FACULTAD DE COMERCIO
Universidad de Valladolid

FACULTAD DE COMERCIO

TRABAJO FIN DE MÁSTER

EN COMERCIO EXTERIOR

“EL BLOCKCHAIN APLIADO A LOS SECTORES EMPRESARIALES: UNA PROPUESTA PARA EL ÁMBITO DEL COMERCIO EXTERIOR.”

DIEGO BLANCO HERRERA

FACULTAD DE COMERCIO

VALLADOLID, ENERO, 2020

FACULTAD DE COMERCIO
Universidad de Valladolid

UNIVERSIDAD DE VALLADOLID

MÁSTER EN COMERCIO EXTERIOR

CURSO ACADÉMICO 2018-2019

TRABAJO FIN DE MÁSTER

"EL BLOCKCHAIN APLIADO A LOS SECTORES EMPRESARIALES: UNA PROPUESTA PARA EL ÁMBITO DEL COMERCIO EXTERIOR."

Trabajo presentado por: Diego Blanco Herrera

Firma:

Tutor: Francisco Javier Gómez González

Firma: GOMEZ GONZALEZ FRANCISCO JAVIER - DNI 13137035X

Firmado digitalmente por GOMEZ GONZALEZ FRANCISCO JAVIER - DNI 13137035X
Nombre de reconocimiento (DN): c=ES, o=UNIVERSIDAD DE VALLADOLID, ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO, serialNumber=IDCES-13137035X, sn=GOMEZ GONZALEZ, givenName=FRANCISCO JAVIER, cn=GOMEZ GONZALEZ FRANCISCO JAVIER - DNI 13137035X
Fecha: 2020.07.29 16:49:41 +02'00'

FACULTAD DE COMERCIO
Universidad de Valladolid

FACULTAD DE COMERCIO

Valladolid, fecha

ÍNDICE

1. INTRODUCCIÓN

1. 1 JUSTIFICACIÓN DEL TRABAJO

El siguiente proyecto de fin de máster se centra en describir el potencial de cambio que tiene la revolución tecnológica llamada Blockchain (también denominada cadenas de bloques) sobre el comercio y los diferentes sectores. En estos momentos ya hay diferentes sectores del comercio que están aplicando este avance tecnológico en sus operaciones diarias obteniendo una importante funcionalidad gracias a la trazabilidad y seguridad, entre algunas de sus muchas prestaciones.

El mundo tal y como funciona actualmente necesita producir, gestionar y almacenar una enorme cantidad de información certificada en todo momento. Este proceso se repite cada díay cada hora. Hasta ahora este proceso está gestionado por humanos, la propuesta de Blockchain es que puedan hacerlo otro tipo de seres incorruptibles, eficaces, sacrificados y cada vez más veloces… los ordenadores.

La cadena de bloques posee su propia estructura, su propia arquitectura. Cada bloque contiene diferentes tipos de información, el ejemplo más famoso es Bitcoin, pero hay muchos otros, ¿Qué contiene cada bloque? Tres cosas:

La primera, la información. En el caso de Bitcoin, por ejemplo la información relativa a las transferencias de dinero, emisor, receptor, fecha, cantidad… La segunda, algo muy importante, el identificador de cada bloque. Se trata de un número único e irrepetible, cada uno de los bloques tiene el suyo propio. La tercera, el identificador de cada bloque anterior, puesto que cada bloque queda conectado con su predecesor y su sucesor. Estos bloques van creando una cadena.

Si se imagina una cadena de bloques como un puzle, se podría decir que la información genera una forma, de manera que, si cambia la información, la forma también cambiará y, consecuentemente, la cadena quedará invalidada.

Desde mi punto de vista, Blockchain representa el fututo más cercano y una nueva forma de pensar, cuya difusión al sector profesional es importante porque hay mucha gente que desconoce este concepto. Decidí enfocar mi proyecto sobre esta revolución tecnológica porque me parece un tema muy novedoso, práctico y que puede suponer una revolución en el comercio a la hora de realizar operaciones de importación y exportación.

Realizando este trabajo de investigación sobre el Blockchain he ampliado mis conocimientos sobre esta tecnología tan innovadora, también sobre las criptomonedas, los tipos existentes, cómo funcionan y qué tecnología está detrás de ella

Para realizar este trabajo, asistí al primer congreso de BlockChain y Criptomonedas en Castilla y León en el mes de abril de 2019. Una serie de conferencias de distintos profesionales y expertos sobre el tema. También tuve el placer de conocer a Carlos Callejo, fundador de Valladolid Blockchain.

1.2 OBJETIVOS

En este trabajo he intentado explicar el Blockchain y su funcionamiento, para poder aplicarlo en diferentes sectores. Esta tecnología va a condicionar el mundo tal y como lo conocemos. De acuerdo con ello, los objetivos de este trabajo son los siguientes:

- Explicar el funcionamiento de la tecnología de bloques, las nuevas tendencias que ofrece, las innovaciones y sus posibles aplicaciones.
- Describir algunas posibles aplicaciones que puede ofrecer Blockchain.
- Explicar cómo afecta la tecnología de bloques tanto en el sector privado, cómo en el sector público.
- Detallar las principales criptomonedas que existen actualmente en el mercado, identificando sus principales características, también las principales ventajas e inconvenientes de su aplicación.
- Crear mi propia criptomoneda. DBH44
- Elaborar una propuesta de curso complementario de la tecnología Blockchain al Máster de Comercio exterior de la Universidad de Valladolid.

1.3 ESTRUCTURA DEL TRABAJO Y METODOLOGÍA

Este proyecto nace para dar alguna respuesta a la fuerte demanda tecnológica a la que nos enfrentamos a día de hoy. El fin de este trabajo es conocer más su funcionamiento, la oferta de empleo tecnológica y la nueva adaptación de las empresas a un plan de transformación digital.

Este trabajo está estructurado en 3 bloques, cuyo contenido se explica a continuación:

En el primer apartado se resumen brevemente la tecnología Blockchain, cómo surge, quién está detrás de ella, para qué se creó en un primer momento, etc. La importancia que tiene la clasificación de sus redes, así como sus características.

En el segundo bloque se describen las criptomonedas, el Bitcoin y las principales criptomonedas del mercado. La evolución que han tenido desde su nacimiento. Posteriormente se explica cómo he creado mi propia criptomoneda, DBH44, todos los pasos necesarios que hay que hacer para conseguir una moneda virtual.

En el ultimo apartado, una vez explicado toda esta tecnología, cómo influye, prácticamente en el día a día y todos los usos que tiene, propongo elaborar un curso complementario al Máster de Comercio Exterior de la Universidad de Valladolid

1.4 AGRADECIMIENTOS

Realizar este proyecto me ha supuesto una adquisición de conocimientos muy valiosos. He de decir que encontré gran cantidad de información, pero lo realmente costoso ha sido clasificar toda esta información. Puedo decir que ha sido un reto desafiante y a la vez muy interesante. Por esta razón me gustaría mencionar a las personas que me han ayudado a conseguirlo y me han apoyado en todo este proceso.

En primer lugar, a mis queridos padres, Ernesto y Carmen, por su apoyo incondicional en todo momento y por darme la oportunidad de realizar estos estudios, sin los cuales no estaría en este punto. A mi novia, Esther, fundamental en todo momento, por sus ánimos, consejos y por recordarme siempre de lo que soy capaz. A mis amigos, en especial a Emilio y Arturo por escuchar mis quejas y siempre motivarme en los momentos más bajos.

Por supuesto, quería tener una mención especial a mi tutor y amigo, Javier Gómez, por toda su paciencia, sus consejos y siempre su inmediata disponibilidad a concederme tutorías. También quería dar las gracias al profesor David Carvajal por sus charlas y gran sentido del humor.

2. BLOCKCHAIN

"*Una máquina para generar confianza…. La tecnología que está detrás de Bitcoin. Permite a la gente que no se conoce o no confía en los demás, construir un libro de contabilidad fiable. Esto tiene implicaciones mucho más allá de las cripto- monedas… podría transformar la forma en la que funciona la economía*" The Economist, Oct 2015.

2.1 INTRODUCCIÓN

Mucha gente cree que el Blockchain tendrá el mismo impacto que tuvo Internet, por lo que se refiere a él como, próxima revolución, según describe en su libro *"El nuevo entorno tecnológico que va a modificar nuestras vidas, Blockchain: La revolución industrial de Internet.* Alex Preukschat (2019)

Originalmente, el Blockchain se construyó como una infraestructura subyacente de Bitcoin. La tecnología Blockchain va mucho más allá de las monedas. Esta tecnología, tiene aplicaciones de gran alcance que puede influir significativamente en la forma en la que interactúan los mercados financieros, así como la inteligencia artificial, los ordenadores y la tecnología.

La tecnología Blockchain, o cadenas de bloques, utiliza el "Libro de tecnología distribuido" o DTL, es un libro mayor distribuido y descentralizado para verificar el registro de las transacciones. Esta tecnología permite a las partes recibir, enviar y registrar valor o información a través de una red de ordenadores de igual a igual.

Blockchain es una plataforma digital que almacena y verifica todo el historial de transacciones entre usuarios a través de la red. Desde un punto de vista técnico, Blockchain es una base de datos que consiste en paquetes de transacciones conocidas como "bloques", contra los cuales cualquier transacción propuesta puede ser comprobada con la confianza en la integridad de cualquier bloque en particular. Una vez que la información ha sido introducida, no puede ser modificada o borrada (Kakavand, 2017)

Es importante señalar que el Blockchain no tiene una sola definición universal acordada, porque hay diferentes dimensiones, operativa, tecnológica, jurídica y reglamentaria.

En este trabajo cuando hacemos referencia al DTL (Libro de tecnología mayor distribuido) se hace referencia a la capacidad de los usuarios de almacenar y acceder a la información o registros relacionados con los activos y las tendencias en una base de datos compartida, capaz de operar sin un sistema central de validación. El DTL tiene un gran número de aplicaciones diversas. Una aplicación importante es el ámbito de los servicios financieros, que permite a los usuarios con acceso a la base de datos compartida, liquidar directamente los valores y el efectivo relacionados con las transferencias entre sí, sin tener que depender de un intermediario (Kost, 2017).

En el aspecto normativo y legal, se han planteado muchas cuestiones en términos de privacidad, riesgo y seguridad. Es importante que se logre el equilibrio adecuado entre

el rápido desarrollo de la tecnología Blockchain y su estabilidad legal, asegurando que las dimensiones legales y regulatorias no obstaculicen la innovación en este espacio.

Cada usuario posee un par de claves privadas y públicas. La clave privada se utiliza para firmar transacciones. Las transacciones firmadas digitalmente se distribuyen por toda la red y luego se accede a ellos mediante claves públicas, que son visibles para todos en la red. La firma digital consta de 2 fases: la fase de firma y la fase de verificación

En este trabajo voy a analizar la historia del surgimiento del Blockchain, la clasificación de sus redes, sus características y, especialmente, cómo el Blockchain es aplicado en el Comercio Exterior y la importancia que tienes los Smart Contracts (Contratos inteligentes).

¿CÓMO FUNCIONA UNA BLOCKCHAIN?

EL profesor Robby Houben lo describe en el documento solicitado por el Comité Especial sobre Crímenes Financieros del Parlamento Europeo, publicada en julio de 2018, cómo una base de datos distribuida, en términos simples. Se inicia con uno de los nodos de la red, que crea un nuevo “bloque” de datos que puede contener todo tipo de información. Este nuevo bloque se transmite a los otros nodos en forma criptográfica para que los detalles de la transacción no sean hechos públicos. Los demás nodos determinan colectivamente la validez del acuerdo mediante un método de verificación con un algoritmo predefinido, comúnmente denominado “mecanismo de consenso”. Una vez que ha sido validado, el nuevo “bloque” se añade a la cadena de bloques, actualizando las operaciones que se distribuyen a través de la red.

En principio, este tipo de mecanismo puede utilizarse para cualquier tipo de operación de valor y puede aplicarse a cualquier activo que pueda ser representado de forma digital.

Los “bloques” de la transacción se firman con una firma digital utilizando una clave privada. Cada usuario de una red de cadenas de bloques tiene un juego de dos llaves. Una clave privada, que se utiliza para crear una firma digital para una transacción, y una pública, que es conocida por todos en la red.

Una llave pública tiene 2 usos: En primer lugar, sirve como una dirección en la red de cadenas de bloques y, en segundo, se utiliza para verificar una firma digital o para validar la identidad del remitente.

Una de las principales ventajas de la tecnología de la cadena de bloques es que permite simplificar la ejecución de una amplia gama de operaciones que normalmente requerirían la intermediación de un tercero, por ejemplo, en un banco, en un sistema de liquidación de valores, etc. La esencia del Blockchain está en descentralizar la confianza y permitir la autentificación descentralizada de las transacciones. En pocas palabras, permite eliminar al “intermediario”. Sin embargo, es importante subrayar que también pueden exponer a las partes que interactúan a ciertos riesgos que antes eran gestionados por estos intermediarios. Por ejemplo, el Banco de Pagos Internacionales (BPI) advirtió recientemente en el informe de 2017 *“Tecnología del libro mayor distribuido en el pago, la compensación y la liquidación”* que la tecnología de la cadena de bloques podría introducir nuevos riesgos de liquidez y nuevas funciones del intermediario.

Los mecanismos de consenso de la cadena de bloques. Cualquier nodo que esté dentro de una red de cadenas de bloques puede proponer añadir nueva información a la cadena de bloques. Para validar esta información, los nodos tienen que llegar a algún tipo de acuerdo, aquí entra el mecanismo de "consenso" para asegurar la secuenciación de las transacciones.

En el caso de las criptodivisas, esta secuencia es necesaria para abordar la cuestión del "doble gasto", es decir, la cuestión de que un mismo instrumento de pago o activo puede ser transferido más de una vez si las transferencias no se registran y controlan de forma centralizada.

2.2 HISTORIA

En 2008 surge por primera vez la tecnología de bloques. Este concepto fue diseñado por un individuo que utilizó el pseudónimo de Satoshi Nakamoto. En 2009 por primera vez se aplica a un componente, las criptomonedas. Bitcoin y las cadenas de bloques están vinculadas, pero son dos realidades diferentes. Blockchain o cadena de bloques es la tecnología en la que está fundamentada la infraestructura virtual de Bitcoin. Este tipo de tecnología puede aplicarse a otros diferentes campos que no sean las criptomonedas.

En 2008 Satoshi Nakamoto publicó un libro (*Bitcoin: un sistema electrónico de efectivo entre iguales*) donde describe un modelo nuevo de privacidad: en una transición, un tercero de confianza entre las dos partes implicadas es sustituido por una validación de una prueba criptográfica, con esto podremos resolver los fallos en el modelo.

La primera aplicación real de las cadenas de bloques fue con el Bitcoin. Hubo que esperar hasta 2013 para que la tecnología de bloques se implementara en otras criptomonedas como es Ethereum. Vitalik Buterin, un joven programador de 19 años publicó un estudio sobre un sistema de bloques en aplicaciones descentralizadas y desarrolló el lenguaje de programación de Ethereum.

En 2015, Ethereum desarrolló los contratos inteligentes, mediante programas informáticos que ejecutan directamente cuando los términos y condiciones del contrato se cumplen. De esta forma queda programado y se elimina el fraude.

En 2016, se desarrolló una plataforma de criptomonedas diseñada para la comunicación entre máquinas IOTA (es una tecnología de contabilidad distribuida de código abierto), cuyo objetivo es permitir de forma segura el intercambio de información y valor en el Internet de las Cosas.

2.3 CLASIFICACIÓN DE REDES

Dependiendo de las características del Blockchain, existen diferentes modelos observando el grado de descentralización, la identidad de los participantes, el acceso, la escalabilidad, el nivel de privacidad, la velocidad… Integrando estos criterios

podemos clasificarlas en tres redes, cada una tiene sus particularidades. A continuación, y siguiendo las clasificaciones de redes desarrolladas por Ahn (2019) se presenta la siguiente clasificación desarrollando sus principales características.

2.3.1 PRIVADA.

En las cadenas de bloques totalmente privadas los permisos para validar y escribir datos en la cadena están controlados por una entidad en la que los demás usuarios depositan toda la confianza, y los participantes están identificados (Ahn, 2019)

En algunos casos puede restringirse el permiso de lectura a algunos usuarios. La entidad que tiene el control puede llegar a modificar las reglas de la cadena de bloques privadas y tiene el poder para llegar a rechazar las transacciones si no cumplen las reglas (Ahn, 2019).

Un número limitado de nodos verifican las transacciones según las reglas y son más eficientes que las redes públicas y necesitan menor potencial informático. Puede llegar a cobrarse una pequeña comisión por la confirmación de las transacciones.

A pesar de sus ventajas, este tipo de redes tiene algunos inconvenientes y es que al ser una red más centralizada es menos resistente a un posible ataque externo y corre un riesgo de ser manipulada por un ser humano. Aún no está claro si tendrá aceptación dentro de las grandes empresas.

2.3.2 PÚBLICA

Fue la primera que existió, en sus comienzos fue diseñada para Bitcoin y otras criptomonedas. En este tipo de plataforma no hay una entidad concreta que gestione y sea responsable. Todas las transacciones son públicas y los usuarios llegan a mantener el anonimato.

No hay un tercero de confianza que valide las transacciones, todo el tipo de registros de operaciones de datos que se realicen, dependen del consenso entre los nodos que intervienen.

En este tipo de redes, la mayoría son cadenas sin permisos, lo que significa, que están abiertas a cualquier posible interesado. Podremos descargar el programa informático necesario sin tener ningún tipo de permiso y configurar un nodo público para validar transacciones, participando en el protocolo. Cualquiera podrá leer y escribir datos en la cadena o tramitar transacciones a través de la red.

Es una red muy descentralizada, son muy seguras y son capaces de aguantar ataques informáticos ya que no tienen un único punto de fallo, sin embargo, poseen problemas de escalabilidad.

Un rasgo característico de esta red es su potencia informática que necesita para validar las transaccione Cualquier persona puede descargarse el código y administrar un nodo público en su máquina local, validando transacciones en la red y participando en el proceso de consenso, lo que hace que cualquiera tenga derecho a participar.

La ventaja de aplicar una red pública es que puede emplearse para crear nuevos modelos de negocio (Ahn, 2019).

Un ejemplo de este tipo de Blockchain son Bitcoin, Dash y Ethereum.

Imagen 1: RED BLOCKCHAN PÚBLICA VS PRIVADA

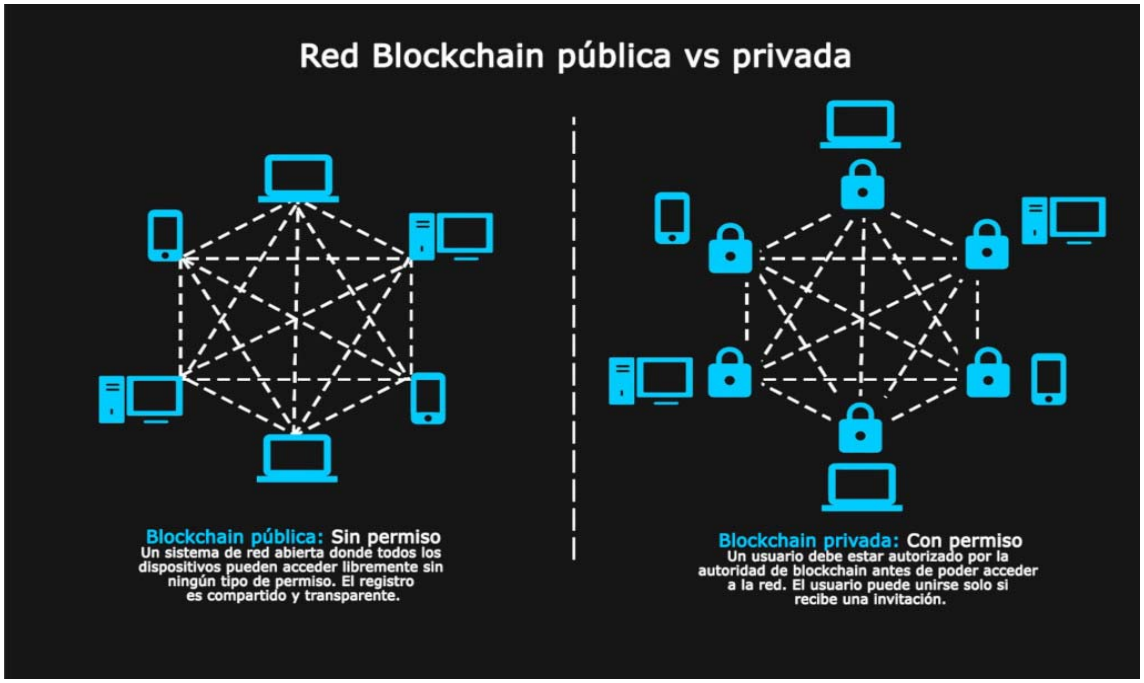


Foto de: 101 Blockchains

2.3.3 HIBRIDA O FEDERADA

Es una mezcla entre una red privada y pública. Se creó para provechar las ventajas de ambas. El Blockchain en este tipo de participación es una red privada, lo que quiere decir que una o varias entidades controlan el acceso a los recursos de la red, pero cualquier persona puede acceder al libro de contabilidad de forma pública. No existen monedas ni criptomonedas y está parcialmente descentralizado.

Este tipo de redes son muy usadas por organizaciones empresariales o gobiernos que quieran compartir o almacenar de forma segura. Este tipo de BlockChain se está aplicando en el sector sanitario y está siendo muy utilizado para guardar los datos de producción de medicamentos. Todos estos datos se pueden almacenar para ser revisados por autoridades competentes, para tener un control de calidad.

El objetivo de esta red de Blockchain es alcanzar un alto nivel de confianza y transparencia (Ahn, 2019)

Imagen 2: MODELO PARA OBTENER CONFIANZA EN EL SISTEMA DE PAGO ELECTRÓNICO BASADO EN BLOCHAIN.

Cuadro 1 Panorama general de las características principales de los distintos tipos de cadenas de bloques

Grado de centralización	Públicas		Consorcios		Privadas	
Gestión	Gestión no centralizada		Múltiples organizaciones		Una única entidad	
Acceso	**Sin permisos**	**Con permisos**	**Con permisos**	**Sin permisos**	**Con permisos**	
	Acceso de lectura abierto/ validación de las transacciones abierta	Acceso de lectura abierto/ validación de las transacciones con permisos	Acceso de lectura con permisos O abierto/ validación de las transacciones con permisos	Acceso de lectura abierto/ validación de las transacciones abierta	Acceso de lectura con permisos/ validación de las transacciones con permisos	
Participantes	Anónimos/ con pseudónimo	Anónimos/ con pseudónimo	Identificados	Normalmente, identificados	Identificados	
Validación basada en un protocolo de consenso	Abierta a cualquier participante de la red	Abierta a cualquier participante de la red, siempre que se cumplan determinadas condiciones	Abierta a participantes previamente autorizados (de las organizaciones del consorcio)	Depende del protocolo de consenso elegido para la plataforma	Abierta a participantes previamente autorizados (de la única entidad)	
Velocidad de validación	Baja	Más rápida	Rápida	Rápida	Rápida	
Privacidad de los usuarios	Ninguna	Ninguna	Adaptada a las necesidades de los participantes	Adaptada a las necesidades de los participantes	Adaptada a las necesidades de los participantes	
Potencia informática necesaria (consumo de energía)	Alta (pero variable en función del mecanismo de consenso)	Intermedia. Variable en función del mecanismo de consenso	Baja	Baja	Baja	
Comisión por transacción	Sí	Sí	Optativa (dependiendo de las reglas de la cadena)	Optativa (dependiendo de las reglas de la cadena)	Optativa (dependiendo de las reglas de la cadena)	
Escalabilidad	Baja	Ligeramente mayor	Mayor	Mayor	Mayor	
Ejemplo(s)	prueba de trabajo (PoW) (Bitcoin, Ethereum)	prueba de participación (Nxt)	Cadenas de bloques basadas en Hyperledger Fabric. Cadenas de bloques con permisos basadas en Ethereum	FastTrackTrade	Cadenas de bloques privadas basadas en Ethereum	

Fuente: Organización Mundial del Comercio

2.4 PRINCIPALES CARACTERISTÍCAS DE LAS CADENAS DE BLOQUES

- Ofrecen un elevado nivel de seguridad, seguimiento e inalterabilidad: gracias a su naturaleza descentralizada, las diferentes técnicas criptográficas utilizadas consiguen hacer que las cadenas de bloques sean muy resistentes a todos los ataques cibernéticos si las comparamos con bases de datos convencionales. Hay un alto nivel de seguridad, pero hay problemas relacionados con las deficiencias en las interfaces, con los contratos inteligentes y con las claves privadas para encriptar, ya que pueden ser robadas mediante ataques convencionales en el caso de que se guarden en un servidor centralizado o en los ordenadores de los usuarios.
  Cuando añadimos información a la cadena de bloques, esta información queda anotada en una marca de tiempo y es muy difícil que se pueda llegar a modificar. Estas son las consecuencias en caso de modificación:

  Las consecuencias de este mecanismo pueden enumerarse de la siguiente manera.

  Primero, el control de los cambios es más fácil. Esto llega a ser muy importante ya que vivimos en un mundo donde los objetos digitales pueden ser modificados, copiados y compartidos de una forma casi gratuita. Gracias a la inalterabilidad que ofrecen las cadenas de bloques podemos autentificar documentos y productos, pero es importante saber que, aunque las cadenas de bloques puedan ayudar a prevenir el fraude en los registros, también puede imposibilitar que se manipule esta tecnología y evita que se registre información falsa.
  La naturaleza distribuida e inalterable que ofrece esta tecnología consigue que no sea necesario hacer copias de seguridad de la base de datos, esto es muy importante porque supone un cambio primordial en los procesos de recuperación en caso de fallo informático. Cuando queda añadida a la cadena de bloques, la información se comparte con el conjunto de la red, se guarda en todos los nodos y es casi imposible modificarla. En caso de que algún nodo resulte afectado por un fallo, se puede recuperar la información fácilmente.

- Una arquitectura transparente, distribuida y de confianza descentralizada: toda la información que se añade a una cadena de bloques se distribuye y se muestra a todos los participantes de la red, cada participante tiene una copia completa. Las actualizaciones se comparten con toda la red, sin necesidad de que haya necesidad de confiar en una entidad central única. Las cadenas de bloques garantizan una transparencia inmediata y generalizada para conseguir los objetivos, la confianza está más centralizada y la lectura de parte de la información queda restringida a aquellos participantes que disponen de los permisos necesarios.

- Automatización: es el caso de la utilización de los contratos inteligentes, estos tienen un lenguaje informático programado y se ejecuta automáticamente para lograr automatizar los procedimientos para los pagos y demás operaciones por lo que es muy interesante el nivel que tiene de eficiencia.

- Anonimato: Cada usuario puede interactuar con la red de cadenas de bloques con una dirección generada. Un usuario puede generar muchas direcciones para evitar la exposición de su identidad. Se descentraliza la información privada de los usuarios. Este mecanismo preserva una cierta privacidad en las transacciones incluidas en la cadena de bloques.

2.5 EL IMPACTO DEL BLOCKCHAIN APLICADO EN EL COMERCIO EXTERIOR, LA INDUSTRIA Y LOS MERCADOS.

El mundo está en un continuo proceso de cambio, impulsado por las innovaciones tecnológicas y está afectando de una manera directa a la forma de hacer negocios. El progreso tecnológico ha estado siempre unido a la historia de la economía mundial.

Las cadenas de bloques se encargarán de resolver las preocupaciones relacionadas con seguridad, la dificultad para coordinar el tráfico de datos entre diferentes países y los diferentes actores que participan en una transacción comercial internacional.

"*Las posibles aplicaciones que tienen las cadenas de bloques en el mundo del comercio son numerosas y podrían transformar significativamente el comercio internacional… pero la tecnología no es la solución para todo*" (OMC 2018).

Según The Economist, el Blockchain es una *"máquina para generar confianza*". Y es precisamente esto lo que necesita el comercio y la economía para seguir creciendo. Poder verificar las transacciones mediante procesos criptográficos, mediante un "protocolo de consenso" (POW) matemático, permitiendo que las personas que no tienen tanta confianza entre sí puedan colaborar sin tener que depender de un tercero de confianza.

¿Puede realmente la cadena de bloques llegar a revolucionar el Comercio Internacional? Esta es una pregunta que se hace mucha gente. El carácter transparente, inalterable y descentralizado que posee la cadena de bloques han llamado el interés de gobiernos y agentes privados. Están buscando una eficiencia tecnológica en los procesos comerciales y es por lo que se están desarrollando proyectos piloto con las cadenas de bloques en el comercio internacional (Ganne, E. 2018).

El número de estudios de viabilidad y proyectos piloto ha aumentado y afectan a todos los sectores de la sociedad y de la economía. Desde el comercio electrónico, pasando por las finanzas, seguridad alimentaria o votaciones electorales. Para llevar a cabo todo esto es imprescindible los "permisos" que necesariamente necesitan disponer de una autorización para incluir una transacción en el registro. Cada vez se está invirtiendo más millones de euros en desarrollar las cadenas de bloques.

El Blockchain trae muchos beneficios y desafíos a los sectores industriales que ya están experimentando con esta tecnología, o que pronto se verán afectadas por esta tecnología.

El Blockchain permite que cualquier tipo de activo digital o digitalizado y sus transacciones asociadas sean registradas, rastreadas y certificadas entre las partes, sin importar la distancia física. Por lo tanto, los sistemas basados en cadenas de bloques podrían facilitar interacciones “sin fisuras” en las cadenas de suministro globales y distribuidas entre actores distantes y desconfiados, incluyendo distribuidores, transportistas, proveedores y consumidores (Francisco, 2018).

Las características de la tecnología garantizan que un producto ha sido procesado o distribuido por un actor específico en una fecha y hora específica, con ninguna posibilidad de que alguien pudiera cambiar el registro.

Varias empresas están experimentando con la integración de la tecnología de cadenas de bloques en teléfonos móviles, etiquetas inteligentes y otros dispositivos de IO para escanear códigos QR en las etiquetas de sus productos y acceder a información en una cadena de bloques sobre su origen, proceso de producción, calidad, fechas de caducidad o números de lote.

2.5.1 ¿VAMOS HACIA UN COMERCIO SIN PAPEL?

Muchos expertos coinciden en señalar que las cadenas de bloques es una herramienta fundamental para avanzar en la eficiencia de procesos comerciales y también para reducir papeleo hasta conseguir un comercio sin papel. El Blockchain tiene repercusiones muy importantes en todos los procesos que tenga que ver con la automatización de la financiación del comercio y de la digitalización, facilitando enormemente la financiación de las cadenas de suministro (OMC, 2018).

Hay muchos bancos que están inmersos en proyectos de colaboración con empresas de tecnología financiera y también con empresas de tecnología de la información. En estos momentos hay muchos proyectos piloto puestos en marcha, sin embargo, para poder llegar a utilizar esta tecnología a gran escala será necesario abordar una serie de problemas normativos y técnicos.

El Blockchain se va a convertir en una herramienta muy interesante para ayudar a la aplicación del Acuerdo sobre Facilitación del Comercio (AFC) de la OMC y los procesos entre empresas y administraciones públicas (B2G) y entre administraciones públicas (G2G) en el plano nacional. Los contratos inteligentes junto con la tecnología Blockchain pueden ayudar a gestionar los procedimientos transfronterizos de una manera más transparente, eficiente y segura. A todo esto, hay que añadir una mejora de la calidad de los datos comerciales (OMC, 2018).

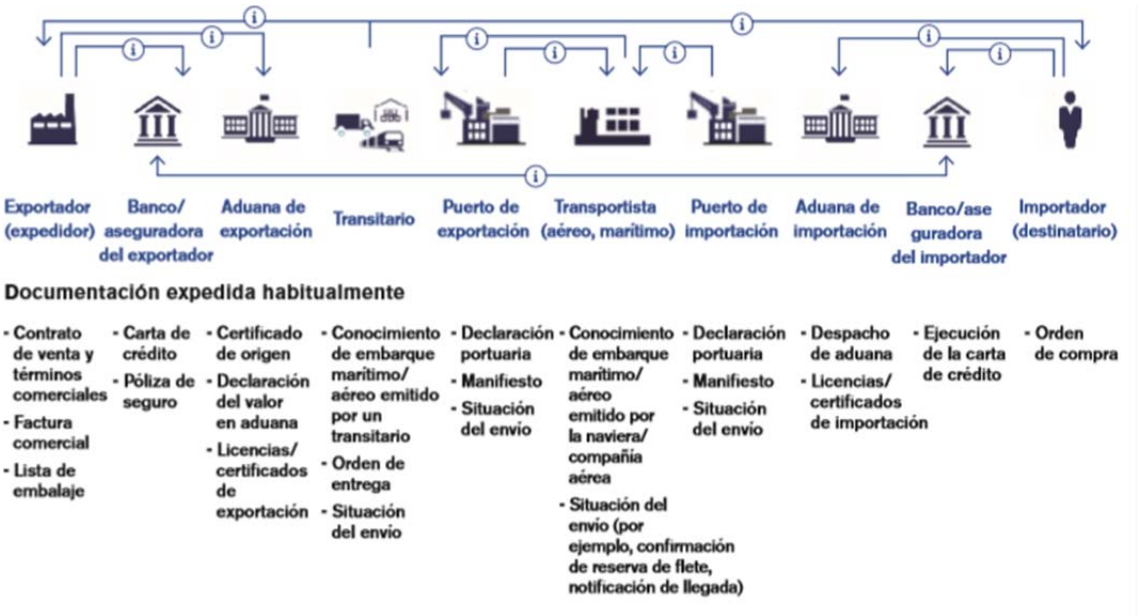
En estos momentos se está trabajando en mejorar la eficiencia de los procesos G2G transfronterizos, resolviendo los problemas de interoperabilidad a nivel técnico y también buscando conseguir una actividad normativa respaldada por una voluntad política, que permita crear un marco reglamentario propicio para el comercio sin papel.

La tecnología solamente podrá desarrollar todo su potencial si se llegan a digitalizar todos los aspectos de las transacciones comerciales fronterizas desde los trámites aduaneros hasta la logística, el trasporte o la financiación del comercio.

Se está analizando de qué manera se puede aprovechar la tecnología Blockchain en el sector de la logística y el transporte, hay un gran número de participantes trabajando en esta materia. Se trabaja en desarrollar plataformas comerciales que permitan conectar a todos los participantes de las cadenas de suministro. Las cadenas de bloques cada vez están evolucionando más para desarrollar una infraestructura comercial eficiente (Ganne, E. 2018).

Cuando realizamos una transacción comercial intervienen diferentes participantes y seguimos utilizando el papel para presentar los diferentes documentos (ver en Imagen 3)

Imagen 3: DOCUMENTOS REQUERIDOS PARA TRANSACCIONES COMERCIALES INTERNACIONALES



Fuente: Accenture

Los 4 procesos en las transacciones comerciales fronterizas son:

- Transacción comercial: Exportador/Importador (Orden de compra, oferta, factura)
- Financiación del comercio: Los bancos (letras de cambio, cartas de crédito…)
- Transporte: Los proveedores de servicios de logística (póliza de seguro, conocimientos de embarque…)

- Medidas de control oficial: Son los ministerios, unifica con los anteriores aduanas (certificados de conformidad, de origen, licencias de exportación/importación)

Se necesita una gran cantidad de papel para hacer estos procesos, lo que provoca que aumenten los costes de coordinación y administrativos. Se pueden producir pérdidas, errores o fraude. Hay Gobiernos y empresas que están investigando como aplicar la cadena de bloques para mejorar los procesos relacionados con el comercio internacional de mercancías y disminuir los trámites burocráticos. Todo ello para lograr avanzar hacia un comercio sin papel.

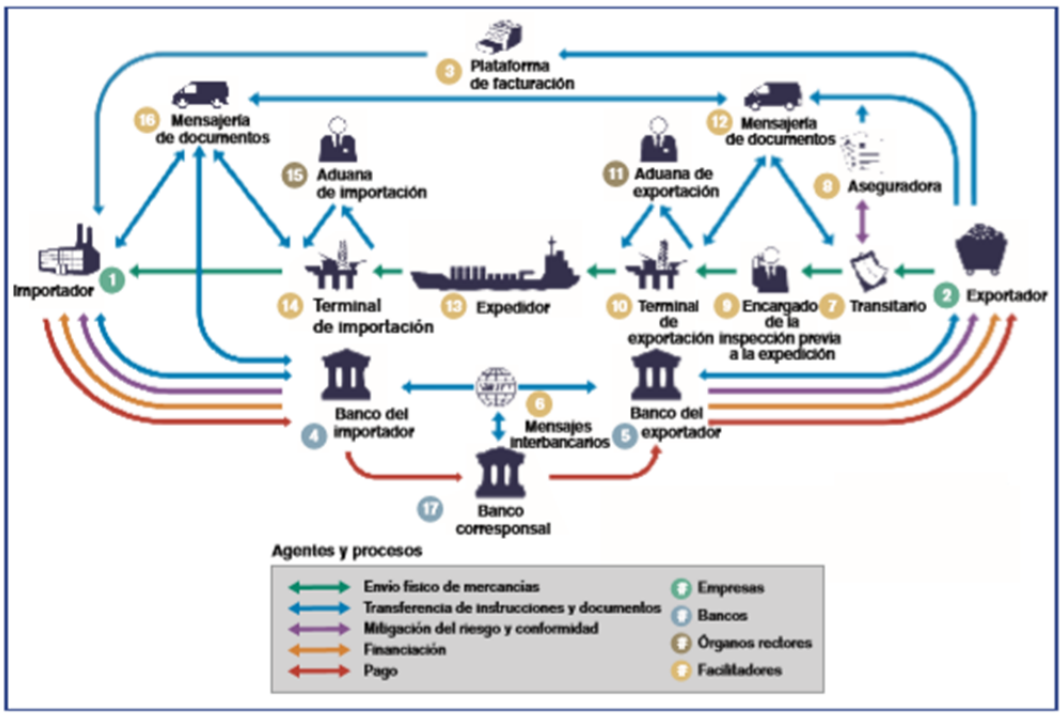
2.5.2 ¿SE PUEDE LOGRAR UNA FINANCIACIÓN DEL COMERCIO A TRAVÉS DE UNA CADENA DE BLOQUES?

En la mayoría de las transacciones comerciales internacionales, los compradores solamente realizan un único pago cuando han recibido correctamente las mercancías. La financiación en el comercio supone un 80% y es fundamental (OMC, 2016).

Generalmente, las cartas de crédito o también llamados créditos documentarios han sido utilizadas de forma generalizada en el comercio, aunque la tendencia está cambiando desde hace unos años se están utilizando más para financiar las cadenas de suministro.

Según un estudio del Boston Consulting Group, en una operación de financiación de comercio hay 20 agentes que participan en el proceso, entre 10 y 20 documentos de datos con unas 5000 interacciones de las cuales solo el 1% crea valor y entre un 85% a 90% no son datos de relevancia Boston Consulting Group

IMAGEN 4: TRANSACCIÓN COMERCIAL INTERNACIONAL



Fuente: Boston Consulting Group (2019)

En los últimos años se han llevado a cabo estudios de viabilidad para automatizar los procesos en los créditos documentarios y ha comenzado a comercializar aplicaciones de cadenas de bloques.

En septiembre de 2016, la compañía financiera inglesa, Barclays, junto con Wave, una nueva empresa de tecnología financiera realizó una operación conjunta de financiación de comercio mediante la tecnología de bloques en tiempo real. Esta operación se realizó mediante un registro con permiso. La operación fue una exportación de mantequillas y queso de una cooperativa indonesia a Seychelles por un valor de 100.00 dólares americanos. Este tipo de operación mediante un crédito documentario que suele tardar entre 7 y 10 días desde la fecha de expedición, gracias a la tecnología de la cadena de bloques se redujo a menos de cinco horas. El crédito documentario se emitió mediante un sistema SWIFT (Sociedad de Telecomunicaciones Financieras Intercambiarías Mundiales).

Respecto al tema de transacciones, en verano de 2016, HSBC, Bank of America y la IDA (Autoridad de Desarrollo de la Información y comunicación de Singapur) desarrollaron una aplicación de cadenas de bloques. Esta aplicación es capaz de reproducir una transacción tradicional mediante un crédito documentario con un intercambio de información entre importadores, exportadores y los diferentes bancos en un registro descentralizado con permisos.

En 2018 el banco HSBC realizó la “primera operación comercial de financiación del mundo viable” mediante una cadena de bloques. Un gran avance, siendo la operación

pionera para la utilización comercial de esta tecnología. Mediante un crédito documentario la compañía Cargill realizó un envío de soja desde Argentina a Malasia.

La revolución tecnológica que está suponiendo esta tecnología está mejorando los procesos tradicionales de financiación del comercio actual, llevando a muchas empresas a desarrollar nuevos productos y modelos de financiación de las cadenas de suministro.

2.5.3 LA INICIATIVA WE TRADE

We trade es una plataforma bancaria con tecnología Blockchain y con la tecnología Hyperledger Fabric (tecnología de código abierto) junto con la participación de 9 bancos en 11 países (datos de julio de 2018). En esta plataforma se inscribieron los comerciantes a través de sus bancos, una vez inscritos los exportadores e importadores registran en ella las transacciones que han acordado en el contrato. Mediante el contrato inteligente se garantiza la liquidación automática y el pago cuando todas las condiciones por ambas partes se cumplen. Los pagos pueden realizarse mediante compromiso bancario o cuentas abiertas. En julio de 2018 está plataforma finalizó sus primeras operaciones en línea, en las cuales llegaron a participar 5 bancos y 20 empresas (Rohr, 2019).

Aparte de We Trade, también existen otras empresas como IBM que tienen procesos de alianza con empresas asiáticas para desarrollar financiación de las cadenas de bloques con permisos. Estas plataformas utilizan tecnología Blockchain y contratos inteligentes para estimular los flujos financieros entre vendedores, compradores y financiadores, aparte de mejorar la rapidez, seguridad y transparencia de las cadenas de suministro. Diferentes estudios demuestran que es beneficioso utilizar las cadenas de bloques ya que todas las partes salen ganando y se reducen los costes de financiación. Es una oportunidad para las PYMES (Pequeñas y Medianas Empresas) ya que en muchas ocasiones tienen problemas para financiar sus actividades comerciales porque no tienen garantías suficientes de contar con crédito. Las cadenas de bloques pueden ayudar a tener más información, un historial crediticio de las empresas y una identificación de los clientes.

En España, Caixa Bank lanza la plataforma “Blockchain” we.trade para ejecutar y financiar transacciones de comercio exterior de sus clientes empresa. (03/01/2020)

2.5.4 BLOCKCHAIN Y LA CADENA DE SUMINISTRO

En particular, en el sector del transporte y la logística, la tecnología de la cadena de bloques podría facilitar el intercambio de información entre muchos agentes como pueden ser: fabricantes, operadores portuarios, compañías navieras y autoridades aduaneras. Por ejemplo, sobre el origen de las mercancías, los códigos arancelarios, los datos de clasificación, los certificados de importación y de exportación, el cumplimiento de las normas de seguridad, etc.

Hay cantidad de documentación para procesar y verificar en cualquier envío transfronterizo, como pueden ser las facturas tradicionales de un cargamento de cualquier mercancía, estas son presentadas, validadas y aprobadas de forma segura a

través de las cadenas de bloques a través de autoridades portuarias, los departamentos de seguridad y operadores de terminales. Junto con los dispositivos IO, la cadena de bloques podría permitir la monitorización de los datos de los contenedores, aviones y camiones, las condiciones del transporte, como humedad, la temperatura, etc.

Actualmente, el proyecto SmartLong está desarrollando una solución de cadena de bloques para el tráfico de transferencia de datos operativo en el sector de logística. Financiado a través del programa Interreg Báltico Central, el Proyecto está liderado por Kouvola Innovation con socios en Suecia, la Agencia de Desarrollo del Condado de Valga de Tallin e IBM. Su objetivo es reducir los tiempos de tránsito de carga de extremo a extremo a lo largo de los corredores de la red central de la RTE-T en el Báltico. Los dispositivos de IO se conectan a los contenedores de transporte para llevar un registro de los movimientos reales y se añaden a un sistema de cadenas de bloques (Polvora, 2019)

Este registro seguro y único se comparte entre todas las empresas participantes a lo largo de la cadena de suministro, con el objetivo de mejorar los flujos operativos, la gestión de recursos y la planificación de la optimización de rutas. En el futuro, los datos podrían fluir sin problemas entre los sistemas operativos de gestión de la información de las empresas mediante sistemas de cadenas de bloques, dentro de un ecosistema transparente y cifrado de transacciones entre múltiples partes.

El objetivo que tiene toda empresa es superar a sus competidores, para ello los equipos de gestión de la cadena de suministro (SMC) estudian tecnologías como Big Data, Internet de las Cosas (IoT) y Blockchain. Gracias a estas tecnologías permiten a los administradores proporcionar y desarrollar productos/servicios complejos de la cadena de suministro más rápidamente y con mayor fiabilidad. Los equipos SMC pueden construir modelos complejos de una cadena de suministro (Ganne, 2018).

Por ejemplo, está creciendo la demanda de aeronaves, SMC se encarga del suministro de red de piezas de repuesto de aeronaves, compra y entrega para el mantenimiento de las aeronaves. Las piezas de repuesto de los aviones se envían a los centros de montaje individuales, estos están localizados globalmente. Todas y cada una de las partes vienen con una determinada expectativa de vida, con unos requerimientos específicos y atributos de mantenimiento. Con miles de piezas de repuesto, cientos de parámetros y número de fabricantes distribuidos por todo el mundo, el equipo SMC necesita tratar con una gran cantidad de datos. La utilización de un sistema descentralizado de Blockchain. Ayuda a mantener el inventario de las piezas del avión, revisar el mantenimiento y su uso.

Estas nuevas tecnologías basadas en las cadenas de datos ayudarán a los responsables de SCM a analizar la oferta, la demanda, la fuente de disponibilidad de las piezas de recambio y proporcionar métodos para adquirirlas de fuentes correctas.

La gestión de la cadena de suministro es la columna vertebral de cualquier sector industrial. Antes de llegar al producto final han pasado por diferentes fases denominadas cadenas de suministro de varios niveles. Como por ejemplo la industria de la aviación. En la mayoría de los casos, cuando no se cumplen los requisitos específicos se devuelven. Las bases de datos registrarán y actualizarán todas las transacciones que fluyan a lo largo de la cadena de suministro, aportando valor

añadido significativo al proceso de negocio a través de un flujo de mejor calidad. (Ganne, 2018).

2.6 SECTORES EN LOS QUE SE PUEDE APLICAR EL BLOCCHAIN

Este apartado se divide en 2 bloques.

Por una parte, la aplicación de la tecnología de bloques en el sector público tiene ámbitos muy interesantes y por otro lado el sector privado en el que se hace especial énfasis en el sector bancario.

2.6.1. APLICACIÓN DE LA TECNOLOGIA DE CADENAS DE BLOQUES EN EL SECTOR PÚBLICO

Las cadenas de bloques podrían tener un impacto notable en los gobiernos al hacer que ciertos servicios proporcionados por el estado sean más eficientes y transparentes. Esto incluye: el voto, el bienestar, los impuestos, etc. Demostrará el potencial que tiene esta tecnología y su contribución a fomentar que los sistemas de gobiernos sean más abiertos y responsables según destacó Emin Gun Sier, profesor de la universidad de Cornell en Nueva York, especializado en sistemas distribuidos." *Si se observa un gobierno que es opaco, que está cerrado detrás de las puertas, frente a uno en el que puedo inspeccionar lo que sucede detrás de él, es un asombroso paso hacia adelante, implementar esta tecnología de cadenas de bloques podría significar dormir mejor por la noche"*

Esta tecnología puede ayudar a reducir el error y aumentar la eficacia de la prestación de los servicios públicos. También puede actuar como vehículo de ayuda en la propiedad intelectual de los ciudadanos y empresas. El Blockchain podría servir como una funcionalidad de back office (oficina de respaldo) para racionalizar, coordinar las compras y las licitaciones entre todos los departamentos, administraciones y otros organismos del sector público (Cheng, 2017).

2.6.1.1 SALUD Y BIOFÁRMACOS

En el sector de la salud, los pacientes, médicos, hospitales y otros profesionales sanitarios podrían almacenar historias clínicas electrónicas en sistemas de gestión descentralizados basados en cadenas, en las que pueden cifrar información personal sensible y conceder acceso a las mismas únicamente a las partes autorizadas mediante las credenciales adecuadas.

La capacidad de registrar y autentificar datos médicos además de personalizar su uso para otras partes podría potenciar el valor informativo y económico de dichos datos. Podría estimular nuevos modelos de negocio para soluciones de conservación de la privacidad, medicina personalizada, puesta en común de datos con fines de investigación sobre medicamentos, tratamientos y salud pública (Kristeten, 2018).

Por ejemplo, la cadena de bloques podría tener un impacto en la rendición de cuentas y la transparencia en los procesos de información y gestión de los ensayos clínicos. Existen diferentes partes en las que debe circular un ensayo clínico (investigadores, agencias reguladoras, proveedores de medicamentos, gestores de datos, pacientes, etc.) Los investigadores podrían beneficiarse significativamente de compartir datos anónimos, conjuntos de datos o planes de análisis en ensayos clínicos a través de canales distribuidos y seguros. Los contratos inteligentes también podrían utilizarse para el control de la fase de ensayo clínico. Los pacientes podrían dar su consentimiento específico para el análisis de datos, por ejemplo, a condición de que la base de datos no se comparta con terceros o se utilice con fines comerciales (Kefa Rabah, 2018).

La confidencialidad de los datos son preocupaciones importantes en este sector, por lo que cualquier solución de cadena de bloques debe establecer sólidos mecanismos de privacidad de conformidad con la normativa de protección de datos. Por ejemplo, desde el punto de vista del paciente, sus datos pueden ser seudónimos anonimizados mediante mecanismos robustos de desidentificación y criptografía. Los pacientes podrían implementar consentimientos dinámicos a través de contratos inteligentes, es decir, definiendo los derechos de acceso a los datos, indicando, por ejemplo, el tipo de datos que deben proporcionarse, los terceros autorizados, las condiciones de revocación o los límites de almacenamiento. En estas condiciones se podrían compartir más fácilmente en sus registros y pedir a diferentes médicos una segunda opinión.

En general, las cadenas de bloques podrían introducir cambios en la forma en que se utilizan y gestionan los datos en el sector de la salud. Hoy en día, los datos de salud están fragmentados, silenciados y opacos. Están bajo el control de unos pocos actores dominantes. El Blockchain podría proporcionar registros permanentes para ser verificados, con acceso mucho más rápido y con mayor seguridad y apertura para todos los involucrados o con la autorización adecuada.

2.6.1.2 TRANSACCIÓN DE TERRENOS Y PROPIEDADES

El Blockchain tiene implicaciones específicas en el contexto de las administraciones públicas y los gobiernos, por ejemplo.

En las administraciones públicas, numerosos registros que contienen datos de ciudadanos, impuestos o títulos de propiedad son costosas en términos de mantenimiento, propensos a errores humanos y expuestos a fallos. Las administraciones públicas pueden utilizar esta tecnología para el registro distribuido de documentos y activos en lugar de registrarlos únicamente de forma centralizada. Se argumenta que los beneficios de la tecnología de cadenas de bloques para los servicios incluyen la capacidad de proporcionar servicios a medida para los ciudadanos específicos, una mayor confianza en los gobiernos y una mejor automatización transparencia y auditabilidad. (Swan, 2017)

El proceso de cambiar o agregar un título de propiedad a través de este sistema se muestra en los siguientes pasos según el artículo de la Comisión Europea sobre la evaluación de impactos multidimensionales d las tecnologías, (Kakavand, 2019).

1. Un ciudadano puede iniciar la solicitud ante un notario para el registro o verificación de un extracto de título de tierra.

2. El notario registra los títulos de propiedad en la cadena privada de bloque de datos.

3. Se garantizan la integridad de todas las operaciones.

4. Los grandes centros de acceso y distribución del tráfico de Internet, NAP, (Network Access Point) proporciona al ciudadano un certificado digital de su activo, apoyado por una prueba criptográfico de la originalidad del extracto, publicada en la cadena de bloques privada.

5. Un ciudadano puede verificar si un título de tierra es legítimo.

Los sistemas de Blockhain puede permitir una mayor eficiencia, transparencia y programabilidad de la financiación pública, especialmente añadiendo las funcionalidades de registro distribuido, gestión de socios, intercambio de información y ejecución automática a través de contratos inteligentes. Operando como redes descentralizadas permitiendo a todos los usuarios gestionar sus transacciones sin tener que depender de terceros. La seguridad y la responsabilidad que proporcionan las cadenas de bloques.

2.6.1.3 EDUCACIÓN

La tecnología Blockchain aplicada a la educación supondrá una mayor seguridad y transparencia en los certificados educativos, en los datos de los estudiantes, datos de los profesores etc. Los registros de todos estos datos deben estar recogidos en bases de cadenas de bloques que asegurarán la verificación de los mismos. Esto ayudará a confiar en los certificados educativos de todos los estudiantes y se actualizarán automáticamente con la aplicación de la tecnología de bloques. El certificado será verazmente verificado.

La Plataforma EduCTX propone una cadena de bloques basado en una plataforma de créditos de educación. Esta plataforma pretende crear un sistema de créditos de calificación de educación superior, basada en código abierto, dirigido a un punto de vista globalmente unificado para los estudiantes y organizadores. Los estudiantes se benefician de una visión única y transparente de los cursos completados, mientras que las instituciones de educación superior tienen acceso a los datos actualizados independientemente de los orígenes educativos del estudiante (Turkanovìc, M. 2017).

Esta es una propuesta basada en el sistema de red P2P distribuido. Transfiere los sistemas de calificación a una base de cadenas de bloques eficiente y simplificada y permite evolucionar hacia un sistema unificado de educación superior.

2.6.1.4 REGISTRO CIVIL

Todos los acontecimientos vitales, como los nacimientos, defunciones o matrimonios, quedan certificados y registrados en las plataformas a través de la tecnología Blockchain. Este uso supondrá un beneficio para el ciudadano ya que contará con registros únicos y nadie podrá interferir o manipular los registros. Están protegidos y son confidenciales y proporcionará a ambas partes sacarán rendimiento de esta tecnología.

2.6.2 SECTOR PRIVADO

La tecnología de la cadena de bloques se está desarrollando a un ritmo rápido, a pesar de su juventud, muy pocas personas conocen las capacidades de la tecnología más allá de las criptomonedas. La tecnología está cambiando muchas industrias existentes y su introducción está motivada supuestamente por el Crak financiero de 2008.

A continuación, se nombran y se explican los sectores privados que pueden tener una gran repercusión y cómo va a afectar esta tecnología.

2.6.2.1. SECTOR BANCARIO

La tecnología Blockchain fue implementada en el sector bancario para resolver los problemas del doble gasto, la cuestión de confianza, consenso sobre una versión correcta del historial de transacciones y evitar que alguien hago una operación sin nuestro permiso.

La cadena de bloques es un sistema de actualización constante. En un libro contable se registran todas las transacciones dentro de una red P2P de tal manera que no puede ser ni alterado ni manipulado. Es transparente de forma que las operaciones se realicen de forma descentralizada y eliminando la necesidad de una autoridad central para verificar la confianza y valor de la transferencia. La aplicación más conocida por esta tecnología es la de Bitcoin, hace unos años creció el interés por esta criptomoneda, sin embargo, ahora ha disminuido el interés debido a la alta volatilidad de sus precios (Buitennheck, M. 2016).

Cada vez hay más bancos que están creando sus propias criptomonedas, muchas de ellas apoyan los valores de la propia entidad realizando la criptomoneda estable en valor ante el mercado para poder usarla y utilizar estas bondades en su día a día y control sobre la masa monetaria de su negocio.

Blockchain tiene un gran potencial para ser una fuerza disruptiva en el sector financiero. Ya es posible ver dónde podría haber un impacto y ver dónde hay un valor comercial real. Esta tecnología tiene la capacidad de marcar la diferencia es muchas de las capas de la industria financiera. Aunque todavía se está en el inicio de muchas de las fases de experimentación se espera que paso a paso se resuelvan casos complejos (Town, S. 2018).

2.6.2.2 SECTOR DE LAS ASEGURADORAS

Este sector es uno de los más beneficiados por esta nueva tecnología y en este caso por la automatización de los Smart Contracts.

Por ejemplo, si hablamos de alimentos, un camión frigorífico que transporte alimentos puede ser monitorizado desde el exterior y utilizar un medidor de temperatura y saber si se ha roto la cadena de frio por un fallo del conductor.

2.6.2.3 APLICACIONES PARA LOS DISTRIBUIDORES Y MINORISTAS DE ALIMENTOS

Los sistemas basados en cadenas de bloques podrían proporcionar un registro preciso y actualizado de los productos a lo largo de su producción, envío y venta, lo que ayudaría, por ejemplo, en el caso de emergencias sanitarias, a determinar con mayor rapidez y precisión los puntos de contaminación (Behnke, K. 2019). También podría mejorar la eficiencia de la gestión en tiempo real de las existencias y la entrega de alimentos, ayudando a determinar dónde y por qué se tiran o si han caducado, con lo que se reducirá potencialmente los desperdicios.

La trazabilidad y el control de la calidad de la forma en que se cultivan, almacenan, inspeccionan y transportan los productos. Podrían mejorar la rendición de cuentas de todas las partes interesadas, incluyendo los proveedores, los reguladores y los consumidores. En un sistema de cadena de bloques, todo el mundo tiene acceso a una copia del mismo registro actualizado, de modo que las partes pertinentes pueden verificarlo o inspeccionarlo en cualquier momento o en momentos específicos. Esto confiere un alto nivel de confianza en las transacciones entre empresas diferentes.

Las autoridades aduaneras, los titulares de derechos y los operadores logísticos también podrían utilizar estos registros de activos resistentes y compartirlos para tomar decisiones más eficaces y adoptar medidas más rápidas contra las infracciones, las falsificaciones y las mercancías robadas. Según un artículo publicado por el European Commission, Joint Research Centre, por Pólvora, A (2019) la cadena de bloques podría facilitar la lucha contra la falsificación y la observación de los derechos de propiedad intelectual mostrando a todos los integrantes de la cadena de suministro quién es el propietario y quién es un licenciado autorizado, lo que permitiría validar un producto autentico y distinguir los productos falsos. Un libro de contabilidad distribuido que contenga información sobre los productos para permitir la autentificación de procedencia, ya que el libro de contabilidad puede registrar detalles objetivamente verificables sobre el origen, el calendario y la producción de los bienes. Esto tendría la ventaja de dar confianza y tranquilidad a las empresas, las autoridades y a los ciudadanos. Por ejemplo, un uso para luchar contra las falsificaciones es la adición a los productos de etiquetas escaneables conectadas en cadena, sellos o impresiones a prueba de manipulaciones.

Los propietarios de marcas pueden informar a las autoridades aduaneras sobre las características de seguridad correctas que deben tener los productos auténticos, lo que permitiría a los funcionarios de fronteras comprobar fácilmente si un producto tiene estas características, evaluando así si es falsificado. De manera similar, esta técnica podría utilizarse para las marcas de certificación de los productos cumplen con las normas prestablecidos.

Por ejemplo, los productos de alto valor, raros y lujosos, como las denominaciones de origen protegidas están especialmente protegidos por esta tecnología. La autenticidad de la procedencia de una botella de vino en particular, por ejemplo, podría garantizarse mediante una cadena de bloques a través de un registro de su “huella digital” única que incluya fotografías de alta resolución, registros de propiedad y almacenamiento e incluso una certificación de la botella real.

Los sistemas basados en cadenas de bloques ofrecen una historia irrevocable, autentificada con sello de tiempo de los productos para llevar un registro no solo de la seguridad y autenticidad de los productos, sino también de las normas éticas. La prueba de origen y el cumplimiento de las normas medioambientales, el etiquetado ecológico, el comercio justo u otras características similares podrían ayudar a los consumidores a tomar decisiones con conocimiento de causa y orientar a las empresas hacia modelos de negocio más sostenibles.

Esta tecnología podría ser la base de ecosistemas más abiertos de productores, cultivadores, comerciantes, empresas de logística, organizaciones de normalización de productos o propietarios de sistemas de certificación, autoridades de supervisión tales como autoridades de acreditación y autoridades de seguridad alimentaria, proveedores de servicios financieros tales como bancos e inversores y consumidores.

2.6.2.4 SISTEMAS ENERGETICOS

Aprovechando su característica de descentralización, la cadena de bloques podría ofrecer alternativas a las ineficiencias y pérdidas de soluciones centralizadas de largos sistemas de datos, apoyándose principalmente en la infraestructura energética de producción masiva. La cadena de bloques múltiples que las partes se coordinen entre sí y ejecuten las operaciones de forma abierta y transparente, permaneciendo las diferencias en función del tipo de arquitectura pública o privada elegida. Muchos lo ven como una infraestructura de coordinación y gestión de datos que podría impulsar la aparición de un sistema descentralizado de transacciones y suministro de energía.

La aplicación de las cadenas de bloques en el sector energético también puede basarse en el uso de contratos inteligentes para gestionar automáticamente los flujos de oferta y demanda en tiempo casi real y hacia un uso optimo uso de la energía disponible. Cuando estos contratos inteligentes se incorporan a otras tecnologías, como contadores inteligentes o sensores, pueden preverse escenarios de negociación entre pares. Los generadores domésticos eléctricos, las baterías, las centrales eléctricas o cualquier punto de la red eléctrica podrían vender y comprar energía de forma constante y automática para equilibrar el mercado. Varias empresas están probando plataformas de comercio basadas en la cadena de bloques para la energía eléctrica el gas natural y otras fuentes que podrían conectar a los grandes productores y fábricas minoristas.

2.7 SMART CONTRACTS

Los Smart Contracts o también llamado criptocontratos son un programa de ordenador que se utilizan para transferir los activos o monedas digitales entre las partes bajo ciertas reglas. Lo hace para determinar las condiciones y también pueden hacer cumplir esos acuerdos. Estos contratos inteligentes se almacenan en cadenas de bloques y utilizan una tecnología Blockchain para almacenar estos contratos por su inmutabilidad y seguridad. Si hay una transacción que se debe de producir, el contrato inteligente determina dónde se debe transferir, devolver la transacción o dónde se originó esta transacción. Ali Haward (2018).

Los contratos inteligentes pueden utilizarse para hacer muchas cosas interesantes. Se utilizan para la (tokenización), son los motores que están detrás de las criptomonedas y otros activos digitales. Se pueden utilizar para codificar y automatizar procesos de negocio que pueden ser compartidos y ejecutados entre múltiples partes, ofreciendo una mayor confianza y fiabilidad en el proceso, a menudo con ganancias significativas en eficiencia y reducción de costes. Del mismo modo, se pueden utilizar en contratos inteligentes para acuerdos entre partes que impliquen transferencia de valor y otros tipos como acuerdos de custodia o de pago frente a entrega de una mercancía. Permite que los contratos sean transparentes y se ejecuten automáticamente según las condiciones predeterminadas, lo que dificulta o imposibilita que una de las partes se retracte. Harris P (2017)

Si se añaden varios tipos de “inteligencia” a los contratos inteligentes, ya sean simples o complejos, basados en el IA (Inteligencia artificial), se puede hacer que estos programas sean altamente autónomos. Capaces de reaccionar a su entorno y tomar decisiones, incluso sobre la compra y la venta, por su cuenta. De forma similar puede modificar las reglas para estructuras organizativas complejas en contratos inteligentes, creando una organización confiable, inmutable y resistente a la manipulación en la que todos los miembros están sujetos a las reglas a través del código. Estas organizaciones pueden incluso automatizarse, creando organizaciones autónomas descentralizadas (DAO) que, una vez liberadas en la naturaleza, realizan sus actividades por su cuenta sin intervención humana. Huckle, S (2016).

2.7.1 VENTAJAS DE LOS CONTRATOS INTELIGENTES

Los contratos inteligentes (Smart Contracts) tienen las siguientes ventajas en comparación con los contratos convencionales según el artículo escrito por (Xie 2019)

- Reducen los riesgos: debido a la inmutabilidad de las cadenas de bloques, los contratos inteligentes no pueden ser alterados con arbitrariedad una vez que son emitidos. Además, todas las transacciones que se almacenan y duplicados a lo largo de toda la cadena de bloques distribuidos son trazables y auditables. Como resultado, los comportamientos como los fraudes financieros pueden ser muy moderados.

- Reduciendo los costes de administración y servicio: las cadenas de bloques nos aseguran confianza de todo el sistema, mediante mecanismos de consenso distribuido sin pasar por un bróker central o mediador. Los contratos inteligentes almacenados en cadenas de bloques pueden ser lanzados automáticamente de forma descentralizada. Por lo tanto, la administración y los servicios de los costes debidos a la intervención de un tercero pueden ahorrarse.

- Mejorar la eficiencia de los procesos de negocio: La eliminación de la dependencia del intermediario puede mejorar significativamente la eficiencia de los procesos de negocio. La liquidación financiera será automáticamente completada de forma paritaria una vez que la predefinición se cumpla (por ejemplo, el comprador confirma la recepción de los productos). Como resultado, el tiempo de entrega puede ser significativamente reducido.

Los contratos inteligentes están impulsando un amplio aspecto de aplicaciones que van desde el Internet industrial hasta el financiero. Los contratos inteligentes tienen un gran potencial para dar nueva forma a los contratos convencionales y procedimientos de negocio. Hay una serie de retos para resolver. Por ejemplo, las cadenas de bloques aseguran el anonimato de las partes del contrato, la privacidad de toda la ejecución del contrato no puede ser preservada ya que todas las transacciones están disponibles globalmente. Ahmed Kosba (2018).

2.7.2 BLOCKCHAIN Y SMART CONTRACT

Los contratos inteligentes se construyen sobre tecnología Blockchain, asegurando la correcta ejecución de los contratos. Las cláusulas contractuales que están incorporados en los contratos inteligentes aplicarán automáticamente cuando se cumple una determinada condición. Las cadenas de bloques permiten que los contratos inteligentes se implementen esencialmente sobre las cadenas de bloques. Las cláusulas contractuales aprobadas se convierten en programas informáticos ejecutables. La ejecución de cada extracto de contrato se registra como una operación inmutable almacenada en las cadenas de bloques (Liang, J. 2017).

Estos contratos garantizan un control de acceso adecuado y el cumplimiento. En particular, los desarrolladores pueden asignar permisos de acceso para cada función del contrato una vez que la condición se ha cumplido.

2.7.3 CICLO DE VIDA DEL CONTRATO

Podemos asignar el ciclo de vida del Contrato Inteligente consta de cuatro fases principales según por Weili Chen (2019) y desarrolladas por Josias Dewey (2019).

1 Creación de contratos inteligentes: a la hora de crear un contrato hay varias partes involucradas. Primero se debe negociar sobre las obligaciones, derechos y

prohibiciones de las partes. Después de realizar las negociaciones se llega a un acuerdo. Los abobados ayudarán a las partes a redactar el acuerdo contractual inicial. Los ingenieros de software convertirán este acuerdo escrito en lenguajes naturales en un contrato inteligente escrito en lenguajes de ordenador, incluyendo lenguajes declarativos y lenguajes de reglas basados en la lógica. De forma similar al desarrollo de software de ordenador.

El procedimiento de conversión de contratos inteligentes se compone de diseño, implementación y validación. La creación de un contrato inteligente implica numerosas rondas de negociaciones y múltiples partes indicadas, como los interesados, abogados e ingenieros de software.

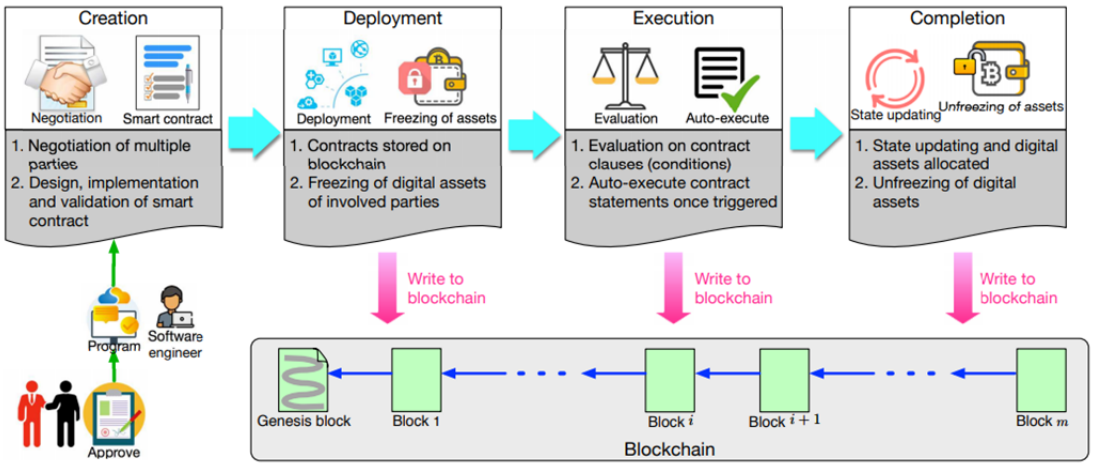
2. Implementación del contrato inteligente: estos contratos son almacenados en las cadenas de bloques y no pueden modificarse debido a la inmutabilidad de las cadenas de bloques. Cualquier corrección o modificación requiere la creación de un nuevo contrato. Una vez que los contratos inteligentes se despliegan en las cadenas de bloques, todas las partes pueden acceder a través de ellos.

Todos los activos digitales de ambas partes involucradas en el contrato se bloquean mediante la congelación de las correspondientes carteras digitales. Las partes pueden ser identificadas por carteras digitales.

3. Ejecución de los contratos inteligentes: una vez que las cláusulas han sido evaluadas. Los procedimientos se ejecutan automáticamente. En estos contratos, el número de declaraciones con conexiones lógicas está unido a una función por la cual si se cumple se ejecuta automáticamente y es validada por los *mineros* en las cadenas de bloques. Todos los registros quedan almacenados en las cadenas de bloques.

4. Finalización de un contrato inteligente: después de que el contrato inteligente se ha ejecutado, los nuevos estados de todas las partes involucradas son actualizados. Como consecuencia, las transacciones durante la ejecución de los contratos inteligentes, así como los estados actualizados se almacenan en cadenas de bloques. Mientras tanto, los activos digitales han sido transferidos de una parte a otra siendo desbloqueados y así es como el Smart contract ha completado todo el ciclo de vida.

Imagen 5: Ciclo de vida de un Smart Contract, sus 4 fases: Creación, implementación, ejecución y finalización



Fuente: An overview on Smart Contracts Zibin Zheng,Shaoan Xie

2.7.4 PRIVACIDAD Y SEGURIDAD

Las plataformas de cadenas de bloques carecen de mecanismos para preservar la seguridad ya que se difunden los registros de las transacciones a través de todas las redes de las cadenas de bloques. Por lo tanto, todas las transacciones son visibles para todos en las redes. Cada vez hay más sistemas de cadenas de bloques que utilizan seudónimos públicos para mejorar el anonimato de sus transacciones. Kristeten,N (2018)

Los sistemas de contratos inteligentes también tienen su vulnerabilidad de software, pueden sufrir ataques. La ejecución de los contratos inteligentes se ejecuta en la parte superior de la cadena de bloques sufriendo vulnerabilidad en el sistema. Por todo ello se han realizado avances recientes de mejora para el desafío en privacidad y seguridad.

En cuanto a la privacidad de los contratos inteligentes, Ahmed Kosba propuso Hawk, un sistema de contratos inteligentes descentralizados para establecer contratos perseverando la seguridad. Consiste en codificar un contrato en un protocolo criptográfico automáticamente. Este programa tiene dos partes. Una parte privada y una parte pública, esta última es utilizada para proteger a los usuarios. Este sistema encripta la información de la transacción y verifica la corrección de las transacciones utilizando pruebas de conocimiento cero (es decir sin ver el contenido de las transacciones. Ahora sí el anonimato de las partes se puede asegurar en los contratos inteligentes. Los algoritmos cartográficos avanzados se utilizan en enigma que distribuye los datos de la cadena de bloques en diferentes nodos. Cada nodo es una transacción.

Respecto a la seguridad, se han hecho esfuerzos para resolver problemas de seguridad en las cadenas de bloques. En concreto, el sistema operativo SABRE ayuda a proteger el enlace entre los clientes y relé mediante la colocación adecuada de los relés apropiadamente. Mientras tanto el sistema operativo SABRE adopta el código de diseño de hardware y software a través unas SND (redes definidas de software) para reducir la carga de tráfico en los relés. Los resultados experimentales demuestran la eficacia contra los ataques BGP (Border Gateway Protocol). Ahmed Kosba (2018).

2.7.5 PLATAFORMAS DE DESARROLLO DE CONTRATOS INTELIGENTES

Últimamente se han desarrollado contratos inteligentes en plataformas basadas en cadenas de bloques. Etas plataformas proporcionan a los desarrolladores con interfaces simples para construir aplicaciones de contratos inteligentes. A continuación, y siguiendo las pautas desarrolladas por Zibin Zheng (2019) Shaoan Xie (2019) se enumerarán y se explicarán las 5 plataforma de contratos inteligentes más importantes:

1 Ethereum: esta es la principal plataforma descentralizada que puede ejecutar contratos inteligentes. Ethereum ha desarrollado el lenguaje Solidity, se utilizan para el lenguaje de las criptomonedas y los contratos inteligentes escritos. Ejecuta contratos inteligentes en la red virtual. El tiempo para la ejecución de la transacción es de tan solo tres segundos y medio.

2. Hyperledger Fabric: es una plataforma distribuida de libros mayores para la ejecución de contratos inteligentes. Es diferente de Ethereum. Hyperledger adopta el contenedor Docker para ejecutar el código. Los contenedores pueden soportar aplicaciones de contratos inteligentes. Fabric es compatible con los lenguajes de programación convencionales de alto nivel como Java y Go. Fabric está diseñado para soportar aplicaciones empresariales generales, la red de cadenas de bloques de Fabric es privada. Los usuarios deben ser autorizados a unirse a la red por las autoridades de certificación (CA). Una vez que el usuario se ha registrado, tiene para solicitar certificados de transacción de la autoridad (TCA). El consenso puede alcanzarse fácilmente dentro de la red de bloqueo permitida.

3. Corda: está especializado en aplicaciones de monedas digitales, se utiliza como una plataforma distribuida para el ahorro y procesa registros históricos de activos digitales. La plataforma Corda adopta lenguajes de programación de alto nivel como Java y se ejecutan sobre máquinas virtuales. Corda apoya a las plataformas privadas, en las que las empresas establecen una red de autor para intercambiar activos digitales de forma privada. Corda adopta el algoritmo de consenso. En lugar de emitir globalmente en cadenas de bloques utiliza el mecanismo de mensajería punto por punto. Los usuarios tienen que especificar a los receptores de los mensajes y la información detallada a enviar.

4. Stellar: es una plataforma parecida a Corda, para aplicaciones de moneda digital. Si la comparamos con Ethereum, Stellar es más simple y accesible. Utiliza diferentes idiomas como son Pyhton, JavaScript y PHP. El coste de ejecución de una transacción es de 0,000002 dólares y el tiempo de ejecución de la transacción es de 5 segundos, Stellar adopta el modelo basado en la cuenta de datos, ha desarrollado su propio algoritmo.

5. Rootstock: se ejecuta sobre Bitcoin, utiliza una ejecución rápida de las transacciones. Esta plataforma es compatible con Ethereum. Roostock ha desarrollado su propio sistema de máquinas para ejecutar contratos inteligentes, el modelo que utiliza se basa en la cuenta de datos.

2.7.6 APLICACIONES DEL SMART CONTRACT

Los contratos inteligentes tienen un amplio abanico de aplicaciones que van desde el Internet hasta la economía de intercambio. Podemos clasificar y desarrollar según Huckle (2016) las principales características y cómo influyen en los sectores de la economía.

- El Internet de las cosas (IO): esta es una de las más importantes ya que son numerosas las aplicaciones que puede abarcar, desde la cadena de suministro, minoristas, control de inventario, sistemas de salud, bibliotecas, etc.

  La principal iniciativa es integrar objetos “inteligentes” en internet para proporcionar servicios a los diversos usuarios, automatizar varias transacciones comerciales de forma implícita. Por ejemplo, la mayoría de los fabricantes actuales mantienen su IO ecosistemas de manera centralizada. Los contratos inteligentes pueden ayudar a acelerar en las cadenas de suministro convencionales, automatizar la contratación derechos y obligaciones durante el pago y la entrega de mercancías mientras que todas las partes en el proceso son de confianza.

- Seguridad en el sistema de distribución: los contratos inteligentes pueden aportar beneficios en la mejora de seguridad de los sistemas de distribución. Las principales amenazas son los DdoS (ataque de denegación de servicio) los atacantes intentan entrar en el equipo con ataques que inundan el equipo con peticiones superfluas para sobrecargar los sistemas, intentando interrumpir constantemente.
  Actualmente se ha elaborado un mecanismo para disminuir los DdoS pudiendo abordar los ataques de manera totalmente descentralizada, consiste en que cuando un servidor es atacado, las direcciones IP informan a los demás nodos de las direcciones donde está siendo atacada y esta información se almacenará automáticamente e inmediatamente se aplican políticas de seguridad, como, por ejemplo, el filtrado de usuarios maliciosos.

- Finanzas: los contratos inteligentes pueden reducir enormemente el potencial de los riesgos financieros, reducir el coste de administración y servicios y mejorar la eficiencia de los servicios financieros. A continuación, explicamos los beneficios que pueden aportar en el mundo de las finanzas:

- Mercados de capitales y banca de inversión: los mercados de capital han sufrido una continua liquidación de ciclos, con los contratos inteligentes se pueden acortar los periodos de veinte días a una semana o diez días, por lo tanto, aumentaría el atractivo de clientes y esto llevaría a unos ingresos en el futuro.

- Banca comercial y minorista: los contratos inteligentes pueden traer beneficios a la industria de los préstamos hipotecarios que son complejos en el proceso de origen, financiación y servicio, causando costes extras y los retrasos. Con los contratos inteligentes se digitaliza los documentos legales en las cadenas de bloques y se reducen los costes.

- Seguros: aplicar los contratos inteligentes al sector seguros puede reducir los gastos generales de procesamiento y ahorrar los costes de gestión de reclamaciones. Por ejemplo, en el seguro de automóviles hay muchas partes implicadas, proveedores de transporte, clientes, aseguradoras, etc. Con los contratos inteligentes se puede automatizar la liquidación de la reclamación de los documentos legales en un libro construido, por lo tanto, se consigue mejorar la eficiencia y reducir el periodo de tramitación de solicitudes y ahorrar costes. En el caso de la aseguradora AXA ha creado un retraso de vuelo basado en un contrato inteligente de Ethereum. Los pasajeros que compran seguros de vuelo firman automáticamente una póliza de seguro inteligente que conecta directamente con la base de datos del tráfico aéreo global. EN caso de que el sistema perciba un retraso de más de dos horas, se activa automáticamente una función del contrato inteligente por lo que a los pasajeros se los indemniza al instante.

- Procedencia de datos: es necesario asegurar la calidad de la información en la investigación científica y de la salud pública, informar sobre la falsificación de datos clínicos. La idea principal de la procedencia de los datos es almacenar la información de los metadatos de origen, derivación y transformación. Hay una serie de desafíos respecto a la procedencia de datos. Las herramientas de registro como Progger y el módulo Trusted Platform almacenan actividades de datos junto con información confidencial.
  Lisa Morhaim (2019) elaboró a partir de un dato, un sistema de procedencia basado en contratos inteligentes y cadenas de bloques, consiste en que los investigadores puedan enviar sus datos encriptados a este sistema, en cuanto hay un cambio en los datos, los contratos inteligentes están autorizados para rastrearlas transformaciones hechas a los datos.

  Xueping Liang (2016) desarrolló la plataforma ProvChain, una arquitectura de procedencia de datos basadas en cadenas de bloques en un entorno de nube con una mayor privacidad y disponibilidad de modo que cualquier modificación de datos sea responsable. Hay 3 procedimientos: recolección de datos de

  procedencia, almacenamiento de datos y validación de la procedencia de datos. Esta plataforma ofrece datos a prueba de manipulaciones, privacidad y

fiabilidad de datos. El contrato inteligente puede ser utilizado para proteger los derechos de propiedad intelectual de los medios digitales creativos.

Por ejemplo, cada producto digital está tocado por una marca de agua digital única. En caso de que haya alguna infracción, como, por ejemplo, el comprador vende el producto digital a otros sin el permiso del creador. El oficial de la ley puede rastrear el archivo ilegal con el archivo original mediante la extracción de la marca de agua digital y la comparación de la dirección de la cartera digital con la del comprador. Como resultado, será fácilmente de identificar la infracción de los derechos de propiedad.

- Economía Colaborativa: tiene muchos beneficios como la reducción de los costes de consumo mediante el préstamo y el reciclaje de artículos. Mejorando la calidad del servicio y reduciendo los impactos medioambientales. Los contratos inteligentes pueden reformar potencialmente la economía.

  Bonger (2016) propone una novedosa plataforma de economía basadas en contratos inteligentes Ethereum basada en permitir a los usuarios registrar y compartir sus artículos sin un tercero de confianza. La fusión de IO (Internet de las cosas) y los contratos inteligentes también pueden avanzar compartiendo aplicaciones de economía.

  Huckle (2016) desarrolló aplicaciones como el pago automático peer-to-peer (P2P), sistemas de viaje, gestión de activos digitales plataformas de cambios de divisas. Principalmente se centran en resolver la fuga de privacidad de sistemas basados en cadenas de bloques. Tiene una gran eficacia.

- Sector público: los contratos inteligentes junto con la tecnología Blockchain puede reformar la gestión del sector público y es precisamente esta tecnología la que evita la falsificación de datos y proporciona una información pública, por ejemplo, una licitación pública. La integración de cadenas de bloques y contratos inteligentes `pueden demostrar identidades de los licitadores y las entidades oferentes, automatizar el proceso de licitación, proporcionar apoyos de auditoria y revisión.

  Existen diferentes desafíos, uno de ellos son verificar la identidad del usuario y preservar la privacidad del usuario. Los contratos inteligentes ofrecen la solución a sistemas de votación electrónica, este es un sistema de votación basado en la cadena de bloques llamado Follow Vote 8 para verificar las identidades de los usuarios sin revelar su privacidad.

  McCorry (2017) utiliza el conocimiento de protocolos para que se puedan contar los votos sin un tercero de confianza para construir un sistema de votación justo basado en contratos inteligentes. De esta manera los votos pueden mantenerse en privado mientras que las identidades de los usuarios son verificables al mismo tiempo.

Los usuarios pueden proteger su información privada a través de contratos inteligentes que otorgan permisos de acceso a otros usuarios por clausulas programables. Todas las transacciones quedan registradas en las cadenas de bloques y no puede ser ni manipulado ni eliminado.

2.8 IDENTIDAD DIGITAL

Toda persona tiene derecho desde que nace a poseer una identidad donde se especifique sus datos como son, nombre, apellido y otros datos de interés general que sirvan para identificarlo en una sociedad.

Hay pocas cosas más importantes para el funcionamiento de una sociedad y de una economía que la identidad. Sin una forma de identificarnos y de identificar nuestras posesiones difícilmente seriamos capaces de construir grandes naciones o crear mercados globales. Drummond Reed (2017)

Cuando hablamos de identidad digital estamos haciendo referencia a como una persona se idéntica en Internet o utiliza diferentes herramientas telemáticas. Hoy en día el control de la identidad digital se realiza de manera centralizada. Al ser centralizada se pierde el control sobre esta información y es nuestra identidad que almacena nuestra identidad la que lo gestiona.

Desafortunadamente hay precedentes y cada vez más graves de problemas con el funcionamiento de la identidad digital.

Apostar por una gestión descentralizada en la identidad digital para que permita gestionar libremente a los usuarios elegir con quien comparte y como se comparte. Todo esto nos permite evitar que algunas empresas den datos e información a terceros sin tener un conocimiento de ello.

Gracias a una combinación de avances tecnológicos, incluyendo la mejora en los Smart Phones, avances en criptografías y la aparición de la cadena de bloques, ahora es posible construir nuevos marcos de identidad basados en el concepto de identidades basados en el concepto de identidades descentralizadas.

A todos nos gusta pensar que sabemos quiénes somos, cuando los demás nos identifican no tienen acceso a nuestro sentido central de nosotros mismos. En cambio, necesitan confiar en varios tipos de información que les proporciona o que son capaces de descubrir nuestro nombre, por ejemplo. Kakavand, H (2017)

Internet se construyó sin una forma estándar y explicita de identificar personas u organizaciones. Así que los sitios web simplemente empezaron a ofrecer sus propias cuentas locales con nombres de usuarios y contraseñas, desde entonces ha sido la solución predominante desde entonces. Poco a poco internet se ha ido expandiendo enormemente y cada vez hay más usuarios que interactúan, por lo que se ha vuelto insostenible.

En estos momentos, existe una creciente ineficiencia económica cuando las organizaciones de alrededor del mundo tienen que recoger, almacenar y proteger el mismo tipo de datos personales en sus propios silos.

2.8.1 NORMATIVAS EUROPEAS RESPECTO A LA IDENTIDAD DIGITAL

El reglamento más importante que trata de la identidad de la UE es el reglamento de Identificación, Autenticación y Servicios Fiduciarios Electrónicos (EIDAS). Este reglamento tendrá un profundo impacto en el marco de la identidad descentralizada. Sobre todo, en lo que se refiere a las credenciales de identidad emitidas y reconocidas por el gobierno.

Los avances técnicos y las normas son obviamente importantes para la aplicación de un nuevo marco de identidad digital, como ocurre con tantos otros aspectos de la tecnología, las cuestiones jurídicas y reglamentarias serán igualmente de importantes. Este es ciertamente el caso en el espacio de la identidad, toca muchos aspectos clave de nuestra vida personal y económica. Bogner (2016)

Si bien la identidad afecta al panorama jurídico y reglamentario en muchos ámbitos, a nivel de la UE hay 2 regímenes reglamentarios que son particularmente importes: el Reglamento General de Protección de Datos (GDPR) y el Reglamento de Identificación, Autenticación y Servicios de Fideicomiso Electrónicos (Eidas).

Etas podrían ser credenciales verificables, pero podrían también comunicar los datos en una cuenta de medios de comunicación social, un historial de transacciones en un sitio de comercio electrónico.

¿A qué desafío tecnológico nos enfrentamos? Se trata de ideas enigmáticas, hacer que funcionen será un desafío tecnológico de enormes proporciones. Para llegar a aplicarlo sería necesario para aplicar un marco de identidad descentralizada. Esto incluye mecanismos que permitan a los individuos crear sus propias identidades, a menudo denominados identificadores descentralizados (DID) así como medios para almacenar datos personales o centros de identidad. También necesitaríamos “carteras” digitales u otros agentes de usuario que permitan a las personas gestionar y utilizar sus identidades,

Aunque la cadena de bloques no es necesaria para la identidad descentralizada, puede ser una solución poderosa para diferentes aspectos del marco de identificación descentralizada. Esto incluye el apoyo a la creación y registro de DID, la certificación notarial de credenciales, la provisión de una infraestructura descentralizada para el control de acceso y el consentimiento para el uso de datos y la posible vinculación de credenciales a contratos inteligentes para, por ejemplo, desencadenar pagos automáticos.

Para crear una economía digital, necesitamos tener tipos de pruebas similares o credenciales en el mundo digital.

Un problema es que el panorama actual de la identidad digital está extremadamente fragmentado. Cuando navegamos por internet se requiere que los usuarios hagan

malabarismos con todas las diferentes identidades asociadas a sus nombres de usuario u otros alias, la mayoría de los cuales no están fuertemente relacionados con sus identidades reales.

Hay un problema grave y son los datos relacionados con la identidad no son seguros. Últimamente nos hemos acostumbrado a las notificaciones semanales de violación de datos que relevan datos confidenciales de los usuarios en masa a hackers, los estafadores pueden crear identidades fraudulentas con facilidad y utilizarlas para cometer robos, incluyendo el robo de identidades de los otros, La completa falta de control que tenemos sobre nuestros datos personales, cuando estamos en línea y que pueden ser y son utilizados para perfilarnos.

No solamente son los individuos luchan contra las deficiencias del actual régimen de identidad digital. Las empresas se enfrentan a costes y complejidades masivas, por no hablar de los riegos normativos y de otro tipo. Proteger los datos de los usuarios como al verificar las identidades de las contrapartes con las que se trata ya sean clientes, proveedores, socios o competidores.

Los gobiernos también tienen motivos para desear mejoras en la forma en que se gestiona la identidad digital. Ya sea para identificar correctamente a los ciudadanos con el fin de proporcionarles credenciales reconocidas por el gobierno, para distribuir correctamente los beneficios, para hacer posible el voto electrónico o para combatir delitos como la financiación del terrorismo o el blanqueo de dinero, los gobiernos dependen en gran medida de las identidades digitales. Ellos querrán que sean confiables. Los gobiernos buscarán el bienestar de sus ciudadanos, empresas, mercados, economías y también que la sociedad tenga acceso a un marco de identidad digital y fácil de usar.

3. CRIPTOMONEDAS

Establecer una definición de las criptodivisas no es una tarea fácil. Al igual que la cadena de bloques, las criptodivisas se han convertido en una “palabra de moda” para referirse a una amplia gama de desarrollos tecnológicos que utilizan una técnica llamada criptografía, esta técnica protege la información transformándola en un formato ilegible que sólo puede ser descifrado por alguien que posea la clave secreta.

3.1 DEFINICIÓN

Las criptomonedas se consideran monedas digitales que actúan como un medio de compra y venta de diferentes servicios y bienes sin pasar por una institución financiera. Blockchain es la base sobre la que construir criptodivisas. A través de un complejo proceso de verificación de transacciones, estas no pueden gastarse más de una vez ni se necesita de ninguna entidad que las gobierne, ya que son los usuarios los que se encargan de ello. Pavel Ciaian (2018)

Mediante la cadena de bloques son utilizadas para resolver problemas para mandar dinero internacionalmente de manera menos costosa y más rápida. También se puede evitar la privatización de acceso a servicios bancarios.

La gestión de riesgo es una de las ventajas de las criptomonedas. Utilizando esta divisa lograremos evitar tres tipos de riesgo:

- De agentes: este tipo de riesgo se da cuando la transacción es realizada por administradores y se hace un mal uso de los tramites llevados a cabo.
- De liquidación: este tipo de riesgo tiene lugar cuando se produce un fallo técnico y automáticamente se devuelve la transición.
- De la otra parte: este tipo de riesgo surge cuando antes de realizar la transacción la otra parte quiebre o es liquidada.

Un actor muy importante en el mercado de las criptomonedas es el "minero" que participa en la validación de las transacciones en la cadena de bloques resolviendo un "rompecabezas criptográfico". El proceso de la minería se relaciona con la criptografía que se basan en un mecanismo de consenso del programa de trabajo. Un minero aprovecha la fuerza de los ordenadores para validar las transacciones y se recompensa con monedas recién extraídas.

Los mineros pueden ser usuarios de criptografía, o, más comúnmente, las partes han hecho un negocio para venderlas por moneda fiduciaria, cómo por ejemplo el Euro o el Dólar.

3.2 BITCOIN

Como hemos podido ver a lo largo de este trabajo Blockchain y Bitcoin van de la mano. En 2008, el Japonés Satoshi Nakamoto presenta dinero electrónico, descentralizado, "peer to peer" (de igual a igual), lo llamó Bitcoin. El primer bloque de Bitcoin fue lanzado el 3 de enero de 20009 por Satoshi Nakamoto. "Solo se podrá emitir 21 millones de unidades en toda su historia". De esta manera, la cantidad de monedas por "acuñar" irá disminuyendo con el paso del tiempo, para intentar lograr evitar futuras inflaciones de la criptomoneda. El primer precio registrado fue en 2010 y es a partir de 2013 cuando comienza su comercialización con la creación de casas de cambio.

El valor del Bitcoin ha ido fluctuando, en sus comienzos su valor era prácticamente nulo. El valor de 1 Bitcoin en 2011 era de 1 USD. A partir de este año su valor

comienza a crecer con algún que otro descenso. En abril de 2013 logra tener un valor de 266 USD.

La fluctuación de esta divisa ha conseguido que el 11 de diciembre de 2017 consiga su máximo histórico con un valor de 19.798 USD. Esto en gran medida lo logra la CME (Chicago Maercantile Exchange) con la venta de Bitcoins. Desde entonces ha estado cayendo con algún altibajo. Detrás hay una enorme especulación.

Bitcoin es la criptomoneda por excelencia, pero actualmente existen 2.835 criptodivisas *investing.com* y se están creando muchos nuevas con el paso de las semanas. Se crean mediante un proceso denominado ICO "Initial Coin Offering", es decir, esto es la Oferta Inicial de Moneda, de esta manera se pretende que una ICO financie el nacimiento de una nueva criptomoneda.

Las principales criptomonedas en estos momentos aparte de Bitcoin son: Ethereum, XRP, Tether y Litecoin. De todas ellas la más utilizada en 2019 fue Ethereum. Las criptomonedas son diferentes entre sí y tienen diferentes utilidades. Se diferencian en los criptoactivos que poseen, son 3 aspectos; la filosofía con la que se utilizan, la tecnología y la encriptación. La tecnología Blockcgain es utilizada para la mayoría, pero no es la única que es utilizada. Respecto a la filosofía, puede haber tantas como monedas.

Imagen 6: Un listado de las 10 principales criptomonedas del mercado.

CRIPTOMONEDA	ABREVIATURA	CAPITALIZACIÓN EN EL MERCADO	CRIPTOMONEDAS EN CIRCULACIÓN
Bitcoin	BTC	$133.44B	18.130.700
Ethereum	ETH	$14.61B	109.078.084
XRP	XRP	$8.45B	43.319.477.613
Tether	USDT	$4.12B	4.108.044.456
Bitcoin Cash	BCH	$3.88B	18.194.938
Litecoin	LTC	$2.77B	63.746.444
EOS	EOS	$2.54B	946.529.022
Binance Coin	BNB	$2.22B	155.536.713
Bitcoin SV	BSV	$1.80B	18.068.415

Fuente: Coin Market Cap

Bitcoin es una divisa, así como lo son el dólar o el euro. Estas últimas se consideran "monedas fiat", la principal diferencia es que el Bitcoin no existe de forma física. Se considera una moneda digital ya que está soportada en la cadena de bloques y para verificar la transacción se realiza mediante un proceso muy sofisticado, ya que no puede utilizarse dos veces. Por lo tanto, cada Bitcoin es diferente y único, pudiendo registrar públicamente cada transacción en un libro de contabilidad digital, este está elaborado mediante estructuras muy complejas en criptografía con la tecnología de cadenas de bloques.

Para realizar el procedimiento de Bitcoin es necesario llevar a cabo un proceso con un equipo llamado "minería" y los responsables de realizar esta actividad son los mineros.

Los mineros son las personas autorizadas que pueden comprar al banco central, ya que son ellos los que por primera vez emiten la criptomoneda y los que también la distribuyen una vez que quieran darle uso.

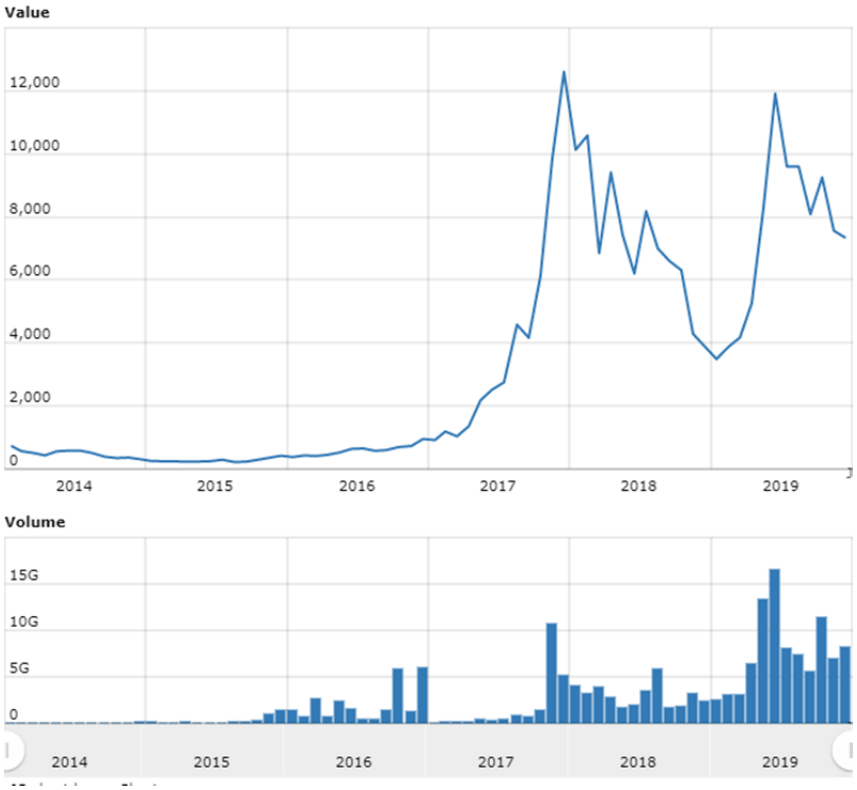
La red de minería en todo el mundo está formada por millones de nodos conectados, actualmente es una red muy segura ya que la dificultad del minado cada vez es más compleja. La función de los mineros es operar en un nodo o unirse a un grupo de minería, también llamado pool. Gracias a las agrupaciones logran solucionar los bloques de una forma más rápida. Intentar hackear el Blockchain, tanto para hacer un doble gasto de las monedas o para ejecutar una transacción falsa es una posibilidad muy muy remota, ya que el hacker tendría que ser capaz de forzar la criptografía donde están protegidos los datos y modificar un gran número de nodos. Valente, P (2017)

Cada minero recibe una recompensa de 50BTC por cada bloque minado, el proceso de minar Bitcoins solamente se puede realizar mediante un ordenador. Como anteriormente hemos comentado, solamente se podían emitir 21 millones de criptomonedas, la reducción programada se llama “halving” y este es un tipo de proceso que sucede cada 210.000 bloques minados (aproximadamente se calcula que ocurre cada 4 años) reduciéndose a la mitad la recompensa por la minería de bloques. En 2012 ocurrió el primer halving, en 2016 el segundo y desde entonces no ha vuelto a ocurrir ningún otro. Se espera que para el año que viene se produzca la siguiente división de recompensas.

El precio de un Bitcoin es volátil e impredecible, puede aumentar o disminuir en poco tiempo ya que tiene una economía joven, es algo nuevo y novedoso. Hay mucha especulación sobre este tipo de moneda. No es aconsejable tener los ahorros en Bitcoin.

En sus comienzos, en febrero de 2011 su precio era de 1 dólar llegando a cotizar a penas cuatro meses más tarde a 29 dólares, fluctuando hasta los 6,55 dólares dos meses más tarde. En noviembre de ese mismo año llegó a estar en 2 dólares.

Imagen 7: Capitalización del Bitcoin.



Fuente: World coin index 2019

3.3 OTRAS CRPTOMONEDAS (ALTCOINS)

Cualquier moneda que no sea un Bitcoin se denomina un “Altcoins” también este concepto incluye a los tokens y criptomonedas. En estos momentos es difícil estimar la cantidad de altcoins ya que la cantidad de tokens que se crean cada mes para financiar distintos proyectos es muy grande.

Los Altcoins más importantes en estos momentos son:

3.3.1 Ripple (XRP)

Fue fundada en 2012 por la compañía Ripple Labs y se consolidó como la plataforma de la criptomoneda XRP, con estas siglas está representada. Ripple está basada en una red que involucra a varias partes para validar las transacciones, esta Altcoin se construyó para convertirse en una moneda puente que permita a las instituciones financieras liquidar los pagos transfronterizos con mucha más rapidez y más barato de lo que pueden usar las redes de pago globales que existan hoy en día, que puede ser lento e involucran a más intermediarios. Sin embargo, la plataforma de pago de Ripple no necesita una moneda para funcionar.

Según Ripple. XRP puede manejar más de 1.500 transacciones por segundo. Todos los datos van encriptados, han validado su propio protocolo de consenso especifico.

A diferencia de Bitcoin, Ripple se ejecuta en una cadena de bloques permitida. La empresa Ripple Labs dtermina quien actúa como validador de transacciones en su propia red. La cadena de bloques es pública ya que puede ser accedida y vista por cualquiera. Se puede convertir en moneda fiduciaria al igual que Bitcoin

Es un sistema de pago digital descentralizada P2P (red peer to peer) de código abierto que permite transferencias casi instantáneas de moneda independientemente de su forma, por ejemplo, euro, dólar, bitcoin, yen…etc.

Ripple tiene un código abierto y está disponible para todo el público, esto significa que cualquiera pueda desplegar una instancia de Ripple. Los nodos pueden llegar a tener tres roles diferentes: los usuarios que reciben/crean pagos, creadores de mercado que actúan como operadores y los validadores de los servidores.

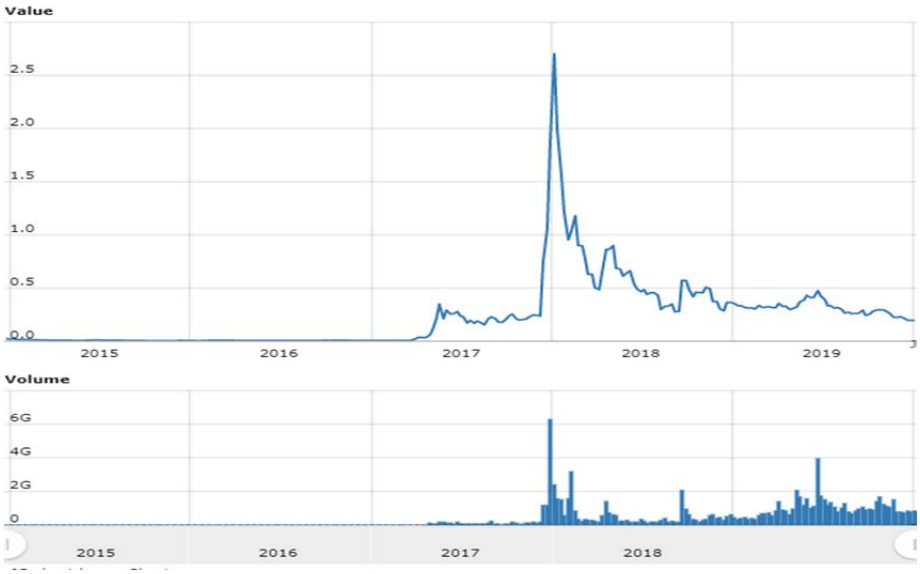
Los usuarios de Ripple son referenciados mediante seudónimos. Los usuarios disponen de un par de claves publicas/privadas, cuando un usuario desea enviar un pago a otro usuario, firma criptográficamente la transferencia de dinero denominada en la propia moneda. Para los pagos realizados en monedas que no sean XRP, por ejemplo: Pedro paga a Esther en otra moneda. Sólo es posible si Esther está dispuesta a aceptar una transacción. No puede llegar a ser aceptada si el precio de la otra moneda es inferior al precio del valor que tiene la operación, para realizar la operación de estas transacciones se necesita la participación de “creadores de mercado” que actuarán como intermediarios. Ripple se basa en un algoritmo de búsqueda de ruta que encuentra la ruta de pago más adecuada para la fuente de destino.

Las diferencias con el Bitcoin es que el coste por realizar una transacción es mucho más barato, las transacciones son inmediatas y no necesita mucho tiempo para que sean confirmadas. Esta Altcoin puede ser intercambiado por monedas fiduciarias.

Ripple fue creada con cien mil millones de tokens desde que se fundó y no posee una cantidad fluctuante en existencia. El principal objetivo es ser una moneda digital es que puedan pagarse bienes y servicios. En otras palabras, ser un sistema de pago, intercambio de moneda y de envío de pagos a los bancos. Ser una alternativa más barata y segura para reemplazar a los sistemas de transferencias con los que operan los bancos en estos momentos, como el sistema de pagos SWIFT (es el acrónimo de Society for world Interbank Financial). Cada vez son más los proveedores y los bancos que incluyen a Ripple entre sus opciones. Se convierte primero el valor de la transferencia en XRP en vez de hacerlo por dólares y se quitan las tarifas por el cambio de divisa al mismo tiempo que el pago es procesado en menos de un minuto.

XRP es capaz de liquidar en sólo cuatro segundos, el uso de los XRP no depende de la red Ripple, sus tokens son completamente independientes.

Imagen 8: Gráfico de los últimos 5 años de la fluctuación de valor que ha tenido Ripple:



Fuente: world coin index 2019

3.3.2 Dash

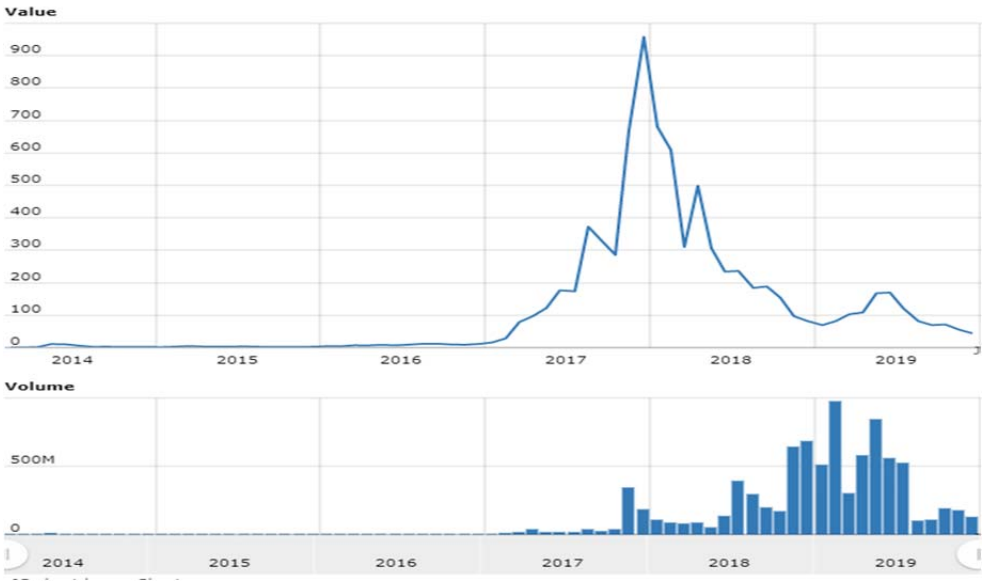
Esta criptomoneda fue emitida en 2014, posee unas características parecidas a Bitcoin. Esta tecnología de bloques es una red descentralizada, pero tiene diferencias en cuanto al anonimato, coste y velocidad.

Posee una criptografía de código abierto P2P centrada en la privacidad. Lo que le hace diferente a la mayoría de las otras monedas, es que tiene una red de dos niveles.

Está asegurada por los llamados “masternodos”, estos se encargan de que la transacción, primero sea válida y luego de difundir la información a la red.

En cuanto a la velocidad para realizar la transacción es de apenas de 4 segundos. El coste de transacción es de apenas de medio dólar respecto a los 6 que se pagan en Bitcoin. Esta criptomoneda ofrece el anonimato.

Imagen 9: Gráfico de los últimos 5 años de la fluctuación de valor que ha tenido Dash:



Fuente: world coin index 2019

3.3.3 Ethereum (ETH)

Es una plataforma descentralizada que cuenta con un lenguaje de programación Turing completamente integrado, permite que se puedan escribir contratos inteligentes y aplicaciones descentralizadas aplicando la lógica en pocas líneas de código. Ejecuta acuerdos entre dos o más empresas.

Fue creado por Vitalik Buterin en 2015 y su moneda para esta plataforma es Ether, su objetivo es ser una plataforma de código abierto, permitiendo a cualquier desarrollador informático ejecutar aplicaciones descentralizadas. La gran diferencia con Bitcoin es qué esta es una criptomoneda infinita y a la hora de realizar las transacciones son mucho más rápidas, menos de 15 segundos.

Imagen 10: Gráfico de los últimos 5 años de la fluctuación de valor que ha tenido Dash:

Fuente: World coin index 2019

3.4 REDES DE CRIPTOMONEDAS

Existen diferentes criptomonedas dependiendo de redes de ordenadores, cada uno con sus ventajas e inconvenientes. Las redes pueden ser descentralizadas, centralizadas y distribuidas.

3.4.1 Redes descentralizadas.

Forman una serie de ordenadores que funcionan en conjunto para controlar y manejar la red. No hay una sola unidad central. Gracias al conjunto de ordenadores contraen determinadas tareas de la red y consiguen agregar un cierto nivel de tolerancia a los fallos. Actúa como una red central dentro de una red más grande. Cuentan con subredes dentro de una gran red y en conjunto son capaces de manejar todos los servicios que prestan.

Aunque el principal inconveniente de este tipo de red es que exista un fallo total y las redes queden fuera de servicio con la caída de un ordenador coordinador y como consecuencia los demás ordenadores queden desconectados y sin servicio de la red principal. En caso de que cayera el ordenador de coordinación, el resto de las redes quedarían dispersados.

Las principales criptomonedas descentralizadas son EOS o Dash. Empresas que utilizan estas redes pueden ser Twitter, Facebook o Google.

3.4.2 Redes centralizadas

En este tipo de red cada ordenador está conectado a una unidad central y es periférico. Toda el poder y la responsabilidad recaen sobre un ordenador. Este tipo de redes son capaces de manejar grandes cantidades de información.

Las redes centralizadas son las más utilizadas por su escabilidad y simplicidad. Sin embargo, este tipo de redes pueden llegará a tener un fallo bastante peligroso, en caso de sufrir un ataque a la unidad central puede llegar a imposibilitar la comunicación con el resto de ordenadores. Un fallo es capaz de afectar a todos dentro de la empresa. Si queremos evitar esto hay servicios paralelos y copias de seguridad.

Un caso de Blockchain centralizada es Ripple o un proyecto de software libre llamao Hyperledger, cuyo objetivo es crear redes de Blockchain para un uso empresarial y con un control centralizado.

3.4.3 Redes distribuidas

La principal característica de este tipo de red es que hay una ausencia de centro individual o colectivo. No hay una idea de centro y periferia como existían en las redes centralizadas y descentralizadas. En este tipo de redes los ordenadores se unen el uno al otro de tal forma que ninguno de ellos tiene poder de filtro sobre la información que se transmite en la red.

Posee una estructura en la que si falla algún ordenador no desconectaría al resto. Internet es un claro ejemplo de este tipo de red, otro ejemplo seria redes para compartir archivos de P2P como por ejemplo Bittorrent, la conforman una serie de nodos interconectados que se encargan de mantener un funcionamiento correcto de la misma. Todo en la red es manejado de forma abierta, distribuida y comunitaria.

3.5 PROCESO DE CREACIÓN DE UNA NUEVA CRIPTOMONEDA

Realizando este trabajo de investigación, encontré información para crear una propia criptomoneda, con el objetivo de mostrar cómo es posible empezar a entender e integrarse en el mundo del Blockchain. Mi aportación en este trabajo es elaborar una propia criptomoneda.

Para crear nuestra propia criptomoneda tenemos dos opciones, una sería: crear nuestra propia red, como puede ser Bitcoin y otra sería mediante Ethereum.

Para este trabajo, dado que no tengo los conocimientos suficientes para hacerlo de otra manera, utilizaré la red Ethereum que entre otras ventajas evita tener que pagar. A continuación, detallaré los siguientes pasos para realizar mi propia criptomoneda, a la que he llamado DBH44.

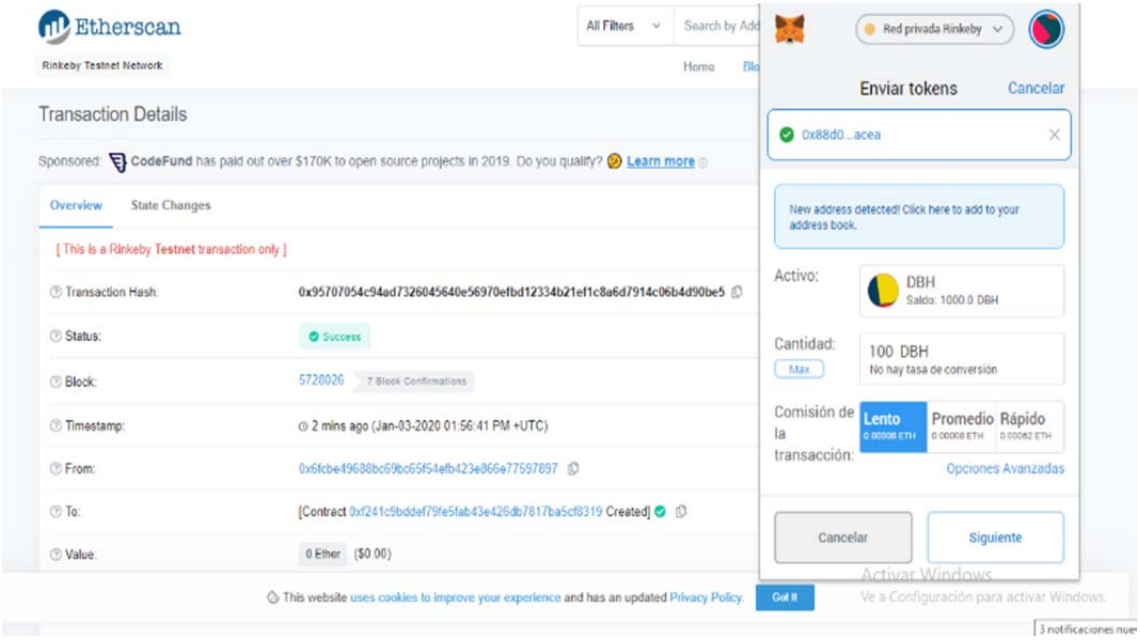
Comenzamos descargando la extensión de Google Chrome llamada Metamask. Gracias a esta extensión podremos ejecutar Ethereum Dapp directamente en el navegador sin necesidad de realizar la descarga completa.

Dentro de Metamask no tendremos que dar nada de información personal, directamente nos ofrece la posibilidad de insertar o crear una cartera.

El primer paso es descargar el monedero, cuando estamos dentro nos proporcionan una clave privada, son 12 palabras aleatorias que deberemos meter en el mismo orden. Es muy importante no perderla, ya que si la perdemos no podrá volver a usarse.

Imagen11: Aspecto de una cartera Metamask

Fuente: Elaboración propia



Para crear mi propia criptomoneda utilizaré Rinkeby, una red de carácter gratuito que se emplea como red de pruebas.

Utilizaremos la red Ethereum para crear un contrato inteligente (Smart Contract), en él podremos escribir información acerca de nuestra moneda, como, por ejemplo, el nombre, la cantidad de monedas que queremos emitir, los decimales…

Utilizaremos el lenguaje Solidity, para poder escribir la información de los Smart Contracts. Este es un tipo de lenguaje informático como puede ser HTML o Java Script. No necesitamos saber utilizar Solidity ya que una página web llamada Github, lo tiene ya escrito.

Buscaremos la página web Github ConsenSys. Una vez dentro, buscaremos Tokens y de primera opción nos aparecerá ConsenSys/Tokens Ethereum tokens contracts, este

el directorio que se debe abrir. Dentro observaremos distintas carpetas y haremos click en eip20.

De momento, dejaremos abierta esta ventana ya que primero se debe realizar otros pasos.

A continuación, tendremos que pedir Ether de prueba. Aquí hay que enlazar y en este programa buscar Rinkeby Authenticated Faucet y el código que nos aparece pegarlo en una publicación en una de nuestras redes sociales (Twitter o Facebook) en mi caso he elegido Twitter. Copiar el link del post y pegarlo en Rinkeby Authenticated Faucet.

Después de realizar esto, deberíamos de tener los Ether que hemos pedido en nuestra cartera Metamask. Cuando busquemos nuestra cartera por defecto nos va a salir Red principal Etherum y ahí tendremos que buscar Rinkeby.

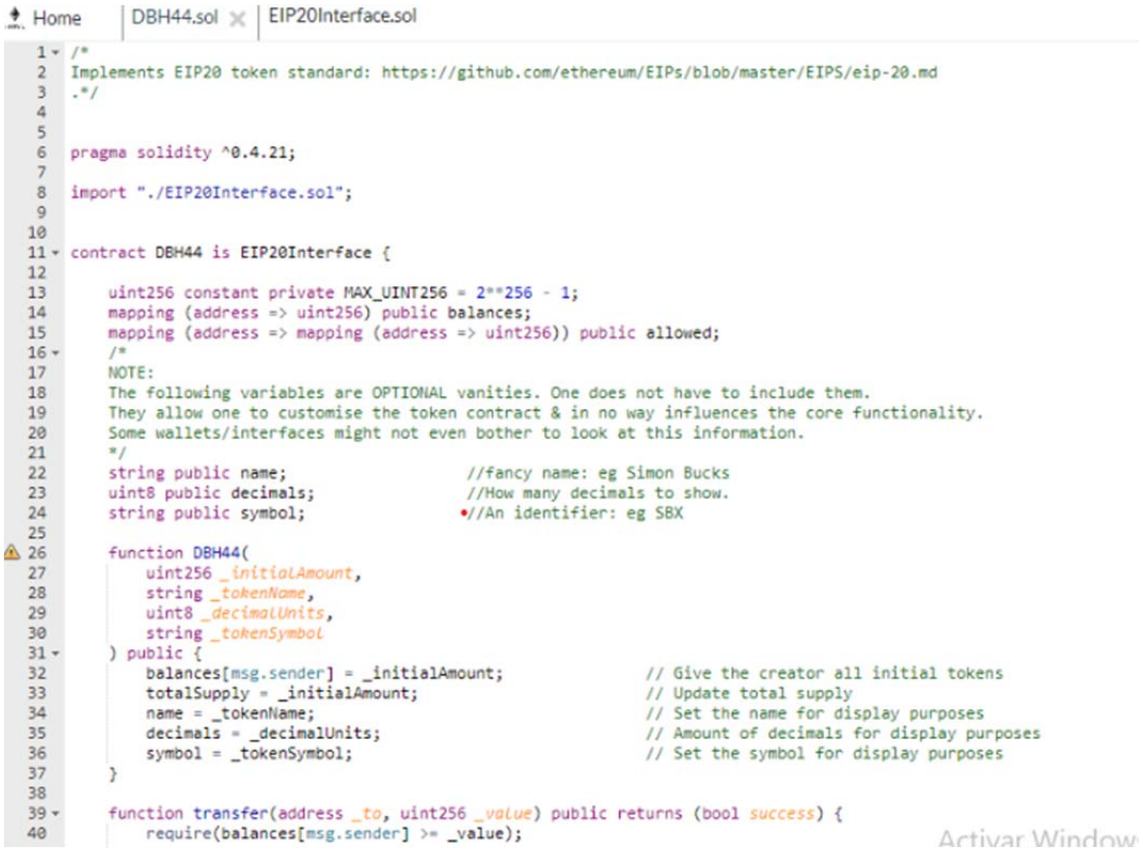
Ir a la página Remix de Ethereum y a la vez a la página que anteriormente hemos abierto de Github.

Encontrar un signo más en la parte superior izquierda de Remix, pinchar aquí para crear un nuevo Smart Contract. Dar un nombre a este contrato, “yo lo he llamado DBH44token”.

Después de nombrarlo, encontraremos una página en blanco donde podremos escribir. Aquí es donde aparece el lenguaje Solidity una vez abierta la página Github.

Pinchamos en EIP20.sol, tendremos que copiar todo lo que este escrito y pegarlo en nuestra página remix.

Imagen 12. Lenguaje Solidity en Smart Contract de Ethereum



Fuente: Elaboración propia.

Una vez que lo hemos pegado, tendremos que cambiar el nombre del contrato, de EIP20 a DBHToken, así como el nombre de la función. Tendremos que dar el mismo nombre tanto a la función como al contrato (DBH44) porque es la función constructora.

En el pantallazo que está arriba podemos observar el documento de Solidity en el que hay otra función integrada. Esto quiere decir que necesitaremos el lenguaje Solidity de esta segunda función. Este documento lo conseguiremos volviendo a la página de Github y en este caso utilizaremos el tercer documento que aparece, EIP20interface.sol.

Volvemos al documento DBH44, en la función que hemos cambiado el nombre, observamos que contiene cuatro apartados. Aquí asignaremos, el nombre del token, la cantidad inicial de tokens, los decimales asignados y también el símbolo.

Mediante la función se depositará en la cartera del creador del contrato todos los tokens que hemos decido crear. En mi caso 1000 tokens.

Una vez que ya está escrito el contrato, ya se puede poner en funcionamiento. Ahora hay que pinchar en la pestaña Run, dentro de la página remix, donde tenemos DBH44.

Dentro de Run, podemos observar la palabra Enviroment y una pestaña que nos da a elegir 3 opciones, elegiremos Injected 3.

En la parte de abajo, podemos escoger DBH44 en vez de EIP20interface.sol y asignar los 4 valores que antes he mencionado.

Los valores que he asignado a mi criptomoneda son:

- Cantidad inicial: 1000
- Nombre del Token: DBH44token
- Decímales: 1
- Símbolo: DBH44

Siempre hay que escribir estos valores entre comillas en el apartado de Create. Click en Create.

Automáticamente se abrirá la ventana Metamask y es cuando los Ether de prueba que hemos pedido entran en juego a través de nuestras redes sociales. Para llevar a cabo cualquier transacción en el sistema Ethereum, hay que gastar Ether.

Una vez hecho esto, tenemos 3 opciones que son: transacción rápida, media o lenta. Dependiendo de cuál seleccionemos tendremos una comisión mayor o menor.

Para mi criptomoneda seleccioné la “media” y tuve que pagar 0.0001 Ether y tan solo tardó unos segundos en realizar la operación.

Una vez que se ha realizado esta transacción, en esta misma página, Remix, encontraremos el balance copiado nuestra dirección pública pegándola donde pone Balance, entre comillas.

Pinchar en el menú izquierdo de Metamask y agregar token para ver nuestro token en nuestra cartera Metamask.

Añadimos token personalizado, pegando la dirección del contrato que hemos creado y el símbolo de la moneda. Directamente nos aparecerá en la pantalla y pinchar en agregar.

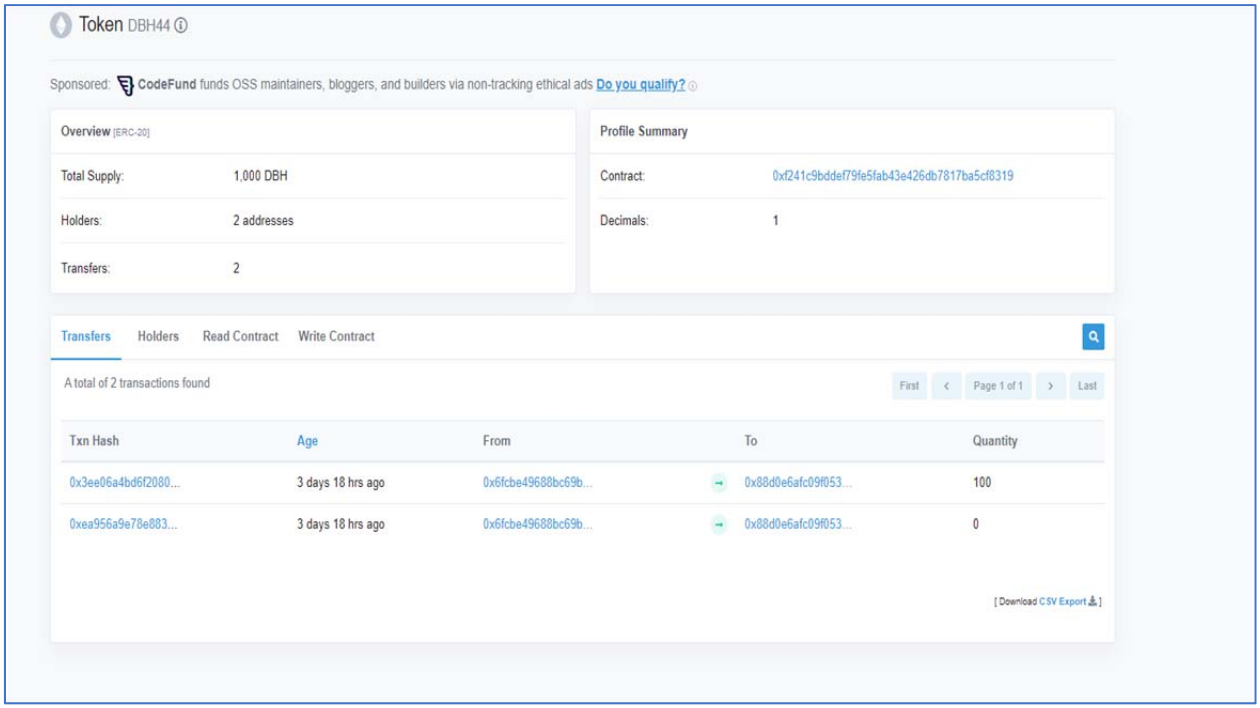
Una vez realizado todo esto ya tendremos el DBH44token en nuestra cartera, en la red Rinkeby y hacer la transacción dentro de esta red de prueba.

Para comprobar el estado de la criptomoneda, lo haremos a través de Etherscan, en esta plataforma podremos buscar en las cadenas de bloques de Etherscan las direcciones, transacciones, fichas, precios, etc.

Siempre tenemos que buscar en la red Rinkeby para encontrar DBH44token. Para seleccionar un símbolo lo encontraremos en la parte superior de la derecha, al lado de iniciar sesión.

Después de esto, escribimos el nombre de nuestra criptomoneda en el buscador y aparecerá la siguiente información:

Imagen 13: Seguimiento de criptomonedas en Ethereum.



Fuente: (EtherScan, 2019)

4.PROPUESTA DE CURSO SOBRE “BLOKCHAIN”

Como finalización del trabajo y para dar una aplicación práctica a la información generada en los capítulos previos, se valora la posibilidad de realizar una oferta formativa sobre blockchain y comercio exterior, desarrollando para ello el formato más adecuado y necesario.

Antes de diseñar esta oferta formativa se plantea la necesidad de analizar la situación del sector formativo sobre Blockchain en el contexto español y universitario. Tras realizar una búsqueda de 8 planes de estudios universitarios sobre Comercio Exterior no se encontró ninguno que ofreciera contenidos de Blockchain ni en los epígrafes de las asignaturas ni en sus descriptores. La búsqueda de grados dedicados específicamente al Comercio exterior, como por ejemplo el Grado de Comercio Exterior de la Universidad de León, no dio resultados positivos puesto que ninguna habla abiertamente sobre la tecnología Blockchain, del mismo modo realicé una búsqueda de Másteres de Comercio exterior, como, por ejemplo, el Máster de Comercio Exterior y Economía Internacional de la Universitat de Barcelona, pero en su programa no hay ninguna asignatura sobre la tecnología Blockchain. En la búsqueda de Másters de “Blockchain” aparecen bastantes, uno de ellos en Valladolid, Campus Internacional de Blockchain, siendo 100% on line, pero ninguna referencia en sus asignaturas al Comercio Exterior. Sin embargo, en los masters de Fintech (centrados en los aspectos financieros y la aplicación de nuevas tecnologías a actividades financieras y de inversión) sí que se desarrolla con detalle la tecnología Blockchain pero dan muy poco peso al comercio internacional, como por ejemplo Fintechschool de modalidad on-line.

Si buscamos en Internet las palabras “Comercio exterior” y “Blockchain” encontramos 329.000 resultados, pero muy pocos de ellos están vinculados a ofertas formativas.

La incorporación de estos contenidos en un máster es muy complicada, porque la tecnología cambia con rapidez, los procedimientos administrativos universitarios son muy lentos e incorporar una asignatura nueva supone cambiar la memoria, negociar cambios en las asignaturas, con los consiguientes conflictos entre departamentos y, en última instancia, asumir que cuando se logran estos procesos, quizás la tecnología ha cambiado.

Por este motivo, en vez de modificar el plan de estudios, se propone realizar un curso complementario relacionado directamente con la tecnología de Blockchain para aportar un conocimiento teórico y a la vez práctico. Blockhain o también llamada la cadena de bloques ha irrumpido con fuerza como la tecnología que permite eliminar intermediarios y ahorrar costes en los procesos de las empresas.

- Este curso se realizará 100% presencial en la Facultad de Comercio de la Universidad de Valladolid.
- Horario: De lunes a jueves de 16:00-21:00
- Duración: 11 de enero al 26 de febrero. 7 semanas

4.1 INTRODUCCIÓN

Este curso se plantea como una oportunidad para aportar a estudiantes y profesionales que quieran dedicarse al comercio exterior con un conocimiento avanzado sobre las tecnologías de futuro en el sector, siendo el Blockchain una de las tecnologías estrella dentro de esta oferta.

El programa está diseñado, a través de casos reales, la aplicación de la tecnología Blockchain en los diferentes modelos de negocio. Aprender de las nuevas oportunidades que nos brinda esta tecnología en los diferentes sectores empresariales. Analizar y aplicar una normativa fiscal relacionada con el Blockchain.

Cada vez son más empresas, gobiernos y reguladores las que ofertan este tipo de servicios para cualquier aplicación que tenga sentido implementar la seguridad, inmutabilidad, rapidez y ahorro de costes que proporciona en muchos casos Blockchain. Veremos cómo la revolución está presente, y cada semana que pasa alcanza una velocidad de vértigo en casi todos los ámbitos industriales y empresariales.

Cada vez son más las funcionalidades que están derivando de esta tecnología y tenemos que estar preparados.

Veremos cómo Blockchain no se centra sólo en las criptomonedas, sino que se van a aplicar en diferentes contextos dentro de la empresa, los Smart Contracts y cómo evolucionan directamente en diferentes departamentos de empresa.

4.2 OBJETIVOS DEL MÁSTER

Preparar a los alumnos ante la nueva revolución digital, aprender conocimientos del Blockhain, conocer los tipos que existen y sus aplicaciones en diferentes sectores para que se puedan dedicar profesionalmente a la gestión de proyectos o en trabajos de asesoría de inversión en un proyecto con tecnología Blockchain.

Se busca desarrollar nuevos modelos de negocio, generar redes de confianza más seguras, conseguir la trazabilidad en la transferencia de información entre partes.

Está destinado a personas que quieran dedicarse profesionalmente al comercio y conocer cómo las tecnologías están cambiando el mundo en el que vivimos, por eso es necesario estar continuamente adaptándonos a nuestro entorno. Durante el máster el alumno tendrá la oportunidad mediante ejercicios prácticos de elaborar un proyecto propio. Al final del curso se presentarán los proyectos más valorados y podrán llevar a cabo su idea.

Tras el auge de los últimos años, Blockchain ha conseguido situarse como una de las tecnologías en la que más invierten las empresas. Sin embargo, aún queda mucho camino por recorrer. ¿El próximo reto? Hacer accesible la tecnología para cualquier usuario.

4.3. PROPUESTA

Se propone para este nuevo curso (2020-2021) desarrollar estos cuatro módulos relacionadas con la tecnología del Blockchain:

- CONCEPTOS DE BLOCKCHAIN & BITCOIN
- OPORTUNIDADES DE NEGOCIO: BLOCKCHAIN PARA EMPRESAS.
- LEGALIDAD FISCAL PERSONALY EMPRESARIALSOBRE EL BLOCKHAIN
- PROGRAMACIÓN BLOCKCHAIN

En este siguiente apartado se desarrollará la temática y el programa de la asignatura y sus objetivos generales. El último módulo es “Programación Blockchain”, después de adquirir todos los conocimientos, el alumno será capaz de desarrollar un proyecto de Blockchain de aplicación en algún sector.

4.3.1 MÓDULO: BLOCHAIN & BITCOIN

(32 horas)

En la introducción a este nuevo máster sobre la tecnología Blockchain, se aportará una visión global sobre los fundamentos de las cadenas de bloques, sus características más importantes y explicar cómo funcionan los sistemas descentralizados de datos. Explicaremos cómo se construye esta tecnología sobre las funciones criptográficas, los datos de sistemas distribuidos y protocolos de comunicación de redes.

Con estos conocimientos, el alumno entenderá el papel fundamental que juegan las cadenas de bloques también de que la expresión “Blockchain” es la conexión múltiple de miles de nodos interconectados. La importancia que tienen los protocolos para generar cadenas y verificar las reglas a la hora de instalar el software.

OBJETIVOS GENERALES

- Comprender la tecnología Blockchain y su importancia.
- Conocer su funcionamiento teórico y práctico.
- Entender por qué se creó Bitcoin, cómo funciona y para qué sirve.
- Saber los tipos de Blockchain que existen.

PROGRAMA DEL MÓDULO

- Definición
- Tipos de cadenas
- Protocolos
- Nodos y tipos de nodos
- Redes

- Reglas de consenso
- Bitcoin
- Caso práctico

4.3.2 MÓDULO: OPORTUNIDADES

(40 horas)

En este máster estamos enfocado a ideas de negocio. La aplicación de esta tecnología a la empresa para implementar el ahorro de costes, seguridad y rapidez. En esta asignatura veremos cómo la revolución tecnológica avanza a pasos agigantados y no podemos quedarnos atrás.

Mostraremos ejemplos de casos de éxito y cuáles son los principales sectores que más se van a beneficiar de aplicar esta tecnología, la importancia de las cadenas de suministro. Las cualidades que tienen los Smart Contracts y las ventajas que ofrece en el sector bancario.

OBJETIVOS GENERALES

- Conocer la importancia digital del S.XXI
- Proyectos que ya utilizan tecnología Blockchain
- Entender la funcionabilidad de los Smart Contracts

PROGRAMA DE LA ASIGNATURA

- Trazabilidad
- Revolución digital
- Casos de éxito
- Smart Contracts
- Sectores más potentes
- Sector bancario
- Criptomonedas

4.3.3 MÓDULO: PROGRAMACIÓN BLOCKCHAIN

(59 horas)

Esta asignatura será de las más importantes del máster, ya que aprenderemos a desarrollar aplicaciones descentralizadas y a utilizar esta tecnología en la práctica. Después de haber adquirido los conocimientos técnicos en los dos módulos anteriores. Explicaremos el lenguaje Solidity, utilizando en los lenguajes de los Smart Contracts en Ethereum.

En el proyecto final de máster, que llevaremos a cabo con The Hyperledger, se construirá el ecosistema Hyperledger Composer y podremos tener una visión general de la Blockchain. Explicaremos los principales componentes de los nodos y de cómo interactúan entre sí. Los componentes necesarios para hacer que una Blockchain funcione, ver de forma práctica el impacto que tiene esta tecnología en aplicaciones y saber programar un Smart Contract

También crearemos nuestra propia criptomoneda desde Ethereum.

OBJETIVOS GENERALES

- Crear nuestra propia criptomoneda
- Saber programar un Smart Contract
- Crear una plataforma y desarrollar herramientas
- Programar mediante el lenguaje Solidity
- Caso práctico final de máster

PROGRAMA DEL MÓDULO

- Desarrollo de Ethereum y sus herramientas.
- Introducción a Solidity
- Instalar
- Datos generales
- Operador
- Estructura
- Crear criptomoneda
- Proyecto The Hyperledger
    - Desarrollo de esta tecnología.
    - Organización
    - Despliege de herramientas

- Proyecto final

4.3.4 MÓDULO: LEGALIDAD, FISCALIDAD PERSONALY EMPRESARIALSOBRE EL BLOCKHAIN

(44 horas)

Se ha discutido mucho sobre las oportunidades que presentan las tecnologías de bloques. Pero, ¿qué significa realmente la adopción sobre las cadenas de bloques para los departamentos legales? ¿Es tan compleja como parece?

En esta asignatura discutiremos sobre las tecnologías de bloques y sus implementaciones prácticas para los departamentos jurídicos de una amplia gama de industrias, centrándonos en casos de la vida real, a la vez que detectar riesgos, obligaciones, beneficios y desafíos asociados a la implementación. Aspectos reglamentarios de la cadena de bloques y ver las distintas jurisdicciones que están abordando el desarrollo y la implementación de tecnologías de libro mayor y distribuido.

OBJETIVOS GENERALES

- Conocer el aspecto regulatorio sobre fiscalidad y legalidad.
- Descubrir posibilidades profesionales en cada sector.
- Saber el estado actual en el que se encuentran las administraciones y su marco regulatorio.

PROGRAMA DEL MÓDULO

- Fiscalidad de los sistemas de registro distribuido y legalidad
- Desarrollo de conceptos técnico jurídico para identificar las cadenas de bloques, requisitos, etc.
- El papel de las empresas, administraciones y ciudadanos a las que está destinada esta tecnología.
- Situación actual de la jurisprudencia.
- Aspectos fiscales
- Marco legal.

4. CERTIFICACIÓN

Una vez finalizados los estudios y superadas las pruebas de evaluación, el alumno recibirá un título de la Universidad de Valladolid que certifica que ha realizado el «curso en Blockchain» por 175 horas.

5. FECHAS DE EXAMENES

Esta información se obtiene automáticamente de la aplicación de gestión del Plan de Organizaciones Docente (POD) de la Universidad de Valladolid. La información de horarios de horarios sido introducida en las aplicaciones por el Centro responsable. Las guías docentes de las asignaturas deben prepararlas los profesores responsables. Las guías detalladas de grupo se pueden consultar en la intranet, accediendo con las credenciales de alumno de la UVA.

6. PRESUPUESTO

La partida fundamental del presupuesto son las remuneraciones al profesorado que se van a calcular mediante un caché de 70 euros hora. Es una valoración baja, pero compatible con la realidad debido a que se contrata bastantes horas a los seis docentes.

En principio, los docentes son de Valladolid o Madrid, de manera que las dietas de transporte no están contempladas, y solo se aplicarían en un caso (profesor de Madrid), con un montante total de 100 euros

El coordinador o coordinadores pertenecerá al equipo de Coordinación del Master en Comercio Exterior. Percibirá mediante nómina una remuneración por su trabajo, siendo esta partida de 300 euros.

El centro Buendía, gestiona las matrículas, la difusión y la emisión de títulos. El porcentaje de ingresos que asume por estas funciones no figura en su información institucional, pero se ha realizado una estimación de 5% de presupuesto global.

Los costes fungibles son, fundamentalmente, papelería, reprografía y alimentación (agua para ponentes)

Presupuesto	Horas	Coste hora		Coste total
Remuneración profesorado	175	70		12250
Dietas de transporte				500
Remuneración al equipo coordinador	30	30		900
Coordinador				600
Remuneración al equipo gestión del centro Buen día				600
Total				14850

	Número de alumnos	Coste alumno/a	Total
Ingresos	30	495	14.850

Si se matriculasen más de 30, se incrementarían los recursos para realizar una conferencia de cierre y un evento de protocolo.

7. MATRÍCULA

La documentación que deberá aportar el alumno para su matriculación en el Máster será la siguiente:

- Titulación Académica.
- Solicitud de admisión.
- Curriculum Vitae
- DNI

Una vez gestionada tu matrícula recibirán un correo electrónico con las claves de acceso al campus virtual, donde encontrarán todo el material de estudio.

CENTRO RESPONSABLE
FACULTAD DE COMERCIO (VA)
CAMPUS
Campus de Valladolid
TIPO
Presencial
RAMA
Ciencias sociales, jurídicas y tecnológicas.
IDIOMAS DE IMPARTICIÓN
Español e inglés
DURACIÓN
7 semanas
NÚMERO DE CRÉDITOS
90 ETCS
PLAZAS

30
WEB
http://www2.emp.uva.es/index.php/master-en-comercio-exterior/
CENTRO
FACULTAD DE COMERCIO (VA)
CONTACTO
Coordinadora: Begoña González Acebes: master.comercio.exterior@uva.es
CONTACTO ADMINISTRATIVO
Servicio de Posgrado y Títulos. Sección de Posgrado – Casa del Estudiante C/ Real de Burgos s/n – 47011 Valladolid - Tfno: 00 34 983 184342 – 4795 - 6488 - 3279 - e-mail: posgradoficial@uva.es

5. CONCLUSIONES

El Blockchain es un tema muy actual y ha sido considerado por los medios de comunicación como una tecnología vanguardista. Picado por la curiosidad, decidí proponer a mi tutor, Javier Gómez, un proyecto de fin de máster enfocado en el Blockchain y el Comercio Exterior.

Este TFG desarrolla de una manera necesariamente sintética la tecnología Blockchain o también llamada, cadena de bloques. Necesitamos comprender la importancia de esta tecnología, cómo funciona y las aplicaciones que puede llegar a tener en los diferentes sectores. Es interesante aprovechar las ventajas que ofrece tanto en seguridad, trazabilidad y transparencia.

Desde mi punto de vista, la tecnología Blockchain representa el futuro más cercano y una nueva forma actuar y pensar que mucha gente desconoce. He decidido realizar este trabajo para contribuir a la difusión de esta tecnología a las personas que aún lo desconocen.

He de decir que documentarme sobre este tema ha sido un gran descubrimiento a nivel personal, tanto por la adquisición de nuevos conocimientos sobre esta tecnología tan innovadora, como por observar casos reales de éxito. Sé que profesionalmente me ha venido muy bien todos estos conocimientos enriquecedores para un futuro.

La tecnología de la cadena de bloques se está desarrollando a un ritmo muy rápido y en estos momentos hay pocas personas conocen las capacidades que ofrece esta tecnología más allá de las criptomonedas. El Blockchain está cambiando muchas industrias existentes, el ejemplo más claro es el del sector bancario y su introducción fue supuestamente motivada por el Crack financiero mundial de 2008.

Hoy en día seguimos dependiendo de terceras partes que aporten y verifiquen nuestra identidad cuando realizamos distintos tipos de transacciones. Sin embargo, gracias a las cualidades que poseen las cadenas de bloques, podemos llegar a eliminar esta confianza y crear una identidad verificable a los usuarios que la utilicen, mediante técnicas criptográficas.

El trabajo que aquí concluye ha estado estructurado en tres grandes bloques. El primero, sobre la tecnología Blockchain, el segundo sobre las criptomonedas y en el último apartado he elaborado una propuesta de curso de Blockchain complementario al máster de Comercio exterior.

En el primer bloque se ha hablado sobre el concepto de Blockhain, cómo funciona, su historia, cómo se pueden clasificar sus redes deprendiendo de las características de las cadenas de bloques, el grado de descentralización, el nivel de privacidad, etc.

A continuación, se han explicado las principales características que posé esta tecnología, cómo son la seguridad, la inalterabilidad, la confianza descentralizada, la automatización de los contratos inteligentes y la trazabilidad.

Un punto muy importante en este bloque es el impacto del Blockchain en el comercio, la industria y los mercados. Las cadenas de bloques se encargan de solucionar preocupaciones relacionadas con la seguridad, la dificultad para coordinar el tráfico de datos entre diferentes países y los diferentes actores que participan en una transacción internacional. Periódicos económicos como por ejemplo The Economist hablan de esta tecnología cómo una “máquina para generar confianza”. El Blockchain trae consigo muchos beneficios y desafíos a los sectores industriales que ya están experimentando con esta tecnología.

Respecto al sector público, ya hay algunos gobiernos cómo, por ejemplo, el alemán que está considerando las formas en que podría utilizarse la cadena de bloques para asegurar el cumplimiento de los impuestos y también el tema de las votaciones.

En mi opinión, la tecnología Blockchain está cambiando y va a cambiar el modo en que vivimos, cómo realizamos y firmamos contratos, cómo compramos, la forma en la que pedimos un préstamo y muchas más posibilidades que esta nueva tecnología nos ofrece.

Cada vez hay más sectores en los que el Blockchain puede ayudar, ya sea con la transparencia de datos, la seguridad o el ahorro de costes. ¡La nueva revolución tecnológica es imparable!

Respecto a los contratos inteligentes, se han creado para transferir activos entre distintas partes mediante unas reglas, estableciendo unas pautas, bajo unas determinadas condiciones. Están programadas mediante el lenguaje Solidity en la plataforma Ethereum, a través de este lenguaje de programación estos datos no pueden sufrir variaciones una vez que está escrito el contrato y programado, por lo que ofrece altos niveles de seguridad e inmutabilidad. Son los motores que están detrás de las criptomonedas. Gracias a la IA (Inteligencia artificial) son capaces de tomar decisiones, reaccionar a su entorno, e incluso vender y comprar por su cuenta.

Sus principales ventajas son: reducen riesgos gracias a la inmutabilidad de las cadenas de bloques, reducen los costes administrativos gracias a la eliminación de un intermediario, mejora los procesos de negocio gracias a la descentralización y reduce el tiempo de entrega.

Los Smart Contracts poseen cláusulas contractuales aprobadas que se convierten inmediatamente en programas informáticos ejecutables. Esta operación queda registrada en la cadena de bloques y es inmutable. Son numerosos los sectores que ya están aplicando los Smarts Contracts como, por ejemplo, el sector de las finanzas, sistemas de distribución y sobre todo el sector público para demostrar las identidades de los licitadores y automatizar el proceso de licitación.

En resumidas cuentas, son capaces de realizar actividades sin intervención humana.

Otro aspecto muy importante que se trata en este trabajo es la Identidad digital, la cual sirve para identificar al usuario en Internet. Hoy en día el control es centralizado, por lo que se pierde control sobre esta información. Gracias a la tecnología de bloques esta

información se puede descentralizar lo que permitiría elegir a quién se comparte la información y cómo se comparte, evitando que esta se comparta a terceros sin permiso.

El reglamento más importante respecto a la identidad digital europea es el EIDAS, (Reglamento de Identificación, Autenticación y Servicios Fiduciarios Electrónicos). Todo lo que tiene que ver con las credenciales emitidas y reconocidas por el gobierno. El objetivo es evitar la suplantación de identidad.

En el segundo Bloque hago referencia a las criptomonedas, en el que hablo abiertamente sobre el Bitcoin, su historia, los comienzos, su continua fluctuación y, sobre todo, toda la especulación que hay detrás de esta moneda digital.

He realizado una tabla sobre las 10 criptomonedas más importantes del mercado. Explicando las cuatro principales y algunos gráficos donde se muestra durante varios años su valor y la cantidad comprada.

Explico qué es el proceso de “minería”, quien realiza esta función, los “mineros”, son las personas autorizadas a emitir las criptomonedas y a distribuirlas una vez que quieran darle uso. Una red de minería está formada por miles de nodos interconectados, evitan que se haga un doble gasto de las monedas y encriptan mediante unos códigos la información para evitar que los hackers puedan falsificarla o atacarla.

Se ha realizado una clasificación de redes de las criptomonedas, pudiendo ser centralizadas, descentralizadas o distribuidas. La mayoría de las criptomonedas poseen una red descentralizada, contando con subredes dentro de una gran red principal, de esta manera son capaces de tener un mayor control y una mejor coordinación.

En el último apartado he creado mi propia criptomoneda a la que la he llamado DBH44, en este apartado he diseñado un manual en el que paso a paso explico los procesos necesarios para crear una propia criptomoneda.

En el tercer y último bloque he elaborado una propuesta de guía de curso sobre la tecnología Blockchain, un curso complementario al máster de Comercio exterior de la Universidad de Valladolid. Impartido en la facultad de comercio del 11 de enero 2021 hasta el 26 de febrero.

Este curso constará de 4 bloques:

- CONCEPTOS DE BLOCKCHAIN & BITCOIN (32 h)
- OPORTUNIDADES DE NEGOCIO: BLOCKCHAIN PARA EMPRESAS. (40 h)
- LEGALIDAD FISCAL PERSONALY EMPRESARIALSOBRE EL BLOCKHAIN (59 h)
- PROGRAMACIÓN BLOCKCHAIN (44 h)

En cada módulo se explica de que trata, los objetivos generales que se pretende conseguir y el programa de la asignatura. Hay un certificado de la universidad de Valladolid «curso en Blockchain» por 175 horas. En la guía también aparece las fechas de exámenes, presupuesto, matrícula y el profesorado.

Con esta aplicación práctica, concretada en una oferta docente, se ha querido respaldar la competitividad del alumnado y de la economía española en el complejo campo de los mercados internacionales y del comercio exterior.

6. BIBLIOGRAFÍA

Ahn, J. (2019). “A Model for Deriving Trust and Reputation on Blockchain-Based e-Payment Syste”, *Appl. Sci*, 9(24), 5362

Ali, H. (2018). “Towards Secure IoT Communication with Smart Contracts in a Blockchain Infrastructure”, *International Journal of Advanced Computer Science and Applications*, Vol. 09, Nº. 10.

Ali, J., Ali, T., Musa, S. *et al*. (2018).” Towards Secure IoT Communication with Smart Contracts in a Blockchain Infrastructure”, *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 09, Nº. 10.

Behnke, K. (2019). “Boundary conditions for traceability in food supply chains using blockchain technolog”, *International Journal of Information Management*, June 2019

Berkely, J. (2015). “The trust machine”, *The Economist*, October 2015.

Bogner, A., Chason, M . et al. (2016). “A Decentralised Sharing App running a Smart Contract on the Ethereum Blockchain”, *Proceedings of the 6th International Conference on the Internet of Things*, November, pages 177–178

Buitennheck, M (2016) “Understanding and applying Blockchain technology in banking: Evolution or revolution?”, *Journal of Digital Banking*, Vol. 1, 2, pages 111–119

Cheng, S., Daub, M., Domeyer, A. et al. (2017). “Using blockchain to improve data management in the public sector, Digital Mckinsey Company”.

Ciaian, P (2018) “ Journal of International Financial Markets, Institutions and Money”, ELSEVIER, Short and long run evidence from BitCoin and altcoin markets, Volumen 52, January 2018

Dewey, J. (2019) “Blockchain &Cryptocurrency”, Global Legal Insights xxxx

Francisco, K (2018) “The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency”, MDPI, January 2018.

Ganne, E (2018). ”¿Pueden las cadenas de bloques revolucionar el comercio internacional?”, Organización Mundial del Comercio.

Harris, P., Eziokwu, I .et al. (2017) “A Triplicate Smart Contract Model using Blockchain Technology”, *Circulation in Computer Science*, June 2017

Houben, R., Snyers, A. (2018). *Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion*, Policy Department for Economic, Scientific and Quality of Life Policies. European Parliament, Brussels.

Huckle, S., Bhattacharya, S . et al. (2016) “Internet of Things, Blockchain and Shared Economy Applications”, *Procedia Computer Science*, December 2016, Pages 461-466, Vol 98

Kakavand, H (2017) “The Blockchain revolution: an analysis of regulation and technology related to distributed ledger technologies” DLA PIPER CONFIDENTIAL DRAFT, January 2017

Kakavand, H., Kost,N (2017).” The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies”, *SSRN Electronic Journal*.

Kosba, A., Miller, A. (2016). “Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts*”. Proceding of 2016 IEEE Symposium on Security and Privacy (SP) 839*-858. 10.1109/SP.2016.55.

Kristeten, N (2018) “Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring”, *Journal of Medical Systems*, Springer.

Küpper, D (2019) *Blockchain in the Factory of the Future,* Boston Consulting Group

Liang, J., Shetty, S. et al. (2017) “ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability”, *IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, May 2017, Pages 468-477

McCorry, P., Shahandashti, F., Siamak, S (2017) “A Smart Contract for Boardroom Voting with Maximum Voter Privacy*” School of Computing Science*, January 2017

Morhaim, L (2019) “Blockchain and cryptocurrencies technologies and network structures: applications, implications and beyond” Hal-02280279

Pólvora, A (2019) “Blockchain and tomorrow assessing multidimensional impacts of distributed ledger technologies”, *Joint Research Centre*, Brussels, July 2019.

Preukschat, A (2019)” El nuevo entorno tecnológico que va a cambiar nuestras vidas, Blockchain: Revolución industrial de Internet”, Booket

Rabah, K (2017) ”Challenges & Opportunities for Blockchain Powered Healthcare Systems”, *Mara Research Journal of Medicine and Health Sciences* Vol. 1, No. 1, October 2017, Pages 45 – 52

Reed, D., Tobin, T (2017). *The inevitable Rise os Self- Sovering Identity*, Sovrin Foundation, March 2017

Rohr, J (2019) “Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets”, *Hastings Law Journal*, Volume 70.

Swan, M (2017) “Anticipating the Economic Benefits of Blockchain”, *Technology Innovation Management Review,* October 2017 (Volume 7, Issue 10).

Torras, J (2018) “Criptomonedas desde cero. Blockchain y *Bitcoin.: Guía de introducción en el mundo de las criptomonedas, de manera simple y con ejemplos prácticos”*

Town, S., “Introduction to Stellar Lumens (XLM) – The Future of Banking”, Stellar Lumens, April 2018.

Turkanovìc, M (2017) “EduCTX: A Blockchain-Based Higher Education Credit Platform”, IEEE Acess

Valente, P., “Bitcoin and Virtual Currencies Are Real: Are Regulators Still Virtual?”, *INTERTAX*, Volume 46, Issue 6 & 7, 541-549.

Zheng, Z., Xie, S. Dai, H. et al. (2020) “An Overview on Smart Contracts: Challenges, Advances and Platforms”, *Future Generation Computer Systems*, Volume 105, April 2020, Pages 475-491.