GRADO EN COMERCIO

TRABAJO FIN DE GRADO

“BLOCKCHAIN Y CRIPTOMONEDAS”

CARLOS ALONSO HERNÁNDEZ

FACULTAD DE COMERCIO

VALLADOLID, JULIO 2019

FACULTAD DE COMERCIO
Universidad de Valladolid

UNIVERSIDAD DE VALLADOLID
GRADO EN COMERCIO

CURSO ACADÉMICO CUARTO

TRABAJO FIN DE GRADO

“BLOCKCHAIN y CRIPTOMONEDAS”

Trabajo presentado por: Carlos Alonso Hernández

Firma:

Tutor: Victoria Cánovas Sánchez

Firma:

FACULTAD DE COMERCIO

Valladolid, Julio 2019

ÍNDICE

Índice de Contenido

Índice de Ilustraciones

1. Introducción

El Blockchain y las Criptomonedas son el reflejo de cómo la tecnología puede cambiar la sociedad y la economía de una forma inimaginable. Se trata de una nueva tecnología que está influyendo en nuestros sistemas y en nuestra forma de comerciar, hasta límites nunca vistos. Son la respuesta a problemas de ámbito financiero, legal o de salud, con utilidades reales como firmas digitales y transacciones instantáneas, contratos inteligentes o el suministro de información en tiempo real, entre otros muchos usos que pueden desarrollarse con esta tecnología.

El objetivo principal de este trabajo es el de conseguir recopilar la máxima información posible acerca de esta nueva tecnología, para así poder explicar qué son, sus ventajas e inconvenientes y sus usos reales, para entender de una manera más clara y sencilla cómo puede beneficiar al conjunto de la sociedad. Centrándome más específicamente en las aplicaciones de la Blockchain y las Criptomonedas, como cuáles son las más importantes, cómo se crean o dónde se pueden obtener entre otros aspectos.

Hablaremos acerca de cómo la tecnología Blockchain elimina los intermediarios en las transacciones, a través de su tecnología de “contabilidad distribuida”, donde se anotan todas las transacciones que suceden en la red, las cuales se agrupan en bloques y están enlazadas entre si. De igual manera hablaremos de los mineros, que son los encargados de autorizar las transacciones dentro de la cadena de bloques, resolviendo un acertijo matemático, del cual reciben a cambio una recompensa en forma de moneda digital.

Para ello buscaremos información en las diferentes secciones y temas correspondientes, dentro de páginas web de desarrolladores, blog especializados o revistas online entre otros. Tratando de ser lo más riguroso y completo para así ofrecer al lector una amplia visión de este panorama tecnológico. Y tratando de tener la información lo más actualizada posible dentro de un panorama cambiante. Además de dar respuesta a preguntas de cómo esta nueva tecnología puede solucionar problemas dentro de los distintos ámbitos sectoriales.

Este Trabajo de Fin de Grado (TFG) busca complementar y desarrollar la formación obtenida durante el transcurso del Grado en Comercio, en ámbitos legales, financieros o de nuevos modelos de negocio entre otros. Y cómo estos afectan en el día a día a clientes, empresas, proveedores y al conjunto de la economía.

El esquema estructural del TFG se divide en dos grandes bloques: la tecnología Blockchain y las Criptomonedas.

La Blockchain tiene un potencial extraordinario y una gran capacidad de desarrollo y expansión. Estamos asistiendo al nacimiento de una tecnología que está empezando a cambiar lentamente las formas de optimizar nuestras relaciones, ahorrar costes administrativos o favorecer cooperaciones entre diferentes sectores. Busca ser la solución a problemas de lucha contra el fraude comercial o contra la propiedad intelectual. Además de las romper barreras internacionales con un mercado globalizado. Para el consumidor de a pie, la Blockchain es la solución al problema de comisiones bancarias y de confianza en el sistema financiero.

Se trata de la tecnología que cambiará nuestras vidas tal y como la cambió la aparición de internet. Solo hay que ver el impacto que han generado empresas punteras en este ámbito como Google, Amazon o Facebook, todas ellas presentes en nuestro día a día. La próxima evolución de internet, es el internet del valor, y es posible gracias al descubrimiento de la tecnología Blockchain.

Permitiendo compartir valor de una forma digital y descentralizada, sin necesidad de una entidad de confianza que imponga sus reglas a los participantes. Esa capacidad es la que convierte a esta tecnología en algo tan novedoso y apasionante. Y que además, tiene todo el potencial necesario para revolucionar nuestra forma de entender el mundo.

Por otra parte, las Criptomonedas son un elemento dentro de la propia Blockchain, que sirven entre otros usos para poder financiar los nuevos proyectos a través de ofertas iniciales de monedas. Así como para el negocio bursátil y especulativo al igual que un mercado bursátil, pero con la diferencia de que estos son descentralizados y no dependen de ninguna entidad central, sino de la confianza depositada en el valor del criptoactivo.

La repercusión de las Criptomonedas es tan alta y el miedo al cambio del sistema tradicional, hace que sean extremadamente volátiles y dificiles de aplicar una regulación por los organismos oficiales. Habiendo quienes ven en esta tecnología un futuro claro y prometedor que permita grandes avances en muchos sectores y los que lo ven como una pura burbuja especulativa y que con el paso del tiempo carecerá de valor. Se trata de un miedo infundido por la falta de información y por una posible competencia.

Lo único que está claro, es que la Blockchain y las Criptomonedas son una realidad y por lo tanto hay que tenerlas en gran consideración pues se trata de una tecnología que puede cambiar el panorama mundial de una manera nunca vista. Y la pregunta que todo

el mundo se hace: ¿Perdurará con el paso de los años? Solo el tiempo y la adopción de esta nos podrán responder a una pregunta sin respuesta.

Por último, me gustaría agradecer la ayuda y orientación de José Ignacio Delgado, apoderado de Gestión integral de Banco Sabadell. Ya que sin él no habría podido desarrollar tan compleja temática. Ha conseguido marcar las pautas y conseguir que transmita la esencia de la temática Blockchain.

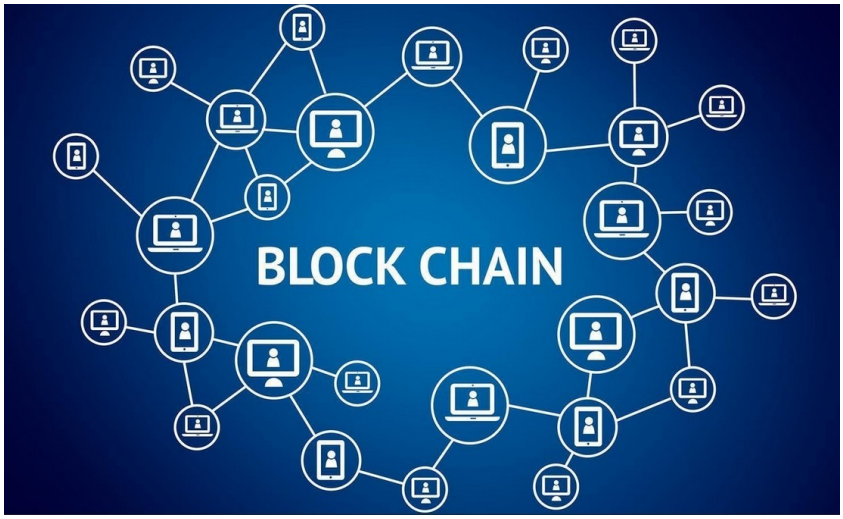
También quiero agradecer a mi profesora y tutora Victoria Cánovas Sánchez, el apoyo recibido para la conclusión de mis estudios universitarios y por la paciencia y asesoramiento durante el TFG. Sin olvidarme de todos los profesores y profesoras que me han impartido clases durante esta etapa.

2. Blockchain

¿Qué es la Blockchain?, explicado en términos coloquiales se trata de una base de datos compartida que hace las funciones de un libro de contabilidad de manera que registra cada operación, con sus cantidades, fechas y participantes. La Blockchain se distribuye en múltiples nodos, que no son más que ordenadores conectados a la red. Todos estos nodos se interconectan entre sí formando una red descentralizada y con la utilización de un protocolo común.

Esto se conoce como un "consenso" y es una de las partes imprescindibles de la Blockchain. Este consenso es su protocolo común que verifica y confirma las transacciones que se realizan y asegura que sean irreversibles. Este otorga a los usuarios, una copia inalterable y actualizada de todas las operaciones que se realiza en la Blockchain.

Ilustración 1 Nodos Blockchain



Fuente: Pastor (2018)

La Blockchain al estar descentralizada presenta unas ventajas enormes para prevenir el fraude. Ya que no se puede hacer copias o manipularla. Tampoco requiere de un intermediario centralizado que identifique y compruebe esta información, sino que se comprueba de manera íntegra entre los nodos que la componen y son estos los que la validan. Pero cuando nos referimos a la Blockchain, no solo se trata de una sola, ya que puede haber tantas como queramos y pueden estar interconectadas entre si. Podemos diferenciar entre "Blockchain privadas", "Blockchain públicas" o incluso "Blockchain híbridas". La primera Blockchain fue lanzada en 2009 y es la red sobre la que trabaja el

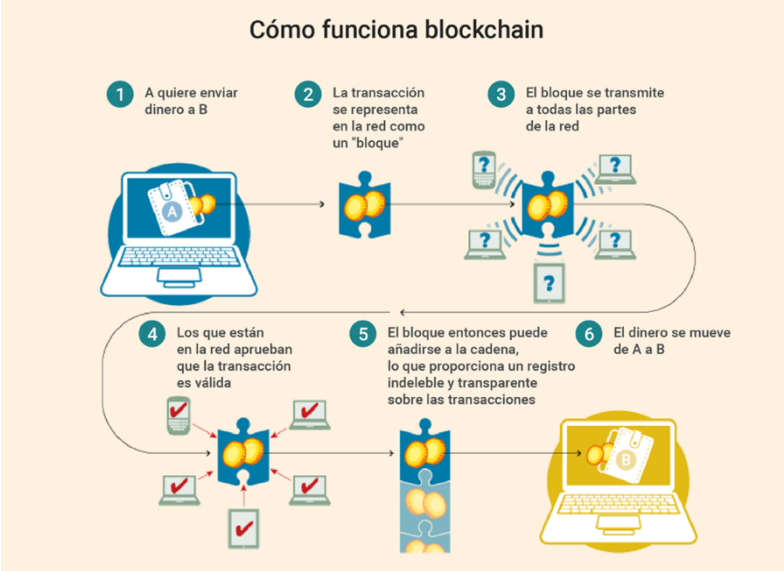
Bitcoin o el Ethereum, y es de carácter público ya que cualquiera puede participar en ella (Vega, 2017).

Los mensajes y transacciones se hacen de manera encriptada a través de un token [1], que no es otra cosa que una representación de información de la red. Esta información puede ser desde un activo financiero, en forma de dinero como un Bitcoin, a un archivo de un contrato de alquiler. Cualquier información, bien o servicio puede ser transferido a través de esta dentro de los marcos legales.

2.1 ¿Cómo funciona la Blockchain?

El proceso para realizar una transacción en la Blockchain puede explicarse de manera muy sencilla:

Ilustración 2 Funcionamiento transacción Blockchain



Fuente: Financial Times (2018)

Una persona A quiere enviar dinero a una persona B, entonces genera una transacción hacia esta persona. Esta transacción se representa como un “bloque” dentro de la red. El bloque al introducirse en la red tiene que ser validado por los diferentes nodos de la red. Una vez que se valida la transacción, el bloque se añade a la cadena de bloques como una anotación a un libro de contabilidad. De manera que este registro es inalterable y se confirmaría el movimiento del dinero de la persona A a la persona B

[1] Token: Conjunto de caracteres que tiene un significado coherente en cierto lenguaje de programación.

2.1 Tipos de Blockchain

Las Blockchains se puede dividir en dos grandes grupos: privadas y públicas. Y una última que sería una mezcla de las dos.

- ◊ Blockchain públicas: Como su propio nombre indica cualquier persona puede acceder y consultar las transacciones realizadas. En este tipo de redes se utiliza un protocolo común que permite a los usuarios registrar transacciones en la base de datos. Las anotaciones que se hacen son inalterables, pero si que pueden verificarse de forma independiente. Son descentralizadas, ya que ningún usuario tiene más poder que otro dentro de la red. Los propietarios que hacen las transacciones no son identificables, pero si sus direcciones que son rastreables, debido a su carácter público.

- ◊ Blockchain privadas: Son redes en las cuales no todos los datos inscritos en la Blockchain tienen difusión pública y solo los usuarios que la componen pueden acceder y consultar transacciones. También se caracterizan por ser distribuidas, ya que el número de nodos que la componen está limitado al número de participantes o a cierto número de ellos. Además de poder establecer el nivel de anonimato que se quiere para la realización y protección de transacciones. De tal manera que los usuarios que registran anotación dentro de la cadena pueden estar identificados o no.

- ◊ Blockchain híbridas: Son la mezcla de las privadas y públicas. Se tratan de redes que normalmente no están abiertas al público y que su gestión corresponde a varias entidades. Suelen ser utilizadas por gobiernos y empresas en las que se producen grandes cantidades de transacciones (Calvo, 2018).

2.2 Elementos básicos Blockchain

Para una mejor comprensión de la tecnología Blockchain (Preukschat, 2017) explicaremos los elementos básicos que la componen:

- ◊ Nodos: pueden ser desde un ordenador personal hasta una megacomputadora. Todos los nodos tienen que poseer el mismo software

para poder comunicarse entre si, ya que sin este no podrían interconectarse ni formar parte de la red de la Blockchain.

◊ Protocolo estándar: es el software informático que permite que los nodos puedan comunicarse entre sí. Existen protocolos muy conocidos como el TCP/IP[2] para internet. El protocolo de la Blockchain actúa de tal manera que genera un estándar común para la comunicación entre los ordenadores participantes en la red.

◊ Una red Peer to Peer (P2P): se trata de una red de nodos interconectados entre sí bajo una misma red. Un ejemplo de red P2P[3] es BitTorrent, que es un protocolo diseñado para el intercambio de archivos P2P a través de Internet.

◊ Un sistema descentralizado: en los sistemas descentralizados a diferencia de los centralizados, todos los ordenadores conectados a la red la controlan de manera igualitaria debido a que están al mismo nivel y se comportan como iguales entre sí, es decir no hay un nodo central ni una jerarquía.

2.3 Aplicaciones Blockchain en los diferentes sectores

Las aplicaciones que tiene la tecnología Blockchain son infinitas e inimaginables muchas de ellas. Van desde aplicaciones dentro del sistema financiero, sistemas de almacenamiento, mercados de valores, etc… Analizaremos las más importantes (Rodriguez, 2016), y las que mayor impacto y proyección de futuro tienen:

[2] TCP/IP: Siglas de Protocolo de Control de Transmisión/Protocolo de Internet
[3] Red P2P o Red peer-to-peer: Se trata de una red entre iguales, una red de ordenadores que funcionan sin servidores fijos, de manera que todos los nodos de esta se comportan como iguales.

1. Aplicaciones tecnológicas dentro del sistema financiero.

La Blockchain va más allá del Bitcoin y de las criptomonedas, de ahí que esta tecnología haya despertado el interés de bancos y otras entidades financieras, hasta el punto de que el FEM [4] considera que la Blockchain será el epicentro financiero mundial dentro de unos años. Más del 80% de los Bancos reconoce estar trabajando en aplicaciones y productos basados en la tecnología Blockchain.

Ilustración 3 Blockchain y Bancos

Fuente: BitcoinOnAir (2017)

El nacimiento de la banca descentralizada fue en la década de los noventa a través de un grupo de personas conocidas como los Cypherpunks.[5] Que decidieron aprovechar el potencial que les ofrecía internet y decidieron crear un sistema financiero abierto sin ninguna entidad centralizada que lo regulara y que además fuera anónimo y transparente.

Pero no fue hasta el año 2008 con el nacimiento del Bitcoin cuando se inicia una primera ola de descentralización en los pagos, transferencias internacionales y las remesas. Lo realmente importante fue mostrar al mundo que no era necesario contar con un banco o ningún otro tercero de confianza para llevar a cabo las laborales que tradicionalmente había desempeñado la banca.

Sin duda también influyo la crisis financiera del año 2008, donde el sector bancario experimento dificultades para mantener los niveles de rentabilidad de los años anteriores. Produciéndose una fuerte tendencia de innovación a partir de la tecnología Blockchain. Desde bancos e instituciones financieras fue invirtiéndose capital para el desarrollo e investigación de la tecnología Blockchain.

El cambio que se está produciendo en la banca, es de carácter cultural y regulatorio, debido a las nuevas formas de consumo y hábitos de vida que hacen que los productos tradicionales se queden obsoletos dando cabida a nuevos competidores y a un importante cambio del modelo comercial.

[4] FEM: Acrónimo de Foro Económico Mundial

[5] Cypherpunks: Grupo de personas que aboga por el uso de la criptografía para garantizar la privacidad de los individuos. El movimiento se inició en la década de 1990.

Estos nuevos competidores son capaces de des-intermediar créditos y pagos. Actualmente contamos con un amplio número de empresas que, frente a la incapacidad de innovar de las grandes firmas, se muestran flexibles y ágiles y completamente volcadas con el cliente.

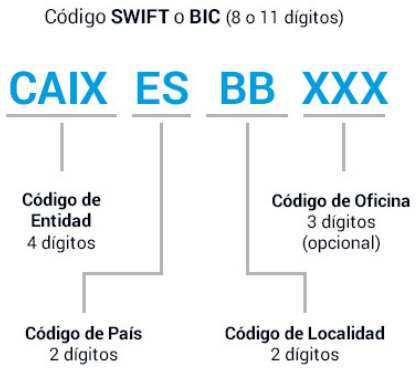
En la era digital en la que vivimos, adquieren un alto valor los servicios de liquidez inmediata que hacen que el usuario tenga una grata experiencia. De tal manera que la propia experiencia del usuario sea la principal ventaja competitiva que determine el crecimiento de estas nuevas empresas. Sin olvidarnos de gigantes tecnológicos como son Google, Apple, Facebook y Amazon que están desarrollando aplicaciones bancarias basadas en la tecnología Blockchain o hasta incluso el lanzamiento de su propia criptomoneda como en el caso de Facebook, que tiene previsto lanzar "Libra" para el año 2020.

La Blockchain nace como alternativa para descentralizar la confianza depositada en las instituciones financieras. De manera que se automaticen procesos para innovar en los mecanismos y modelos de negocios. Pero va más allá de programar el dinero, nos genera confianza, identidad, activos y contratos. Y nos permite realizar pagos, transacciones, autentificaciones y transmisión segura de información en tiempo real.

Tradicionalmente, ha existido un problema de falta de operatividad entre las distintas entidades financieras debido a la diferente regulación que se aplica en cada país. Actualmente existen numerosos proveedores de pagos, siendo el más popular y utilizado el sistema SWIFT[6] que utilizan la mayoría de los bancos para comunicarse entre si.

La propia naturaleza del sistema SWIFT hace que las transferencias entre bancos se demoren entre dos y cuatros días. Lo que abre la necesidad de establecer líneas de crédito para aquellas empresas que tengan operaciones globales. Si estos pagos fueran instantáneos, reducirían en gran medida el volumen del circulante. Afortunadamente gracias a las Blockchains este problema puede solucionarse, siendo una vía para llevar a cabo pagos internacionales.

Ilustración 4 Código SWIFT



Fuente: Imagin Bank (2019)

[6] SWIFT: Acrónimo del ingles: Society for Worldwide Interbank Financial Telecommunication.

2. Almacenamiento en la nube distribuido.

La tecnología Blockchain permite no depender de almacenamientos centralizados, ofreciendo la posibilidad de un almacenamiento de datos y archivos en una red P2P de manera que no toda la información quede guardada en un mismo sitio.

Ilustración 5 Storj.io

Fuente: Storj (2019)

Los datos se encriptarían dentro de la Blockchain y se distribuirían entre los distintos nodos. De forma que hubiera múltiples copias en distintos lugares de la red, haciendo al sistema más seguro ante posibles ataques de hackers o pérdida de información por problemas técnicos o catástrofes naturales.

La empresa pionera en gestión de datos descentralizados ha sido Storj. Desarrollando un sistema en el que los usuarios pueden alquilar automáticamente el espacio sin usar de sus ordenadores a otros usuarios, mientras que los que necesiten espacio pueden pagar por ello.

Los costes se abaratarían hasta un 80% en comparación con los operadores tradicionales de almacenamientos de datos (Storj, 2018).

3. Gestión de Identidades

La tecnología Blockchain permite a los usuarios tener una identidad digital difícil de manipular, a través de una ID basada en la Blockchain, que permitirá reemplazar los usuarios y contraseñas online. De tal manera que con nuestra identidad podamos acceder a aplicaciones y sitios web, firma de documentos digitales, etc. Ya hay algunas compañías que ofrecen este servicio como son Onename o Keybase.

La compañía Onename ofrece un puente entre la identidad física y digital (Onename, 2019). De tal manera que la identidad sea más segura, de confianza y privada dentro del panorama digital.

4. Registro y verificación de datos

Al igual que se pueden almacenar archivos, la Blockchain también sirve para almacenar cualquier otro tipo de información, generando un registro altamente inalterable, más seguro que los datos tradicionales y sin intervención de terceros. Empresas como Tierion o Proof of Existence ya ofrecen este tipo de servicios.

Ilustración 6 Tierion

Fuente: Tierion (2019)

Sus posibilidades son infinitas y van desde el sector público hasta el privado, entre las que destacan:

- ◊ Clínicas y Hospitales: Registro universal de datos y historial médico de pacientes de manera que se pudiera gestionar de manera conjunta en todos los centros.
- ◊ Registro de la propiedad: Creación de un registro en el que figure el propietario de cada inmueble y sus transacciones de compraventa. Evitando manipulación y fraude. Ya hay algunos países que están desarrollando programas de registro como son Japón o Suecia, entre otros.
- ◊ Registro de propiedad intelectual y creación de productos digitales: Registro universal que proteja a los autores de música, fotos o libros electrónicos entre otros. De tal manera que se recoja la autoría y la fecha de creación para que esta información se quede cifrada en la Blockchain. La compañía Proof of existence ya ofrece dicho servicio por unos costes realmente bajos a los tradicionales.
- ◊ Registro de antecedentes penales a nivel internacional: Registro de datos de antecedentes penales de todos los ciudadanos del mundo, de manera que se cree un entorno más seguro.

5. Ejecución automática de contratos

Algunas Blockchain, como por ejemplo la de Ethereum permiten la posibilidad de crear “contratos inteligentes”. Se tratan de programas de software que recogen los términos de un acuerdo entre ambas partes, los cuales se almacenan en la Blockchain y se auto ejecutan cuando se cumplen las condiciones especificadas en el contrato.

De esta manera se eliminan los intermediarios, agilizando tiempos, costes y retrasos burocráticos. Las posibilidades son enormes y más si se combinan con tecnologías como el IoT[7]. Destacan:

- ◊ Conexión de información de un contrato de compraventa vía GPS[8]: de forma que se emita el pago al proveedor y al transportista cuando el paquete llegue al destino sin necesidad de hacer ningún tramite adicional. De tal manera que el proceso sea automático y eficaz.

- ◊ Elaboración de contratos inteligentes para leasing de vehículos: que permitan entre otras funciones, bloquear el acceso o impedir el acceso al vehículo el caso de impago.

6. Seguimiento de la cadena de suministros y prueba de procedencia

En la actualidad es muy habitual que muchas empresas, tengan diferentes proveedores para realizar sus productos, estableciendo una larga cadena de suministros, que en muchas ocasiones hace que sea difícil hacer un seguimiento de esta.

Ilustración 7 Skuchain

Fuente: Skuchain (2019)

Compañías como SkuChain o Everledger ya están utilizando esta tecnología para hacer todo tipo de seguimientos y garantizar la procedencia de los productos, desde ingredientes alimenticios, hasta obras de artes. De tal manera que se eviten falsificaciones y se pueda facilitar la trazabilidad de los productos de cara a certificaciones.

La propia compañía Skuchain está desarrollando un programa piloto en asociación con el Banco Nacional de Canadá, para lograr una solución viable para la cadena de suministros, basada en tecnología de contabilidad distribuida.

[7] IoT: Acrónimo del ingles “Internet of Things” o Internet de las cosas.
[8] GPS: Sistema de Posicionamiento Global

7. Servicios de notaría

La utilización de servicios de notaría dentro de la Blockchain es muy fácil y barata en comparación con el servicio tradicional. Permitiendo crear registros inmuebles, verificando la autenticidad de cualquier documento registrado y eliminando la necesidad de que una autoridad centralizada o tercero lo certifique.

Ilustración 8 Stampery

Fuente: Stampery (2019)

Stampery y Blockverify son dos compañías que utilizan la Blockchain para verificar todo tipo de documentos, de manera que se certifique la fe de autoría (quien lo ha creado), de existencia (momento en el que se creó) y de su integridad (que no ha sido manipulado).

Garantizando la privacidad del documento registrado y de aquellos que solicitan el servicio, de manera que se confirma la seguridad y se abaratan los costes de notaría eliminando las elevadas tarifas de los notarios.

8. Votar por internet

La Blockchain puede resolver uno de los grandes problemas de los sistemas de votación por internet, como es el anonimato del voto. De tal manera que se pueda garantizar que una persona no vote más de una vez y la privacidad de su voto. Además de que al no estar gestionada por ninguna autoridad central no es posible su manipulación.

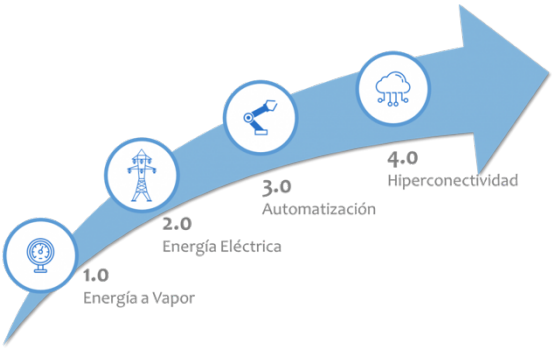
También hay que hablar de otra ventaja como es la auditabilidad que ofrece la blockchain frente a los sistemas tradicionales. Se podría incluir nodos públicos, nodos auditores y nodos de medios de comunicación, permitiendo auditar todo el proceso y comunicando los resultados a tiempo real sin que ello comprometa la seguridad del sistema.

Este tipo sistemas mejoraría la rapidez y abarataría los costes, facilitando cualquier tipo de votación. La primera votación con tecnología Blockchain fue llevada a cabo por el partido político danés Liberal Alliance en el año 2014. Además de que países europeos como Estonia y Suiza, ya utilizan el voto online que ha sido recogido de manera satisfactoria por los ciudadanos residentes en el extranjero.

2.4 La industria 4.0 y Blockchain

Actualmente nos encontramos inmersos dentro de la cuarta revolución industrial. La digitalización y la coordinación cooperativa de las unidades productivas va a ser un nuevo hito dentro del desarrollo industrial. Actualmente, la demanda cada vez es más sofisticada y requiere que las empresas den un salto de calidad haciendo productos cada vez más inteligentes y sofisticados. El objetivo de esta cuarta revolución industrial viene determinado por las nuevas fábricas inteligentes, capaces de producir miles de configuraciones diferentes de un producto o fabricar pequeños lotes de productos a precios muy reducidos.

Ilustración 9 Evolución de las industrias



Fuente: Rioja2 (2017)

La digitalización es la base de esta revolución industrial, que dará lugar a la denominada industria inteligente, sustentada en tecnologías como el IoT, las comunicaciones M2M[9], plataformas en la nube, robots inteligentes o impresiones 3D entre otras aplicaciones. Como toda nueva innovación tecnológica, se generan nuevos retos tecnológicos que están estrechamente relacionados con la cadena de bloques.

Autentificación e integridad de datos en dispositivos industriales

El internet de las cosas es una de las tecnologías clave de esta revolución, ya que las necesidades muy específicas que tiene este sector industrial permiten el desarrollo de ecosistemas amplios, escalables y con fácil integración dentro de los sistemas empresariales. La Blockchain podría ser una de las posibles soluciones al reto de identidad de los dispositivos IIoT[10], ya que ofrecen una gestión de identidad descentralizada, sin depender de una autoridad de certificación centralizada. Además, que actualmente las soluciones industriales requieren del despliegue de una CA[11] por cada fabricante industrial, que provoca una gran dependencia de sus proveedores, falta de control e incertidumbre.

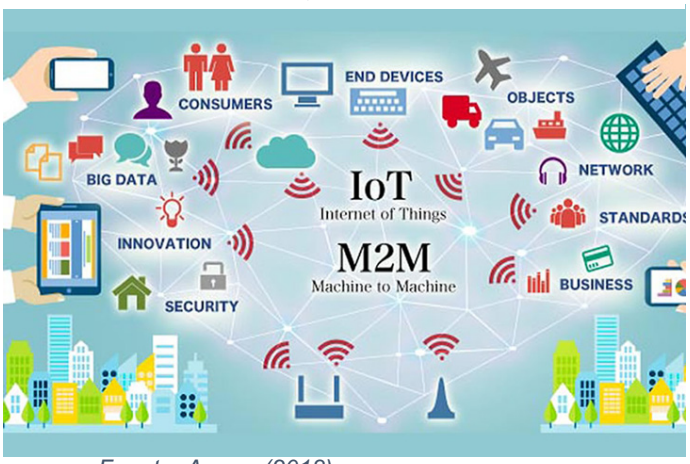
[9] Comunicaciones M2M: Comunicación Machine to Machine, intercambio de información o de comunicación en formato de datos entre dos maquinas remotas.
[10] IIoT: Industrial Internet of Things, Aplicaciones industriales del Internet de las cosas.
[11] CA: Certification Authority, Autoridad de Certificación.

La descentralización de la Blockchain permitiría gracias a sus características el registro de la actividad de cada sensor dentro de las redes industriales, garantizando la integridad de los datos y evitando manipulación de registros.

Transacciones M2M en la Blockchain

Las fabricas inteligentes del futuro, estarán compuestas por dispositivos IIoT que funcionarán de manera autosuficiente. La Blockchain facilita el uso de tal manera que los propios dispositivos mediante comunicaciones M2M, serian capaces de llegar a acuerdos de suministros de materias primas, mantenimientos o logísticos. Quedando reflejados a través de Smart Contracts y cuyos pagos se ejecutarían automáticamente cuando se cumplan las condiciones establecidas en el contrato.

Ilustración 10 M2M y IOT



Fuente: Amper (2018)

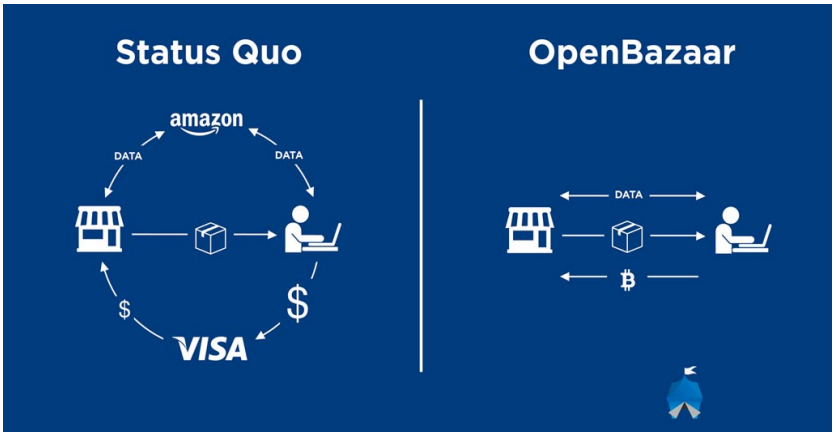
Con esta automatización de procesos se pretende eliminar o disminuir la intermediación de terceros y la interacción humana.

Los Marketplaces industriales y la Blockchain

Como ya hemos dicho anteriormente, la automatización de procesos es la clave para que la fabricación inteligente pueda llegar a producir lotes unitarios del mismo rango de precios que los que actualmente ofrecen las grandes fábricas. Según expertos en la industria 4.0, la solución de este problema pasa por la desintermediación del proceso productivo, de tal manera que las empresas puedan recibir peticiones a través de un portal descentralizado y fabricar lotes pequeños.

El acercamiento físico entre el productor y el destino final de los productos repercute en la reducción de costes logísticos y facilita que la producción pueda ser realizada por pequeñas pymes locales. Esta plataforma descentralizada es posible gracias a la cadena de bloques y a los Smarts Contracts que servirá para que no haya ningún tipo de intervención de ninguna de las partes.

Ilustración 11 Status Quo vs OpenBazaar



Fuente: AcademybyBit2me (2018)

Un ejemplo de ello es la empresa OpenBazaar, una alternativa distribuida y gratuita que pretende competir con compañías como eBay, cuya única forma de pago es a través de las Criptomonedas y del Bitcoin.

2.5 Dapps y Descentralized Autonomous Organizations (DAO)

Se tratan de aplicaciones descentralizas con tecnología P2P, tienen un código abiertos y las mejoras dentro de las mismas se aprueban en consenso por los usuarios de la aplicación. Sus datos están encriptados y almacenados en una Blockchain pública. Se necesita de un token (como el Bitcoin o Ethereum) para acceder a ella y las contribuciones de valor de los mineros se recompensan con el mismo token.

La importancia de las Dapps es su constitución como un nuevo modelo de aplicaciones y del futuro de la web. A través de Bitcoin se demostró que este nuevo modelo es viable económica y técnicamente. Las primeras Dapps proponen alternativas a gigantes del mundo digital, como OpenBazaar para eBay, Storj para Dropbox y FireChat para WhatsApp entre otras.

El pago o no por estos servicios es una opción viable. La mayoría de los usuarios de Facebook considera que es un servicio gratuito, pero realmente pagas con tu información personal, gracias a la cual Facebook ha hecho su fortuna (BBVA, 2018).

Ilustración 12 State of the DApps

Fuente: Mr.ADDON (2019)

Pero con el uso de Dapps se habilitan nuevas opciones como en las que aceptas compartir todos o parte de tus datos para acceder a los servicios, o incuso recibir ingresos por el uso de tus datos como recompensa a contribuir con la Dapp. Desde su origen la Blockchain de Ethereum ha servido para habilitar un entorno favorable para el desarrollo de estas aplicaciones y siendo la plataforma más utilizada. Surgiendo más de 2667 DApps recogidas todas en un mismo portal: The State of The DApps.

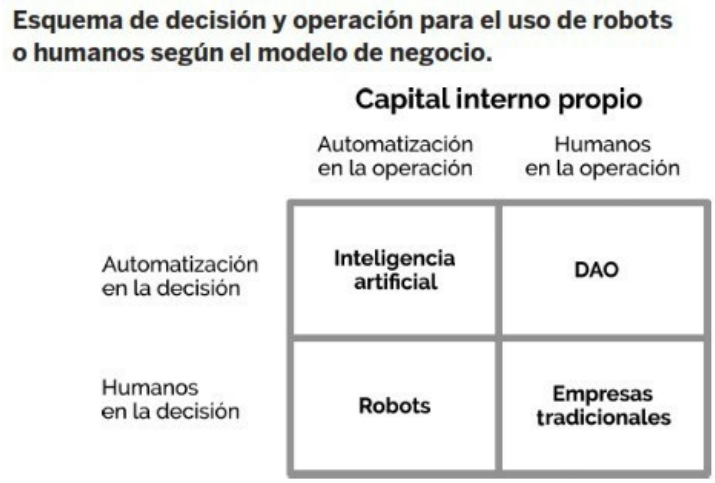
Descentralized Autonomous Organizations (DAO)

Las DAO se podrían definir como una subclase de Dapps. Dentro de las cuales se pueden ver dos conceptos:

Por una parte, las Descentralized Organizations (DO) que hacen referencia a un modelo de organización en las que los usuarios siguen un protocolo establecido por un código y ejecutado en la Blockchain. De esta manera el "poder" se divide de manera equitativas entre los participantes.

Por otra parte, están las Autonomous Agents (AA) que son el sueño de la inteligencia artificial, ya que son autómatas que capaces de emular el cerebro humano y tomar decisiones, adaptarse a situaciones y evolucionar. En la actualidad no existen versiones tan avanzadas de esto, pero si sencillas, como los virus informáticos.

Ilustración 13 Esquema de decisión en las DAO



Fuente: Preukschat (2017)

Vitalik Buterin, cofundado de Ethereum, define las DAO como: "entidades que viven en internet, existen de forma autónoma y depende de personas para realizar aquellas tareas que no pueden ejecutar por sí mismas". Una característica importante de las DAO es que tienen un capital interno de valor que sirve para remunerar como por ejemplo el trabajo de sus empleados humanos.

2.6 Seguridad y Blockchain

La seguridad representa un apartado muy importante a la hora de que una empresa o persona tome la decisión de inversión. Esto queda reflejado en los 81.600 millones de dólares que las empresas destinaron en seguridad en 2016 (Preukschat, 2017). Aun así,

con una cifra tan alto, hay muchas de ellas que no invierten lo suficiente y se convierten en el blanco perfecto para todo tipo de ataques.

Ilustración 14. Seguridad Blockchain

Fuente: Compteg Solution (2018)

Cuantos más dispositivos estén conectados a la red durante un ataque mayor es la incertidumbre de este ya que hay más focos potenciales de amenaza. Este último tiene una importante clave debido al IoT, ya que se estima que tendremos más de 6 billones de dispositivos conectados en un plazo inferior a 5 años (Criptonoticias, 2018). La interacción entre estos dispositivos y la Blockchain es una de las grandes promesas, por lo tanto, la seguridad tiene que ser primordial.

Amenazas en el mundo de la Blockchain

Las amenazas se van actualizando a medida que los sistemas avanzan, pero las más comunes son:

Ingeniería Social, donde sin duda el usuario es el eslabón más débil. Y lo que más utiliza son las redes sociales. Facebook, Twitter, Instagram entre otras plataformas proporcionan a los hackers una gran cantidad de información de los usuarios. Así como nuevas rutas de ataque que pueden llegar a determinar los movimientos que un usuario hace dentro de la cadena de bloques.

Servicios en la nube, son mecanismos muy útiles para reducción de costes y mejorar la escalabilidad de los sistemas de información y cada vez aumentan más. Actualmente la cadena de bloques no reside en ordenadores públicos o bajo el control de una empresa, sino que están dentro de la “nube”, de tal manera que si se compromete su seguridad se compromete la seguridad de la cadena de bloques.

Factores de riesgo internos, no se tratan de ataques externos de hackers, sino hechos por personas de dentro de las organizaciones o de dentro de las aplicaciones. La existencia de puertas traseras que permiten el acceso desde el exterior a los sistemas pone en peligro la seguridad de la Blockchain.

Reglas de seguridad y Blockchain

Las medidas de seguridad persiguen intentar prevenir en mayor medidas ataques al sistema y se tratan de propiedades que son básicas pero que ayudan a proteger la cadena de bloques:

Confidencialidad: solo los usuarios autorizados tienen acceso a la información y nadie más que ellos. En las Blockchains privadas, solamente los usuarios que tengan los permisos adecuados y estén previamente autentificados podrán acceder a la información. En las públicas, como cualquier información de cualquier nodo puede ser consultada, el nivel de confiablidad es menor.

Integridad de la información: se trata de la garantía que permite confirmar que la información original almacenada, no será alterada ni accidental ni intencionadamente. Esto significa que ninguno de los bloques, ni de las transacciones puede ser alteradas por ningún mecanismo. El número de nodos juega un papel decisivo, ya que cuantos más nodos existan, más difícil será para el atacante tener un poder computacional mayor que el del resto de la red. Y por lo tanto más difícil es alterar la información y la historia de la cadena de bloques. Llevando un histórico de todas las transacciones desde su puesta en marcha y disponiendo de un mayor número de nodos honestos, el problema quedaría resuelto. Es aplicable por igual a Blockchains privadas y públicas.

Autentificación de usuario: es un proceso que permite al sistema verificar si el usuario que pretende acceder al sistema es quien dice ser. La autentificación es complementaria a la confidencialidad y es el paso previo para conectar con la cadena de bloques. La autentificación en cadenas públicas es un intercambio de parámetros de conexión, ya que todos los ordenadores tienen el mismo derecho a usar la cadena y a conectarse. En cambio, en las cadenas privadas, la autentificación suele pasar por múltiples niveles de validación e intercambio de credenciales antes de poder acceder.

Autentificación de remitente y destinatario: este proceso permite al usuario certificar que el mensaje recibido fue enviado por el remitente y no por un suplantador. En las transacciones se conoce quien las emite, quien las recibe y a quien pertenecen los tokens (cuando nos referimos a tokens nos referimos a Criptomonedas, ya que en la Blockchain se puede intercambiar cualquier tipo de información). En la red de Bitcoin, el token clásico es la propia Criptomoneda, pero en Ethereum al poderse crear tokens la autentificación del remitente y del destinatario debe de quedar garantizada.

No repudio en origen y destino: esto se resume que en cuanto se reciba un mensaje, el remitente no puede negar haberlo enviado y el destinatario haberlo recibido.

Ya que en las cadenas de bloques toda transacción queda registrada desde sus inicios. Cada vez que un nuevo nodo participa en la red de la cadena de bloques, debe aceptar las reglas de funcionamiento y operar siguiendo las mismas.

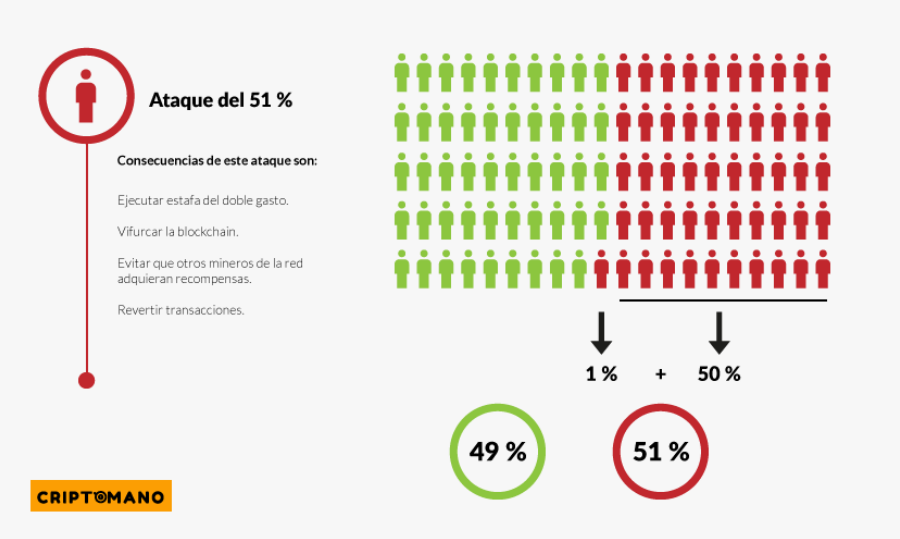
Accesibilidad: Siempre los sistemas de seguridad han de ser los más transparentes y sencillos para el usuario final. De tal manera que la interfaz no obstaculice la operativa de trabajo, manteniendo un equilibrio entre protección y facilidad de uso.

Ataques clásicos a la Blockchain

Al igual que hemos comentado la seguridad que deberían tener los sistemas Blockchain, debemos de comentar los ataques más identificados y que más se han producido durante el transcurso de esta nueva tecnología. Resaltando la importancia de invertir en la seguridad de la cadena de bloques.

Ataques del 51% en las blockchain públicas: para que se den este tipo de ataques, tendrían que ponerse de acuerdo y coordinarse para falsear la cadena de bloques el 51% de los mineros de la Blockchain. Se trata de un ataque complicado, por que no es fácil poner de acuerdo a más de la mitad de una Blockchain, ya que debería de tener más potencia de cálculo que el resto de la red. Se generen bloques falsos y se den por buenos anexándolos a la cadena de bloques. De esta manera cualquier modificación, ya sea revertiendo transacciones o haciendo dobles gastos, será dada por válida y se confirmará dentro de la cadena. Este tipo de ataque afecta a cualquier sistema descentralizado en el que se tomen las decisiones por consenso.

Ilustración 15 Ataque 51% blockchain



Fuente: Gonzales (2017)

Maleabilidad de las transacciones: se trata de un problema que se originó desde la implementación original de Bitcoin, actualmente tiene soluciones, pero en su momento

tuvo una gran repercusión. El problema consiste en que la información que hay dentro de las operaciones está muy bien protegida, pero los campos que rodean la transacción no. De tal manera que se alteraba el valor del hash de la transacción, sin validar. Pero si esta transacción se validara antes de que un minero de la red la validara, la propia Blockchain la consideraría como válida.

2.7 Aspectos legales de los Smarts Contracts

Uno de los mayores problemas de la tecnología Blockchain, es las dudas que suscita a nivel legal y que tardaran tiempo en encontrar respuesta. Sobre todo, surgen en sus aplicaciones más novedosas como son los Smarts Contracts y las DAO.

El termino de Smarts Contracts puede abarcar desde clausulas contractuales en lenguaje natural hasta casos más complejos en código informático. El mundo legal y comercial actual, no termina de encajar con la forma de operar de los Smart Contracts. Esto se debe a que no tiene la madurez suficiente, ni un uso lo suficientemente extendido.

Solo de ese modo seria posible la identificación de las buenas prácticas y la comprensión de los reguladores. Hasta que no llegue ese momento, no se podrá destapar la incertidumbre jurídica que los rodea en la actualidad. Sobre todo, a la hora de explicar que condiciones debe de reunir un Smart Contract para ser considerado legalmente vinculante ante los tribunales, desde un punto de vista de normativa de contratación. Además de que es necesario que reúna los requisitos legales de todo contracto, que tenga el consentimiento de las partes, un objeto lícito y una causa.

Ilustración 16 Smarts Contracts

Fuente: Herrera (2018)

Nuestro entorno legal concede a las partes contractuales un amplio margen para alcanzar acuerdos y contratar libremente los términos que consideren, dentro de los limites legales de objetos ilícitos o contrarios al orden público. Pero sin embargo la lógica de auto ejecución de los propios Smarts Contacts encajaría bien en la posibilidad de sometimiento de los contactos a una condición suspensiva o resolutoria.

Para que un Smart Contract aporte verdadera seguridad jurídica resulta esencial que el entorno sea testado con anterioridad y que las transacciones dentro del mismo puedan ser consideras fiables. Es esencial que se permita una serie de características:

- ◊ Acreditación de la identidad de ambas partes y de sus atributos (edad y capacidad para contratar o poderes de representación de la empresa).

- ◊ Acreditación de la integridad de los registros de las transacciones, dando una prueba de su contenido y no siendo posible su alteración a posteriori.
- ◊ Cumplimiento de requisitos regulatorios específicos de formalización o supervisión por parte de las autoridades regulatorias.
- ◊ Responsabilidades de posibles problemas de funcionamiento de un Smart Contract o por brechas de seguridad.
- ◊ Normativa de protección de datos de carácter personal, para evitar riesgos de filtración de datos.
- ◊ La sujeción a otras normas relevantes como las de derecho de la competencia o las tributarias.

Como resumen el uso de Smart Contracts, necesita una madurez y adopción que en la actualidad no tiene. Pero a medida que se acumule experiencia en el mercado se podrá contar con un grado razonable de certidumbre legal y judicial. Lo único que si que sabemos es que es necesario de la participación de profesionales con habilidades jurídicas para asegurar que el diseño de las plataformas y programas se ajusten a la normativa legal.

3. Criptomonedas

Para conocer el origen de las Criptomonedas nos tenemos que remontar a 2008, a la crisis financiera de Estados Unidos cuyos efectos del desastre económico se notaron a nivel mundial. La crisis financiera provocó la devaluación del dólar, que fue solventada con la implementación de la "flexibilización cuantitativa" por parte de los gobiernos de todo el mundo. Básicamente se trata de imprimir más dinero para inyectar efectivo en sus economías, de tal manera que se evitara otra crisis.

Ilustración 17 Criptomonedas

Fuente: TyN Magazine (2018)

Esto entre otros factores generó un nuevo problema para los bancos, ya que el valor de las monedas era bajo y las tasas de interés se habían visto recortadas, de manera que los gobiernos se vieron obligados a rescatarlos con dinero de los contribuyentes. Este proceso devaluó más la oferta de dinero existente, de tal manera que fue en este momento donde Satoshi Nakamoto entra en acción.

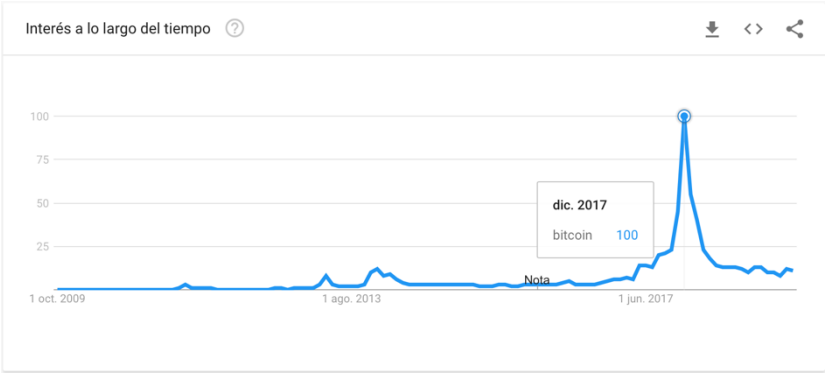
Pero ¿Quién es Satoshi Nakamoto?, se trata del inventor y desarrollador del Bitcoin. Su verdadera identidad sigue siendo desconocida hasta el día de hoy, de manera que nadie sabe ni quién es y de si se trata de una persona o de un equipo de personas. Satoshi al ver el estado financiero del mundo, decidió cambiar totalmente la forma de pensar acerca del dinero y publicó en 2008 un artículo sobre la tecnología Bitcoin detallando su funcionamiento y como se ejecutan las transacciones "peer to peer" o lo que es lo mismo entre redes de iguales. Meses más tarde proporcionó el software para poder realizar estas transacciones.

En resumen, la respuesta ante el problema financiero fue la creación de una moneda completamente descentralizada y abierta a todos, sin ningún banco central que la controle. Esta descentralización permite que todos formemos parte de la economía de Bitcoin y seamos su fuerza impulsora, en lugar de un banco central que controle su valor y su cantidad.

Aunque Satoshi no fue la primera persona en trabajar en la moneda digital descentralizada, ya que anteriormente codificadores y criptógrafos lo habrían intentado, pero sin éxito. Ya que no habrían conseguido resolver el desafío de la descentralización, que es mantener un libro global de transacciones. En este sistema descentralizado no hay ningún banco y cualquiera puede enviar una solicitud de transacción a la red, haciéndola vulnerables a ataques. Este problema fue solucionado por Satoshi con la cadena de bloques o "Blockchain" que permite mantener el libro mayor seguro utilizando marcas de tiempo, mucha potencia de procesamiento computacional y criptografía.

Como podemos comprobar en estos últimos años en Interés del Bitcoin y de las Criptomonedas ha ido creciendo de manera exponencial. Sobre todo, en los últimos dos años, alcanzando su máximo en diciembre de 2017 donde la plataforma Google Trends establece el máximo de actividad de búsquedas de dicha palabra. Así mismo siguen una tendencia similar las búsquedas de: compra de Criptomoneda (buy cryptocurrency) y compra de Vitcoin (buy bitcoin).

Ilustración 18 Búsquedas palabra Bitcoin en Google



Fuente: Google Trends (2019)

Actualmente existen más de 2100 Criptomonedas y aumentado cada día. Todo el conjunto de estas representa una capitalización de 166 Billones de euros. Aunque la mayor parte de esta capitalización está agrupada en las tres Criptomonedas más importantes: Bitcoin con un 57,78%, Ethereum con un 9,51% y Ripple con un 6,71% (Coinmarketcap, 2019).

Cabe destacar que desde su creación Bitcoin nunca ha abandonado la primera posición, siendo la Criptomoneda que más capitalización de mercado ha tenido.

3.1 Criptografía: Orígenes e Historia

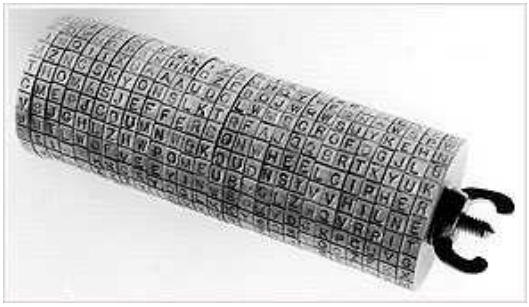
El término Criptomoneda comprende dos palabras, cripto y moneda. La palabra cripto hace referencia a la criptografía, que es la técnica que protege documentos y datos, a través de cifras y códigos (Criptotario, 2018).

La criptografía se lleva utilizando desde hace más de 4000 años, se empezó a utilizar en los jeroglíficos del Antiguo Egipto los cuales necesitaban de la Piedra de Rosetta para ser descifrados (Velasco, 2014). Vemos también referencias en libros antiguos como La Biblia que hace referencia a un sistema de sustitución de letras que data del 600 A.C o la Ilíada de Homero, donde encontramos numerosas referencias al uso de cifrado de mensaje.

Por otra parte, en la Antigua Roma se utilizaba el cifrado Cesar, que consistía en el desplazamiento de letras y la sustitución de estas por otras letras que se encuentra con un número del alfabeto, invención del genio Julio Cesar. Durante la Edad Media, la gran revolución tuvo lugar en el mundo árabe. En el siglo IX Al-Kindi sentaría las bases de ruptura de mensajes cifrados gracias a la lectura y estudio del Coran, a través del análisis de frecuencia que se basaba en analizar patrones de los mensajes cifrados para localizar repeticiones y buscar la correlación con la probabilidad de que aparezcan determinadas letras en un texto escrito.

Con el paso del tiempo la criptografía se convirtió en una pieza clave dentro de los ejércitos de todo el mundo. En la guerra de la Independencia, donde las colonias británicas de América interceptaban los mensajes del Ejercito británico y donde se desarrolló nuevos métodos de cifrado como la rueda de cifrado de Thomas Jefferson.

Ilustración 19 Cilindró de Jefferson



Fuente: Velasco J.J. (2014)

Posteriormente estuvo presente durante la Guerra de Crimea, donde Reino Unido consiguió una importante ventaja gracias al matemático Charles Babbage, el cual descifró los códigos de Vigenerère que eran considerados muy robustos y que dotó de una ventaja clave al Reino Unido.

También durante la Primera Guerra Mundial, tuvo gran importancia. Ya que Alemania había desarrollado el código Ubchi que fue desarmado por Francia y Reino Unido, permitiendo obtener una ventaja vital para adelantarse a Alemania.

Pero sin duda donde la criptografía adquiere una importancia clave es durante la Segunda Guerra mundial, hasta el punto de cambiar el curso de la guerra. Alemania llevaba ventaja en la guerra donde había conseguido dominar el Atlántico con su flota de submarinos y con unas comunicaciones indescifrables gracias a la Máquina Enigma. Hasta que un grupo de matemáticos, ingenieros y físicos del bando aliado entre los que se encontraba Alan Turing consiguió descifrarla, cambiando así el curso de la guerra.

Ilustración 20 Máquina Enigma

Fuente: Velasco J.J. (2014)

Por otra parte, el Ejercito de Estados Unidos rescató una técnica que había utilizado durante la Primera Guerra Mundial que consistía en usar como código los idiomas de los americanos nativos. Ya que contaba con más de medio millar de nativos americanos que servían como operadores de radio, y que cifraban dichos mensajes, de tal manera que el Ejercito japonés no pudiera entender nada.

Posteriormente tras la Segunda Guerra mundial, la criptografía dió un gran salto gracias a Claude Shannon, conocido como el padre de la comunicación. Gracias a la modernización de las técnicas de codificación que se transforrmaban en procesos matemáticos. Este gran avance vino gracias a las computadoras, que es convirtieron en un instrumento clave para el cifrado y descifrado de mensajes.

El primer gran avance, se produjo a través de la empresa IBM que consiguió desarrollar el algoritmo de cifrado DES [12] que fue muy utilizado por la NSA [13] y posteriormente en todo el mundo.

El segundo gran avance tuvo su origen también en los años 70, concretamente en 1976 cuando Whitfield Diffie y Martin Hellman sentaron las bases de la criptografía asimétrica, la cual es fundamental hoy en día para todo tipo de transacciones realizadas en internet.

Como podemos comprobar la criptografía ha tenido un papel fundamental en la historia de la humanidad, a través de las diferentes épocas. Y más hoy en día, desde realizar una llamada en nuestro teléfono móvil hasta una compra por internet.

3.2 Tipos de Criptografía

Dentro de la criptografía existen diferentes tipos de mecanismos que nos permiten conocer mejor cómo funciona la Blockchain y las Criptomonedas:

[12] DES: Data Encryption Standard.
[13] NSA: National Security Agency. Agencia de Seguridad de Estados Unidos de América.

Criptografía Simétrica

La criptografía simétrica utiliza una sola clave para descifrar y cifrar los mensajes. Se trata de uso de algoritmos secretos dentro de los mensajes, pero tienen un problema de seguridad ya que cualquiera que conozca su clave puede descifrarlos.

Criptografía Asimétrica

La criptografía asimétrica utiliza dos claves, una privada y otra pública, ambas creada y vinculadas entre si. De tal manera que permiten que se cree una clave pública a partir de una privada de manera aleatoria.

La clave privada se guardaría en secreto y la pública la podría conocer todo el mundo, de tal manera que con la clave publica cualquiera podría cifrar los mensajes secretos que nos quieren enviar y solo nosotros podríamos descifrarlos con la clave privada. La ventaja de este método es que la clave que cifra el mensaje no sirve para descifrarlo.

Pondremos un ejemplo:

Ilustración 21 Clave pública y privada

Fuente: Preukschat (2017)

Si Alicia quiere enviar información secreta a Bob, tiene que buscar y verificar su clave pública, cifrar el mensaje con la clave y enviárselo a Bob. Cuando Bob reciba el mensaje usará su clave privada para descifrarlo. Si conocemos la clave privada, podemos averiguar cual es la clave pública. Pero si conociéramos la clave pública no podríamos obtener la privada.

Ilustración 22 Proceso envió Bitcoin

Fuente: Preukschat (2017)

3.3 ¿Cómo se compra o invierte en Criptomonedas?

Hay tres modos de poder adquirir Criptomonedas. Ordenados de más sencillos a más complejos:

1. Exchanges: se tratan de casas de cambios. Dentro de estas diferenciamos dos tipos de casas de cambios. En primer lugar, las que permiten intercambiar Bitcoin u otras Criptomonedas por euros o dólares y luego están las que permiten intercambios entre Criptomonedas con el Bitcoin como moneda de referencia. Todas las casas operan con un procedimiento de KYC[14] para una mayor seguridad y control de los usuarios.

2. Intercambiando bienes y servicios: Ya hay muchas empresas que pagan a sus empleados con Criptomonedas. Es el caso de la empresa de seguridad online Cobalt.io , que utiliza Bitcoins para la remuneración de sus trabajadores. Además de esta empresa existen otras empresas que ofrecen la posibilidad de obtener remuneración en diferentes criptoactivos.

3. Minería: la tercera opción de obtener Bitcoins "minando". Dicho proceso consiste en una prueba de trabajo que asegura que se realicen las transacciones gracias a la capacidad de cálculo de un ordenador o de un conjunto de ellos. Este proceso de minería

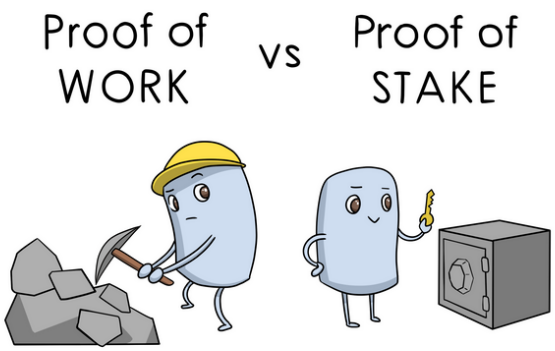
[14] KYC: Know your Customer. Política de identificación de clientes para prevención del blanqueo de capitales.

se ha ido profesionalizando con el paso de los años y no suele salir rentable para una persona, ya que conlleva una gran inversión.

La minería tiene dos métodos principales: la prueba de trabajo (Proof of work) que se utiliza en los protocolos de Bitcoin y Ethereum y la prueba de participación (Proof of Stake), por la cual los propietarios de las Criptomonedas son recompensados de forma progresiva con nuevas unidades por poseer las mismas.

En el modelo de Proof of Stake se suele realizar una operación conocida como "premiado" que consiste en que los desarrolladores del protocolo distribuyen una cantidad fija de Criptomonedas a un pequeño grupo de inversores para más tarde cuando se lance al público se pueda inflar los precios para obtener unos mayores beneficios. Esto permite que el desarrollador del protocolo tenga cierto control sobre la distribución de las monedas a diferencia de lo que pasa en Proof of Work que es difícilmente controlable.

Ilustración 23 Proof of Work vs Proof of Stake



Fuente: Steemit (2018)

3.4 Financiación en el mundo de la Criptomoneda (ICO)

En el mundo de las Criptomonedas se utiliza un instrumento que se conoce como ICO[15] y que su finalidad es la de financiar el desarrollo de nuevos protocolos. Es como una salida a bolsa, pero de un protocolo descentralizado y sin un régimen regulatorio y legal definido.

La mayor parte de las ICOs están vinculadas al protocolo de Ethereum. Durante su lanzamiento en el verano de 2014, Ethereum recaudo 31.531 bitcoins (15 millones de dólares al cambio del momento) gracias a un sistema de pre-minado. En su momento, el lanzamiento de ether fue una de las campañas de crowfunding más exitosas de cualquier protocolo y posicionó a Ethereum y su Criptomoneda como un serio competidor del Bitcoin, captando la atención de inversores y desarrolladores.

[15] ICO: del inglés, Initial Coin Offering.

Históricamente, los inversores y especuladores que han invertido en las ICOs han seguido los lanzamientos de nuevos proyectos y Criptomonedas. Intentado beneficiarse de la posterior revalorización una vez que se lanzaran al mercado.

Desde entonces los proyectos ICO más sonados e importantes se han desarrollado utilizando Ethereum como protocolo de referencia. Las más conocidas han sido:

El ICO de theDao

En 2016 el Startup del ecosistema Ethereum, Slock.it anunció el lanzamiento de TheDAO a través de una campaña de financiación colectiva que ponía a la venta tokens de DAO (Descentralized Autonomous Organization). Se recaudaron más de 12 millones de ETH[16] (más de 150 millones de dólares).

Ilustración 24 TheDao

Fuente: TheDao (2019)

El proyecto se basaba en un fondo de capital riesgo abierto donde cualquier persona del mundo podía participar para invertir en proyectos basados en el protocolo de Ethereum, con contratos inteligentes automatizados. La idea fue bien recibida por la comunidad, pero fracaso.

Su fracaso fue debido a que un hacker logro bloquear más de 3 millones de ETH, haciendo que se provocara una ruptura en la comunidad, dividendo a Ethereum en dos protocolos, Ethereum Classic y Ethereum. Esto provocó una bajada importante de la cotización de esta moneda.

El ICO de Z-Cash

El proyecto de Z-Cash apareció en 2016, recibiendo más de 3 millones de dólares para su desarrollo. Se reservó el 10% de las monedas, para inversores y desarrolladores, de tal manera que se reembolsaran en los cuatro primeros años desde su lanzamiento.

Ilustración 25 Z-cash

Fuente: Jimenez (2019)

El proyecto pretendía lanzar una criptomoneda totalmente privada y con transparencia selectiva de las transacciones, en la que el remitente, el destinatario y el monto de la transacción serían privados.

Las semanas anteriores al lanzamiento, su precio fue subiendo hasta situarse en 3300 Bitcoins por ZEC[17] (unos 2 millones de dólares),

[16] ETH: Código que se utiliza en la moneda de Ethereum
[17] ZEC: Código que se utiliza en la moneda de Z-Cash

pero posteriormente su precio cayó. Esto se debe a la ley de la oferta y la demanda que regula el mercado. Ya que inicialmente había muy pocos ZEC, por lo que su valor aumentó exponencialmente, pero a medida que se fueron minando, su precio bajo hasta los 60 dólares que alcanzo a finales de 2016.

3.5 Características generales Criptomonedas

Las Criptomonedas tienen una serie de características comunes que las hacen diferenciales y que permiten justificar su utilidad y valor económico. Aunque cada criptomoneda tenga sus características particulares, estás son las más comunes:

- ◊ **Descentralización:** Cuando decimos que las Criptomonedas están descentralizadas, nos referimos a que no están vinculadas a ningún organismo gubernamental ni económico.
- ◊ **Operatividad:** No están reguladas por ningún mercado oficial por lo tanto las hace operativas durante 7 días a la semana y 24 horas al día.
- ◊ **Limitadas:** Hay un número limitado de Criptomonedas, de manera similar al oro, y se comportan como una moneda deflacionaria[18] ya que cuanto más tiempo pase menos habrá disponible.
- ◊ **Transparencia:** Todas las transacciones quedan registradas en el "libro de contabilidad", que esta compartido por toda la red y es prácticamente imposible de manipular.
- ◊ **Inmediatez:** Las Criptomonedas son rápidas, la mayoría de las transacciones se confirman en menos de 10 minutos de medio, e incluso se pueden hacer transferencias de manera casi instantánea en algunas de ellas como Ripple que tardan menos de 1 minuto.
- ◊ **Costes:** Los costes se reducen en comparación con los sistemas tradicionales de transferencias de dinero, ya que se eliminan los intermediarios.
- ◊ **Whitepaper:** Todas las Criptomonedas tienen este documento. Este documento debe explicar cuál es el problema que se quiere resolver, cómo se resolverá, la fase de financiación, la cantidad de token que se dispondrán y una hoja de ruta (Roadmap) de implementación del proyecto, entre otros detalles destacables.

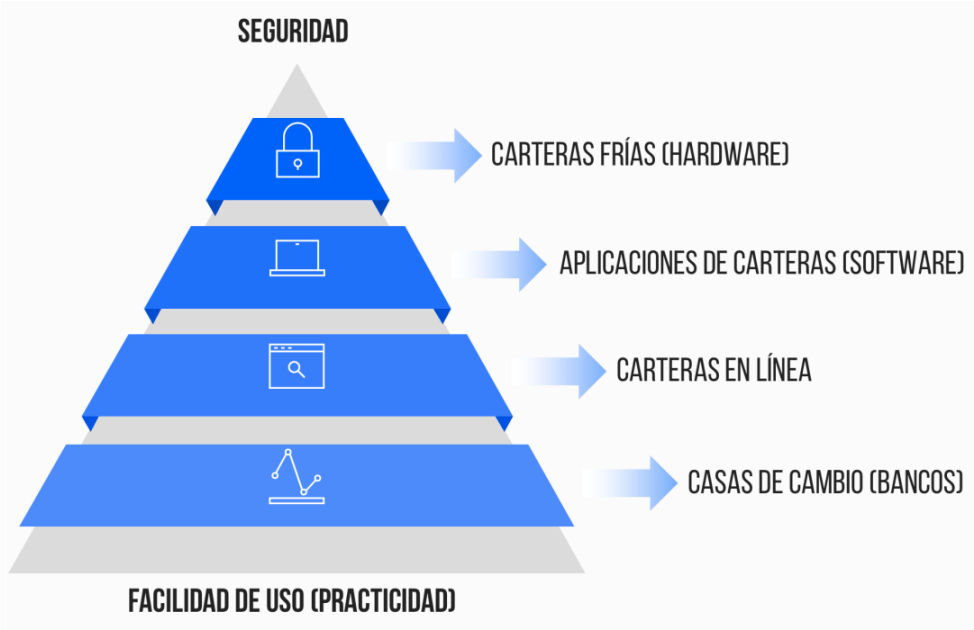
[18] Moneda deflacionaria: Moneda que gana valor con el paso del tiempo.

3.6 Monederos

Para poder hacer un intercambio es necesario una wallet o cartera para poder almacenar las diferentes Criptomonedas. Estas carteras tienen una clave privada que permite acceder a los saldos de la cartera y permite modificarlos y una clave pública dentro de la cadena de bloques que permite gastar el saldo dentro de la cartera.

Podemos identificar dos variables claves a la hora de diferenciar los diferentes tipos de wallets: la seguridad que ofrecen y su facilidad de uso. Hablaremos de 4 tipos de wallets: Carteras frías, Aplicaciones de carteras en línea, Carteras en línea y Casas de cambio.

Ilustración 26 Tipos de Wallets



Fuente: Criptonoticias (2018)

Empezaremos con las más usadas y prácticas y terminaremos con las más seguras:

- ◊ **Casas de cambio o "Exchanges"**: Son las más fáciles de usar, actúan como un banco de Criptomonedas y son las más usadas por su comodidad de utilización. Se pueden intercambiar dinero FIAT [19] por Criptomonedas o Criptomonedas entre si. La casa de cambio gestiona las direcciones en nombre de usuario. Son propensas a ataques de hackers, caídas del

[19] Dinero FIAT: Se trata del dinero fiduciario, aquel que esta respaldado por la confianza de una sociedad, es decir no se basa en el valor de metales preciosos sino en la creencia general de que ese dinero tiene valor. Como por ejemplo el euro, el dólar o el yuan.

servicio y demás riesgos. Por lo tanto, son las menos seguras de todas, ya que puedes perder el dinero, tenerlo bloqueado durante días o cambios de condiciones y cierres de cuenta. Es el punto de entrada de moneda física (euros, dólares, etc.) dentro del mercado digital de las criptomonedas. Algunas de ellas son: Coinbase, Kraken, Kucoin o Binance.

Ilustración 27 Kraken

Fuente: Kraken (2019)

◊ **Carteras en línea**: Son sitios web, que permiten al usuario sin necesidad de instalar ningún software, controlar sus claves privadas a través de la plataforma online, de forma totalmente autónoma. Se genera una clave de respaldo llamada semílla [20] con el fin de asegurar que esos fondos pertenecen al usuario. La probabilidad de hackeo disminuye con respeto a las casas de cambio, aun así, siguen siendo altos. También está el inconveniente de la disponibilidad ya que pueden ocasionarse caídas temporales. Algunos de ellos son: Blockchain y MyEtherWallet.

Ilustración 28 MyEtheWallet

Fuente: MyEtherWallet (2019)

◊ **Aplicaciones de cartera**: Se tratan de software instalados en ordenadores o en móviles que sirven de interfaz para visualizar saldos y realizar transacciones de carteras al usuario. Permiten la generación de una semilla al igual que en las carteras en línea, pero incluyen la activación de un código o clave extra (como un PIN o un sistema de autentificación de doble factor). Estas aplicaciones eliminan el problema de la disponibilidad, ya que ahora depende del usuario. Algunos ejemplos son: Exodus, Jaxx o Electrum.

Ilustración 29 Exodus

Fuente: Exodus (2019)

[20] Semilla de recuperación: Clave numérica de 12 o más palabras, introducidas en un orden especifico permiten al usuario recuperar las claves privadas si el dispositivo se rompe o sufre un robo, permitiendo el acceso a la cartera y a las Criptomonedas.

◊ **Carteras frías**: Se tratan de dispositivos físicos de hardware, que albergan la clave privada fuera de línea, de ahí su nombre de carteras frías. Lo que permiten es que a través del dispositivo físico se conecten al ordenador (normalmente mediante USB) y garanticen las transacciones sin exponer la semillas, permitiendo realizar transacciones en entornos inseguros, como ordenadores ajenos o públicos. Estas carteras llevan un coste para el usuario, ya que se trata de un dispositivo físico, pero son sin lugar a duda las más seguras. Las más usadas son: Trezor y Ledger.

Ilustración 30 Trezor

Fuente: Trezor (2019(

3.7 Bitcoin

Se trata de la primera Criptomoneda, que marca las bases del resto. Fue lanzada en 2008 por Satoshi Nakamoto y el propósito por el que fue creado es para eliminar intermediarios y poder hacer transacciones de manera autónoma sin el respaldo de ningún tercero.

El Bitcoin usa la criptografía para la creación de su moneda, teniendo un numero máximo de 21 millones de Bitcoin, limite que esta programado dentro de su protocolo. Para el año 2140 se estima que se alcanza dicho límite. El límite de monedas que tiene el Bitcoin, es una de las características más diferenciales y más importantes de esta moneda.

Ilustración 31 Bitcoin

Fuente: Bitcoin (2017)

Como ya hemos dicho anteriormente utiliza el sistema de “Proof of Work” para recompensar a sus mineros por la creación de nueva moneda y por la confirmación de transacciones.

3.8 Ethereum

Ilustración 32 Ethereum

Fuente: Dan Mueller (2017)

Nace en 2014 como una plataforma de código abierto sobre la que construir aplicaciones descentralizadas y contratos inteligentes. Está constituida y desarrollada sobre la tecnología de la Blockchain y es la base sobre la que se desarrollan nuevos proyectos y su código es utilizado como referencia de otras Criptomonedas.

Vitalik Buterin[21] uno de sus creadores y máximo representante, cuando desarrollo Ethereum afirmó (Pérez, 2018):

"Cuando se me ocurrió Ethereum, lo primero que pensé fue: bueno, esto es demasiado bueno para ser verdad y voy a tener a cinco criptógrafos profesionales lloviendo sobre mí y diciéndome lo estúpido que soy por no ver un montón de cosas, fallas obvias. Dos semanas después, me sorprendió mucho que nada de eso sucediera. Al final resultó que la idea central de Ethereum era buena, fundamentalmente, completamente sólida."

Actualmente, Vitalik continua al frente del proyecto de la Criptomoneda, contando con más de 90 personas dentro de su proyecto, entre los que se incluyen desarrolladores y contribuyentes

3.9 Stablecoins

Se tratan de Criptomonedas cuyo valor está estable, ya que está controlado mediante algoritmos, para así tratar de evitar la fuerte volatilidad que caracteriza a las Criptomonedas de referencia como Bitcoin o Ether. La principal motivación para la creación de una Stablecoin es la de dar refugio a los inversores en momentos de fuerte volatilidad.

Dentro de las Stablecoins diferenciamos varios tipos:

- ◊ **Respaldo en monedas FIAT**: Se trata del método más común. Se respalda el criptoactivo con una proporción igual (1:1) con cada token de la moneda. Suelen utilizarse el Euro o Dólar Estadounidense como monedas de referencia. La finalidad es garantizar el valor del token en una unidad de la moneda FIAT. Algunos ejemplos son

Ilustración 33 Tether

Fuente: AcademybyBit2me (2018)

[21] Vitalik Buterin: Cripto-activista y cofundador de Ethereum. Se trata de una de las personas más influyentes dentro del mundo de las Criptomonedas y Blockchain

TrueUSD o Tether, que fue creado en 2014. Los inconvenientes de estas Stablecoins, es la transparencia de las reservas que hay para dar valor al token.

◊ **Respaldo en Commodities**: La Criptomoneda se respalda en base al valor de una materia prima. Como puede ser: el oro, la plata o el petróleo. Sigue una proporción 1:1. Un ejemplo sería Digix Gold, que establece que cada gramo de oro sea igual a una unidad del token (SeSocio, 2018). De tal manera que el oro se mantiene en lingotes como reserva, permitiendo que la Criptomoneda tenga un respaldo.

Ilustración 34 Digix Gold

Fuente: SeSocio (2018)

◊ **Respaldo en otras Criptomonedas**: Se trata de uno de los esquemas más utilizados junto con el respaldo en monedas FIAT. Para estabilizar los precios se utiliza un complejo sistema económico que busca proteger el precio del Stablecoin con respecto a la variación de valor del criptoactivo de referencia. Este método presenta inconvenientes, como que las propias Criptomonedas ya son inestables de por si. La mayoría de las Criptomonedas que utilizan este método son Tokens ERC-20[22]. Un ejemplo seria DAI, una Criptomoneda respaldada por el valor del Ethereum.

[22] Tokens ERC-20: Son tokens que pertenecen a la plataforma descentralizada de contratos inteligentes de Ethereum.

4. Conclusiones

Una vez recopilada la máxima información posible, de la manera más rigurosa y completa posible sobre la Blockchain y las Criptomonedas, procedemos a sacar las conclusiones.

Lo primero que hay que tener claro es el gran avance y desarrollo que ha tenido, está teniendo y va a tener internet en nuestras vidas. A través de esta tecnología se están cambiando el comportamiento de las personas y su forma de ver el mundo. Muchas veces no se valora el cambio que ha supuesto ya que se trata de una tecnología que “no se ve”.

Empezaremos analizando lo que supone la Blockchain dentro del Sector Bancario. “Mejorar los servicios gracias al potencial que nos proporciona la Blockchain nos permitirá ofrecer productos personalizados para clientes a partir del análisis de grandes cantidades de datos” Son palabras de Jaume Guardiola, consejero Delegado de Banco Sabadell. También añade: “El Bitcoin ha demostrado que necesitamos una solución digital al dinero”.

Por otra parte, Banco Santander, ha lanzado un servicio de transferencias internacionales basado en la tecnología Blockchain para agilizar tiempos entre transferencias internacionales.

Con estas declaraciones, pretendo hacer ver que no se trata de una tecnología pasajera o de una moda temporal. Sino que ya muchos Bancos y empresas invierten en ella. Para ello, están creando departamentos de investigación e innovación, e incluso aceptan pagos en Criptomonedas, como ocurren en algunas Pequeñas y Medianas Empresas (PYMES) dentro de nuestro país.

Desde otros campos, como el campo de la Sanidad, se están realizando fuertes inversiones. Se pretende que gracias a la tecnología Blockchain los registros médicos puedan ser universales y que sean los propios pacientes quien proporcionen acceso total o parcial a su historial médico.

Miriam Barrena de Deusto Business, afirma que la financiación de proyectos relacionados con la Blockchain ha aumentado del año 2017 al 2018 más de un 85% y con una inversión de más de 10 Billones. Y este último año ha aumentado aún más.

Como en toda nueva tecnología, tiene una curva de aprendizaje y un proceso de adaptación que suele ser lento. Ya que en este caso se trata de una transformación enorme y requiere de un proceso de maduración y de un desarrollo tecnológico. Y por último y no

menos importante, requiere de un aprendizaje y aceptación por parte de los usuarios que actualmente a día de hoy, es minoritaria.

Por otra parte, la volatilidad que tienen las Criptomonedas, unido a las pocas posibilidades de hacer pagos en el día a día y su concepto abstracto, hacen que los usuarios desconfíen de esta nueva forma de pago y en muchos casos se dictamine que no tiene futuro. Debido en gran medida a la alta especulación que se ha creado alrededor de las Criptomonedas, planteándose en algunos casos como una burbuja especulativa o estafa a gran escala.

El desconocimiento de la sociedad y la falta de información hacen que se genere una desconfianza. Los inversores y usuarios tienen miedo hacia la posible pérdida de sus activos financieros debido a hackeos o robos informáticos. Y sobre todo si no tienes un tercero al que reclamar esta pérdida.

Las ICO han mostrado al mundo que se puede financiar un proyecto con valor y potencial y unos ideales sólidos. Estas nuevas formas de financiarse permiten unos resultados sorprendentes, pero poco claros de cara a los inversores ya que se carece de la información sobre el destino de su inversión.

Pero sin duda el gran reto al que se enfrenta esta nueva tecnología es acerca del marco legal y regulatorio que la rodea. Actualmente no hay una legislación clara que regule las Criptomonedas de manera unitaria y mundial. Cada país tiene su regulación, una regulación muy abierta y poco clara, que no tiene mucho sentido ya que se tratan de activos financieros mundiales.

Sobre todo, es necesario normativa que asegure la correcta protección y seguridad del usuario, la tributación fiscal o el ofrecer una mayor información. Desde nuestro país, ya se han pronunciado acerca del tema fiscal. El Ministerio de Hacienda dictamina: “El intercambio entre monedas virtuales diferentes realizado por el contribuyente al margen de una actividad económica da lugar a la obtención de renta que se califica como ganancia o pérdida patrimonial”.

Lo que esta claro es que la tecnología Blockchain y todos los avances que la rodean están cambiando la visión del conjunto la sociedad. Y se plantea la pregunta ¿Tiene la tecnología Blockchain la capacidad para cambiar nuestras vidas?, ¿Las Criptomonedas se utilizarán en un futuro?

Además, actualmente debido a su baja aceptación carece de una confianza, que es esencial para la correcta utilización. Ya que, si nadie cree que valga la pena, carecerá de

valor y por lo tanto no tendrá una perspectiva de futuro favorable. La falta de información del usuario sobre esta nueva tecnología tiene gran parte de culpa, y en muchos casos genera una alta desconfianza.

El gran desafío que plantea la nueva revolución tecnológica de la Blockchain y las Criptomonedas no tiene un futuro asegurado con certeza. Pero lo que si que tiene es el potencial necesario para cambiar nuestra forma de comerciar, de comunicarnos y lo que es más importante, cambiar nuestros hábitos.

5. Bibliografía

AcademybyBit2me. (2018). *¿Qué es y cómo funciona OpenBazaar?* Obtenido de Academy by Bit2me: http://bit.ly/2RIGwjQ

AcademybyBit2me. (2019). *¿ Que es un Whitepaper?* Obtenido de Academy by Bit2me: http://bit.ly/2JbbOPb

Alonso, P. (2018). *Criptomonedas: Qué son , caracteristicas y tipos*. Obtenido de Opinred: http://bit.ly/2VO1ceR

Amper. (2018). *M2M-IoT-Connectivity*. Obtenido de Amper: http://bit.ly/2KLOKal

BBVA. (2018). *Qué son las DApps y por qué serán cada vez más importantes*. Obtenido de BBVA: https://bbva.info/320YVgN

BitcoinOnAir. (2017). *Por qué los bancos están adoptando The Blockchain*. Obtenido de Bitcoin on air: http://bit.ly/2IUBLko

Calvo, M. (2018). *Conoce los diferentes tipos de blockchain*. Obtenido de Blockchain Services: http://bit.ly/2FpKk4C

Coinmarketcap. (2019). *Coinmarketcap*. Obtenido de http://bit.ly/2VOCWt6

Compteg Solution. (2018). *Día Internacional de seguridad y información*. Obtenido de Compteg Solution: http://bit.ly/2Jd35JL

CriptoNoticias. (2018). *Blockchains y criptomonedas: fundamentos y características*. Obtenido de http://bit.ly/2KXKDc4

CriptoNoticias. (2018). *¿Cómo elegir un monedero de bitcoin, otras criptomonedas y criptoactivos?* Obtenido de http://bit.ly/2vfeWAo

Criptotario. (2018). *¿Cuáles son los Tipos de Criptomonedas principales?* Obtenido de Criptotario: http://bit.ly/2JdK9Ni

Dan Mueller. (2017). *Ethereum, la próxima Internet*. Obtenido de Seeking Alpha: http://bit.ly/2XILz9C

Exodus. (2019). *Exodus*. Obtenido de Exodus Wallet: http://bit.ly/2Yr4DpI

Futurizable. (2017). *Todo lo que vamos a poder hacer con Blockchain*. Obtenido de Futurizable: http://bit.ly/2J6gFyx

Gonzales, F. (2017). *Ataques del 51%: el punto flaco de la Blockchain*. Obtenido de Criptomano: http://bit.ly/31YqYxh

Google Trends. (2019). *Google Trends*. Obtenido de http://bit.ly/2VhWHoI

Herrera, C. (2018). *¿Qué es un Token ERC20?* Obtenido de Tekcrispy: http://bit.ly/2XtIUMT

Herrera, C. (2018). *¿Que son los Contratos Inteligentes o Smart Contracts?* Obtenido de TekCrispy: http://bit.ly/327jOXF

Heselaars, T. (2018). *Blockchain: La manera de solucionar problemas a futuro*. Obtenido de Emol: http://bit.ly/2XdZOPu

Imagin Bank. (2019). *Codigo SWIFT*. Obtenido de Imagin Bank: http://bit.ly/2RK85JI

Jimenez, S. (2018). *Siete puntos para entender el proyecto de Zcash*. Obtenido de Criptotendencia: http://bit.ly/3201i3i

Keybase. (2019). Obtenido de Keybase: http://bit.ly/2JfwxyE

Kraken. (2019). *Kraken Exchange*. Obtenido de Kraken Exchange: http://bit.ly/2YnsQgB

Linares, V. (2017). *Experto de Bitcoin considera que la moneda electrónica puede ser muy útil para los salvadoreños*. Obtenido de El Salvador: http://bit.ly/2vXKTxm

MR. ADDON. (2019). Obtenido de MR. ADDON: http://bit.ly/2YqaTyf

Muy Interesante Mexico. (2019). *El origen de las criptomonedas.* Obtenido de Muy Interesante: http://bit.ly/2GwK6Zc

MyEtherWallet. (2019). *MyEtherWallet*. Obtenido de MyEtherWallet: http://bit.ly/2FMwdXh

Onename. (2019). *Onename.com*. Obtenido de http://bit.ly/31R0Vbn

Pastor, J. (2018). *Monederos físicos de bitcoin: qué son y cómo funcionan a la hora de proteger tus inversiones*. Obtenido de Xataka: http://bit.ly/2IMJiSV

Pastor, J. (2019). *Qué es blockchain: la explicación definitiva para la tecnología más de moda.* Obtenido de http://bit.ly/2DtspJs

Pérez, I. (2018). *¿Quién es Vitalik Buterin?* Obtenido de Criptonoticias: http://bit.ly/32hRge4

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

Rioja2. (2017). *Industria 4.0: Indagando en la historia moderna*. Obtenido de Rioja2: http://bit.ly/2NmPDYW

Rodriguez, M. (2016). *15 aplicaciones de la tecnología blockchain más allá de bitcoin*. Obtenido de Fin-Tech: http://bit.ly/2MuyvA9

SeSocio. (2018). *Invertí en oro a través de Digix con la tranquilidad de operar sobre Blockchain*. Obtenido de SeSocio: http://bit.ly/2XNH1ig

Skuchain. (2019). Obtenido de Skuchain: http://bit.ly/2KMM7VC

Steemit. (2018). *Proof of Work vs. Proof of Stake*. Obtenido de Steemit: http://bit.ly/2NibmRS

Storj. (2018). Obtenido de Storj.io: http://bit.ly/2X3hjqi

Trezor. (2019). Obtenido de Trezor : http://bit.ly/307DPLV

TyN Magazine. (2018). *Ventajas y desventajas de las 10 criptomonedas más populares del mundo*. Obtenido de TyN Magazine: http://bit.ly/31ZDpsG

Vega, G. (2017). *Guía básica para entender de una vez qué es eso del 'blockchain'*. Obtenido de El Pais: http://bit.ly/2EN3iC1

Velasco, J. J. (2014). *Breve historia de la criptografía*. Obtenido de eldiario.es: http://bit.ly/30k1Zn0

Zamorano, V. (2018). *¿Quienes son los cypherpunks?* Obtenido de Blockchain Services: http://bit.ly/2Yl6KLV