían una retirada de un medicamento a tiempo, evitaría muchas ventas de productos peligros y en mal estado. Se alcanzaría así una protección necesaria sobre ciudadano.

Además, consiguiendo un seguimiento adecuado y de calidad a lo largo de todo el ciclo de vida del medicamento, se **eliminarían** algunos **intermediarios**; no habría necesidad de certificaciones.

La red blockchain almacenaría la información requerida y haría cumplir las regulaciones estipulados a lo largo de toda la cadena de suministros. En este sentido, blockchain podría actuar como una fuente fiable y certificada de información acerca del historial de un medicamente, tal y como actúan hoy en día muchas organizaciones.

Podría haber **una sola plataforma** con toda la información que cualquier interviniente de la cadena de suministros pudiese necesitar. Supondría muchos beneficios para el paciente, para la regulación y para la reducción de costes.

6.3.1.3. Limitaciones de IoT

La mejora en la cadena de suministros gracias a IoT parece inevitable. Sin embargo, existen también algunas limitaciones, sobretodo técnicas, que hay que intentar paliar y, así, alcanzar esa optimización de la cadena. Algunos de esos aspectos técnicos son:

- **Mejoras en los elementos de infraestructura básica**: el coste de fabricación de los componentes principales debe continuar disminuyendo para que las aplicaciones de IoT sean rentables. Hoy en día, muchas aplicaciones son técnicamente factibles, pero el alto coste de los componentes hace que la implementación no sea viable. No obstante, existe actualmente una tendencia positiva en cuanto a la disminución del precio de componentes imprescindibles para esta tecnología.

- **Mejoras del software y de la analítica de datos**
  El valor real de las aplicaciones de IoT viene de analizar grandes cantidades de datos y tomar decisiones en base a ellos. Pero hoy en día, el software de análisis no está lo suficientemente desarrollado como para dar una solución para cada uno de las diferentes casuísticas, por lo que muchos datos se quedan sin ser explotados.
  La definición exacta de los diferentes algoritmos para cada uno de los casos posibles aún no se ha realizado y las habilidades y capacidades para realizar este trabajo siguen siendo escasas. Esto podría suponer una gran barrera para la adopción total de la tecnología IoT, especialmente en el contexto de la última milla, donde las aplicaciones tienes que ser muy precisas.

- **Soluciones tecnológicas para la interoperabilidad**
  Como se mencionó anteriormente, se necesita una gran cantidad de datos para que IoT ofrezca resultados de calidad, es decir, se necesita interoperabilidad entre diferentes dispositivos y productos.
  Las principales barreras para la interoperabilidad incluyen la falta de interfaces de software comunes. Una creación de estándares de tecnología comunes ayudaría a este problema.

Estos son tres de los problemas principales para la adopción íntegra de la tecnología IoT. La solución requiere la colaboración conjunta de partes muy diferentes. No es fácil, pero el potencial de esta tecnología es enorme. ¡No se puede desperdiciar!

6.3.2. Drones

El **tiempo de vuelo** de un dron depende de su peso y el peso depende de la carga y de la energía almacenada en su batería. Bajo estos factores determinantes en el uso de drones como mecanismos de entrega se han hecho varios estudios para ver el alcance que pueden tener. En el caso 'Primer Air' (Amazon), se ha llegado a desarrollar un helicóptero capaz de transportar una **carga de 2.3 kg durante 16 km** y volver vacío (James Vincent, 2015).

Esta **limitación** puede parecer importante de peso transportado y espacio recorrido, incluso aunque 4 de cada 5 pedidos de Amazon pesen menos de 2.3 kg. Para poder sustituir los métodos convencionales de entrega por los drones no es aceptable este porcentaje. Se necesita aún que se siga evolucionando en esta área, cuyo potencial no es pequeño. Especialmente en la última milla.

6.3.2.1. Puntos de mejora gracias a los drones

Una ventaja que presentan los drones frente a los métodos tradicionales es el **acceso** a **zonas** geográficamente **mal ubicadas**. Para los drones el acceso es el mismo sea cual sea la ubicación, siempre que la regulación aérea lo permita.

Además, los drones no están limitados por la infraestructura de carretera y la congestión producida por el tráfico, pueden entregar paquetes **más rápidos** que los coches o los camiones, siempre que la localización de almacenaje sea cercana. Además, pueden atravesar sin problema **terrenos complicados** y seguir una ruta mucho más directa, casi en línea recta. De la misma manera, pueden también volar sobre **agua**.

Para la entrega de envíos de medicamentos u otras **necesidades de urgencia**, también presentan una gran ventaja. Aunque esta entrega implique un mayor coste, en ocasiones la rapidez de entrega es mucho más importante que el coste de la misma.

Los drones, como medio de transporte en la última milla, y combinados con IoT y blockchain mejorarían aún más el funcionamiento y resultado de la cadena de suministros. Cada dron podría llevar, aparte del producto, un sensor que mediante IoT permitiese poder conocer en cualquier momento el estado de un pedido. Además, de las ventajas ya vistas de los drones frente a los medios de entrega actuales.

6.3.2.2. Limitaciones en el uso de drones

Como cualquier implementación de nueva, la incorporación de drones requiere un tiempo y una adaptación. Hasta que llegue ese momento de incorporación plena de los

drones a la cadena de suministros, existen algunas limitaciones que hay que conseguir erradicar.

- **Disponibilidad de producto vs. Coste de Inventario**: una de las premisas en la logística es ofrecer siempre disponibilidad del producto, aun con el gran coste de inventario que ello implica. Las empresas siempre desarrollan sus estrategias buscando un balance entre ambas incógnitas y viendo qué es lo óptimo para un mayor beneficio. Una manera bastante consolidada de llegar a establecer un buen equilibrio es mediante la centralización de puntos de distribución. Se ha estudiado que una empresa reduce, por norma general, sus costes centralizando la demanda y el inventario. Sin embargo, esta **centralización** no es beneficiosa para los drones, cuya capacidad para hacer entregas a larga distancia está aún muy acotada.
- **Capacidad de carga de los drones vs**. **Camiones**: los drones solo pueden llevar un paquete por desplazamiento, mientras que los camiones pueden aprovechar el camino para llevar varios paquetes a la vez. Además, si se consideran los costes adicionales de inventario para los drones, así como los costes de mantenimiento y propiedad, es probable que el envío por dron sea considerado una opción cara. Estas altas tarifas podrían traducirse a que el envío con dron se limite a un sector de la población rica.
- **Instalaciones de recepción para los drones**: la gran mayoría de anuncios que se ven actualmente sobre los drones, muestran un video sobre cómo un dron aterriza en el jardín de una casa (caso de Amazon con *Prime Air)*, el receptor recoge el paquete y el dron se va. Pero esto no es tan sencillo, se requiere una instalación determinada para poder recepcionar un paquete mediante un dron. Y esta instalación requiere una inversión y no todo el mundo estaría dispuesto a pagar una plataforma de aterrizaje para un dron para poder recibir pedidos.
- **Seguridad:** hay que tener en cuenta la seguridad sobre el propio dron, sobre la empresa propietaria y sobre los ciudadanos. Riesgos que pueden sufrir los drones:
    - Colisión de drones por mal tiempo
    - Intercepción de drones y robo de la mercancía
    - Vandalismo y uso de drones como objetivos para disparar
    - Mal funcionamiento de los drones que acaben encolisiones con ciudadanos
    - Hackeo del sistema de control de los drones

Como se puede ver, existe todavía una gran área de investigación y mejora. Pero no se debe dejar atrás por su dificultad. Las consecuencias positivas pueden ser también muchas.

6.4. Ventajas y desventajas generales del blockchain

Analizados todos los casos vistos de blockchain, con ayuda de tecnologías como IoT o drones, en la cadena de suministro, se han recopilado las **ventajas más relevantes** de la implantación e incorporación de esta tecnología al sector:

- **Limitación de intermediarios**: uso de las capacidades de confianza distribuidas de blockchain para formar una red auto gestionada. Con condiciones fijadas que desencadenas unas acciones, sin necesidad de intermediarios, gracias a los Smart Contracts.
- **Identidad digital**: comprobación inmediata y garantía de la documentación legal presentada de manera unívoca y segura.
- **Mejora de la confianza entre actores**: gracias al registro inalterable de información en la red de blockchain.
- **Historial de proveedores**: se dispondrá de un historial fidedigno de cada proveedor, que favorecerá a aquellos proveedores que hayan proporcionado un servicio de calidad y correspondiente a lo ofrecido.
- **Mejora de la transparencia**: conocimiento a tiempo real de la información de la cadena, registrada de manera inalterable en la red.
- **Mejora de la trazabilidad**: gracias al uso de IoT de manera conjunto con blockchain, que ofrece conocer a tiempo real conocer cualquier información acerca de todo producto, sea cual sea el punto de la cadena en el que se encuentre.
- **Mejora de procesos**: los Smart Contracts eficientan mucho los procesos, sustituyendo la intervención humana, el papel y las supervisiones, siempre sujeto a error, por automatizaciones. Ello ayuda a reducción de tiempo, traducido en mejora para los diferentes actores de la cadena y la consecuente reducción de costes. Se consigue:
    - Una optimización en el intercambio de información y documentación
    - Un nuevo sistema de financiación
    - Una automatización de los procesos entre compañías

Todas estas mejoras, sin olvidar algunas de las limitaciones más importantes de blokchain:

- Es una tecnología incipiente

- No se sabe si se van a poder satisfacer los requerimientos de almacenamiento en la red
- No se conoce la evolución que va a tener la potencia computacional y los tiempos de procesamiento
- La existencia de múltiples redes/plataformas que no se complementen y que sean incompatibles, pueden dar lugar a un aumento de costes.

En manos de la sociedad estará evolucionar. Lo que se puede vislumbrar parece alentador, pero requiere esfuerzo, ilusión y colaboración conjunta entre muchos.

7. Encuestas

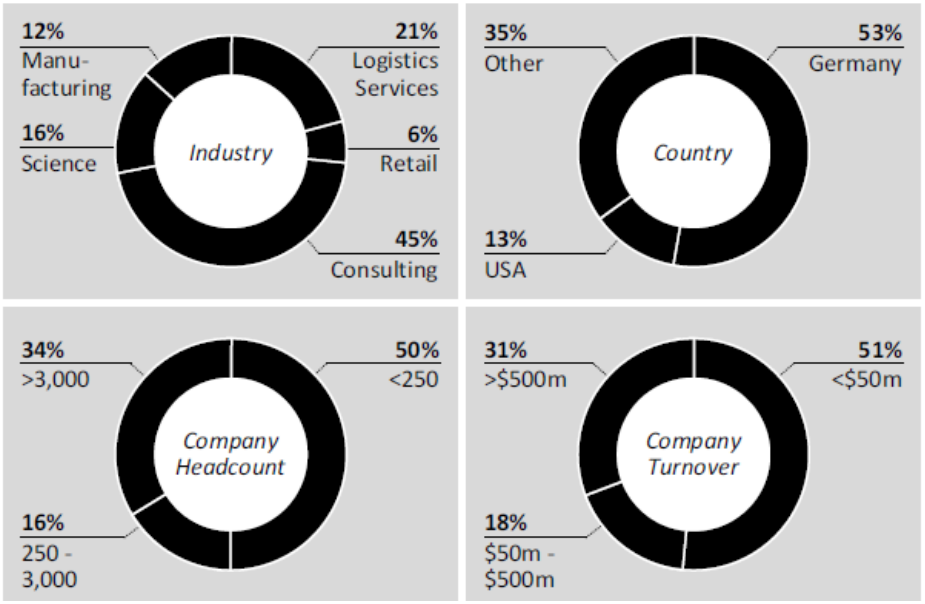
En el 2017 se realizó una **encuesta** para *Hamburg International Conference of Logistic*, HICL**,** acerca de la aplicación de blockchain en el sector logístivo y, más en concreto, en la cadena de suministros**.** Se desarrolló utilizando Typeform, un software que se especializa en la creación de formularios y encuestas en línea (Hackius, 2017).

Para ello, primero se les proporcionó a los encuestados un **conocimiento** sobre logística, sobre la cadena de suministros y sobre Blockchain, para que las encuestas estuviesen fundamentadas. A continuación, se les facilitó **cuatro casos de uso** para que comentasen los beneficios de implantar en esos casos de uso el blockchain. En tercer lugar, se les preguntó de manera general sobre el **impacto** (positivo, negativo, barreras, limitaciones, etc.) que pensaban que tendría el blockchain. Y, por último, se les preguntó **detalles** sobre sus empresas y sus propios trabajos.

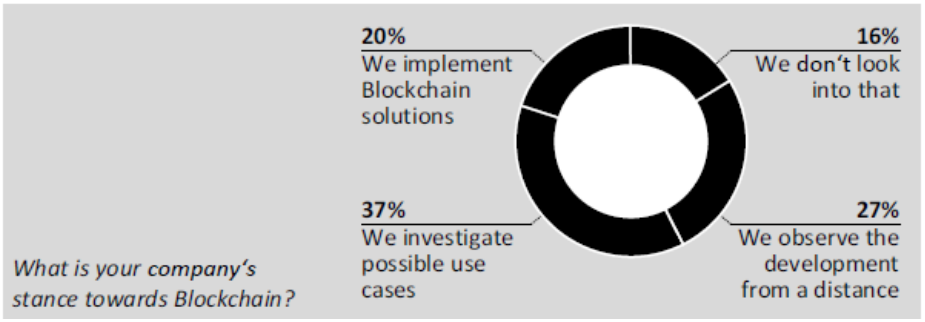
Los datos se recogieron durante dos meses. Los participantes fueron seleccionados no arbitrariamente. Se eligieron **personas** de clase social media y que habían mostrado en las redes sociales profesionales algún **interés** acerca de la **logística o el blockchain**.

Participaron **152 personas**: la gran mayoría **trabaja en consultoría**, seguido por los que trabajaban en servicios logísticos. Más de la mitad eran de Alemania, seguidos por los de EEUU, Suiza y Francia. De los trabajadores de consultoría, la gran mayoría trabajaban en pequeñas-medianas empresas con menos de 250 trabajadores y una facturación por debajo de los 50 millones de USD. En cuanto a los **trabajadores del sector logístico**, acerca del 60% trabajaban en empresas de más de 3.000 empleados y con una facturación superior a los 500 millones de USD.

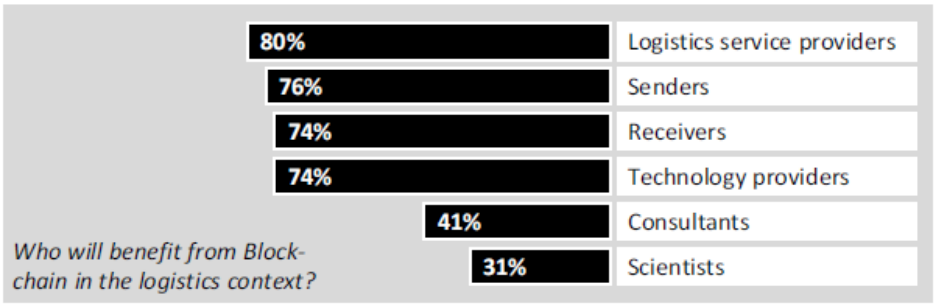
Los resultados que se obtuvieron se muestran a continuación:



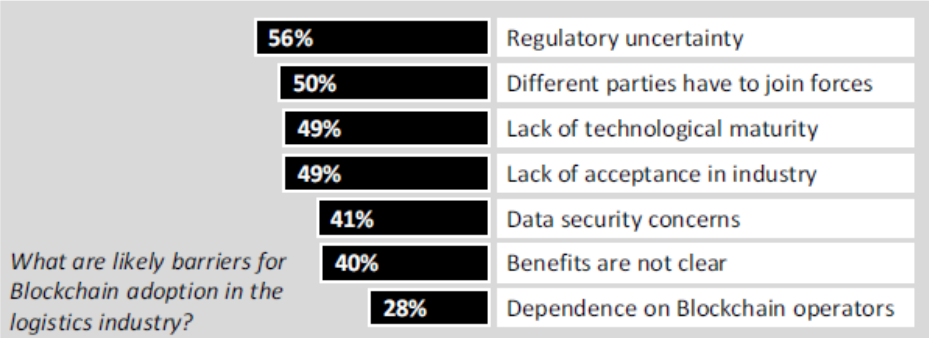
Información sobre de los participantes y sus compañías



Postura de las compañías hacia el blockchain



Beneficiarios en el sector logístico de la adopción del blockchain



Limitaciones en la adopción de blockchain

Como conclusión a esta encuesta realizada a una muestra tan diversa, se puede observar unas respuestas que definen un patrón de comportamiento habitual ante esta situación. Por norma general, la postura ante esta tecnología nueva es conservadora.

Apuestan por esperar a ver la respuesta en otros para empezar a aplicar ellos mismos. Aunque parece que sí confían en que puede beneficiar a diferentes actores del sector logístico.

8. Cómo promover el desarrollo de blockchain

Como se ha comentado a lo largo del trabajo en varias ocasiones, estamos ante una posible gran revolución: la tecnología blockchain. Pero para su desarrollo se necesita que las empresas confíen en ella y la incorporen a sus modelos de negocio, favoreciendo así a su crecimiento y consolidación.

Para ayudar a que esto suceda se podrían dar los siguientes pasos, que impulsasen a las empresas a actuar:

1. **Socialización interna**
   Presentar el posible motivo de discusión de ver el interés que puede despertar está tecnología en un negocio viendo la aplicabilidad potencial.
2. **Educación**
   Una vez que se ha aceptado el uso potencial de blockchain, invertir en adquirir un conocimiento práctico sobre la tecnología: qué es, beneficios asociados, variantes de la tecnología, etc.
3. **Idea**
   Trabajar con un equipo experto para evaluar la posible relación de blockchain con el negocio, incluso definir una estrategia de aplicación de blockchain.
4. **Diseño de caso de uso**
   De todos los casos de uso posibles en los que aplicar blockchain en la empresa, priorizarlos. Tener en cuenta que, para empezar, es mejor elegir un caso de uso sencillo que ayude al impulso inicial y así llegar a confiar en esta nueva tecnología.
5. **Implementación**
6. **Avanzar** lo más rápido posible en el desarrollo del **caso de uso** priorizado. Darle un enfoque cada vez más comercial y que ayude a continuar con otros casos de usos, previamente ya analizados.

9. Conclusión

El **sector logístico** es uno de los sectores que más interés ha mostrado por la tecnología blockchain. En conferencias y reuniones del sector ya es inevitable abordar este tema y empezar a pensar en cómo integrar esta tecnología en las diferentes áreas para optimizar el funcionamiento del sistema en general.

Puede parecer que la implementación de blockchain empieza por un cambio tecnológico profundo, pero el cambio realmente comienza por un **cambio** en la forma de desarrollarse las **relaciones comerciales**.

Es evidente que este cambio será solo posible si se desarrolla esta tecnología, pero hay que ser consciente de que lo que hay que cambiar realmente es **el sistema de negocio**. Afortunadamente, este cambio viene en un momento en el que la economía colaborativa y las plataformas de desintermediación están al alza.

Este nuevo modelo de negocio con **enfoque colaborativo-competitivo** exige un cambio en el plan de acción y en las dinámicas existentes, marcadas por un cambio en la estrategia. Ésta deberá definirse sin olvidar uno de los principios de blockchain: **la transparencia**.

También hay que entender que este cambio tiene que realizarse de manera conjunta y no individualizada, de la misma manera que está evolucionando el mundo. Además de que tiene que ser **end-to-end**, es decir, desde el análisis de la información que se tiene que compartir a lo largo de la cadena hasta la definición de los modelos más sólidos de trazabilidad y, siempre, con visión al **cliente final**.

Al encontrarse el mayor potencial de blockchain en situaciones complejas con numerosos intervinientes, conforme mayor sea ese enfoque colaborativo mejor se podrá explotar el potencial de esta tecnología. La intervención de **organizaciones del sector** en la distribución de información o impulsión de iniciativas ayudaría bastante.

En el momento en el que se está ahora mismo, parece que blockchain tiene un **camino largo** por delante y, especialmente, en el sector logístico. Si las empresas se aprovechan de esto y empezasen a desarrollar algunos casos de uso, se posicionarían favorablemente frente a la competencia e impulsarían a otras también.

Hay que llegar a entender la gran ventaja competitiva que puede suponer el blockchain. La posibilidad de integración; de escalabilidad; de cooperación entre productores, proveedores, fabricantes y repartidores; y lo que puede ayudar ello a la **reducción de tiempo, papeleo, litigios y costes**.

Respecto al **coste de implementación** de esta tecnología sería muy significativo, pues se trata de un cambio integral del modelo de negocio actual. Aun así, si la participación de las empresas aumenta y con ellos las inversiones, este coste sería asumible.

Y, por último, de la misma manera que no hay que ignorar las nuevas oportunidades, no ignorar tampoco las **limitaciones** del blockchain, uno de los principales retos de su evolución. Hay dudas importantes sobre el alcance de la red, su rendimiento, su estandarización y sobre la confidencialidad de su contenido. Pero la inversión que se está alcanzando es alta y los recursos tecnológicos actuales están preparados para afrontar estos problemas.

Así que, motivados por una **revolución del sector logístico** a mejor y sin desatender tanto los puntos de mejora, como los puntos que quedan al descubierto, hay que empezar a pensar en esa redefinición de los procesos que determinarán un nuevo y gran modelo de negocio.

10. Anexos

Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer

Satoshi Nakamoto

Resumen

Una forma de dinero en efectivo electrónico puramente peer-to-peer debería permitir enviar pagos online directamente entre las partes y sin pasar a través de una institución financiera. Las firmas digitales son parte de la solución, pero los beneficios principales desaparecen si un tercero de confianza sigue siendo imprescindible para prevenir el doble gasto. Proponemos una solución para el problema del doble gasto usando una red peer-to-peer. La red sella las transacciones en el tiempo en una cadena continua de proof-of-work2 basada en hash3, estableciendo un registro que no se puede modificar sin rehacer la proof-of-work. La cadena más larga no solo sirve de prueba efectiva de la secuencia de eventos, sino que también demuestra que procede del conjunto de CPU más potente. Mientras la mayoría de la potencia CPU esté controlada por nodos que no cooperen para atacar la propia red, se generará la cadena más larga y se aventajará a los atacantes. La red en sí misma precisa de una estructura mínima. Los mensajes se transmiten en base a "mejor esfuerzo" 4, y los nodos pueden abandonar la red y regresar a ella a voluntad, aceptando la cadena proof-of-work más larga como prueba de lo que ha sucedido durante su ausencia.

1. **Introducción**

El comercio en Internet ha llegado a depender casi exclusivamente de las instituciones financieras como terceros de confianza en el proceso de los pagos electrónicos. A pesar de que el sistema funciona suficientemente bien en la mayor parte de las transacciones, sufre la debilidad inherente al modelo basado en confianza. Las transacciones completamente irreversibles no son posibles debido a que las instituciones financieras no pueden evitar mediar en las disputas. El coste de esta mediación incrementa los costes de transacción, limitando su tamaño mínimo útil y eliminando la posibilidad de realizar pequeñas transacciones ocasionales, y hay un coste mayor al perderse la posibilidad de hacer transacciones irreversibles para servicios irreversibles. Con la posibilidad de ser reversible, la necesidad de confianza crece. Los comerciantes deben tener precaución con sus clientes, solicitándoles más datos de los que de otra forma serían necesarios. Se acepta como inevitable un cierto porcentaje de fraude. Esos costes y la incertidumbre en los pagos se pueden evitar cuando se usa dinero físico en persona, pero no existe mecanismo que permita realizar pagos a través de un canal de

comunicación sin la participación de un tercero de confianza. Es necesario, por tanto, un sistema de pago electrónico basado en prueba criptográfica en lugar de confianza, permitiendo que dos partes interesadas realicen transacciones directamente entre ellas, sin necesidad de un tercero de confianza. Si las transacciones son computacionalmente imposibles de revertir, protegerán a los vendedores del fraude, y cualquier mecanismo de depósito de garantía se puede implementar fácilmente para proteger al comprador. En este documento proponemos una solución al problema del doble gasto usando un servidor de sellado de tiempo, distribuido y peer-to-peer, para generar la prueba computacional del orden cronológico de las transacciones. El sistema es seguro mientras los nodos honestos controlen colectivamente más potencia CPU que cualquier grupo cooperante de nodos atacantes.

2. Transacciones

Definimos una moneda electrónica como una cadena de firmas digitales. Cada propietario transfiere la moneda al siguiente propietario firmando digitalmente un hash de la transacción previa y la clave pública del siguiente propietario, y añadiendo ambos al final de la moneda. El beneficiario puede verificar las firmas para verificar la cadena de propiedad. El problema, por supuesto, es que el beneficiario no puede verificar que uno de los propietarios no haya gastado dos veces la misma moneda. La solución habitual es introducir una autoridad central de confianza, o casa de la moneda, que comprueba cada transacción para que eso no se produzca. Tras cada transacción, la moneda debe regresar a la casa de la moneda para distribuir una nueva moneda, y solo las monedas emitidas directamente desde ella están libres de la sospecha de doble gasto. El problema de esta solución es que el destino de todo el sistema de dinero depende de la compañía que gestiona la casa de la moneda, por la cual pasa cada transacción, igual que un banco. Necesitamos una forma de que el beneficiario sepa que los propietarios previos no han firmado transacciones anteriores. Para nuestros propósitos, la transacción más temprana es la que cuenta, así que no nos preocupamos de los intentos de doble gasto posteriores. La única manera de confirmar la ausencia de una transacción es tener conocimiento de todas las transacciones. En el modelo de la casa de la moneda, esta tiene conocimiento de todas las transacciones y decide cuáles llegaron primero. Para lograr esto sin la participación de una parte de confianza, las transacciones han de ser anunciadas públicamente [1], y necesitamos un sistema para que los participantes estén de acuerdo en un único historial del orden en que fueron recibidas. El beneficiario necesita prueba de que en el momento de la transacción la mayor parte de los nodos estaban de acuerdo en que esa fue la primera que se recibió.

3. Servidor de sellado de tiempo

La solución que proponemos comienza con un servidor de sellado de tiempo. Un servidor de sellado de tiempo trabaja tomando el hash de un bloque de ítems para sellarlos en el tiempo y notificar públicamente su hash, como un periódico o un post Usenet [2-5]. El sellado de tiempo prueba que los datos han existido en el tiempo, obviamente, para entrar en el hash. Cada sellado de tiempo incluye el sellado de tiempo previo en su hash, formando una cadena, con cada sellado de tiempo adicional reforzando al que estaba antes. 2 Bloque Ítem Ítem ... Hash Bloque Ítem Ítem ... Hash Transacción Clave pública del propietario 1 Firma del propietario 0 Hash Transacción Clave pública del propietario 2 Firma del propietario 1 Hash Transacción Clave pública del propietario 3 Firma del propietario 2 Hash Verificar Clave privada del propietario 2 Clave privada del propietario 1 Firmar Clave privada del propietario 3 Verificar Firmar

4. Proof-of-work

Para implementar un servidor de sellado de tiempo distribuido de forma peer-to-peer, necesitaremos emplear un sistema de proof-of-work similar al Hashcash de Adam Back [6], más que al de los periódicos o los post Usenet. La proof-of-work consiste en escanear en busca de un valor que cuando fue hasheado, al igual que con SHA-256, el hash comience con un número de cero bits. El trabajo medio que hace falta es exponencial en el número de cero bits requeridos y puede verificarse ejecutando un único hash. Para nuestra red de sellado de tiempo, implementamos la proof-of-work incrementando un nonce5 en el bloque hasta que se encuentre un valor que dé al hash del bloque los cero bits requeridos. Una vez que se ha agotado el esfuerzo de CPU para satisfacer la proof-of-work, el bloque no se puede cambiar sin rehacer el trabajo. A medida que bloques posteriores se encadenen tras él, el trabajo para cambiar un bloque incluiría rehacer todos los bloques siguientes. La proof-of-work también resuelve el problema de determinar la representación en la toma de decisiones mayoritarias. Si la mayoría estuviera basada en un voto por IP, podría subvertirse por cualquiera capaz de asignar muchas IPs. La proof-of-work es esencialmente un voto por CPU. La decisión de la mayoría está representada por la cadena más larga, en la cual se ha invertido el mayor esfuerzo de proof-of-work. Si la mayoría de la potencia CPU está controlada por nodos honestos, la cadena honesta crecerá más rápido y dejará atrás cualquier cadena que compita. Para modificar un bloque pasado, un atacante tendría que rehacer la proof-of-work del bloque y de todos los bloques posteriores, y entonces alcanzar el trabajo de los nodos honestos. Demostraremos más adelante que la probabilidad de que un atacante más lento los alcance, disminuye exponencialmente a medida que se añaden bloques posteriores. Para compensar el aumento en la velocidad del hardware y el

interés variable de los nodos activos a lo largo del tiempo, la dificultad de la proof-of-work está determinada por una media móvil que apunta a un número medio de bloques por hora. Si se generan muy deprisa, la dificultad aumenta.

5.Red

Los pasos para ejecutar la red son los siguientes:

1º. Las transacciones nuevas se transmiten a todos los nodos.
2º. Cada nodo recoge todas las transacciones en un bloque.
3º. Cada nodo trabaja en resolver una proof-of-work compleja para su bloque.
4º. Cuando un nodo resuelve una proof-of-work, transmite el bloque a todos los nodos. 5) Los nodos aceptan el bloque si todas las transacciones en él son válidas y no se han gastado con anterioridad.
5º. Los nodos expresan su aceptación del bloque al trabajar en crear el siguiente bloque en la cadena, usando el hash del bloque aceptado como hash previo.

Los nodos siempre consideran correcta a la cadena más larga y se mantendrán trabajando para extenderla. Si dos nodos transmiten simultáneamente diferentes versiones del siguiente bloque, algunos nodos recibirán una antes que la otra. En ese caso, trabajarán sobre la primera que hayan recibido, pero guardarán la otra ramificación por si acaso se convierte en la más larga. El empate se romperá cuando se encuentre la siguiente proof-of-work y una ramificación se convierta en la más larga; los nodos que trabajaban en la otra ramificación cambiarán automáticamente a la más larga. 3 Bloque Hash previo Nonce Tr. Tr. ... Bloque Hash previo Nonce Tr. Tr. ... La transmisión de nuevas transacciones no precisa alcanzar todos los nodos. Con alcanzar a la mayoría de los nodos, entrarán en un bloque en poco tiempo. Las transmisiones de nodos también toleran mensajes perdidos. Si un nodo no recibe un bloque, lo reclamará cuando reciba el siguiente bloque y se dé cuenta de que falta uno.

1. Incentivo

Por convención, la primera transacción en un bloque es una transacción especial con la que comienza una moneda nueva, propiedad del creador del bloque. Esto añade un incentivo a los nodos para soportar la red, y proporciona una forma de poner las monedas en circulación, dado que no hay autoridad central que las distribuya. La adición estable de una constante de monedas nuevas es análoga a los mineros de oro que consumen recursos para añadir oro a la circulación. En nuestro caso, es tiempo de CPU y electricidad lo que se gasta. El incentivo también se basa en las comisiones por transacción. Si el valor de salida de una transacción es menor que el valor de entrada, la diferencia es una comisión por transacción que se añade al valor de incentivo del

bloque que contiene la transacción. Una vez que un número predeterminado de monedas ha entrado en circulación, el incentivo puede evolucionar hacia comisiones de transacción y estar completamente libre de inflación. El incentivo puede ayudar a que los nodos permanezcan honestos. Si un atacante codicioso fuera capaz de reunir más potencia CPU que la de todos los nodos honestos, tendría que escoger entre usarla para defraudar a la gente robándoles los pagos recibidos, o usarla para generar nuevas monedas. Debe encontrar más rentable respetar las reglas, esas reglas que le favorecen entregándole más monedas nuevas que a todos los demás en conjunto, que socavar el sistema y la validez de su propia riqueza.

2. Recuperación de espacio de disco

Cuando la última transacción de una moneda está enterrada bajo suficientes bloques, las transacciones gastadas antes que esta última se pueden descartar para ahorrar espacio de disco. Para facilitar esto sin romper el hash del bloque, las transacciones son hasheadas en un Árbol de Merkle [7][2][5], incluyendo solo la raíz en el hash del bloque. Los bloques viejos pueden compactarse podando ramas del árbol. Los hashes interiores no necesitan ser guardados. Una cabecera de bloque sin transacciones pesaría unos 80 bytes. Si suponemos que los bloques se generan cada 10 minutos, 80 bytes × 6 × 24 × 365 = 4.2MB por año. Siendo habitual la venta de ordenadores con 2GB de RAM en 2008, y con la Ley de Moore prediciendo un crecimiento de 1.2GB anual, el almacenamiento no debería suponer un problema incluso si hubiera que conservar en la memoria las cabeceras de bloque. 4 Bloque Bloque Cabecera de bloque (Hash del bloque) Hash previo Nonce Hash01 Hash0 Hash1 Hash2 Hash3 Hash23 Hash raíz Hash01 Hash2 Tr. 3 Hash23 Cabecera de bloque (Hash del bloque) Hash raíz Transacciones hasheadas en un Árbol de Merkle Tras eliminar las Tr. 0-2 del bloque Hash previo Nonce Hash3 Tr. 0 Tr. 1 Tr. 2 Tr. 3

3. Verificación de pagos simplificada

Es posible verificar pagos sin ejecutar un nodo plenamente en red. El usuario solo necesita tener una copia de las cabeceras de bloque de la cadena más larga de proof-of-work, que puede conseguir solicitándola a los nodos de red hasta estar convencido de que tiene la cadena más larga, y obtener la rama Merkle que enlaza la transacción con el bloque en que está sellado en el tiempo. El usuario no puede comprobar la transacción por sí mismo pero, al enlazarla a un lugar en la cadena, puede ver que un nodo de la red la ha aceptado, y los bloques añadidos posteriormente confirman además que la red la ha aceptado. Como tal, la verificación es fiable en tanto que los nodos honestos controlen la red, pero es más vulnerable si un atacante domina la red. Mientras

que los nodos de red pueden verificar las transacciones por sí mismos, el método simplificado puede ser engañado por transacciones fabricadas por un atacante, en tanto el atacante pueda continuar dominando la red. Una estrategia para protegerse contra esto podría ser aceptar alertas de los nodos de red cuando detecten un bloque no válido, sugiriendo al software del usuario que descargue el bloque entero y las transacciones con aviso para confirmar la inconsistencia. Los negocios que reciban pagos con frecuencia seguramente preferirán tener sus propios nodos ejecutándose para tener más seguridad independiente y verificación más rápida.

4. Combinando y dividiendo valor

Aunque sería posible manipular monedas individualmente, no sería manejable hacer una transacción para cada céntimo en una transferencia. Para permitir que el valor se divida y combine, las transacciones contienen múltiples entradas y salidas. Normalmente habrá, o bien una entrada simple de una transacción anterior mayor, o bien múltiples entradas combinando pequeñas cantidades, y como máximo dos salidas: una para el pago y otra devolviendo el cambio, si lo hubiera, al emisor. Cabe señalar que la diseminación de control6, donde una transacción depende de varias transacciones, y esas transacciones dependen de muchas más, no supone aquí un problema. No existe la necesidad de extraer una copia completa e independiente del historial de una transacción.

5. Privacidad

El modelo tradicional de banca consigue un nivel de privacidad limitando el acceso a la información a las partes implicadas y el tercero de confianza. La necesidad de anunciar públicamente todas las transacciones excluye este método, pero aún así se puede mantener la privacidad rompiendo el flujo de información en otro punto: manteniendo las claves públicas anónimas. El público puede ver que alguien está enviando una cantidad a otro alguien, pero sin que haya información vinculando la transacción con nadie. Esto es similar al nivel de información que comunican las bolsas de valores, donde el tiempo y tamaño de las operaciones individuales, la "cinta", son hechos públicos, pero sin decir quiénes fueron las partes. Como cortafuego adicional, debería usarse un nuevo par de claves en cada transacción para evitar que se relacionen con un propietario común. Con las transacciones multientrada será inevitable algún tipo de vinculación, pues revelan necesariamente que sus entradas pertenecieron al mismo propietario. El riesgo es que si se revela la identidad del propietario de una clave, la vinculación podría revelar otras transacciones que pertenecieron al mismo propietario.

6. Cálculos

Consideramos el escenario de un atacante intentando generar una cadena alternativa más rápido que la cadena honesta. Incluso si se consigue, el sistema no queda abierto a cambios arbitrarios como crear valor de la nada o tomar dinero que nunca perteneció al atacante. Los nodos no van a aceptar una transacción inválida como pago y los nodos honestos nunca aceptarán un bloque que las contenga. Un atacante solo puede tratar de cambiar una de sus propias transacciones para recuperar dinero que ha gastado recientemente. La carrera entre la cadena honesta y la cadena de un atacante puede verse como un paseo aleatorio binomial7. El suceso que prospera es la cadena honesta creciendo un bloque, aumentando su liderato por +1, y el suceso que fracasa es la cadena del atacante creciendo un bloque, reduciendo la brecha en -1. La probabilidad de que un ataque alcance [la cadena honesta] desde un déficit dado es análoga al problema de la ruina del jugador8. Supongamos que un jugador con crédito ilimitado comienza con un déficit y juega en potencia un número infinito de intentos para alcanzar un punto de equilibrio. Podemos calcular la probabilidad de que alcance ese punto, o de que un ataque alcance alguna vez a la cadena honesta, como sigue [8]: p = probabilidad de que un nodo honesto encuentre el siguiente bloque q = probabilidad de que el atacante encuentre el siguiente bloque qz = probabilidad de que el atacante alcance [la cadena honesta] desde z bloques atrás Asumiendo que p > q, la probabilidad cae de forma exponencial a medida que aumenta el número de bloques que el atacante tiene que alcanzar. Con las probabilidades en su contra, si no tiene un 6 qz={ 1 if p≤q □q/ p□ z if p□q} Identidades Transacciones Tercero de confianza Contraparte Público Identidad Transacciones Público Nuevo modelo de privacidad Modelo tradicional de privacidad golpe de suerte que lo haga avanzar desde el principio, sus oportunidades se irán desvaneciendo a medida que se va quedando atrás. Consideremos ahora cuánto tiempo necesita esperar el receptor de una transacción para tener la suficiente seguridad de que el emisor no puede cambiarla. Asumimos que el emisor es un atacante que quiere que el receptor crea durante un tiempo que le ha pagado; entonces cambiará el pago para devolvérselo a sí mismo un tiempo después. El receptor recibirá un aviso cuando esto suceda, pero el emisor espera que ya sea demasiado tarde. El receptor genera un nuevo par de claves y da la clave pública al emisor poco antes de firmar. Esto impide que el emisor pueda preparar una cadena de bloques previa trabajando de continuo en ella hasta tener la suerte suficiente como para ponerse a la cabeza y, entonces, ejecutar la transacción. Una vez que la transacción se ha emitido, el emisor deshonesto comienza a trabajar en secreto en una cadena paralela que contiene una versión alternativa de su transacción. El receptor espera hasta que la transacción se ha añadido

al bloque y z bloques se han enlazado tras él. No sabe la cantidad de progreso que ha realizado el atacante, pero asumiendo que los bloques honestos han tomado la media de tiempo esperada por bloque, el potencial de progreso del atacante será una distribución de Poisson9 con un valor esperado: Para obtener la probabilidad de que el atacante pueda ponerse al día incluso ahora, multiplicamos la densidad de Poisson para cada aumento en el progreso que podría haber realizado, por la probabilidad que podría haber alcanzado desde ese punto: Reordenándola para evitar sumar la cola infinita de la distribución... Convertida a lenguaje de programación C... 7 □=z q p ∑ k=0 ∞ □ k e −□ k! ·{ □q / p□ □z−k □ if k ≤z 1 if k □z} 1−∑ k=0 z □ k e −□ k! □1−□q/ p□ □z−k □ □ #include double AttackerSuccessProbability(double q, int z) { double p = 1.0 - q; double lambda = z * (q / p); double sum = 1.0; int i, k; for (k = 0; k <= z; k++) { double poisson = exp(-lambda); for (i = 1; i <= k; i++) poisson *= lambda / i; sum -= poisson * (1 - pow(q / p, z - k)); } return sum; } Ejecutando algunos resultados, podemos ver que la probabilidad disminuye exponencialmente con z. Resolviendo para P menor que 0.1%...

7. Conclusión

Hemos propuesto un sistema para realizar transacciones electrónicas sin depender de confianza. Comenzamos con el marco habitual de monedas creadas a partir de firmas digitales, lo cual permite un firme control de la propiedad, pero que está incompleto sin una forma de prevenir el doble gasto. Para resolver esto, hemos propuesto una red peer-to-peer usando proof-of-work para realizar un registro público de las transacciones que rápidamente se hace computacionalmente inviable de cambiar para un atacante si la mayoría de la potencia CPU está controlada por nodos honestos. La red es robusta dada su simplicidad no estructurada. Los nodos trabajan todos a la vez, precisando poca coordinación. No necesitan ser identificados dado que los mensajes no se envían a ningún lugar en particular, y solo necesitan ser emitidos en base a "mejor esfuerzo". Los nodos pueden abandonar y reincorporarse a la red a voluntad, aceptando la cadena proof-of-work como prueba de lo que ha sucedido mientras estaban ausentes. Votan con su potencia CPU, expresando su aceptación de los bloques válidos trabajando en extenderlos y descartando los bloques no válidos al rechazar trabajar en ellos. Cualesquiera reglas e incentivos necesarios pueden ser aplicados con este mecanismo de consenso.

11. Bibliografía

Aitken, R. (14 de 12 de 2017). *Forbes*. Obtenido de IBM & Walmart Launching Blockchain Food Safety Alliance In China With Fortune 500's JD.com: https://www.forbes.com/sites/rogeraitken/2017/12/14/ibm-walmart-launching-blockchain-food-safety-alliance-in-china-with-fortune-500s-jd-com/#108744b07d9c

Anderson, R. (2011). *Security engineering: a guide to building dependable distributed systems.* New Yersey: Wiley.

Antonopoulos, A. M. (12 de 06 de 2017). *Mastering Bitcoin: Programming the Open Blockchain.* O'Reilly Media, Inc.

Arvind Narayanan, J. B. (2016). *Bitcoin and Cryptocurrency Technologies.* New Jersey: Princeton University Press.

Blogchainers. (14 de 11 de 2017). *Medium*. Obtenido de Las 3 propiedades primordiales de las funciones Hash: https://medium.com/@_Blockchainers_/las-3-propiedades-primordiales-de-las-funciones-hash-f007e8568f71

Clement, A. (13 de 06 de 2018). *Medium*. Obtenido de https://medium.com/@humanGamepad/fizzy-axa-smart-contract-explaind-740df52894fd

Clemente, A. (13 de Junio de 2018). *Medium*. Obtenido de fizzy.axa Smart Contract explained: https://medium.com/@humanGamepad/fizzy-axa-smart-contract-explaind-740df52894fd

Federation of American Scientists. (2015). Obtenido de Unmanned aircraft systems roadma: https://fas.org/irp/program/collect/uav_roadmap2005.pdf

Francois Laurent, G. C. (2016). *Accenture.* Obtenido de A business approach for the use of drones in the Engineering & Construction Industries: https://www.accenture.com/_acnmedia/PDF-24/Accenture-Drones-Construction-Service.pdf

Función hash: concepto y aplicación en Bitcoin. (s.f.). Obtenido de Academy: https://academy.bit2me.com/como-funciona-el-hash-en-bitcoin/

Guru 99. (s.f.). Obtenido de Design Verification & Validation Process: https://www.guru99.com/design-verification-process.html

Hackius, N. (11 de 2017). *Research Gate, Moritz Petersen*. Obtenido de Blockchain in Logistics and Supply Chain: Trick or Treat?: https://www.researchgate.net/publication/318724655_Blockchain_in_Logistics_and_Supply_Chain_Trick_or_Treat

Hash, M. (26 de Febrero de 2018). *#TraceChain major benefits. Part 2*. Obtenido de Medium: https://medium.com/metahash/tracechain-major-benefits-part-2-5e279fcb6fd2

James Macaulay, L. B. (2015). *Delivering tomorrow.* Obtenido de Internet of things in logistics: https://delivering-tomorrow.com/wp-content/uploads/2015/08/DHLTrendReport_Internet_of_things.pdf

James Vincent, C. G. (5 de 6 de 2015). *The Verge*. Obtenido de Here's Amazon's new transforming Prime Air delivery drone: https://www.theverge.com/2019/6/5/18654044/amazon-prime-air-delivery-drone-new-design-safety-transforming-flight-video

King, R. (21 de Junio de 2019). *Bit degree*. Obtenido de What Is a Smart Contract and How Does it Work?: https://www.bitdegree.org/tutorials/what-is-a-smart-contract/

Martin Joerss, J. S. (September de 2016). *McKingsey Company.* Obtenido de Parcel delivery. The future of last mile: https://www.mckinsey.com/~/media/mckinsey/industries/travel%20transport%20and%20logistics/our%20insights/how%20customer%20demands%20are%20reshaping%20last%20mile%20delivery/parcel_delivery_the_future_of_last_mile.ashx

Minsait. (2017). Obtenido de Cómo impacta blockchain en la logística 4.0: https://www.minsait.com/sites/default/files/newsroom_documents/informe_blockchain_logistica_uno_e_0.pdf

Moller, A. (09 de 08 de 2018). *IBM*. 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

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Obtenido de Academy: https://bitcoin.org/bitcoin.pdf

Nietzsche, F. W. (2015). *DHL*. Obtenido de hat doesn't destroy, strengthens.: https://www.dhl.com/content/dam/Campaigns/risk-and-resilience/dhl_insighton_final.pdf

Paula. (18 de Octubre de 2018). *CYSAE.* Obtenido de Recompensa del minado ¿por qué 12,5 BTC por bloque?: Ittay Eyal and Emin G¨un Sirer

Pérez, J. L. (10 de Enero de 2018). *Comunycarse*. Obtenido de Reglamento Europeo de Protección de Datos 2018 (GDPR): https://www.comunycarse.com/es/reglamento-europeo-proteccion-datos-2018-gdpr/

Preukschat, A. (2017). *Blockchain: la revolución industrial de internet.* Madrid: Grupo Planeta.

Search compliance. (Abril de 2018). Obtenido de Smart Contract: https://searchcompliance.techtarget.com/definition/smart-contract

Sirer, I. E. (2013). *Cornell CIS Computer Sience.* Obtenido de Majority is not Enough: Bitcoin Mining is Vulnerable.

Tascot, D. (2017). *La recolución blockchain.* Barcelona: DEUSTO S.A. EDICIONES.

Terzia, N. (10 de 09 de 2011). *Science Direct.* Obtenido de The impact of e-commerce on international trade and employment: https://www.sciencedirect.com/science/article/pii/S1877042811015382

Victor Sánchez Horreo, F. C. (2017). *Minsait.* Obtenido de Cómo impacta blockchain en la logística 4.0: https://www.minsait.com/sites/default/files/newsroom_documents/informe_blockchain_logistica_uno_e_0.pdf

Wihbey, J. (s.f.). *Lincoln Institute of Land Policy*. Obtenido de La revolución de los drones: https://www.lincolninst.edu/es/publications/articles/la-revolucion-los-drones

WOLT. (s.f.). Obtenido de https://volttech.io/blockchain-last-mile-delivery-challenges/

Yousaf Bin Zikria, H. Y. (Agosto de 2018). *Research Gate.* Obtenido de Internet of Things (IoT): Operating System, Applications and Protocols Design, and Validation Techniques: https://www.researchgate.net/publication/327138483_Internet_of_Things_IoT_Operating_System_Applications_and_Protocols_Design_and_Validation_Techniques

Referencia statista, punto 5.3

Referencia ‘The Ultimate Guide to Last Mile & White Glove Logistics’ punto 5.3

Punto 6.2.2. Para eliminar este tipo de procesos ineficientes.. IBM y Maersk