Universidad de Oviedo

Universidad de Oviedo

FACULTAD DE ECONOMÍA Y EMPRESA

GRADO EN CONTABILIDAD Y FINANZAS

CURSO ACADÉMICO 2020-2021

TRABAJO FIN DE GRADO

"CRIPTOMONEDAS Y BLOCKCHAIN"

TERESA LÓPEZ GÓMEZ-CADIÑANOS

OVIEDO, JUNIO 2021

Anexo

TRABAJO FIN DE GRADO QUE SE REALICEN EN LENGUA ESPAÑOLA

TÍTULO EN ESPAÑOL: CRIPTOMONEDAS Y BLOCKCHAIN

RESUMEN EN ESPAÑOL: De entre todas las criptomonedas que existen en la actualidad, sin duda alguna Bitcoin es la más conocida ya que fue el inicio de este sistema que permitió comenzar a realizar intercambios y adquirir productos y servicios electrónicamente. Tras ella, fueron surgiendo nuevas criptodivisas a lo largo del tiempo. Utilizan la tecnología Blockchain para su funcionamiento. Blockchain es un sistema seguro, transparente e imborrable, que permite registrar transacciones o actuación en internet de forma veraz e infalseable, sin la necesidad de la existencia de un tercero.

Este proyecto se divide en dos partes: en primer lugar, explicaremos el concepto de criptomoneda, centrándonos en el Bitcoin y analizaremos otras criptomonedas más actuales. Además, estudiaremos la situación de las criptomonedas durante la pandemia de Covid-19 y la relación con los bancos central. En segundo lugar, nos focalizaremos en la tecnología Blockchain, sus características y los ámbitos en los que se puede emplear.

TÍTULO EN INGLÉS: CRIPTOCURRENCIES AND BLOCKCHAIN

RESUMEN EN INGLÉS: There are many cryptocurrencies on the market, but Bitcoin was the first. Some time later, new crytocurrencies appeared. It is a system that allows electronic exchanges and purchase electronic products and services. It uses Blockchain technology for its operation. Blockchain is a safe, transparent and indelible system, which allows sign verified transactions or actions on the internet, without the necessity for a third part.

This project is divided in two parts: First, we will explain the concept of cryptocurrency, focusing on Bitcoin. In addition, we will mention a new digital cryptocurrency and the situation of these with Covid-19 and the relation with Central Banks. Second, we Will focalize on Blockchain technology, its characteristics and in what scenarios it can be utilize.

RESUMEN

De entre todas las criptomonedas que existen en la actualidad, sin duda alguna Bitcoin es la más conocida ya que fue el inicio de este sistema que permitió comenzar a realizar intercambios y adquirir productos y servicios electrónicamente. Tras ella, fueron surgiendo nuevas criptodivisas a lo largo del tiempo. Utilizan la tecnología Blockchain para su funcionamiento. Blockchain es un sistema seguro, transparente e imborrable, que permite registrar transacciones o actuaciones en internet de forma veraz e infalseable, sin la necesidad de la existencia de un tercero.

Este proyecto se divide en dos partes: en primer lugar, explicaremos el concepto de criptomoneda, centrándonos en el Bitcoin y analizaremos otras criptomonedas más actuales. Además, estudiaremos la situación de las criptomonedas durante la pandemia de Covid-19 y la relación con los bancos centrales. En segundo lugar, nos focalizaremos en la tecnología Blockchain, sus características y los ámbitos en los que se puede emplear.

ABSTRACT

There are many cryptocurrencies on the market, but Bitcoin was the first. Some time later, new crytocurrencies appeared. It is a system that allows electronic exchanges and purchase electronic products and services. It uses Blockchain technology for its operation. Blockchain is a safe, transparent and indelible system, which allows sign verified transactions or actions on the internet, without the necessity for a third part.

This project is divided in two parts: First, we will explain the concept of cryptocurrency, focusing on Bitcoin. In addition, we will mention a new digital cryptocurrency and the situation of these with Covid-19 and the relation with Central Banks. Second, we will focalize on Blockchain technology, its characteristics and in what scenarios it can be utilize.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

1. INTRODUCCIÓN Y OBJETIVOS.

1.1 INTRODUCCIÓN.

La tecnología Blockchain y las criptomonedas tienen un largo recorrido a lo largo de la historia, más de cuarenta años de investigaciones.

Durante la primera mitad del siglo XX, numerosos proyectos, la mayor parte relacionados con el ámbito militar, establecieron las bases técnicas de la criptografía, la cual fue propiedad del gobierno durante un largo periodo ya que se percataron de la importancia de la codificación y descodificación. Ésto era un elemento esencial en Blockchain ya que permite compartir información de manera encriptada entre enormes redes de ordenadores sin jerarquía alguna.

En los años 70, un grupo de investigadores progresó en la libertad en las comunicaciones que brindaba esta técnica. A partir de este momento, se desarrollaron una serie de algoritmos que dieron lugar a la "criptografía de clave pública", un precursor imprescindible en el desarrollo de "Blockchain" y Bitcoin. En el año 1976, Whitfield Diffie y Martin Hellman crearon el Algoritmo Diffie-Hellman, con el cual sugieren dividir los códigos encriptados en dos, uno público y otro privado. Con la clave pública se podría encriptar un mensaje, pero para poder desencriptarlo sería indispensable la clave privada. Otro adelanto decisivo fue la invención de los Árboles de Merkle, por el estadounidense Ralf Merkle. Es una estructura de datos en forma de árbol que ofrece la verificación segura y eficiente del contenido en grandes estructuras de datos entre dos partes que lleguen a un acuerdo. Solo un año después, Ron Rivest, Adi Shamir y Leonard Adleman, también procedentes de Estados Unidos, inventaron el Algoritmo RSA para la generación de códigos, el cifrado y el descifrado de mensajes. Para poder probar el funcionamiento, publicaron un prueba para los lectores de una revista en la cual podrían descifrar un mensaje a cambio de 100 dólares. Nadie fue capaz hasta mediados de los 90, cuando Derek Atkins, Michael Graff, Arjen K. Lenstra y Paul C. Leyland llegaron a la conclusión de que era necesario que varios ordenadores de personas diferentes y de distintas partes del mundo se ocupasen de un mismo problema para aumentar la capacidad de trabajo y cómputo.

En la década de los 90 comenzó la búsqueda de un sistema descentralizado vinculado a la libertad de información. Apareció el primer precedente de la criptomoneda, se publicó el "Bitcoin P2P e-cash".

Y éstos fueron fenómenos importantes en el movimiento del "ciberpunk", el cual defiende la libertad de expresión, el acceso a la información y la privacidad, considerados elementos básicos que se deben defender con la criptografía y la tecnología.

Este proceso está vinculado a un cambio estructural que tuvo consecuencias económicas: la figura del intermediario para validar las transacciones desaparece. Este hecho supone un ahorro significativo en los costes, lo que vuelve a estas tecnologías especialmente atractivas para las empresas.

1.2 OBJETIVOS.

Hasta la actualidad, y más aun con la pandemia del Covid-19, la sociedad ha comenzado a interesarse por el mundo de las criptomonedas, ya que se ha observado la posibilidad de operar con ellas. Por otro lado, las empresas se interesan por la Blockchain, ya que es un método para intercambiar información de forma segura y privada entre distintos agentes. También es posible automatizar procesos ahorrando tiempo y dinero, tales como la gestión de nóminas o de pedidos o la emisión de facturas.

En este proyecto explicaremos el funcionamiento y la situación actual de varias criptomonedas, tanto la precursora, el Bitcoin, como nuevas, como es el caso de Libra, y analizaremos el estado de éstas durante la pandemia de Covid-19, y por otro lado, explicaremos de manera detallada la tecnología Blockchain y la aplicación de ella en las empresas y entre distintos agentes, lo cual es importante recalcar ya que es útil para los miembros de las sociedades.

2. CRIPTOMONEDAS.

2.1 DEFINICIÓN.

En la actualidad, no existe una definición exacta de "Criptomoneda" en el diccionario de la Real Academia de la Lengua Española, pero podemos encontrar diferentes explicaciones sobre ello en otros documentos. Según el Banco Central Europeo "es la representación digital de valor, no emitida por ninguna autoridad central, institución de crédito o emisor de dinero electrónico reconocido que en ciertas ocasiones, puede ser utilizada como medio de pago alternativo al dinero" (*European Central Bank, "Virtual currency schemes – a further analysis",* 2015, p.25).

El diccionario de Oxford lo definió como "una moneda digital que emplea técnicas de cifrado para reglamentar la generación de unidades de moneda y verificar la transferencia de fondos, y que opera de forma independiente de un banco central" (2013). Por su parte, el diccionario de Cambridge lo define como "una moneda digital producida por una red pública en lugar de cualquier gobierno, que utiliza la criptografía para asegurar que los pagos se envían y reciben de forma segura".

Por lo tanto, las criptomonedas son un tipo de moneda digital, pero no las únicas. No existen de manera física, pero permiten realizar transacciones instantáneas a nivel mundial, es decir, son una moneda de intercambio entre usuarios. Otros tipos de moneda digital son el dinero electrónico o los cupones de internet, entre otros.

2.2 ORIGEN Y EVOLUCIÓN.

A lo largo del tiempo, podemos encontrar distintos medios de intercambio de bienes y servicios, como han sido el caso del trueque o el uso de materiales preciosos. Muchos de ellos han evolucionado o han desaparecido hasta la actualidad, dando paso a las monedas y los billetes. No obstante, hoy en día y con la tecnología avanzando a gran velocidad, ha sido necesario encontrar un método de intercambio más acorde con el presente: la criptomoneda.

En la década de los 80 surgió el movimiento Cypherpunk, y con ello la criptomoneda. Éstos apoyaban el uso de la escritura con claves secretas que únicamente lo entendería quien fuese capaz de descifrarlas. "A diferencia de los dólares y centavos que se pueden intercambiar y rastrear físicamente, las criptomonedas existen solo en el dominio digital." *(History of Cryptocurrency, 2021)*. Una década más tarde, Adam Black presenta Hashcash, un sistema para controlar los spam y los ataques de denegación de servicio.

Hasta 2008 no aparece el Bitcoin, propuesto por una persona o grupo de personas anónimas apodados como Satoshi Nakamoto, las cuales publicaron a través de un correo masivo de criptografía un documento compuesto por nueve páginas con el título "Bitcoin: A Peer-to-Peer Electronic Cash System". En él se incluía cómo funcionaba esta moneda digital en esa red peer-to-peer y la filosofía de ésta era, fundamentalmente, "un sistema de transacciones electrónicas sin depender de la confianza" *(Nakamoto, 2008)*.

Bitcoin sería la primera criptomoneda totalmente descentralizada que utilizaba el sistema digital conocido como Blockchain. En la actualidad no se conoce la identidad de Natamoto, a pesar de la existencia de algunas afirmaciones sobre ella. Actualmente, existen multitud de criptomonedas derivadas del Bitcoin, con algunas variaciones respecto a ésta.

2.3 BITCOIN.

2.3.1 Definición y uso.

Para poder entender el concepto de Criptomoneda, es esencial identificar Bitcoin: "Es una moneda digital, lo que significa que no existe ninguna forma material de la misma" *(Nakamoto, 2008)*. El Bitcoin es una moneda que utilizan los miembros de una comunidad para realizar intercambio de bienes y servicios, siempre y cuando se acepte su valor. Serán los usuarios los que, a partir del uso de la propia moneda, le darán un valor. Esta moneda no existe físicamente, es una moneda electrónica, libre y descentralizada que hará posibles las transacciones sin ningún intermediario, lo que promete costes más bajos. La diferencia entre una moneda o billete no virtual y el Bitcoin es que no es posible rastrear a los compradores y vendedores que utilizan está divisa, por lo que resulta interesante para los usuarios que buscan privacidad en sus transacciones.

El Bitcoin no es dinero fiduciario, es decir no está respaldado por ningún banco o entidad. Sin embargo, sí disponen de un sistema de trabajo que les permite evitar un doble gasto y de esta forma logran entrelazar todos los nodos que operan en la red, lo conocido como Blockchain. El sistema de la cadena de bloques es fundamental en las transacciones con Bitcoin, ya que al ser una base pública y abierta, existen cientos de copias de cada una de ellas y sería prácticamente imposible falsificarlas.

Los bitcoin son generados por usuarios llamados mineros, es un proceso que consiste en resolver problemas matemáticos gracias a procesadores informáticos, para poder continuar con su trabajo, ya sea crear más bitcoins o validar transacciones. Por cada bloque resuelto, los mineros obtienen una bonificación. En el origen, cuando fue creada esta criptomoneda, el creador decidió que cada diez minutos nuevas unidades de bitcoin se lanzarían al mercado y así surgió el proceso, aunque cada vez es más reducido. El límite de la oferta de bitcoin es de 21.000 millones de unidades. "Sin embargo, debido a que la tasa de bitcoins "extraídos" se reduce con el tiempo, el bitcoin final circulará hasta alrededor del año 2140. Esto no significa que las transacciones dejarán de ser verificadas. Los mineros continuarán verificando las transacciones y se les pagará una tarifa por hacerlo para mantener la integridad de la red de Bitcoin." *(How does Bitcoin mining work?, Mayo 2021).*Y no hay que confundir la oferta limitada con la cantidad de bitcoin que hay en el mercado, ya que aunque se alcanzase esa cifra, la oferta del mercado no alcanzaría ese valor, ya que los bitcoin se pueden perder. Este límite puede parecer de antemano una desventaja pero en realidad es atractivo para los usuarios el hecho de poder obtener valor de propia creación en un tiempo limitado y que la cantidad no se disparará en el futuro desplomando su precio. Este límite proporciona confianza a los inversores.

Para poder obtener bitcoins, es necesario poseer un monedero digital, que pueden guardarse en los dispositivos móviles, ordenadores, en forma física o en nuestra memoria.

Lo que se almacena en el monedero es una clave alfanumérica que permitirá a los usuarios acceder al sistema y consultar y realizar transacciones en el libro mayor. Es imprescindible recordar las claves, ya que en el caso de pérdida, no sería posible para el usuario acceder a su capital. En cuanto a los tipos de monederos que existen podemos distinguir:

- Escritorio: Este tipo de monederos son programas informáticos que permiten a los usuarios guardar los bitcoin almacenando las claves en el ordenador. Es compatible con todos los sistemas operativos: Linux, Mac y Windows. Existen dos tipos de clientes, el cliente completo (full client) o el cliente parcial (lightweight). Si se utiliza el primer monedero, se descarga en el ordenador la cadena de bloques completa que pesa aproximadamente 90 gigabytes y se convierte en un nodo del Bitcoin, pudiendo tener la información actualizada en todo momento. La única desventaja es que es poco eficiente y ocupa mucha memoria. En el caso de los clientes parciales, en su escritorio solo se guarda la parte de la cadena de bloques que le corresponde, no el nodo completo. Siempre será necesario un tercero para poder acceder a la red completa de Bitcoin.
- Móvil o app: Este tipo de monederos son aplicaciones que los usuarios tienen en sus dispositivos electrónicos que les permiten, tanto guardar bitcoins como realizar transacciones con comerciantes y con otros usuarios. Algunas aplicaciones funcionan como lightweight wallet y ocupan poco espacio, mientras que otras cumplen una función intermedia entre los lightweight wallet y los full client, son los Simplified Payment Verification (SPV). Este servicio no descarga la cadena de bloques entera, pero sí lo suficiente para poder comprobar en todo momento las transacciones y hacer frente a ataques externos, además de poder realizar pagos en los comercios. Es posible conectarlos con otros dispositivos y crear aplicaciones multiplataforma, que se puedan conectar desde móviles u ordenadores. Para garantizar la seguridad de las transacciones, es importante usar medios que tengan autentificación en dos pasos, es decir, que para acceder al sistema sean necesarias tanto las claves personales como el código de un único uso enviadas al dispositivo móvil para respaldar la identidad del usuario. De esta forma los clientes estarán protegidos frente a terceros.
- Web: A este tipo de monederos se puede acceder a través de un navegador. Funcionan de manera similar a los anteriores, con la desventaja de que algunas plataformas web utilizan sus propios navegadores para almacenar las claves, lo que las convierte en vulnerables frente a ataques externos. Será importante mantener actualizadas las aplicaciones, ya que estos soportes intentan mejorar su seguridad continuamente.
- Hardware: Este tipo de monederos no están conectados a la red, sino que se guardan en dispositivos externos, como puede ser un disco duro o un USB. Para poder realizar cualquier transacción será necesario conectar el dispositivo externo a un ordenador y un software se encargará de cargar, validar y permitir las transacciones. La ventaja principal de este sistema es que es inmune a ataques externos, ya que las claves de acceso solo se pueden encontrar en dispositivos externos y solamente se comprobarán online las necesarias. Por otro lado, se pueden encontrar algunos inconvenientes, como el hecho de que puede producir un robo físico y que será necesario asumir un coste para adquirir el dispositivo externo. Tampoco los usuarios podrán olvidar las contraseñas ya que serán necesarias en caso de cualquier problema.
- Monederos en la memoria o Brain wallet: Los usuarios solo podrán adquirir este tipo de monederos si son capaces de memorizar las claves alfanuméricas de

acceso, entre 25 y 36 caracteres. La ventaja principal es que será imposible que sufran ataques externos o de terceros, ya que las claves solo se encontrarán en la memoria de los usuarios. Es el método más seguro, pero a la vez el más arriesgado, ya que con un solo error del orden de los caracteres se perderá el acceso al capital. Además si el usuario quedara incapacitado o falleciera, y nadie más supiese de la existencia de esas claves, los bitcoins se perderían.

2.3.2 Seguridad.

El sistema de Bitcoin es una plataforma mucho más segura que los bancos y las tarjetas de crédito. Debido a la tecnología que se aplica, es un sistema completamente seguro. Lo que lo hace inseguro es la incorporación de intermediarios al realizar operaciones. El sistema Blockchain es infranqueable y falsificar movimientos dentro de él es imposible. Pero si se dispone de monederos online o de plataformas de compraventa de bitcoin es fácil que surjan robos y ataques.

Las empresas realizan grandes inversiones en seguridad para evitar ser hackeadas. Los clientes deben de encargarse de controlar que las plataformas online donde se guarda el capital estén actualizadas para no ser vulnerables a estos ataques. También es importante comprobar quienes son los proveedores de estos servicios para confirmar que es la empresa realmente y no un fraude.

En el sistema Bitcoin es posible conocer todas las transacciones realizadas desde el 2009, cuando fue lanzado al mercado de criptomonedas. Cualquier operación que se realice queda registrada y visible y es imposible eliminarla. Todos y cada uno de los movimientos realizados con esta criptodivisa carecen de intermediarios para evitar que se disponga de información de ésta sin el consentimiento de las partes que la realizan. Es posible que las partes quieran ser anónimas. Aunque cabe recalcar que el "anonimato" en el mercado de Bitcoin va ligado a una clave alfanumérica personal donde se envían y reciben los ingresos de otros usuarios. "Los nodos mineros utilizan algoritmos matemáticos para convertir la información de un bloque en un código alfanumérico o hash que enlace al hash del bloque anterior y encadenar los bloques entre sí. Por cada bloque añadido a la cadena, el nodo minero percibe una remuneración en criptomonedas o una participación en el negocio objeto de la transacción; una vez agregado un bloque, éste es inmutable. La participación de los nodos mineros sigue las reglas definidas por cada plataforma relativas al mecanismo de consenso, el cual determina en gran medida la seguridad, fiabilidad, velocidad y coste computacional y energético del proceso"*(Javier Alonso Lecuit. ARI106/2019, 2019)*. Por esta razón, no se consideran transacciones anónimas, sino seudónimas. En el caso de que nadie consiguiese averiguar quién está detrás de ese seudónimo, sería anónimo. Es posible que la identidad de un usuario pueda ser descubierta de varias formas:

I. Compartir la identidad en casa de cambio de manera voluntaria.
   En el caso de que se disponga de una cartera con este sistema, es obligatorio que el usuario se identifique, por lo tanto todos los movimientos y transacciones son fáciles de rastrear y relacionarlos con una persona. En teoría, la empresa no podrá desvelar la identidad de éste, solo podrá utilizarla para realizar el registro. Este supuesto tiene un riesgo, los ataques informáticos.

Un estudio realizado por OBPP (Open Bitcoin Privacy Project) sobre la seguridad de las carteras online demuestra que las que disponen de mayor capitalización no son las más seguras, sino que hay otras más sólidas. El principal factor de estas empresas es la privacidad, ya que un robo haría perder toda la credibilidad. Por ello se realizan inversiones en seguridad y es importante mantener las aplicaciones actualizadas.

II. Utilizar la misma cuenta de forma continuada sin precauciones.
Una recomendación que se le hace a los usuarios es que cambien de cuenta cada vez que realicen una transacción para que no sea posible relacionarlas entre ellas. Es un error que se comete habitualmente el de mantener una dirección durante un periodo largo de tiempo. Es posible que se averigüe quien es la persona a través de dicha dirección, observando las transacciones que realiza el usuario.

III. Registro de la IP.
Será relativamente sencillo llegar hasta el propietario de una transacción realizada a través de un ordenador ya que una IP es una secuencia de números y cifras que son identificables en la red. Para evitar dicho suceso, los clientes de Bitcoin pueden aislar en cierta medida su conexión IP codificando los datos a cambio de una comisión. También podrán mezclar bitcoins de diferentes transacciones antes de llegar al destinatario, manteniéndose las cantidades pero no se sabe el origen realmente. El usuario buscará alcanzar el grado de protección que desee, sin poder alcanzar el 100% en ningún caso.
Actualmente ha aparecido un nuevo contrincante en la red, el Big Data. Gracias a esta base de datos será posible destapar a personas que se esconden detrás de seudónimos del Bitcoin.

IV. Identificación no voluntaria: Las fuerzas del orden.
En algunos casos, tendrán que intervenir las fuerzas de seguridad, sobre todo en asunto criminales. A través de tecnologías más avanzadas podrán rastrear operaciones de Bitcoin e identificar a los usuarios. De esta manera facilita la búsqueda de usuarios que cometen actos criminales y aumenta la seguridad en la red.

2.3.3 Futuro del Bitcoin.

El sistema tecnológico y financiero mundial ha sido revolucionado por la Blockchain y las criptomonedas, ya que permiten realizar transacciones entre personas en cualquier lugar del mundo. No es necesario un intermediario para poder realizarlas, ni una cuenta bancaria, por lo que no habrá riesgo de falsificación porque sería necesario conocer el 51% de los usuarios anónimos y repartidos por todo el planeta. Los usuarios pueden observar las operaciones ya que son públicas, seudónimas e inalterables, y no podrán ser eliminadas. Esta posibilidad les permite tomar decisiones libremente y con total confidencialidad, aunque no al 100%, como quería Satoshi.

Como ya se ha dicho anteriormente, la oferta de bitcoin está limitada a 21.000 millones de unidades. El hecho de poder conocer la cantidad de monedas que existen en un instante es una ventaja , ya que los usuarios estarán advertidos de cualquier decisión que tomen las autoridades que pueda alterar el valor de su capital. También, como señala Cristina Pintado en el periódico BBC news (2021) “el hecho de que su creación tenga un límite de 21 millones (uno de los cuales está en manos de Nakamoto y fuera de circulación), lo convierte en un activo escaso y con gran potencial de revalorización.”

De todas formas, esta criptodivisa tiene algunos inconvenientes, como puede ser que solo se puede realizar siete operaciones por segundo y es un problema que no es posible solucionarlo ya que el sistema se creó así. Otras criptomonedas, como el Ethereum son más avanzadas. Además, minar bitcoins cada vez es más caro y las retribuciones son menores. Existen terceras partes como es el caso de las plataformas de intercambio, que dañan el sistema ya que sufre ataques que minimizan la confianza en todo el sistema. Otro inconveniente es su alta volatilidad, lo que no le permite competir contra una moneda estable o con el oro. Por último, otra traba que se encuentra es la falta de aceptación por parte de la sociedad, ya que los usuarios y el comercio son reacios a arriesgarse a probar métodos de pago desconocidos.

Por lo tanto, el bitcoin está lejos de considerarse una moneda como tal y ser usada a diario en la vida cotidiana. Habría que mejorar ciertos aspectos, como por ejemplo: Habría que alcanzar una estabilidad del valor respecto al dólar o al euro para poder hacer comparaciones de precios. También sería aconsejable el uso de subdivisiones de esta moneda virtual en los cobros y pagos cotidianos para evitar utilizar decimales y evitar los costes de actualización de precios. Finalmente, también sería importante que las transacciones fueran instantáneas para los comercios. Como indica Juan Pedro Asencio Flores en Funds People (2021), podemos destacar una mayor adopción de Bitcoin como forma de pago tras el respaldo de grandes compañías cotizadas como Tesla y compañías de referencia. Medios de pago como Visa, Mastercard, Paypal y Square´s Cash App han indicado sus planes para permitir depositar Bitcoin en sus wallets para realizar pagos y permitir su compra y venta.

“Cuanto mayor sea su aceptación, más tenderá a valer (en su equivalente en dólares o euros) dada una cantidad de bitcoins en circulación. Pero el grado de aceptación futuro es una gran incógnita. La fuerte volatilidad de su cotización refleja, en buena medida, cambios en la percepción sobre dicho grado de aceptación. El día que Ben Bernanke, por ejemplo, declaró en el Senado de los EE. UU. que el bitcoin podía ser una promesa de futuro, su cotización se disparó por encima de los 1.000 dólares. Días más tarde, cuando las autoridades chinas prohibieron a los bancos de ese país procesar pagos en bitcoin, su cotización se desplomó por debajo de los 600 dólares.” *(Antonio Escoda, 2014)*

Por otro lado, los usuarios han observado que los inversores que manejan bitcoins desde sus comienzos, su capital ha ido aumentando año tras año. Por lo tanto se percibe que puede ser rentable a largo plazo como depósito de valor, siempre que se esté dispuesto a asumir el riesgo de la volatilidad.

En conclusión, el bitcoin resulta interesante para los economistas y los expertos en este campo por su alta volatilidad, y un reto para las personas que desean invertir o trabajar con criptomonedas.

2.4 ¿CÓMO INVERTIR O COMPRAR EN CRIPTOMONEDAS?

Lo primero que debe de saber un usuario cuando va a adquirir criptomonedas es que funcionan como el dinero real, en muchas ocasiones respaldadas por divisas legales como el euro o el dólar. La forma de obtenerlas es a través de internet, ya que no existen físicamente y deben almacenarse en un monedero virtual. Existen tres formas de obtener criptomonedas:

I. Compra al contado.
La manera más utilizada de comprar es a través de plataformas Exchange, que a su vez se utilizan de monedero digital. Es un método que suele ser fiable y seguro, ya que no requiere de intermediarios para realizar las transacciones. Por lo tanto, los costes son mínimos.
En estas plataformas se puede comprar, vender o cambiar criptomonedas, bien por otra criptodivisa o por monedas reales. También es posible negociar en un mercado estableciendo el usuario el tipo de cambio. Este tipo de inversiones son similares a la adquisición de acciones. Se compra y se espera a que aumente su valor. Esta estrategia se llama "buy and hold" (comprar y mantener).
Este tipo de mercado al contado es un mercado OTC, descentralizado y muy opaco.

II. Minería de criptomonedas.
No solo se pueden obtener bitcoins comprándolos en el mercado, sino que se pueden generar a través del proceso de minería, un proceso de solución de algoritmos matemáticos que mantienen la red que actúa como base de las transacciones. Es un procedimiento que necesita potentes equipos informáticos para poder procesar los problemas matemáticos que hay que resolver para obtenerlas y además hay que almacenar la información encriptada de las criptodivisas. Esta manera de obtener bitcoins requiere de una alta inversión inicial y un equipo de trabajo que pueda llevar a cabo la actividad.

III. Salario en divisas electrónicas.
Hoy en día existen empresas que pagan el salario de sus empleados en criptomonedas, utilizando el bitcoin como referencia. Algunos casos, como es el Burger King en Rusia, ha creado su propia divisa la cual pueden utilizar tanto empleados como clientes. Otro claro ejemplo sería OMG Internet, que comenzó a pagar a sus empleados con monedas virtuales en 2018.

2.5 OTRAS CRIPTOMONEDAS DEL MERCADO: DIREFENCIAS CON EL BITCOIN.

Desde la aparición del Bitcoin, la precursora, y con el aumento de inversiones en criptomonedas, muchas empresas han querido aprovecharse de ello. Han ido surgiendo nuevas, llegando a existir cientos de criptodivisas. En estos último años, algunas han tenido más éxito que otras, como ha sido el caso de las siguientes :

- Ethereum (ETH) "es una plataforma descentralizada de código abierto y escrita con un lenguaje de programación Turing completo integrado. Este código de programación es incorporado a la tecnología mejorada de la Blockchain para posibilitar la creación de la piedra angular de Ethereum: las aplicaciones distribuidas.." *(Melodía, Mayo 2021)*. Esto quiere decir que, a diferencia de otras criptomonedas, Ethereum se desarrolló en un medio innovador en el que toda su información no se sitúa físicamente en ningún servidor, por lo que disminuyen los riesgos de censuras o problemas técnicos, entre otros. Desde su lanzamiento en 2015, Ethereum alcanzó el segundo puesto como criptomoneda mejor cotizada después de Bitcoin.
  A diferencia de este último, no existe una cantidad máxima de generación de ether. Por otro lado, la velocidad de las transacciones en Ethereum es de únicamente 12 segundos y el coste se basa en los recursos utilizados en la red, mientras que Bitcoin tarda aproximadamente 10 minutos, y el coste de dichas transacciones es idéntica, limitadas por el tamaño del bloque.

- Ripple (XRP), sucesor del Bitcoin, es un software encriptado que posee su propia criptomoneda. "Ripple se trata de un sistema totalmente seguro y encriptado cuya información de las transacciones son públicas pero la información del pago no. Es decir, es un sistema confidencial donde el emisor y receptor son los únicos que disponen de la información y el código que la desencripta*."(Javier Sáez Hurtado, 2021)*. Fue creado para mejorar las transferencias monetarias en las entidades bancarias: Simplificar el empleo de capitales disminuyendo los costes de servicio y aumentando la velocidad de los pagos internacionales.
  Ryan Fugger, un desarrollador de webs, comenzó este proyecto en 2004, aunque su lanzamiento no tuvo lugar hasta 2012. Al principio fue llamado RipplePlay, cuyo objetivo era crear un sistema monetario descentralizado para poder realizar pagos seguros entre los usuarios. Ahora se ocupa del progreso del futuro de la criptomoneda.
  A diferencia del Bitcoin, Ripple es aceptado por parte de las entidades bancarias. Muchas de ellas están optando por la tecnología de este software para reducir los tiempos de las operaciones. Cabe destacar también el volumen de transacciones que se pueden realizar con Ripple, ya que es capaz de procesar 1500 simultáneamente mientras que Bitcoin es posible entre 3 y 6.

- Litecoin (LTC, Ł) "es una criptomoneda que se sustenta en una red P2P y sobre un software de código abierto publicado con licencia MIT"*(Melodía, 2020).*
  Se desarrolló con el fin de ser la alternativa a Bitcoin, ya que produce cuatro veces más unidades que ésta. Aplica una función que posibilita minar a muchos más usuarios al estar adaptado a CPUs. La cantidad máxima de LCT es de 84 millones, por lo que también supera a Bitcoin. El inconveniente es que la recompensa por cada bloque minado se divide a la mitad cada 4 años.

- Cardano (ADA) es una plataforma y protocolo de Blockchain formada por tres compañías (a Cardano-Foundation, las empresas IOHK y Emurgo**)** creada con la finalidad de solucionar los problemas y debilidades de anteriores Blockchain y ser la más avanzada en la actualidad. En los últimos años, se ha convertido en una de las criptomonedas con mayor crecimiento, llegando a multiplicar 45 veces su valor en este último año. "Además, se ha reescrito todo su código en un nuevo lenguaje de programación conocido como Haskell, considerado más seguro y confiable." *(Melodía, 2020)*
  Cabe la posibilidad de producir 45 billones de ADAs, a diferencia de los 21 millones de Bitcoin. Además, Cardano está desarrollando una plataforma que dará la posibilidad de negociar sin acudir al dinero fiduciario y legitimidad garantizada proporcionando la interacción de protocolos de las criptomonedas y la comunidad financiera.

CRIPTOMONEDA	CAPACIDAD DE MERCADO	CANTIDAD MÁXIMA	LANZAMIENTO
Bitcoin (BTC)	+/- 44%	21 millones	2009
Ethereum	+/- 17%	Sin límites	2015
Ripple (XRP)	+/- 8%	100 millones	2012
Litecoin (LTC, Ł)	+/- 3%	84 millones LTC	2011
Cardano (ADA)	< 1%	45 billones ADA	2017

Tabla 1. Tabla comparativa de criptomonedas (Broker Online, 2021)

Aparte de las mencionadas anteriormente, no hay que perder de vista una criptodivisa que ha causado revolución por parte de las empresas y que ha estado presentes en el mercado financiero durante el último año ya que su lanzamiento se ha ido aplazando por diversos motivos.

"Libra" fue la criptomoneda creada por Facebook, aunque se rumorea en la actualidad que su nombre pasará a ser "Diem". En 2019, la empresa presentaba la nueva criptodivisa creada por veintisiete socios, incluidos algunos como Uber, Sportify, Visa o Mastercard. Su tecnología principal es Blockchain. Libra pretenden que esté respaldada por activos financieros para intentar evitar la volatilidad y será una divisa constante estando su valor vinculado a monedas estables y reguladas ya existentes, como el dólar estadounidense, el euro o la libra esterlina. Facebook puede alcanzar a un gran número de usuarios entre las aplicaciones de WhatsApp, Messenger e Instagram. Además, esta red social ha creado su propia cartera digital para almacenar el dinero, Calibra. Con ésta, no sería necesario disponer de una cuenta corriente en un banco.

Entre otras ventajas por las que destaca esta criptomoneda, es que es una moneda global y tiene un sistema de programación propio, pero esto se ha ido desvaneciendo a medida que los gobiernos y los organismos económicos han impuesto problemas.

Por parte de los gobiernos ha producido rechazo ya que no está regulada y podría poner en peligro la estabilidad financiera. Además, el público en general tampoco la acepta porque esta divisa está respaldada por Facebook, compañía que ha sido nombrada en varias polémicas por la cesión de datos personales. A pesar de que Facebook ha asegurado que no controlará los movimientos que se realicen, crea incertidumbre entre los potenciales inversores. Para dar tranquilidad a los bancos y a los gobiernos, Libra dejó de ser una criptomoneda global como al principio y pasó a ser una "stablecoin", es decir, "el valor de Diem no fluctuará, no variará dependiendo del interés de los usuarios en ella, sino que estará vinculado a una moneda estatal. Es decir, un Diem en la zona euro tendría el valor de un euro, un Diem en EEUU tendría el valor de un dólar, etc., o sea, que tendrá el mismo valor que la moneda del país donde se opere. Todo esto nos llevaría a una criptomoneda menos volátil y más supervisada" *(Trading y bolsa, 2021).*Así Facebook perdería cierto control y poder sobre ésta de forma voluntaria y transmitiría confianza a los reguladores. Este hecho tendría beneficios para zonas más desfavorecidas en las que sus monedas locales son poco líquidas e ineficientes, provocando exclusión del sistema financiero y perdiendo oportunidades. La creación de esta plataforma que pone en contacto a multitud de personas suscita esperanza de una mayor inclusión financiera.

Ilustración 1. Estado de los socios de Libra (Ibercampus, 2019)

Por otra parte, algunos socios del proyecto Libra, como es el caso de Ebay, Mastercard o Visa abandonaron el proyecto ya que no está siendo respaldados por los principales países aun estando compuesto por una cesta de Libra tokens con las principales divisas. Un ejemplo es el Ministro Federal de Finanzas de Alemania, que se opone al proyecto Libra por considerarlo un gran riesgo para el sistema financiero global debido al gran volumen de usuarios de la plataforma Facebook. Con más de dos mil millones de usuarios, Libra podría llegar a cualquier lugar del mundo y causa miedo en las organizaciones gubernamentales por la capacidad que tiene de provocar un terremoto financiero. Otro caso de oposición al proyecto es el del profesor de finanzas de Stanford. El principal motivo de rechazo es la probabilidad de que las criptomonedas trastoquen el sistema tradicional de los bancos en el futuro y acaben con sus ganancias originadas por las bajas tasas de interés.

Estos acontecimientos han producido que los usuarios observen las demás criptomonedas. Éstas podrían sufrir caídas notorias ya que si Facebook tiene que abandonar el proyecto, Libra por no contar con el apoyo de los reguladores de Estados Unidos, podría crear un efecto pánico que afectaría a todas las criptodivisas. Otro factor que afecta a este mercado

es el posible acuerdo entre China y Estados Unidos, ya que si se hiciese real este hecho, éstas dejarían de ser interesantes para los inversores como valores refugio. La único opción es mantenerse a la espera de que Facebook lance su moneda al mercado este año para observar la reacciones, aunque con la pandemia de Coronavirus todo puede cambiar. En el siguiente apartado se explican las consecuencias de este suceso.

2.6 SITUACIÓN DE CRIPTOMONEDAS EN COVID-19.

Durante el año 2020, tras la aparición de la pandemia Covid-19, la economía se ha parado a nivel mundial y con ello, ha afectado a la mayor parte de los sectores. Por este motivo, y ante la necesidad de mantener activas las cadenas productivas, ha sido beneficioso el uso de herramientas como blockchain, que garantiza las ventajas de menor contacto físico y mayor eficiencia. De esta manera las empresas han podido conseguir que el comercio exterior se mantenga activo. Blockchain es una forma segura a través de ciertos servidores y diversos controles de asegurar operaciones sin contacto humano.

Numerosas empresas ya utilizan este tecnología en el comercio internacional, ofreciendo servicios de cobros y pagos a través de ella, el control de inventario y el seguimiento de los envíos. En el comercio exterior existen ciertos protocolos que con esta nueva tecnología brindaría celeridad y transparencia ya que todos los participantes tendrían toda la información en tiempo real, ya que ésta no podría ser borrada ni modificada. Además, se ahorraría tiempo y costes causantes de ineficiencia e incertidumbre en las operaciones. En este sentido, el coronavirus se puede tomar como una oportunidad para modificar y transformar el comercio exterior.

En cuanto a las criptomonedas, muchos inversores temían perder sus ahorros por lo que han recurridos a ellas buscando valores refugio que los protegiesen de las consecuencias económicas de la pandemia global. De hecho, en el comienzo de la pandemia, los mercados bursátiles sufrieron un colapso del sistema tradicional, consiguiendo que las bolsas cayesen desmesuradamente, incluso llegando a suspender operaciones, lo que provocó en los inversores desespero e incertidumbre sobre el futuro. Como indica Alan Draguilow, CEO de ChangeTheBlock en el artículo “Bitcoin en época de coronavirus: del desplome al imprevisible 'halving' (2020),”, “Lamentablemente, ante esta crisis del coronavirus, se ha podido ver que todavía el bitcoin no es considerado un valor refugio tan seguro como el oro. Los mercados han aguantado el comienzo de la crisis cuando la mayoría de la población afectada era la china, pero una vez que se propagó a nivel mundial sus efectos fueron devastadores para todo el mercado de las criptomonedas.”

La principal ventaja de las criptomonedas es la descentralización y con ello el poder entrar y salir del mercado criptográfico en cualquier momento. Por eso los inversores que lo utilizan, les permite tomar decisiones con fluidez. Durante estos meses pasados, el mercado de criptomonedas dio un giro inesperado. A medida que los casos de coronavirus aumentaban, se incrementaban tanto los precios como el volumen. La paralización de la economía y con ello, la falta de liquidez, abre un campo de oportunidades a las criptomonedas. Según un estudio elaborado por los profesores de la universidad Oxford “el estudio indica que en los picos más altos de la pandemia los inversiones utilizaron las criptomonedas como valores refugio”, lo que indica que en el momento que se comenzó a controlar el contagio, disminuyó el uso de las criptomonedas.

Relacionado con este tema, los mineros y los exchanges también sienten las consecuencias del coronavirus, por lo que tuvieron que tomar decisiones sobre la rentabilidad y la seguridad de los trabajadores.

En el caso de los mineros, algunos de los menos eficientes no consiguieron alcanzar rentabilidad suficiente ni obtener ganancias con los precios del momento y cerraron sus plataformas. Esto lleva a que la protección de la red ("hashrate") disminuya considerablemente y posteriormente, esto se convirtió en un incentivo para que los mineros volvieran a conectarse. "El resultado es que hemos visto un intenso aumento en la volatilidad del hashrate de Bitcoin, que comenzó un par de semanas después del 24 de febrero, cuando los mercados comenzaron a desplomarse." *(David Borman, 2020)*

Por otro lado, otra manera que la pandemia ha afectado a los mineros, es que al no ver rentabilidad en sus trabajos, donaron parte de sus ganancias para investigar la vacuna contra el coronavirus.

En cuanto a los exchanges de criptomonedas, han sufrido ciertos cambios. En muchos casos, las plataformas de intercambios se pueden utilizar sin necesidad de que haya trabajadores en las oficinas, ya que la mayoría de ellas existen en Internet. Como en el caso de Coinbase, disponen de las herramientas necesarias para trabajar desde los hogares de forma remota, y así mantener a seguros a sus empleados. Gracias a esto, las plataformas de intercambio no han sufrido grandes variaciones en el funcionamiento, al menos en la parte del usuario. También los exchanges de criptomonedas han estado contribuyendo a la búsqueda de la vacuna contra el coronavirus realizando donaciones a los fondos de investigación, como fue el caso de Ripple y Binance, entre otras.

Los mercados también fueron muy afectados en los trading de futuros, ya que se generó incertidumbre sobre lo que iba a ocurrir en el futuro tanto en la economía global como en las criptomonedas. El valor de los contratos de futuros de Bitcoin aumentó notablemente. "Recientemente, tanto CME Group como Bakkt han informado un aumento considerable en el volumen de sus operaciones de futuros de BTC, ya que claramente los inversores están tratando de bloquear los precios contra nuevas caídas del mercado, y los especuladores están tratando de beneficiarse de la volatilidad." *(Luis Jesús Blanco Crespo, 2020)*

Por último, y siguiendo con las consecuencias de la pandemia en el mercado de criptomonedas, también se puede observar como la percepción del público hacia ellas ha cambiado durante este periodo. Muchos describieron el inicio de los contagios como una masacre, ya que el Bitcoin cayó un 50%. Este hecho creó dudas sobre si realmente las criptomonedas son reservas sólidas, ya que las fluctuaciones son posibles. Estas dudas provienen de la manera en la que la crisis del coronavirus está afectando al valor de dinero en todo el mundo. La Reserva Federal de Estados Unidos está generando un millón de dólares por segundo. Esto podría potenciar una inflación el dólar estadounidense, que podría provocar que tanto ciudadanos como inversores se refugien en criptodivisas, que deberían ser muy resistentes a la inflación. A raíz de la pandemia, ha habido numerosas quiebras bancarias y rescates, por lo que la confianza del público disminuye y podría provocar que comenzasen a extraer su dinero de las entidades bancarias. Esto se denomina "corralito bancario". En el caso de que este suceso se desarrollase, las entidades bancarias no tendrían suficientes fondos para devolver a los clientes su dinero, y beneficiaría al mercado de criptomonedas ya que parte del público podría refugiarse en ello.

Por otro lado, esta crisis podría ser una causa de necesidad de crear una o más monedas del Banco Central, tanto para utilizarlo, como un medio para distribuir fondos de ayuda,

o para evitar la transmisión de virus a través del papel moneda. Esto ha hecho que el público en general se interesase por los activos digitales, con el fin de ayudar a frenar el contagio. Un ejemplo anterior a la pandemia fue China, que había explorado la opción de crear una moneda nacional basada en blockchain, pero ahora más naciones se interesan por este tipo de proyectos.

2.7 RELACIÓN ENTRE EL BANCO CENTRAL Y LAS CRIPTOMONEDAS.

En un periodo inferior a 10 años, el Bitcoin ha pasado a ser utilizado por gran parte de la población, y ha aumentado su valor por encima de los 4.000 dólares. Ésta y todas las criptomonedas que han ido surgiendo han demostrado la viabilidad de las cadenas de bloques subyacentes, una variante de la tecnología de registros distribuidos (DLT). Esta tecnología se diferencia de la cadena de bloques tradicional en que se quiere restringir la información pública de las para que dispongan de una mayor confidencialidad y escalabilidad. Los expertos en capital riesgo y en instituciones financieras han realizado numerosa inversiones en DLT, y finalmente, los bancos centrales han sido los últimos en incorporarse a este experimento.

Las criptomonedas en los bancos centrales trataban de definirlas en un informe del Comité de Pagos e Infraestructuras del Mercado (CPMI, 2015) como "electrónicas; no constituyen un pasivo de nadie; y permiten el intercambio entre pares". Sin embargo, esta definición no tiene en cuenta la característica de accesibilidad. "En la actualidad, una forma de dinero de bancos centrales –el efectivo– está a disposición de todo el mundo, mientras que a las cuentas de liquidación de bancos centrales sólo pueden tener acceso algunas entidades, fundamentalmente bancos" (CPSS, 2003, p.3). Por este motivo, Berg (2017) incluye la propiedad de acceso universal, fácil de obtener y utilizar, a la definición de monedas electrónicas y emitidas por los bancos centrales. Uniendo las cualidades de CPMI (2015) y Bjerg (2017) se forma una nueva división del dinero, las monedas digitales de los bancos centrales (CBCC).

"Las propiedades utilizadas en dicha taxonomía son: emisor (banco central u otro tipo); formato (electrónico o físico); accesibilidad (universal o restringida); y mecanismo de transferencia (centralizado o descentralizado, es decir, entre pares*)."(Morten Bech Rodney Garratt, p.5)* Esta nueva clasificación crea dos posibles tipos de CBCC emitidas por los bancos centrales. Una clase que a dirigida al público en general, es decir, minorista, mientras que existe otra que está enfocada a instituciones financieras, quiere decir a nivel mayorista.

En el caso de las monedas digitales minoristas, actualmente no existen, pero generan un gran debate por diversos motivos. Sería necesario lograr un equilibrio entre las ventajas y los inconvenientes de éstas. "Si el público pudiera convertir fácilmente el dinero que tiene depositado en bancos comerciales en pasivos de bancos centrales libres de riesgo se podrían producir más rápidamente episodios de retirada masiva de fondos bancarios" *(Tolle, 2016)*. Otra incógnita es el anonimato, ya que en muchos casos preferirían que las partes fuesen totalmente ocultas ya que "el conocimiento por parte de un tercero del nombre del beneficiario, el importe y la fecha de pago de cada transacción realizada por una persona puede revelar gran cantidad de información sobre el paradero, las relaciones y el estilo de vida de esta" *(David Chaum, 1983).* Un inconveniente de no revelar la

identidad es que puede favorecer a la actividad delictiva o el blanqueo de capitales. Por otro lado, los bancos perderían la desintermediación entre los consumidores y se perdería el seguimiento de ellos, punto que sería positivos para los usuarios ya que se reducirían además los costes.

En el otro extremo, mientras que las anteriores no existen aún en el mercado, las criptomonedas de bancos centrales para pagos mayoristas se están quedando obsoletas ya que utilizan diseños de bases de datos con los que no es posibles alcanzar los objetivos y es caro mantenerlas. Además, los accesos son restringidos, es necesaria una autorización. Por lo que tendrían que crear un sistema más útil y seguro para una nueva variante de estas CBCC. Por otro lado, estas monedas digitales mayoristas permitirían aumentar la eficiencia con operaciones de valores y derivados. Otro inconveniente serían los límites de la cantidad de criptomonedas que se pudiesen emitir en el mercado. "Con frecuencia se habla de distintos tipos de límites cuantitativos o topes para el uso de CBDC o las posiciones en estas monedas, como método para controlar consecuencias no deseables o para orientar el uso en determinada dirección." (Banco de pagos internacionales, 2018) Lo que quiere decir que sería negativo para los pagos mayoristas.

En conclusión, es un proyecto que genera cierta tensión en el mercado por el impacto que pueden generar sobre las criptomonedas ya existentes, e influirán aspectos como la regulación, los problemas de seguridad y la velocidad de las transacciones.

3. BLOCKCHAIN.

3.1 DEFINICIÓN DE BLOCKCHAIN.

"Una Blockchain es un libro de contabilidad digital de transacciones económicas que es totalmente público, actualizado de manera continua por innumerables usuarios, y considerado por muchos imposible de corromper" (Carlozo, 2017), y es posible realizar cualquier tipo de operación entre dos personas sin necesidad de ningún intermediario. Está protegida criptográficamente y cada usuario podrá registrar operaciones que se irán uniendo en forma de bloques, hasta que finalmente se termine creando una cadena. Otra cuestión a resaltar es que el sistema blockchain permite que todos los participantes del mismo puedan confiar plenamente en la información registrada en él. Esto nos hace pensar que es un medio seguro, transparente e imborrable, en el que cualquier dato es público.

La información se transfiere a través de una Blockchain. Un bloque es un conjunto de transacciones que se agrupan y encriptan y son enviadas a todos los nodos de la red. En cada bloque se almacena una cantidad limitada de registros válidos, información referente a ese bloque en concreto, y el vínculo que tiene con el bloque anterior y el siguiente, a través de un código único que sería como la huella digital de ese bloque. Esa contraseña se denomina "hash".

Cuando dos usuarios realizan una transacción y es aceptada por todos los nodos de esa red, ésta pasa a completarse y a formar parte del bloque de transacciones. En el momento que el bloque alcanza su capacidad limitada de transacciones, se minan los bloques. Esto quiere decir que queda registrado de forma permanente es la cadena de bloques, y no podrá ser modificado sin alterar el resto de bloques que están enlazados a él. Por lo tanto, cada bloque tendrá un lugar específico e inamovible dentro de la cadena. En cada nodo que forma la blockchain se guarda la cadena completa, es decir, se almacenan copias exactas de ésta en todos los participantes de la red.

Para realizar estas operaciones se utiliza una red P2P. Esto es una red de ordenadores que funciona sin servidores fijos, es una serie de nodos que se comportan de manera idéntica entre ellos.

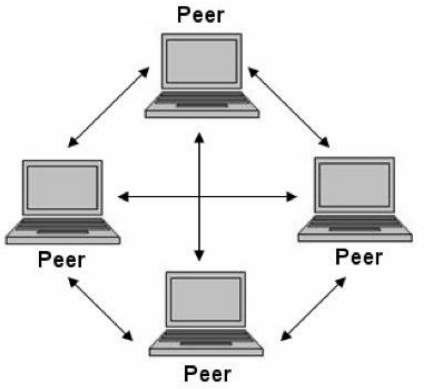

Ilustración 2. Red peer to peer (P2P)

La diferencia más destacable entre la blockchain y otras bases de datos es que está distribuida. Esto significa que no es necesario ningún tercero que se encargue de almacenar y controlar los datos. La información la encontraremos dispersada por toda la red. Esta es la clave central del sistema blockchain, miles de ordenadores se encargan de controlar y administrar el libro mayor, que es público y de libre acceso. Cualquier persona que disponga de conexión a internet podrá consultarlo en cualquier momento. Esta situación tiene una ventaja principal, la corrupción de este sistema es imposible.

3.2 ELEMENTOS BÁSICOS DE BLOCKCHAIN.

Para poder entender la tecnología y el funcionamiento de la blockchain, es necesario conocer los elementos básicos que la sustentan. Son los siguientes:

3. En primer lugar encontramos los **nodos**, son los equipos informáticos de la red que sostiene la cadena de bloques, es decir, su infraestructura. Dependiendo de lo compleja que sea la red, puede ser desde un ordenador personal a una megacomputadora. Almacenan el libro de cuentas como un libro mayor de contabilidad. Todos los nodos, independientemente de la capacidad que tengan las unidades, deben de tener el mismo protocolo para comunicarse entre sí. Si esto no sucede, no pueden conectarse ni formar parte de la red de una blockchain, sea pública, privada o híbrida. La diferencia entre una red pública y una red privada es que en la pública los nodos no tienen por qué identificarse mientras que en la privada se conocen entre sí, pudiendo ser iguales entre ellos.
4. Un **protocolo estándar**, en forma de software informático. Todos los ordenadores de la red deben de comunicarse en el mismo lenguaje. Existen protocolos muy conocidos, como pueden ser el TCP/IP para internet o el SMPT para el intercambio de correos electrónicos. El objetivo del protocolo es alcanzar un consenso sobre cuál será la versión válida de registro y definir la comunicación entre los ordenadores participantes en la red.
5. Otro elemento importante es una **red de pares o P2P** (Peer-to-Peer). Se trata de una red de pares distribuida, en la que los nodos u ordenadores se encuentran conectados entre sí. En esta red no existe jerarquía. En las blockchain privadas pueden existir casos en los que sí existan nodos con diferentes autoridades.
6. Por último, no puede faltar un **sistema descentralizado**. En los sistemas centralizados existe una jerarquía, es decir, todos los ordenadores están controlados por una única entidad. En cambio, en los sistemas centralizados los sistemas conectados a la red la controlan de forma equivalente debido a que son iguales entre sí. Esto quiere decir que no existen rangos, al menos en la blockchain pública. En una blockchain privada sí que se puede dar el caso.

3.3 TIPOS DE BLOCKCHAIN.

Se suele hablar de la tecnología blockchain como si únicamente existiera un tipo, pero en realidad hay diversas. Desde su aparición, está tecnología ha ido evolucionando y fue de interés para muchos individuos por la transformación y revolución que traía consigo. Al comienzo eran blockchain públicas y al alcance de todos con el único objetivo de mejorarla y participar activamente en ellas. Con el paso del tiempo, los gobiernos y empresas comenzaron a interesarse por esta nueva tecnología y dio origen al nacimiento de una nueva visión: Blockchain privadas y blockchain híbridas. Las diferencias entre ellas se encuentran en las funcionalidades, protocolos de consenso o las reglas para validar las transacciones.

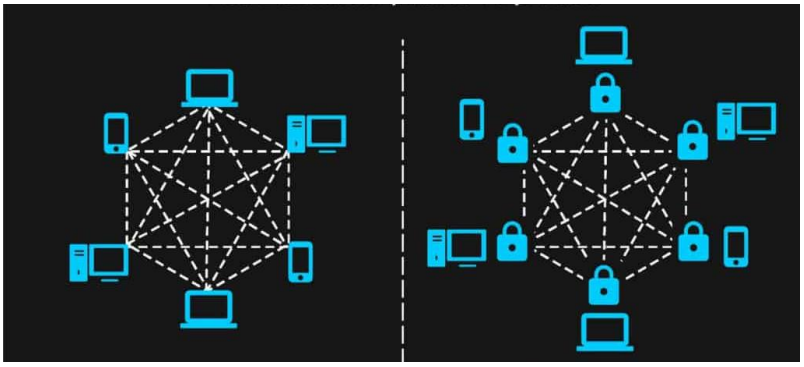

Ilustración 3. Bockchain pública (izq.) vs. Blockchain privada (dcha.)

3.3.1 Las Blockchain públicas.

Las blockchain públicas fueron el primer tipo que existió y se puede acceder a ellas públicamente desde Internet.

En este tipo de blockchain, los datos, el software y su desarrollo se mantiene abierto al público, de manera que cualquier individuo puede revisar, desarrollar o mejorar los mismos. En la red completamente descentralizada cualquier persona puede crear bloques y participar en el proceso de validación. Un conjunto de ordenadores se encargan de validar y controlar las transacciones que se introducen y consiguen que sea un sistema de confianza para todos los usuarios.

Por regla general, las blockchain públicas suelen tener ciertas características en común:

7. Son públicas, es decir, cualquier persona puede formar parte de la red, bien sea como usuario, minero o administrador de un nodo. Además, cualquier individuo sin ser usuario puede acceder a la red y consultar las transacciones realizadas sin restricción alguna.
8. Son abiertas, lo que quiere decir que el funcionamiento de la red es completamente transparente. Los datos de la blockchain están disponibles para todos los usuarios sin restricciones y cualquiera con unos conocimientos mínimos podrá participar en el protocolo común y revisar el funcionamiento de la red y su software.

9. Son descentralizadas, ya que no existe ninguna entidad que tenga poder sobre el resto ni controle su funcionamiento. Todos los nodos son iguales entre ellos.
10. Son pseudónimas, es decir, los usuarios son desconocidos. Aun no siendo identificables, se podrán rastrear sus direcciones debido a su carácter público. Este es el motivo principal por el que la mayor parte de las blockchain públicas no pueden ser anónimas, excepto las que se crean especialmente para que lo sean.

Las blockchain públicas más conocidas son Bitcoin y Ethereum.

3.3.2 Las blockchain privadas.

Las blockchain privadas se pueden definir como cadenas de bloques que necesitan de un permiso para entrar en ellas. Este tipo de blockchain suele contar con los mismos elementos que la blockchain pública, pero con una diferencia, una única entidad central que se encarga de ejercer el control sobre las acciones que se realizan en la cadena. Esto quiere decir que la escritura se centraliza en una única empresa. Además, esta unidad central permite el acceso a los usuarios que quieren realizar transacciones y controla las funciones que realizan dentro de la blockchain. El acceso a esta red solo se puede obtener a través de una invitación. Este tipo de blockchain suele estar pensada para realizar intercambios de grandes volúmenes en los que no interesa que terceros puedan tener acceso a los mismos. Por ello, la lectura de la red puede ser pública o limitada, dependiendo de la decisión de la organización principal.

Este tipo de blockchain suelen tener las siguientes características:

- En primer lugar, son privadas ya que solo algunos datos anotados en la blockchain serán emitidos de forma pública y únicamente los participantes pueden acceder e informarse o efectuar algunas transacciones.

- Otra característica es que son cerradas, es decir, solo podrán adquirir la condición de usuarios o registradores de las transacciones aquellas personas a través de una invitación. Además, no todos los usuarios tendrán las mismas capacidades dentro de la red, unos podrán registrar información mientras que otros estarán vetados. Siempre dependerá del objetivo que se pretenda cumplir.

- Son distribuidas, lo que significa que es una base de datos divididas en varios nodos. La cantidad de nodos que formen una blockchain pueden limitarse al número de participantes o a cierto número de ellos. Una de las fortalezas que tiene la blockchain privada es que los nodos se conocen entre ellos y la protegen, y también los incentivos que pueden obtener por cumplir esta función. Cuanto mayor sea el número de nodos, menor será el riesgo de fraude. A diferencia de las blockchain públicas en las que los nodos protegen la blockchain de forma voluntaria, en la privada se comprometen a cumplir esta función y mantener el sistema estable. Esto quiere decir que una blockchain privada no será tan versátil como una pública, ya que es de mera importancia que se definan las medidas para garantizar la protección.

- Las blockchain privadas también son anónimas. Con el objetivo de proteger las transacciones podrán establecer el grado de anonimato que deseen. Los usuarios que realizan transacciones podrán estar o no identificados.

3.3.3 Las blockchain híbridas.

Las blockchain híbridas son una mezcla entre las públicas y las privadas. En estas blockchain, la participación de los nodos es privada, es decir, pueden entrar en la red mediante invitación y todos se comprometen al mantenimiento y seguridad de ésta. Sin embargo, el libro de contabilidad es accesible para cualquier usuario. Las transacciones son públicas y visibles para cualquier usuario, mientras que en la blockchain privadas las transacciones son privadas también. Este tipo de blockchain son parcialmente descentralizadas y tiene como objetivo ofrecer un alto grado de transparencia y confianza.

Características	**Blockchain públicas**	**Blockchain híbridas**	**Blockchain privadas**
Nivel de acceso	Todos los mineros	Conjunto seleccionado de nodos	Una sola organización
Participación	Público	Podría ser público o restringido	Podría ser público o restringido
Inalterabilidad	Casi imposible de manipular	Podría ser manipulada	Podría ser manipulada
Rendimiento	Bajo	Alto	Alto
¿Centralizado?	No	Parcialmente	Sí
Proceso de consenso	Sin permiso	Autorizado	Autorizado

Tabla 2. Taba comparativa de tipos de Blockchain (Inetum, 2017)

3.4 BLOCKCHAIN Y LA INDUSTRIA 4.0

La Industria 4.0 o también llamada Cuarta revolución industrial es la unión de sistemas avanzados de producción y operaciones de nuevas tecnologías, como son la robótica, nanotecnología, el Internet of Things (IoT), entre otras. Esta combinación tiene como objetivo que las empresas mejoren y puedan satisfacer de manera óptima sus necesidades y las de sus clientes. Esta transformación permite crear un ciclo continuo entre el mundo físico y el digital gracias a un flujo continuo de información en tiempo real. Se capta la información del mundo físico y se crea un apunte digital de ésta. Seguidamente se comparte dicha información y se interpreta con la finalidad de captar lo más relevante. Por último, se transforman en datos físicos a través del uso de algoritmos.

Gracias a estos avances, podremos observar cambios que afectarán a todas las industrias, sectores e incluso a la sociedad. En primer lugar, aparecerán nuevos modelos de negocio,

ya que este sistema asegura intercambios de datos fiables, seguros y transparentes, se podrán crear empresas basadas en la economía colaborativa y en modelo peer to peer. También se podrán conseguir máquinas más autónomas que serán capaces de autogestionarse, estar en contacto con clientes y proveedores para la entrega de productos, controlar el almacén de materias primas o hacer pedidos y realizar pagos de manera automática, siempre y cuando se hayan pactado unas condiciones en un "Smart Contract". Por otro lado, con el uso de Blockchain, se automatizarán lo procesos productivos, pudiendo fabricar productos más personalizados a precios competitivos, minimizando costes. Además, se podrán conocer los movimientos de un producto desde que es enviado en su lugar de origen hasta que llegue al consumidor final. Por último, en el mundo financiero, facilitará los micropagos. La tecnología de bloques permitirá a las empresas realizar transacciones con monedas virtuales sin comisión alguna.

Estas trasformaciones serán un gran paso en la industria actual, ofreciendo a las empresas más control, flexibilidad y eficiencia.

3.5 POLÍTICAS DE INNOVACIÓN DE LA BLOCKCHAIN Y EVOLUCIÓN DE LAS TECNOLOGÍAS INSTITUCIONALES.

Desde la creación de las cadenas de bloques en 2008 por Nakamoto, éstas se encuentran hasta día de hoy en fase experimental de desarrollo y rodeadas de incertidumbres tecnológicas, económicas y políticas. A lo largo del siglo pasado, numerosos economistas propusieron una serie de teorías relacionadas con el cambio tecnológico, la innovación y la dinámica industrial, en las que se alude un entorno institucional estable. Sin embargo, una nueva tecnología como es la cadena de bloques, disminuye los costes de la iniciativa empresarial, por lo que impulsaría un proceso de evolución institucional. Esto daría lugar a la formación y el desarrollo de las instituciones tanto en la dirección como en la coordinación económicas.

Blockchain es una plataforma digital para monedas digitales, activos digitales, identidades digitales y los contratos inteligentes. Es un protocolo que pretende poner en marcha una economía descentralizada, por lo tanto sería una innovación a nivel financiero, en plataformas digitales o en organizaciones autónomas.

Por un lado, las plataformas digitales "tradicionales", a pesar de operar en mercados multisectoriales, son empresas institucionales y se dirigen de forma centralizada, por lo que el poder recae sobre un número de accionistas o de gerentes. Por el contrario, las cadenas de bloques son plataformas digitales en las que la dirección está distribuida o descentralizada entre un gran número de mineros. En este reparto del mandato se puede observar que la Blockchain es una plataforma institucional diferente de las tecnologías industriales. Las tecnologías industriales suelen verse reflejados sus cambios en la productividad de una empresa, mientras que en las tecnologías institucionales se ven reflejados en los costes de transacción y en la organización económica entre una red de agentes económicos. La innovación con la Blockchain está surgiendo en numerosos sectores de manera simultánea , entre ellos, las finanzas, el comercio y la logística, la sanidad y los servicios gubernamentales. Desde su aparición ha habido un gran avance en cuanto a los mecanismos de consenso y los contratos inteligentes programables.

Dado que las tecnologías institucionales son tecnologías de gobierno, es necesario que sean adoptadas por grupos, no por individuos. Los individuos elegirán este tipo de avances en función de los costes de transacción generados en el intercambio y las expectativas que tengan ambas partes. La innovación en este ámbito se encuentra en el margen de selección competitivo de los costes más bajos.

La evolución institucional se caracteriza más como un nuevo tipo de innovación que con un nuevo proceso económico evolutivo, lo que tiene implicaciones en las políticas de innovación. Novak (2019) y Berg (2019) lo describen como una "política criptoamigable", "un marco de políticas adaptable para facilitar la adopción de la política de Blockchain por los diversos interesados". Si los gobiernos adoptasen la criptografía como principio general de la política, facilitaría el proceso de evolución institucional y de competencia. El objetivo de los gobiernos es minimizar los costes de la innovación institucional estructural y coordinar los reglamentos inconexos de los dominios dentro y entre los estados nación. Las políticas públicas facilitan la inversión, la adopción y el uso de blockchain. También dan lugar a descubrimientos empresariales en instituciones por parte de proveedores y usuarios de aplicaciones y soluciones de blockchain, aumentando así las teorías de innovación que se limitan mayormente a mejora en productos y procesos.

3.5.1 La evolución de las tecnologías institucionales.

Las tecnologías institucionales son procedimientos y mecanismos que permiten el intercambio económico en sistemas de gobernanza. Entre 1973 y 1985 Williamson, economista estadounidense, estudió diversos sistemas institucionales, entre ellos, los mercados, empresas y gobiernos. El análisis de éste está ligado a la teoría de Coase (1937), economista americano. Coase subraya la capacidad del gerente en la empresa para coordinar las transacciones según los costes de transacción anteriores a la definición de los precios. Sin embargo, Williamson basa tu teoría en la superación de los costes de transacción posteriores a dichos intercambios derivados del oportunismo y tipo de producto. Argumenta que dichos costes existen porque los contratos nunca pueden ser completos ya que surgirán situaciones imprevistas que requerirán una renegociación posterior, lo cual tendrá un valor.

Las empresas pueden ayudar a disminuir estos costos jerarquizando las acciones y resolviendo las discrepancias por decreto. De una manera similar, los gobiernos proporcionan bienes públicos mediante restricciones baratas en lugar de costosas negociaciones. Williamson incluyó al estudio de las empresas, los mercados y los gobiernos, los clubes y la gestión de bienes comunes. De esta forma, con una amplia gama de sistemas de gobernanzas y uniendo las tecnologías institucionales, es posible disminuir los costes de transacción en los intercambios voluntarios.

Por lo tanto, el modelo de costes de transacción de Williamson nos permite realizar análisis comparativos. Por otro lado, los empresarios pueden innovar en sus productos y también en sus estructuras dentro de las empresas, pudiendo utilizar tecnologías institucionales. Estas nuevas configuraciones de las empresas deben probarse con el fin de solucionar problemas y mejorar la coordinación de los sistemas económicos. De forma similar y basándose en un entorno de desarrollo, Leeson y Boettke mencionan la iniciativa empresarial como un sistema para proteger los derecho de propiedad, es decir, como una manera de protección, a diferencia de la tradicional iniciativa empresarial basada en el nivel de producción. "En términos más generales, la iniciativa empresarial

institucional puede referirse a grupos de personas y entidades que, mediante la acción colectiva, tratan de transformar las instituciones." *(Aldrich, 2011)*

Respecto al avance de la sociedad a lo largo de la historia, podemos observar que las tecnologías que facilitan la gerencia de las empresas, los mercados, los gobiernos y los bienes comunes, se innovan paulatinamente en el transcurso de las décadas. Además, el progreso de las tecnologías cambia a medida que la población observa cambios tecnológicos en el mundo real. Entre otros, entre los años 1750 y 1960, se observaron las mejoras en la producción industrial, obteniendo mayor rentabilidad con menos suministros. Además, en la mitad del siglo XX, apareció el internet como una nueva plataforma para el intercambio económico en la sociedad, por lo que fue notable el progreso en la información y la comunicación.

A raíz de los cambios tecnológicos, los economistas desarrollaron distintos modelos de la evolución económica. Se saca en conclusión que se tiende a tratar las instituciones como una constante en cuanto a la modelización de la dinámica evolutiva. También tratamos así el cambio cultural, que se modifica muy a largo plazo, a diferencia de las tecnologías industriales que evolucionan de forma repentina. Sin embargo, con la llegada de las tecnologías institucionales, como es el caso de la cadena de bloques, la estabilidad de las instituciones se pone en duda. Las cadenas de bloques son tecnologías institucionales que reducen el coste de la iniciativa empresarial y provocan a las empresas competir entre ellas en cuanto a dinero y pagos, registro y transferencia de activos, contratación y otras infraestructuras económicas administrativas.

3.5.2 Modelo.

El concepto principal en los modelos neo-schumpetarios de evolución económica es que la variación, selección y replicación es una idea industrial compleja sobre el conocimiento. Dicho conocimiento se refiere generalmente a las capacidades tecnológicas de las empresas, formándose así poblaciones industriales, esto son sociedades que pretenden la máxima producción con una organización de trabajo. La evolución económica se define como la frecuencia de cambio en la población en el conocimiento. Algunos factores se mantienen constantes en esta dinámica industrial.

Uno de ellos es el entorno institucional, I , suele evolucionar pero en un periodo de tiempo más extenso. Suele atribuirse este contexto al gobierno, pero también pueden proporcionar reglas para la dirección de una empresa empresarios del sector privado. La tecnología Blockchain facilita la oferta de las instituciones económicas como una nueva clase de gobierno en el margen económico de seguimiento y costes de red. Se dice que estas tecnologías institucionales forman una población institucional, $I \in \mathbf{I}$. Existe una población institucional formada por diversos sistemas institucionales, $\mathbf{I}$, que se amplía con empresarios institucionales y las cuales actúan para mantener dichos sistemas institucionales. Se podría pensar que este proceso de evolución se caracteriza de una manera familiar.

La acción empresarial, es decir los títulos de la sociedad que representan fracciones en las que se divide su capital, sobre las tecnologías institucionales, como es el caso de la cadena de bloques, puede ampliar los sistemas institucionales. En el momento en el que la acción empresarial se refiere específicamente al diseño y la aplicación de tecnologías institucionales, dan lugar a novedosas estructuras de derechos, obligaciones y facultades

que instaura nuevos sistema de autoridad en las sociedades. Esto también podrían ser nuevas combinaciones de estructuras de capital de la economía para aprovechar nuevas oportunidades, excepto que el capital apoye más a los sistemas institucionales que a la producción industrial. A medida que se adoptan las tecnologías institucionales, se define un proceso evolutivo de variación y selección.

La economía institucional es el estudio que se centra en la comprensión del proceso evolutivo y el papel de las instituciones sociales en cuanto al comportamiento económico. El contrato es la parte fundamental de estudio en la economía institucional. Asumimos el contrato de forma simplificada, ya que el contrato formal está focalizado en la descripción de los contratos óptimos, nos centramos en el contexto institucional en el que existen.

Consideramos un contrato entre dos agentes i y j como una función $p_{ij}(x_t)$ que representa los pagos que hace i a j condicionados a una circunstancia concreta en el mundo x_t , en el tiempo t. Por lo tanto, pensamos en un sistema de gobernanza particular $I \in \mathbf{I}$, como un input que transforma ese sistema en costes de transacción $C_T(I)$ asociados al total de costes comunes de redacción, negociación, ejecución y cumplimiento de un contrato $p_{ij}(X_t)$. Para simplificar, asumiremos que los costes de transacción son constantes en todos los contratos celebrados en un sistema I. Siguiendo la teoría de Coase (1937) y Williamson (1973, 1985), decimos que las tecnologías institucionales que apoyan estos sistemas son seleccionadas según la medida en que aminoren los costes de transacción.

Ahora podemos interpretar la evolución de las tecnologías institucionales utilizando el teorema fundamental de selección de Fisher, que expone que el cambio de las características medias de la aptitud es igual a la variación de esa característica en toda la población. Como se indica en el apartado (1) del Anexo 1, basándonos en la evolución de las tecnologías institucionales, la tasa de cambio medio en los costes de transacción en el conjunto de sistemas, $E_{I \in \mathbf{I}} c_T(I)$, es igual a la negativa de la variación de dichos costes de transacción $V_{I \in \mathbf{I}}[c_t(I)]$, reconociendo que la aptitud mejora a medida que disminuyen los costes de transacción, y donde la varianza $V[\cdot]$ es definida de manera habitual, como podemos ver en el apartado (2) del Anexo 1. Dentro del apartado mencionado, distinguimos que |P(I)| es el tamaño de la plataforma en la cual el sistema I aporta el gobierno a las instituciones, definida como el conjunto de contratos P(I) que están sujetas al sistema de gobernanza institucional I, y |P(**I**)| que es el conjunto de todos los contratos en todos los sistemas $I \in \boldsymbol{I}$. Los costes medios de transacción también se definen como aparece en la formulación (3) de dicho Anexo.

Como ocurre con cualquier otro tipo de evolución, el progreso de las tecnologías institucionales dependen del tamaño de la población, aunque con un rasgo particular. En este caso, el desarrollo se produce según los cambios que haya en el conjunto de contratos P(I), para el cual el sistema institucional I habilitado por la tecnología institucional proporciona el gobierno. Los elementos de este conjunto son determinados por las decisiones de contratación que tomen los agentes i y j. A medida que contratan de un sistema u otro, ejercen una presión de selección sobre el conjunto de tecnologías institucionales.

Por otra parte, para poder firmar un contrato, es necesario que los agentes estén de acuerdo con la forma de contrato $P_{ij}(X_t)$. para que exista entre ellos. En el caso de que hubiese distintos sistemas institucionales en los que se pueda celebrar el contrato, los agentes, además de decidir la forma de contrato, también acordarán el sistema institucional de

gobierno I al cual estará sujeta su relación contractual, la cual se convierte en una secuencia de elementos $a_{k=i,j} = \{p_{ij} (x_t) I\}$. Si se lograse el convenio, ese contrato será analizado e incluido en el conjunto de contratos que estén sujetos al sistema institucional que los agentes hayan elegido, como se demuestra en la expresión (4) del Anexo.

Por lo tanto, de esta forma se puede determinar el grupo de contratos celebrados que estén sujetos al sistema institucional II en un momento dado, explicado en el apartado (5).

Como se demuestra en la formulación (6) del Anexo, la tasa de cambio de este conjunto depende la evolución de las tecnologías institucionales. En el caso de que el diferencial sea positivo, el sistema institucional *I* y la tecnología que lo respalda están siendo elegidos de manera diferencial por la evolución de las tecnologías institucionales. Por el contrario, si el diferencial es negativo, el sistema institucional y la tecnología que lo respalda está siendo rechazado. Este hecho se manifiesta a nivel poblacional a través de la ecuación de Fisher en la convergencia de los costes medios de transacción en toda la población de las tecnologías institucionales para éstas que son seleccionadas de manera diferencial.

3.5.3 Coordinación y evolución institucional.

Con la explicación anterior, se puede observar que la evolución de las tecnologías institucionales depende de la coordinación. El resultado dependerá, específicamente, tanto de las tecnologías como de los costes de coordinación de algunas configuraciones de las instituciones. Estos costes de coordinación solo van a existir cuando existan costes de transacción y existan varios sistemas institucionales en los que se ejerza presión, ya que en el modelo estándar, con un único sistema, estos costes van a ser cero. En el caso de que los agentes i y j no coordinen su elección de contrato y selección de sistema institucional, no se celebrará ningún contrato, asociada la explicación a la expresión (7) del Anexo.

Por lo tanto, a medida que se van resolviendo los problemas de coordinación, las tecnologías institucionales avanzan para particulares sistemas $I \in \mathbf{I}$ dentro de la población. Cuando los agentes i y j consiguen la coordinación de la forma de los contratos que se van a celebrar $p_{ij} (x_t)$ y el sistema institucional de gobierno *I* al que estarán sujetos esos contratos, el conjunto de los contratos celebrados sujetos a ese sistema crece , y este sistema se dice que es seleccionado diferencialmente por la evolución institucional. En el caso de que la coordinación no sea lograda por los agentes en la forma y en el sistema, el conjunto de contratos celebrados que están sujetos a ese sistema crecerá, y ese sistema no será seleccionado diferencialmente por la evolución institucional.

La evolución institucional se explica mediante la solución diferencial de los problemas de "coordinación de los puntos de Schelling" (1960). La parte *j* toma la decisión de entrar en una relación contractual en un sistema de gobierno, por lo que las partes *i* deberían de aceptar lo mismo, y viceversa. Por lo tanto, existe un efecto de prioridad en la evolución de las tecnologías de las instituciones. Un inconveniente que puede contrarrestar este efecto es el aumento de costes de transacción, siendo un problema de impulso para los empresarias institucionales ya que no se puede seleccionar una tecnología institucional si no es adoptada por otros agentes. En el mundo de las criptomonedas existe el problema de la adopción de coordinación, normalmente sin comunicación, por lo que se espera que la evolución de dichas tecnologías se adopten entre la población. Una vez que un determinado sistema institucional sea apoyado por una tecnología institucional, será más

probable que se continúe adoptando como sistema de gobierno, ya que los problemas de coordinación se resolverán de manera más sencilla.

3.5.4. Las tecnologías institucionales determinadas por los costes de transacción.

Para poder escrutar aún más la manera en la que evolucionan las tecnologías institucionales, vamos a hacer una suposición sobre cómo i y j toman decisiones sobre los contratos y los sistemas institucionales de éstos. Vamos a suponer que, a lo largo del tiempo, el comportamiento promedio de contratación se oriente hacia la maximización del valor esperado de los contratos entre i y j $p_{ij}(x_t)$. Podemos expresar de una forma muy simple este valor esperado de contratación $a_{k=i,j}= \{p_{ij}(x_t)\ I\}$. Consideramos que el contrato pij(xt) daría los beneficios esperados de $E_{xt\in xt}\pi_k\ [p_{ij}(x_t)]$, con las expectativas que hay en el mundo $x_t \in X_t$ que existen dentro del conjunto conocido de los mismos X_t. El contrato $p_{ij}(x_t)$ decimos que está asociado a los costes de transaccion c_T (I). Para sintetizar, los podemos definir como una función del sistema institucional por sí solos e incluimos el valor perdido de los beneficios esperados $E_{xt\in xt}\pi_k\ [p_{ij}(x_t)]$. El valor esperado de contratación si la coordinación no se logra es cero.

Como se observa en el enunciado (8) del Anexo 1, el valor esperado se optimiza en el comportamiento contractual $a_{k=i,j}= \{p_{ij}(x_t)\ I\}$, el cual consta de dos partes, el contrato $p_{ij}(x_t)$ escrito entre *i* y *j* y el sistema institucional al que está sujeto, *I*. La maximización del valor esperado en la forma del contrato $p_{ij}(x_t)$ escrito entre *i* y *j* se puede pensar que es una condición necesaria para la solución de los problemas de coordinación que provoca un sistema institucional II y la tecnología institucional que permite su selección. La forma de contrato $p_{ij}(x_t)$ que maximiza el valor esperado del comportamiento de contratación, formulación (8) del Anexo 1,es lo que Hart y Moore (1988) consideraron como contratación óptima. Sin embargo, solo nos interesa la forma de contratación optima ya que con el descubrimiento de la misma, en promedio y a lo largo del tiempo, para ser coordinada entre los agente i y j proporcionando la condición necesarias para resolver el problema de contratación por el cual se seleccionará una tecnología institucional por el proceso de selección.

En la elección del sistema institucional *I,* la maximización del valor esperado de cualquier contrato entre *i* y *j* podemos pensar que caracteriza una condición suficiente para la solución de los problemas de coordinación que causara un sistema institucional y la tecnología institucional que permite su selección. El sistema institucional que maximiza el valor esperado del comportamiento de contratación se define en el apartado (9).

Por lo tanto, si se lograse coordinar la forma $p^*_{ij}(x_t)$ de contrato y el sistema institucional al que estará sujeto dicho contrato que maximicen dicho valor esperado de la conducta contractual, esto es, $\{p^*_{ij}(x_t)\ I^*\} = a^*_i\ ,\ a^*_j$, el problema de coordinación seria solventado por los agentes *i* y *j* quienes, en promedio y a lo largo del tiempo convergerán en el comportamiento contractual que maximiza el valor esperado. Hay que tener en cuenta las condiciones en las que esto ocurre, ya que nos informará de la evolución de las tecnologías institucionales. Cuanto mayores sean los costes de transacción y los costes de supervisión se minimicen por cualquier sistema institucional $I \in \mathbf{I}$ entonces, mayor será el grado de coordinación que se logrará en el comportamiento de contratación. Por lo tanto, cuanto mayor sea el número de contratos que se realicen en dicho sistema

institucional, más valor económico se creará, y mayor será el grado en que ese sistema y a tecnología institucional que lo respalda serán seleccionados por el proceso de evolución.

3.5.5 Los modelos tradicionales de evolución económica como un caso especial.

Los modelos tradicionales de evolución económica de las tecnologías instituciones se consideran un caso especial con poca variedad en la población de tecnologías institucionales, por lo que la coordinación en el sistema institucional en el que se va a llevar a cabo la contratación es insignificante. Por lo tanto, en este modelo asumimos que **I** = *I*.

En este caso no es importante tener en cuenta ni la decisión de la forma del contrato $a_{k=i,j}=\{p_{ij}(x_t)\ I\}$ ni el sistema institucional al que está sujeto *I*, existe un solo sistema institucional en el que se puede atacar. Por lo tanto, consideraremos que la única decisión que hay que tomar es la forma, de modo que $a_{k=i,j} = \{p_{ij}(x_t)\ \mathrm{I}\}$. La única evolución dentro de la economía es el conjunto de contratos P(I) alcanzados dentro del sistema institucional, pudiendo ignorar dichas instituciones suprimiéndolas, como en la formulación (10) del Anexo 1.

En este caso especial, la característica a resaltar del sistema económico es que la diversidad de la tecnología institucional es cero. La evolución que aparece del conjunto de contratos proviene de la dinámica de estos contratos $\{p_{ij}(x_t)\}_{j\in N}$ en los cuales los agentes i chocan con otros miembros de la población $j \in N$, como en el apartado (11) del Anexo 1.

Esto puede representar los modelos de Metcalfe de la evolución de las tecnologías institucionales especificando el teorema fundamental de Fisher sobre las características de las tecnologías de producción utilizadas por i de las que dependen los contratos. Para ello, tendríamos que asumir que los contratos $p_{ij}(x_t)$ son simples intercambios y que los agentes *i* deben coordinarse en cualquier decisión de *j* sobre la forma de los contratos. La tendencia promedio es que el comportamiento contractual de la parte *j* converja hacia la maximización del valor esperado de los contratos $p_{ij}(x_t)$ entre *i* y *j*. Se podría observar esta evolución en la mejora de las características y los precios de los productos a través de la innovación de los procesos y productos.

3.5.6 La criptografía de la cadena de bloques como política de innovación.

El modelo descrito en el apartado anterior explica la ampliación de posibilidades de coordinación de contratos en la economía eliminando costes de transacción. Ajustando los costes de supervisión y confirmación, y facilitando la descentralización de la red en los intercambios económicos, se puede confirmar que la Blockchain es un tipo de tecnología institucional para la contratación de los términos y condiciones de las ganancias por ambas partes. La Blockchain se da uso tanto en el ámbito privado como en el público, es decir, son suministradas tanto por empresarios privados como por el gobierno. Este último es un método fundamental para facilitar el desarrollo de la cadena de bloques como tecnología institucional para la coordinación económica a gran escala.

Es necesario que el entorno sea el adecuado para la evolución de las tecnologías institucionales. Debe entenderse como política de innovación.

En los últimos años, el progreso y alcance de las actividades relacionadas con la cadena de bloques, ha sido el centro de atención en muchas ocasiones de los responsables de la formulación de políticas, lo que ha llevado a respuestas fiscales, legislativas y regulatorias. El apoyo ha sido motivado principalmente por querer informatizar los libros mayores y asegurar la eficiencia de la administración pública y la prestación de servicios sociales, así como para alcanzar objetivos económicos más amplios. En cuanto a las diferentes respuestas obtenidas en cuanto a la tecnología blockchain, se distinguen grados de adaptación a la tecnología de los libros mayores distribuidos. Este fenómeno se denomina "cripto-amigable", cuanto más "cripto-amigable" sea el entorno político, más fácil será la adopción y el uso por múltiples usuarios.

A pesar de los diferentes pensamientos políticos, el desarrollo en Blockchain por parte de la política se fomenta con el fin de introducirlo en la práctica y regulación fiscal existente. Además, se esfuerza por adaptarse a esta nueva tecnología con el fin de minimizar los costes estructurales planteados por esta tecnología o para mantener la capacidad de generación de renta a través de los libros contables intermedios. El acercamiento a este proyecto por parte de la política existente es porque "trata de intervenir en el nivel operativo de los precios, las cantidades o las estructuras de los flujos de ingresos" (Dopfer y Potts, 2008, pág. 94).

Se observa que las políticas públicas influyen y son influenciadas por los costes de transacción y la manera en la que aparecen. Oliver Williamson indica que en entornos económicos con coherencia limitada y la especificidad de los activos, cuando los agentes incurren en costes de transacción en el proceso de intercambio, las políticas públicas pueden tener influencia en el estímulo de contratar. La cadena de bloques favorece la innovación institucional al potenciar la reducción de estos costes, y simplifica los procesos de coordinación en el cambio de valor económico entre agentes heterogéneos. La innovación institucional consiste en la inserción de novedades en los gobiernos para el intercambio económico, y en este caso, la innovación se representa como la reducción de los costes de transacción. Por lo tanto, la política pública criptográfica puede considerarse como tal, impulsando a remodelar el gobierno y la coordinación de las relaciones de intercambio y las instituciones que realizan esa actividad.

Las políticas que apoyan la adopción y el uso de la tecnología blockchain también ponen a prueba la coordinación institucional mediante aplicaciones de blockchain, y promueve la creación de competencias en programadores, inversores y usuarios. Además, respecto a la innovación tecnológica dentro de las plataformas digitales, las políticas "cripto-amigables" pueden ayer a comprender los movimientos externos e internos del desarrollo institucional y los usuarios que operan en plataformas blockchain.

Por otro lado, entendiendo esta nueva tecnología como una nueva alternativa de la política de innovación en la política, conduce a reconsiderar las medidas económicas utilizando tecnología de cadena de bloques en los libros de contabilidad. En muchos países se observa que las nuevas leyes para la adopción y uso de blockchain se llevan a cabo de forma aislada y no global, pero los legisladores estudian los desajustes políticos para mejorar las capacidades de coordinación y gobierno de blockchain como tecnología institucional. Las posturas políticas es probable que faciliten la introducción de la cadena de bloques en la economía para aumentar las posibilidades de coordinación entre todos los centros de dirección. Es decir, se espera que los legisladores no solo ofrezcan

oportunidades de utilizar blockchain a programadores, inversores y usuarios de la cadena de bloques de participar en las preferencias del entorno de las políticas "cripto-amigables", sino que se provea el aprendizaje de reglas respecto a la integridad y el rendimiento institucional.

4. CONCLUSIONES.

Las criptomonedas, y en especial el "Bitcoin", han causado una gran revolución en la economía desde sus comienzos en el año 2009. Forman una nueva forma de entender y de dar uso al dinero de forma digital. La sociedad lo asocia a una simple forma de pago, pero, sin embargo, las monedas virtuales tienen unas características que van más allá. Uno de los aspectos más relevantes y al cual no se le da mucha importancia es la descentralización del dinero o la tecnología de bloques (Blockchain) que les da soporte.

Haciendo mayor hincapié ahora en esta tecnología, a lo largo de todos estos años, se ha podido observar como Blockchain ha ido aumentando sus aplicaciones. En sus inicios, se esperaba que únicamente hiciese la función de sustento para la emisión de criptomonedas. Pero en la actualidad podemos observar como grandes empresas e instituciones financieras a nivel mundial investigan cómo poder implicar esta tecnología en numerosos proyectos y en acuerdos entre agentes de cualquier parte. Una cosa hay que tener clara respecto a Blockchain: En el futuro será adoptadas por instituciones tanto públicas como privadas.

En relación a las criptomonedas, existen muchos tipos de ellas. Pero el más conocido, ya sea por el uso o por el volumen de negociación que acumula, es el Bitcoin. En la actualidad, y con la época de pandemia que estamos viviendo, esta moneda digital ha sufrido grandes fluctuaciones, ya que para algunos agentes generaba confianza invertir en él y para otros no tanto. Esto se debe a que, cuando se invierte en ello, se hace con el propósito de que el futuro de ésta sea bueno y se generen beneficios. Normalmente, las criptomonedas se utilizan para especular, aunque hay otras que se han creado exclusivamente para realizar pagos. Existen numerosas diferencias entre todas las criptodivisas que existen en el mercado.

Los mayores problemas a los que se encaran son la incertidumbre y la intangibilidad. En primer lugar, en el momento en el que comienzan a cotizar, las criptomonedas adquieren una gran volatilidad que no transmite al usuario la suficiente confianza, en algunos casos, para dar el paso a invertir en ellas. Por otro lado, aunque las criptomonedas puedan almacenarse en monederos virtuales, sigue siendo dinero electrónico. Esto significa que no es tangible y genera cierta indecisión entre la población. La solución a ambos problemas es la normalización y adaptación de la sociedad a este nuevo método de pago, dejando de lado la especulación.

En la actualidad cabe destacar la inquietud que genera la idea de creación de una moneda digital por parte de los bancos centrales, ya que se cree que podría afectar a las criptomonedas ya existentes.

En conclusión, es incierto tanto el futuro de las criptodivisas como de la Blockchain o tecnología de bloques. Pero al menos, a corto plazo, se espera que las empresas, instituciones financieras e incluso los bancos centrales sigan volcándose en este proyecto e introduciendo las nuevas tecnologías en el día a día, y tratando de conseguir la regulación de todas las monedas virtuales por el gobierno. A pesar de todo, y de manera indiscutible, ambos conceptos han transformado y evolucionado el sistema monetario.

5. BIBLIOGRAFÍA.

- **Alonso Hernández, Carlos (2019):** "Blockchain y criptomonedas". Disponible en: https://uvadoc.uva.es/bitstream/handle/10324/37430/TFG-J-%2023.pdf?sequence=1 (Consultado en febrero de 2021)

- **El Aboussi Martínez, Ismael (Trabajo Fin de Grado defendido en la Universidad de Oviedo, 2018) :** "Blockchain y criptomonedas".

- **Guerrina Criado, Maria Luz (Trabajo Fin de Grado defendido en la Universidad de Oviedo, 2019):** "The impact of the Bitcoin revolution".

- **Gutiérrez Hernández, Pedro (2015):** "El Bitcoin, ¿Presente y futuro del dinero?". Disponible en: https://repositorio.comillas.edu/jspui/bitstream/11531/4523/1/TFG001313.pd (Consultado en enero de 2021)

- **Nakamoto, Satoshi (2008):** "Bitcoin: a Peer-to-Peer Electronic Cash System". Disponible en: https://bitcoin.org/bitcoin.pdf (Consultado en febrero de 2021)

- **Puyod Pardos, Sergio (2020):** "El uso en el mercado económico de los sistemas de criptodivisas". Disponible en: https://zaguan.unizar.es/record/90092/files/TAZ-TFG-2020-291.pdf (Consultado en enero de 2021)

REFERENCIAS BIBLIOGRÁFICAS:

- **Boar, Andrei (2018):** "Descubriendo el Bitcoin: Cómo funciona, como comprar, invertir, desinvertir…" (Consultado en marzo de 2020).

- **Darcy Allen, Chris Berg, Brendan Markey-Towler, Mikayla Novak and Jason Potts (24 de septiembre de 2019):** "Blockchain and the evolution of institutional technologies: Implications for innovation policy." Disponible en: Blockchain and the Evolution of Institutional Technologies: Implications for Innovation Policy by Darcy W E Allen, Chris Berg, Brendan Markey-Towler, Mikayla Novak, Jason Potts :: SSRN (Consultado en enero de 2021).

- **Preukschat, Alex (2017):** "Blockchain: La revolución industrial de internet". (Consultado en marzo de 2020).

- **Tapscott D. , Tapscott A. (2017):** "La revolución blockchain: Descubre cómo esta nueva tecnología transformará la economía global". (Consultado en marzo de 2020).

PÁGINAS WEB CONSULTADAS:

- **Admiral Markerts (11 de febrero de 2021):** "¿Qué es el Bitcoin? Estrategias de Trading BTC" Disponible en: ¿Qué es el Bitcoin? ¿Cómo invertir en BTC? -> CFD Bitcoin - Admirals (admiralmarkets.com) (Consultado el 01 de marzo de 2021)

- **Banco Central Europeo (13 de febrero de 2018):** "¿Qué es el Bitcoin?" Disponible en: ¿Qué es el bitcóin? (europa.eu) (Consultado el 25 de julio de 2020).

- **Bancos de Pagos Internacionales (2018): "Monedas digitales emitidas por bancos centrales"**. Disponible en: https://www.bis.org/cpmi/publ/d174_es.pdf (Consultado el día 09 de junio de 2021)

- **BBC news, Cristina Pintado (11 de enero de 2021): Bitcoin: ¿a qué se debe la espectacular revalorización de la criptomoneda, que llegó a superar los US$40.000?":** Disponible en: https://www.bbc.com/mundo/noticias-55618604 (Consultado el 05 de junio de 2021).

- **Beincrypto, David Borman (30 de abril de 2020):** "Las criptomonedas más afectadas durante la crisis del coronavirus." Disponible en: Las criptomonedas más afectadas durante la crisis del coronavirus - BeInCrypto (Consultado el 05 de mayo de 2020).

- **Biblioteca del Congreso Nacional de Chile, Fabiola Cabrera Valencia (09 de mayo de 2018):** "Tecnología Blockchain: elementos básicos, aplicaciones y marcos regulatorio." Disponible en: Microsoft Word - Bolckchain_conceptos_impacto_en_industrias_y_marcos_regulatorios Final SUP.docx (bcn.cl) (Consultado el 01 de junio de 2020).

- **Bitcobie, Jose Maldonado (10 de junio 2019):** "Industria 4.0: la blockchain transformando espacios industriales". Disponible en: Industria 4.0: la blockchain transformando espacios industriales - bitcobie (Consultado el 08 de junio de 2020).

- **Bitsofproof:** "¿Qué es la tecnología Blockchain?". Disponible en: ¿Qué es la tecnología Blockchain? Una guía para entender cómo funciona (bitsofproof.com) (Consultado el 01 de junio de 2020).

- **Blockchainservices, Mar Calvo (28 de julio de 2018):** "Conoce los diferentes tipos de blockchain.". Disponible en: Conoce los diferentes tipos de blockchain – BLOCKCHAIN SERVICES (Consultado el 03 de junio de 2020)

- **Bit2me Academy:** "¿Cuántos tipos de blockchain hay? Disponible en: Cuántos tipos de blockchain hay | Bit2Me Academy (Consultado el 06 de junio de 2020)

- **Bit2me Academy:** "¿Qué es Libra? Facebook tiene ¿criptomoneda?" Disponible en: ¿Qué es Libra? Facebook tiene ¿criptomoneda? | Bit2Me Academy (Consultado el 15 de diciembre de 2020)

- **Broker Online, Melodía (12 de mayo de 2021): "Las 10 mejores criptomonedas".**Disponible en: https://www.brokeronline.es/criptomonedas/ranking/ (Consultado el 07 de junio de 2021).

- **CaixaBank Research, Antonio Escoda (11 de marzo de 2014): "Bitcoin: ¿burbuja especulativa o moneda del futuro?"** Disponible en: https://www.caixabankresearch.com/es/economia-y-mercados/mercados-financieros/bitcoin-burbuja-especulativa-o-moneda-del-futuro (Consultado el 19 de mayo de 2020)

- **CEMLA, Morten Bech, Rodney Garratt (Octubre de 2017): "CRIPTOMONEDAS DE BANCOS CENTRALES".** Disponible en: https://www.cemla.org/PDF/boletin/PUB_BOL_LXIV-01-03.pdf (Consultado el 09 de junio de 2021)

- **Economipedia, Iris Barceló Ferre (25 de septiembre de 2017**): "Criptomoneda". Disponible en: Criptomoneda - Qué es, definición y concepto | 2021 | Economipedia (Consultado el 20 de julio de 2020)

- **El Confidencial (13 de junio de 2019):** "Llega la moneda de Facebook que aspira a cambiarlo todo: ¿cómo funcionará?" Disponible en: Llega la moneda de Facebook que aspira a cambiarlo todo: ¿Cómo funcionará? (elconfidencial.com) (Consultado el 02 de marzo de 2021)

- **El Periódico (24 de marzo de 2020) :** "Bitcoin en época de coronavirus: del desplome al imprevisible 'halving'". Disponible en: Bitcoin en época de coronavirus: del desplome al imprevisible 'halving (elperiodico.com) (Consultado el 01 de mayo de 2020).

- **European Central Bank:** "Virtual currency schemes: a further analysis". Disponible en: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (Consultado el 20 de mayo de 2021)

- **Finanzas.com (30 de octubre de 2019):** "¿Qué está pasando con la criptomoneda LIBRA de Facebook?" Disponible en: ¿Qué está pasando con la criptomoneda LIBRA de Facebook? (finanzas.com) (Consultado el 02 de marzo de 2021).

- **Finanzas.com (03 de mayo de 2021):** "Criptomonedas. Hay espacio para otro ganador además del Bitcoin". Disponible en: Mercado de divisas: Cotizaciones divisas en tiempo real » finanzas.com (Consultado el 03 de mayo de 2020).

- **Finanzas para todos:** "Bitcoin: origen, funcionalidades y riesgos de la moneda virtual". Disponible en: Bitcoin: origen, funcionalidades y riesgos de la moneda virtual (finanzasparatodos.es) (Consultado el 21 de julio de 2020)

- **Funds People, Juan Pedro Asencio Flores (22 de abril de 2021): "El atractivo del bitcoin para los inversores institucionales".** Disponible en: https://fundspeople.com/es/opinion/el-atractivo-del-bitcoin-para-los-inversores-institucionales/ (Consultado el 26 de mayo de 2021).

- **Hablemos de Empresas, Juan F. Samaniego (19 de septiembre de 2018):** "Blockchain, la tecnología imprescindible en el avance de la Industria 4.0." Disponible en: "Blockchain, la tecnología imprescindible en el avance de la Industria 4.0." Disponible en: La tecnología blockchain en la industria 4.0: casos y aplicaciones (hablemosdeempresas.com) (Consultado el 08 de junio de 2020)

- **IEBSschool, Javier Sáez Hurtado (24 de mayo de 2021): "Las criptodivisas (o criptomonedas) con más futuro).** Disponible en: https://www.iebschool.com/blog/criptodivisas-criptomonedas-invertir-finanzas/ (Consultado el 08 de junio de 2021)

- **Real Instituto elcano, Javier Alonso Lecuit (12 de noviembre de 2019) :** "**La seguridad y la privacidad del blockchain, más allá de la tecnología y las criptomonedas."** Disponible en: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciberseguridad/ari106-2019-alonsolecuit-seguridad-y-privacidad-del-blockchain-mas-alla-de-tecnologia-y-criptomoneda (Consultado el 22 de mayo de 2021).

- **The balance, Eric Rosenberg (30 de marzo de 2021**): "History of Cryptocurrency." Disponible en https://www.thebalance.com/history-of-cryptocurrency-5119511

- **Theeconomyjournal.com , Fernando Anaya:** "La seguridad del Bitcoin". Disponible en: La seguridad del Bitcoin (theeconomyjournal.com) (Consultado el 27 de julio de 2020).

- **Trading y bolsa para torpes, Adrián Viteri (30 de noviembre de 2020): "Libra de Facebook en 2020. "¿Qué pasará con esta criptomoneda?"** Disponible en: https://www.tradingybolsaparatorpes.com/blog/vera-la-luz-libra-criptomoneda-facebook (Consultado el 09 de junio de 2021)

- **TreceBits, Juan Carlos Rubio (01 de abril de 2020):** "Cómo ha afectado al Bitcoin la crisis del coronavirus" Disponible en: Cómo ha afectado al Bitcoin la crisis del coronavirus (trecebits.com) (Consultado el 04 de mayo de 2020)

- **Welivesecurity, Cecilia Pastorino (2018):** "Blockchain: qué es, cómo funciona y cómo se está usando en el mercado". Disponible en: Blockchain: qué es, cómo funciona y cómo se está usando en el mercado | WeLiveSecurity . (Consultado el 15 de mayo de 2020).

- **Xataka, Javier Pastor (Septiembre, 2018):** "Qué es blockchain: la explicación definitiva para la tecnología más de moda." Disponible en: Qué es blockchain: la explicación definitiva para la tecnología más de moda (xataka.com) (Consultado el 18 de mayo de 2020).

- **Xataka, Cristian Rus (16 de abril de 2020):** "Libra, la criptomoneda respaldada por Facebook, se reestructura por completo y será más similar a PayPal que a Bitcoin". Disponible en: Libra, la criptomoneda respaldada por Facebook, se reestructura por completo y será más similar a PayPal que a Bitcoin (xataka.com) (Consultado el 02 de marzo de 2021)

6. ANEXO 1

(1) $-\frac{\partial}{\partial t}\, E_{I\in I} c_T(I) = V_{I\in I}[c_T(I)]$

(2) $V_{I\in I}\,[c_T(I)] = \sum_{I\in I} \frac{|P(I)|}{|P(I)|}[C_T(I) - E_{I\in I} c_T(I)]^2$

(3) $-\frac{\partial}{\partial \mathrm{t}} \mathrm{E}_{\mathrm{I}\in\mathrm{I}} \mathrm{c}_{\mathrm{T}}(\mathrm{I}) = \mathrm{V}_{\mathrm{I}\in\mathrm{I}}[\mathrm{c}_{\mathrm{T}}(\mathrm{I})]$

(4) $p_{ij}(x_t) \in P(I) \;\leftrightarrow\; a_i^* = a_j^* \,\&\, I \in a_i^*, a_j^*$

(5) $P(I) = \{p_{ij}(x_t) \colon a_i^* = a_j^* \,\&\, I \in a_i^*, a_j^*\}$

(6) $\frac{\partial |P(I)|}{\partial t} = \frac{\partial}{\partial t} |\{p_{ij}(x_t) \colon a_i^* = a_j^* \,\&\, I \in a_i^*, a_j^*\}|$

(7) $a_i^* \neq a_j^* \rightarrow p_{ij}(x_t) \notin P(I)$

(8) $E_{x_t \in X_t} V_{k=i,j}[p_{ij}(x_t)\, I] = E_{x_t \in X_t} \pi_k[p_{ij}(x_t)] - C_T(I)$

(9) $I^* = I \colon c_T(I') \geq c_T(I) \forall I' \in I$

(10) $P = \{p_{ij}(x_t) \colon a_i^* = a_j^*\}$

(11) $\frac{\partial}{\partial t} \left| \{p_{ij}(x_t)\}_{j\in N} \right|$

7. ANEXO 2.

TABLA COMPARATIVA DE TRABAJOS FIN DE GRADO DE AÑOS ANTERIORES.

	AÑO PRESENTACIÓN	TEMA
"El Bitcoin, ¿Presente y futuro del dinero?" **Gutiérrez Hernández, Pedro**	2015	Estudio sobre si el Bitcoin se puede considerar dinero y la regulación de éste.
"The impact of the Bitcoin revolution" **Maria Luz Guerrina Criado**	2019	Estudio de la evolución económica del Bitoin, la relevancia en la sociedad y el papel de las autoridades.
"Blockchain y criptomonedas". **Ismael El Aboussi Martínez**	2018	Estudio de las características de Blockchain y de Bitcoin como método de pago.
"El uso en el mercado económico de los sistemas de criptodivisas". **Sergio Puyod Pardos**	2020	Evolución de las criptomonedas desde 2016, y la previsión del futuro.
"Blockchain y criptomonedas". **Carlos Alonso Hernández**	2019	Rasgos generales de criptomonedas y seguridad de Blockchain.