ANEXO I

MODELO DE PORTADA

TRABAJO FIN DE GRADO

GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

CURSO ACADÉMICO …2023/2024

CONVOCATORIA …Tercera

RETOS Y OPORTUNIDADES DE LA IMPLEMENTACIÓN DE LA "*BLOCKCHAIN*" EN EL SECTOR FINANCIERO.

AUTOR: Maseda Bustillo, Julio

DNI: 50635584A

En Madrid, a 30 de mayo de 2024

ÍNDICE

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

(I) INTRODUCCIÓN.

1.1 Planteamiento del problema.

El sector financiero actual se enfrenta a diversos desafíos que impactan negativamente en la experiencia de los usuarios y la eficiencia del sistema. Estos obstáculos que durante años se han considerado perpetuos en el mundo financiero que se conoce, desde hace no mucho y cada vez con más fuerza, ven amenazada su existencia debido a nuevas tecnologías emergentes que prometen minimizarlos e incluso hacerlos desaparecer en muchos casos. Los principales desafíos históricamente perennes a los que esta tecnología se enfrenta serían los siguientes:

Ineficiencia en las transferencias: Las ratios de error, ya sea en referencia al importe, destinatario, emisor, o motivación de estas, en las transferencias bancarias nacionales rondan el 0,05%, es decir, una de cada dos mil. En las internacionales esa ratio crece considerablemente, incluso duplicándose, siendo la ratio del 0,1%, o lo que es igual, una de cada mil. (Asociación Española de Banca, s. f.) lo que representa un volumen considerable de transacciones fallidas o con errores teniendo en cuenta que se realizan anualmente unos 10.900 millones de transferencias solo en España, dejando unos 30 millones de transferencias diarias, de las que unas 15.000 contarán con algún error, que le supondrá un gasto extra de recursos y tiempo a entidad bancaria y usuario. (Asociación Española de Banca, 2024).

Brechas de seguridad: Las constantes vulnerabilidades en los sistemas bancarios tradicionales, como las copias de tarjetas o la domiciliación de cargos usando IBAN copiados, generan desconfianza e inseguridad en los usuarios. Estas amenazas se cuentan ya por miles, aumentando año a año, siendo el último reporte de 10.361 operaciones solo en España, en el año 2022, significando un 30,3% de las reclamaciones y suponiendo que los bancos españoles hayan tenido que devolver más de 6 millones de €, la cifra más alta de la historia. (Gutiérrez et al., 2023)

Tardanza en las transacciones: Las transferencias internacionales, especialmente entre diferentes zonas horarias, pueden tardar varios días en completarse. Mientras que las nacionales, si no se desea pagar una comisión de inmediatez, tarda un mínimo de un día hábil, siendo nulos los fines de semana. Suponiendo una espera de casi tres días si la transferencia se realiza un viernes.

Altas comisiones por la inmediatez: La rapidez en las transacciones suele implicar comisiones adicionales elevadas para los usuarios. Rondando los 10€ la comisión mínima. Si las cantidades fuesen elevadas esa comisión aumentaría de manera directamente proporcional. La alternativa del “Bizum” ha sido recientemente limitada en cuanto al número de veces que se puede utilizar mensualmente y en cuanto a las cantidades tanto máximas como mínimas. Las cifras como receptor serían un máximo de 60 operaciones de recepción de efectivo al mes, nunca superando los 2.000€ diarios recibidos. Mientras, como emisor el número de bizums es ilimitado, siendo la cantidad enviada la que sufre limitaciones, siendo el máximo de 2.000€ diarios y 5.000€ mensuales. El importe mínimo por transferir o recibir está limitado a 50 cts. (BIZUM, 2024).

Falta de transparencia internacional: La opacidad en las operaciones y procesos de las transacciones internacionales, especialmente por los acuerdos entre países, dificulta la comprensión y el control por parte de los usuarios. Esto provoca la aparición de intermediarios

como son las empresas “remesadoras”, que ofrecen el envío seguro y rápido de su efectivo al extranjero, a cambio de elevadas comisiones. Este servicio es comúnmente usado por inmigrantes que envían dinero a sus países de origen. Esta contingencia internacional provoca una disminución del poder adquisitivo del emisor de efectivo ya que no solo tiene que someterse al tipo de cambio de su divisa, sino que deberá pagar una comisión aun mayor que la que pagaría a su banco para hacer llegar su dinero de manera rápida y segura. Estas comisiones de media son del 10,5% (Público, 2023)

Falsificación de efectivo necesario para micro pagos. Estos dos problemas se han agrupado ya que su resolución va de la mano. El tejido empresarial español está en un 99,8% compuesto por PYMES en cuanto a número y conforman el 62% del Valor Añadido Bruto (VAB) del país. (Ministerio de Industria, 2023). Las operaciones de estas empresas en muchas ocasiones son consideradas como “micro pagos”, estas operaciones si se realizasen mediante pago con tarjeta bancaria, las comisiones o tarifas por servicio harían desaparecer el beneficio que generan, obligando a pagar en efectivo o a perder un posible cliente. El efectivo es falsificable, lo que supone un riesgo adicional al pequeño comercio. El porcentaje de billetes falsos es muy reducido, suponiendo un 0,00017% en comparación de los legítimos (Banco de España, 2022) pero es otro de esos desafíos que asumimos como perpetuos en la economía.

1.2 Justificación y Objetivos.

El sector financiero, casi como el resto de los grandes sectores que mueven el mundo, atraviesa una etapa de transformación crucial impulsada por el avance tecnológico y las nuevas demandas de los usuarios. Ante este panorama, la tecnología *blockchain* surge como una herramienta disruptiva con el potencial de revolucionar el funcionamiento de las finanzas.

Los desafíos del sistema financiero tradicional son evidentes: ineficiencia en las transferencias, vulnerabilidades de seguridad, lentitud en las transacciones internacionales, comisiones elevadas y falta de transparencia. Estas problemáticas ya explicadas anteriormente generan insatisfacción en los usuarios y limitan el desarrollo del sector.

La tecnología *blockchain* ofrece una solución innovadora a estos desafíos. Su naturaleza descentralizada, inmutable, transparente y segura permite agilizar y reducir el costo de las transacciones, mejorar la seguridad y confianza en el sistema financiero, promover la transparencia y trazabilidad de las operaciones, y desarrollar nuevos modelos de negocio y productos financieros.

Sin embargo, la implementación de la *blockchain* en el sector financiero no está exenta de retos. La ausencia de regulaciones claras, la necesidad de interoperabilidad entre diferentes redes y la resistencia al cambio por parte de las instituciones tradicionales, debido en gran parte al desconocimiento de esta, son algunos de los obstáculos que deben superarse.

Este TFG se propone analizar en profundidad las oportunidades y los retos que presenta la implementación de la *blockchain* en el sector financiero. A través de una revisión exhaustiva de la literatura y el análisis de casos de estudio, se busca evaluar el impacto potencial de la tecnología en el sector, identificar a los principales actores y proyectos en desarrollo, explorar las barreras para su adopción y proponer soluciones, y desarrollar una visión estratégica para su implementación exitosa.

El segundo gran objetivo de este trabajo será darle forma real a la tecnología *blockchain*, de manera que la población ajena pero interesada en conocer acerca de esta tecnología, cuente con una fuente lo más objetiva posible sobre ella. Esto es necesario debido a que los más escuchados informadores de la actualidad, en la mayoría de las ocasiones están ciertamente sesgados por sus intereses o pasiones personales. Siendo una tecnología estrictamente ligada a otra de las tecnologías emergentes como son las criptomonedas, esto genera en muchas ocasiones, conflictos de interés entre los divulgadores principales del tema.

Esta investigación tiene un gran potencial para contribuir al avance del conocimiento sobre la tecnología *blockchain* y su aplicación en las finanzas. Los resultados del estudio podrán ser utilizados por diversos actores, como instituciones financieras, reguladores, empresas tecnológicas, divulgadores y el público en general, para tomar decisiones informadas sobre la adopción de esta tecnología disruptiva.

En conclusión, la presente investigación se justifica por la importancia de comprender el papel que puede jugar la cadena de bloques en la transformación del sector financiero. Abordar este tema de manera rigurosa y exhaustiva permitirá aprovechar las oportunidades que ofrece esta tecnología para construir un sistema financiero más eficiente, seguro, transparente e inclusivo.

1.3 Metodología.

Para comprender las oportunidades y retos de la *blockchain* en las finanzas, este TFG utilizará una metodología de investigación que combina diversas técnicas:

Se analizará críticamente la literatura académica y científica sobre este sistema, sus aplicaciones financieras, y los desafíos y oportunidades asociados a su implementación. Las fuentes principales serán bases de datos, revistas especializadas, y publicaciones de organismos internacionales.

Se seleccionarán empresas e instituciones financieras que ya utilizan esta tecnología, analizando en profundidad sus experiencias para identificar mejores prácticas, desafíos y lecciones aprendidas. La información se obtendrá de sitios web oficiales, artículos de prensa e informes.

Se compararán los sistemas financieros tradicionales con los basados en esta nueva tecnología, evaluando sus ventajas y desventajas en eficiencia, seguridad, transparencia, costos y accesibilidad. Se utilizarán indicadores como velocidad de transacciones, comisiones, seguridad de datos, transparencia operativa, costos de implementación y adopción por parte de los usuarios.

Se sintetizará la información recopilada a través de las diferentes metodologías para elaborar conclusiones sobre las oportunidades y retos de la *blockchain* en las finanzas. Se propondrán recomendaciones para su adopción exitosa, teniendo en cuenta las necesidades de los usuarios, las regulaciones existentes y las mejores prácticas de la industria.

Esta metodología permitirá obtener una visión completa y profunda del tema. La combinación de técnicas contribuirá a la creación de sinergias entre los puntos tratados y aumentará la confiabilidad de los resultados. Las limitaciones de tiempo y recursos se tendrán en cuenta, ajustando la metodología si es necesario para garantizar la viabilidad del estudio.

(II) MARCO TEÓRICO.

2.1 Historia y definición de la *Blockchain*.

2.1.1 Historia.

La tecnología *blockchain*, también conocida como "cadena de bloques", ha experimentado un auge considerable en la última década. Su potencial para revolucionar diversos sectores ha generado un gran interés tanto en el ámbito académico como en el empresarial. Sin embargo, la historia de esta tecnología se remonta a varias décadas atrás, con una serie de investigaciones y desarrollos que sentaron las bases para su eventual creación.

Aunque el término "*blockchain*" no se acuñó hasta 2008, los conceptos y tecnologías que la sustentan vieron la luz por primera vez durante la década de 1990, de la mano de Stuart Haber y W. Scott Stornetta. (Haber & Stornetta, 1991)

Proponen un sistema de "cadena de tiempo" para garantizar la integridad de documentos digitales. Lo más destacable de este trabajo es la idea de una estructura de datos en la que los registros se enlazan secuencialmente, imposibilitando la modificación de estos datos, aparece la inmutabilidad, un elemento fundamental de la *blockchain* actual.

En 1995, David Chaum desarrolla "*DigiCash*", un sistema de efectivo electrónico anónimo basado en criptografía. Este proyecto pionero descrito en el año 1989, explora la descentralización y la seguridad en las transacciones digitales, otros dos conceptos clave para la red que conocemos hoy. (Chaum, 1989)

Nick Szabo, en 1996, introduce el concepto de "contratos inteligentes" o "*smart contracts*", como se conocen popularmente en la actualidad. Estos son programas informáticos que automatizan la ejecución de acuerdos contractuales, evitando el incumplimiento. Esta idea se integraría a la tecnología *blockchain* de la mano de Vitalik Buterin en una de las blockchains más populares, Ethereum. (Szabo, 1996)

Ya en 2008, Satoshi Nakamoto publica un artículo que describe el funcionamiento de Bitcoin, la primera criptomoneda basada en la tecnología *blockchain*, que se define como un gran libro contable digitalizado e infinito en directo, en el que sus anotaciones contables están correlacionadas. Esas anotaciones se agrupan en lo que se conoce como "bloques".

Este evento marca un punto de inflexión en la historia de la *blockchain*, impulsando su desarrollo y adopción a gran escala.

En 2011 se lanza la red Bitcoin, iniciando la era de las criptomonedas y la aplicación de la *blockchain* en el ámbito financiero. Posteriormente aparecerían nuevas redes que añadirían nuevas aplicaciones y mejorarían el funcionamiento de las existentes.

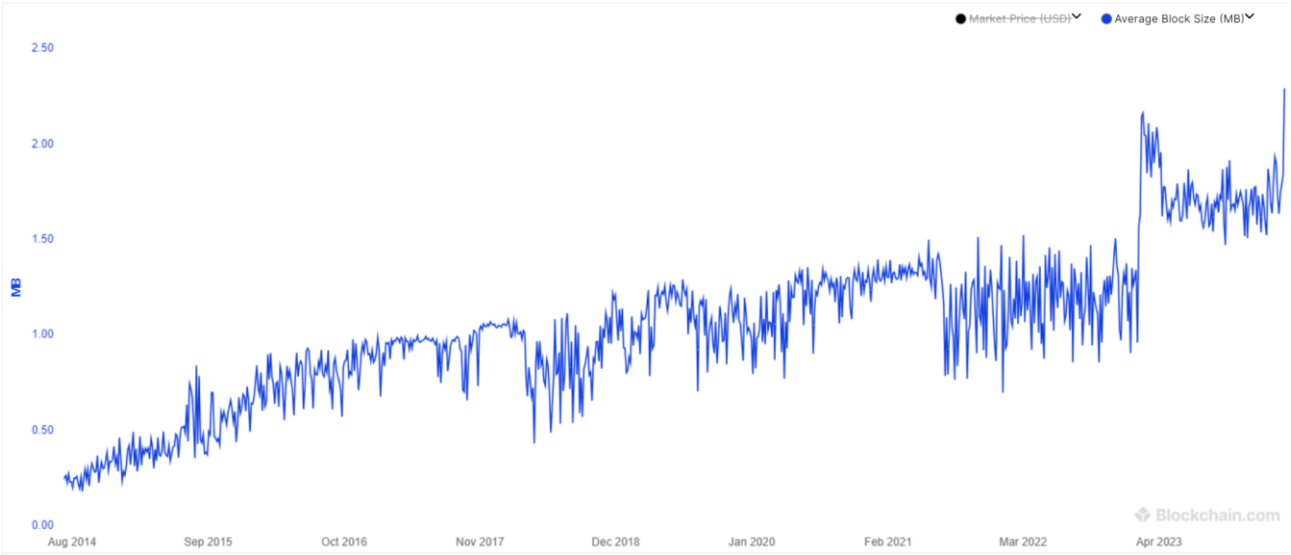
Dependiendo de la red y del momento esos bloques tendrán un tamaño u otro. En la red de Bitcoin, el tamaño varía entre los 0,7MB y los 2,5MB en la actualidad. Lo que varía algo menos es la frecuencia de bloques, ya que se terminan de rellenar para insertar su información en el siguiente, dándolo por finalizado y comenzando el siguiente, en aproximadamente 10 minutos.

En 2017 el tamaño del documento completo de la cadena de bloques de la *blockchain* de Bitcoin, que contiene todas las transacciones que se han llevado a cabo, alcanzó los 100 GB.

En enero de 2018 había crecido hasta los casi 150 GB, dos años después el tamaño rondaba los 250 GB y en enero de 2024, tras unos años de crisis, inflación y una caída de más del 70% del mercado de las criptomonedas, principal sustento del sistema, además de un notable pesimismo con respecto a estas tecnologías, en los que se podría esperar un parón en el crecimiento. La cifra alcanzada supera los 500GB de información almacenada (*Blockchain*.info, 2024).

La información almacenada en un bloque depende de la cantidad de transacciones diarias que se realicen, por lo que el tamaño de los bloques es un indicador que nos permite apreciar al ritmo al que progresa la adopción de esta tecnología y nos permite saber en qué estado de madurez está. Como vemos en el gráfico la adopción crece de manera sostenible.

Ilustración 1: Evolución del tamaño de bloque



Fuente: (*Blockchain*.info, 2024)

Desde el lanzamiento de la red Bitcoin, considerada la madre de las blockchains se han creado nuevas redes con nuevas funcionalidades, además de mejorar las existentes en la red principal. Las más importantes serían la creación de Smart contracts, las distintas formas de validar esa información registrada, cada vez más eficientes como la prueba de participación (Proof of stake, PoS), y la escalabilidad de las redes, creando nuevos algoritmos que hagan más eficiente el registro de información sin comprometer la seguridad de la red.

La historia de la cadena de bloques queda completamente abierta a cambios y nuevas apariciones, pues cada día es menos llamativa esta aplicación inicial, que era esencialmente la posibilidad de realizar transacciones, debido a que innumerables nuevas redes especializadas aparecen para solventar nuevos problemas.

2.1.2 Definición.

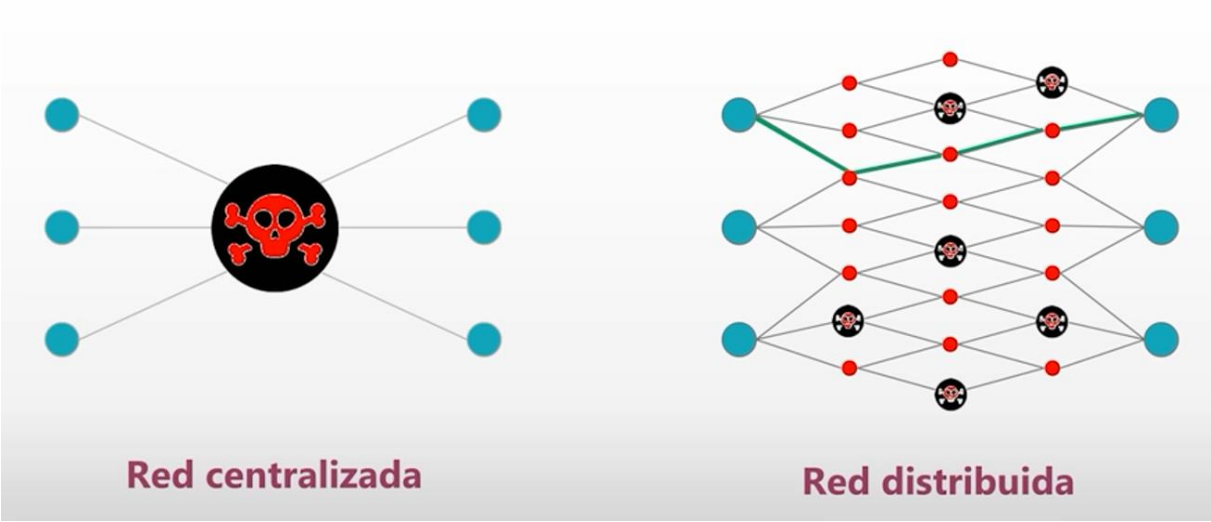
La tecnología *blockchain* se caracteriza fundamentalmente por funcionar como un libro de contabilidad. A diferencia de los sistemas tradicionales, donde una entidad única verifica y almacena los datos, este libro diario distribuye esta responsabilidad entre una red de nodos informáticos democráticamente insesgados. Esta arquitectura descentralizada y distribuida

ofrece una mayor seguridad, transparencia y resistencia a la censura. Esta descentralización se consigue gracias a los ordenadores de los usuarios, que actúan como nodos.

El uso de nodos como fuente de almacenamiento elimina la necesidad de un servidor central que almacene y filtre esa información, como utiliza el propio internet, debido a que la información será almacenada y registrada por el ordenador de todos los usuarios activos de la red, esto también protege frente a ataques ya que si la conexión entre dos nodos se destruye, hay infinitas conexiones entre esos dos nodos con todos los demás que están registrando esa misma información, posibilitando la conexión entre los dos nodos atacados por otro camino. Esto permite que la veracidad de la información no se vea comprometida

Cómo vemos en la siguiente ilustración, en las redes centralizadas, si el servidor central o la conexión con algún ordenador se ataca y se consigue destruir, la información tanto del servidor como de ese ordenador se ve amenazada, mientras que, en una red descentralizada bien distribuida, cuando se atacan y destruyen ciertos nodos, siempre existirá una manera de comunicar uno con otro.

Ilustración 2: Redes centralizadas vs Distribuidas



Fuente: (CEU Digital & Monteverde, 2019)

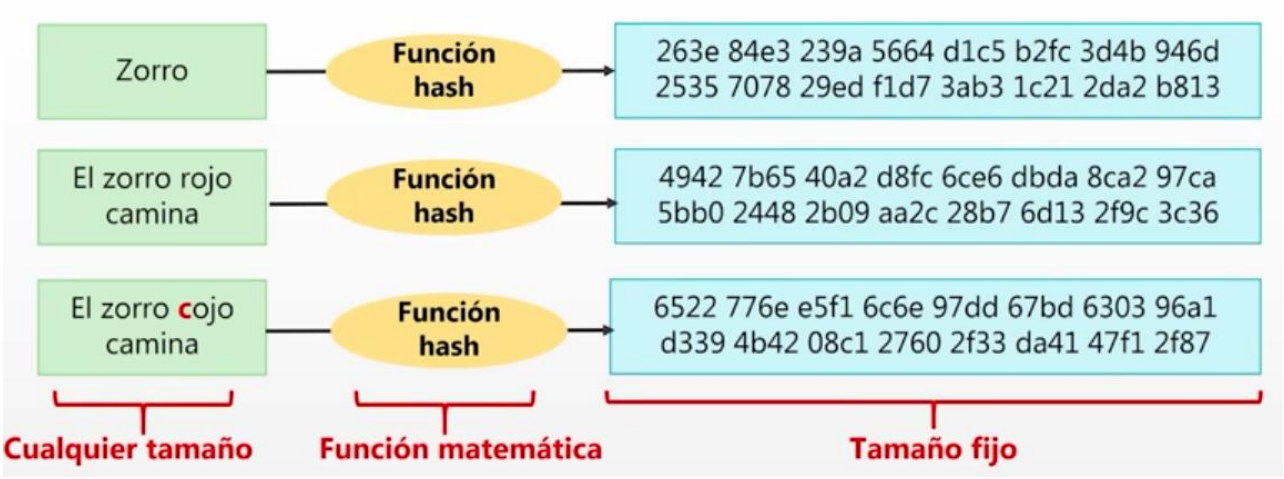
Los datos registrados en la *blockchain* son inmutables, lo que significa que no pueden ser modificados o eliminados sin el conocimiento y la participación de la mayoría de la red. Esta característica garantiza la integridad y la confiabilidad de la información visible en toda la red.

La inmutabilidad se consigue gracias a la manera en que los bloques están conectados, junto al sistema criptográfico utilizado, conocido como "*hash*". La codificación *hash* utiliza un algoritmo matemático para convertir datos de entrada, en este caso la información del bloque, en una cadena de longitud fija (160 bits/20 caracteres).

Este algoritmo procesa los datos de entrada de manera determinista, lo que significa que siempre producirá la misma salida para una entrada dada. La salida de la codificación *hash* se llama "*hash*" o "resumen *hash*". El *hash* generado es único para cada conjunto de datos de entrada, un pequeño cambio en los datos de entrada producirá un *hash* completamente diferente.

En la siguiente ilustración vemos un ejemplo con palabras codificadas con *hash*:

Ilustración 3: Codificación HASH



Fuente: (CEU Digital & Monteverde, 2019)

Es por esto por lo que, al crearse un nuevo bloque en el que la primera entrada de información es el "resumen *hash*" codificado del bloque anterior, si algo en el bloque anterior cambia, lo haría el *hash* resumen del bloque, resultando en una incongruencia en la cadena muy fácil de detectar.

Gracias a este sistema de criptografía la *blockchain* se considera inmutable. Los algoritmos de codificación *hash* son diseñados para ser rápidos y eficientes, pues, aunque la longitud del *hash* sea fija, el número de valores posibles es enorme. Por ejemplo, un *hash* de 256 bits o 32 caracteres puede tener hasta 2^256 o 10^77 valores diferentes, lo que es un número parecido al que se cree que es el número de átomos en el universo observable (10^78).

La red utiliza algoritmos de consenso, que sirven para validar la información introducida en los bloques, algunos ejemplos son la Prueba de Trabajo (PoW) o la Prueba de Participación (PoS), tienen como finalidad garantizar que todos los nodos de la red estén de acuerdo en el estado actual del libro mayor y en la validez de las transacciones, es decir, que lo que se introduce como información, sucede en la realidad.

Una duda que surge tras escuchar la manera en que se valida esta información es porque alguien va a querer invertir sus recursos en validar y verificar información de otros. Esto sucede en la realidad, pero no de manera gratuita, estos validadores compiten entre sí para ser los primeros en validar esa información. Al estar codificada, la validación de la información pasa a ser un problema matemático extremadamente complejo, solo posible de resolver mediante poder computacional, es decir, gracias a ordenadores que prueban resultados al azar, técnica conocida como "fuerza bruta".

El premio al validador que consiga resolver el problema y por lo tanto validador del bloque es en forma de BTC y es variable, reduciéndose a la mitad cada cuatro años aproximadamente (evento conocido como "*halving*"), actualmente el premio son 6.25 BTC, teniendo en cuenta el precio actual de 1 BTC (70.000$), el premio que se reparte en forma de BTC cada 10 minutos al primer validador que consiga validar el bloque son más de 430.000$, esto compensa no solo el tiempo invertido sino que también hace frente a los costes energéticos soportados por el empleo de sistemas informáticos en el proceso.

La aplicación más conocida de la *blockchain* son las criptomonedas, usadas como forma de pago para transferencias dentro de la red, como Bitcoin, la primera criptomoneda descentralizada. Ethereum, Litecoin y Ripple son otras criptomonedas que también se basan en esta tecnología, pero cuentan con ciertos matices, ya que no son totalmente descentralizados.

Las criptomonedas hoy en día son consideradas un híbrido entre las monedas fiduciarias y las acciones, contando con valor intrínseco asociado a un proyecto y viéndose afectado por el éxito de este, además de servir como forma de pago dentro de la red al operar dentro de ella.

. El impacto de este sistema se extiende más allá de las finanzas, pero dentro del sector financiero, esta tecnología puede usarse para realizar micro pagos, transacciones financieras transfronterizas más rápidas, seguras y eficientes, así como para automatizar procesos como la gestión de activos y la prevención del fraude en el sector financiero.

2.1.3 Bitcoin y BTC. La red y la criptomoneda

Hasta el momento hemos hablado de *blockchain* como tecnología, pero vamos a hacer un inciso en la principal red y en su principal "*token*" o criptomoneda, que son la red Bitcoin y su token BTC.

Bitcoin fue definida por el anteriormente mencionado Satoshi Nakamoto en su artículo "Bitcoin: Un sistema de efectivo electrónico entre pares", como bien dice en su título, un nuevo sistema financiero que eliminase intermediarios, que él consideraba abusivos.

Este nuevo sistema financiero cuenta con 5 principales características, que no serán de estricto requerimiento para el resto de las redes, pero sentaron una base de los valores que este nuevo sistema financiero requería. (Nakamoto, 2008)

2.1.3.1 Un sistema de efectivo electrónico "*peer-to-peer*"

A lo que el artículo se cree que hace referencia con esta característica es a la omisión de intermediarios en las transacciones financieras, aportando esa llamativa descentralización. El software de Bitcoin permite a los usuarios enviar y recibir pagos directamente entre sí. Estas transacciones serán verificadas y registradas en la *blockchain*, red pública y transparente. (Nakamoto, 2008)

2.1.3.2 Una moneda digital descentralizada

La moneda que utilizar en este nuevo sistema financiero no sería ni el dólar, ni el Euro ni el yen, ni ninguna otra conocida hasta el momento, iba a ser el BTC, token de utilidad dentro de la red de Bitcoin. Esta decisión se tomaría para evitar que la actividad dentro de la red estuviese sujeta a ningún control gubernamental o financiero.

Esta moneda se almacenaría en una billetera, el número de billeteras que se pueden crear es casi ilimitado, ya que la billetera es anónima, no hay nombre ni apellidos ni número de identificación fiscal. Una persona física puede tener tantas billeteras como desee. (Nakamoto, 2008)

Una billetera en la red se identifica por una serie de bits transformados en caracteres alfanuméricos como el siguiente: "1AGNa15ZQXAZUgFiqJ2i7Z2DPU2J6hW62i" (CEU Digital & Monteverde, 2019)

Es necesaria una billetera para poder realizar operaciones, ya que sin ellas no hay manera de almacenar, comprar, vender o transferir criptomonedas o información.

El nivel de seguridad y protección de la billetera lo define el usuario, ya que la clave para acceder a ella y poder realizar cualquier operación es una frase incongruente de 12, 24 o 25 palabras de longitud indefinida, imposible de adivinar o descifrar por fuerza bruta. Esta frase se llama "frase semilla", un ejemplo puede ser:

"*island distance scout ice hotel account merge exile symbol token insect modify vast dumb myth logic rally whisper party"* (CEU Digital & Monteverde, 2019)

Hay dos tipos de billeteras, con custodia o sin custodia:

Las billeteras con custodia son aquellas creadas por un tercero, como puede ser un "*Exchange*", sitio en el que se compran, venden e intercambian criptomonedas a una cotización ofrecida, son una casa de cambio para las divisas digitales. Al ser creadas por un tercero, será ese tercero el responsable de la frase semilla y de los fondos que se encuentran en la billetera.

El usuario desconoce la frase semilla, esto en teoría evita estafas y robos, además de ser más fáciles de utilizar, pero en la práctica se ha visto que estas plataformas sufren ataques en ocasiones exitosos que terminan en el robo de todas las frases semilla y por consecuencia el robo de millones de dólares en forma de criptomonedas, estos robos no son rastreables debido a la codificación de la red, por lo que el usuario queda más expuesto.

Las billeteras sin custodia son aquellas que el usuario crea la propia billetera y se hace responsable de la frase semilla otorgada, así como de los fondos que en ella residen.

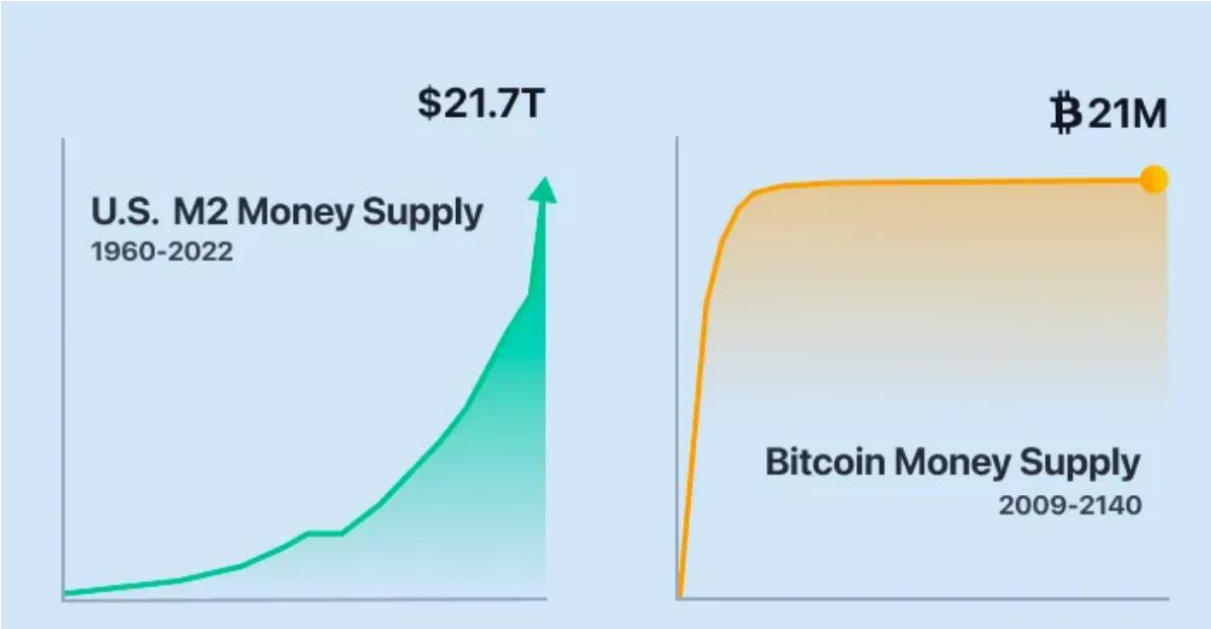
2.1.3.3 Un activo digital escaso

Esta moneda tendría ciertas peculiaridades. Aprovechando su creación, se tratarían de solventar otros problemas propios de las monedas fiduciarias, como la inflación. El número de BTC existentes sería limitado, en concreto 21 Millones de BTC. Estos BTC, además, serían puestos en circulación de manera programada, como recompensa a los validadores de la red, también conocidos como mineros, siendo imposible su emisión forzada.

Esta escasez es vista como una propiedad deflacionaria, algo percibido por el mercado como un activo similar al oro, por lo que BTC puede actuar como reserva de valor para sus inversores.

En el siguiente gráfico podemos ver la comparativa entre la evolución en la cantidad de BTC programados para ser emitidos, que se prevé que terminen de emitirse en el año 2140 con la evolución en la emisión de dólares estadounidenses hasta el año 2022:

Ilustración 4: Comparativa entre efectivo en circulación USD vs BTC



Fuente: (Saleem, 2023)

2.1.3.4 Un sistema de pago resistente a la censura y el control.

Las transacciones en Bitcoin son irreversibles y no pueden ser censuradas por ninguna autoridad. Esto elimina la posibilidad de que se pongan inconvenientes a la hora de gastar tu capital. Las instituciones financieras tradicionales, por normativas legales además de intereses propios, realizan consultas acerca de los motivos de ciertas transferencias de importes elevados, esto no sería necesario en esta red. El anonimato y las nulas barreras convierten Bitcoin en una herramienta atractiva para aquellos que buscan proteger su privacidad y libertad financiera.

2.1.3.5 Un protocolo abierto y sin permiso

Cualquiera puede participar en la red Bitcoin y contribuir a su desarrollo. Esto permite una mayor transparencia y seguridad que los sistemas financieros tradicionales.

2.1.3.6 Mitos de Bitcoin y la tecnología *blockchain*.

Existen varios mitos sobre esta tecnología que, debido a la desinformación que generan, perjudican la credibilidad y el prestigio de esta tecnología:

Se dice que *blockchain* sirve solo para operar con criptomonedas. Si bien es cierto que las criptomonedas popularizaron esta tecnología, la red tiene un potencial mucho más amplio. Se puede usar para crear registros seguros y transparentes para diversos fines, como cadenas de suministro, registros médicos y votación electrónica. Además de por supuesto crear sistemas híbridos que mediante micro pagos hagan más segura esta información

Se puede leer e incluso se ha escuchado a líderes políticos decir que *blockchain* es demasiado lento y costoso: Es cierto que algunas, como la red de Bitcoin, pueden ser lentas y costosas de usar. Sin embargo, existen otras de "segunda generación" y "tercera generación" que están diseñadas para ser más rápidas y eficientes. Hay que tener en cuenta que Bitcoin es

la primera que vio la luz. Al igual que sucedió con internet, la tecnología ya se ha optimizado y seguirá haciéndolo.

Es popularmente aceptado que esta nueva tecnología no se acoge a ninguna regulación. Es cierto que existen desafíos para integrarla con los marcos regulatorios existentes, al igual que sucede con todas las nuevas invenciones o el constante desarrollo tecnológico. Sin embargo, se están desarrollando soluciones y colaboraciones entre el sector público y privado para abordar estas cuestiones, pues *blockchain* ya es una tecnología que solo en su desarrollo mueve miles de millones de dólares al año a nivel mundial.

Es importante recordar que este sistema todavía está en sus primeras etapas de desarrollo. Hay muchos desafíos que deben abordarse antes de que pueda alcanzar su máximo potencial. Es vital no dejarse disuadir por los mitos y la desinformación, eso solo ralentiza la evolución y su progreso.

2.2 Funcionamiento de la *Blockchain*.

Tras contar con una visión general de lo que es una *blockchain*, se va a tratar de explicar el funcionamiento de esta, ejemplificando desde el registro de información dentro de la red hasta la transferencia de valor usando esta tecnología, pasando por el tipo de codificación criptográfica empleada en ella, que es la base sobre la que se sustenta esta tecnología y explicando la esencialidad del minado como parte de la red.

Para poder hacerlo se va a usar como ejemplo la operación más básica a realizar dentro de la red, la transferencia de una cantidad definida de BTC de una cartera a otra.

2.2.1 Fases de una operación en la cadena de bloques.

2.2.1.1. Inicio de la transacción:

Un usuario crea una transacción usando su billetera digital, previamente creada mediante otra operación en la red.

La billetera digital, independientemente del tipo que sea, almacena las claves criptográficas privadas del usuario, que son necesarias para firmar la transacción.

La transacción incluye información como la dirección de la billetera del remitente, la dirección de la billetera del destinatario, la cantidad de criptomonedas a enviar y una tarifa que se cobrará por efectuar la transacción. (Bit2me Academy, 2023a)

2.2.1.2. Transmisión de la transacción a la red:

La transacción se transmite a la red de nodos.

Los nodos son las computadoras que ejecutan el software y que mantienen una copia completa de la cadena de bloques. Los nodos son responsables de verificar las transacciones, agregar nuevos bloques a la cadena de bloques y mantener la red segura.

Los nodos retransmiten la transacción a otros nodos en la red hasta que se propaga por toda la red. (Netflix & Hoffmann, 2020)

2.2.1.3. Verificación de la transacción:

Los nodos también se encargan de validar la transacción. Se comprueba que la dirección del remitente tenga fondos suficientes para cubrir la transacción y la tarifa. Posteriormente se verifica la firma digital del remitente para asegurar que la transacción no ha sido manipulada. Por último, se comprueba que la transacción no viola ninguna regla de la red, como las reglas de gasto doble, que impide a una billetera hacer dos operaciones simultaneas que se validen a la vez, gastando el doble de lo que posee. (Bit2me Academy, 2023a)

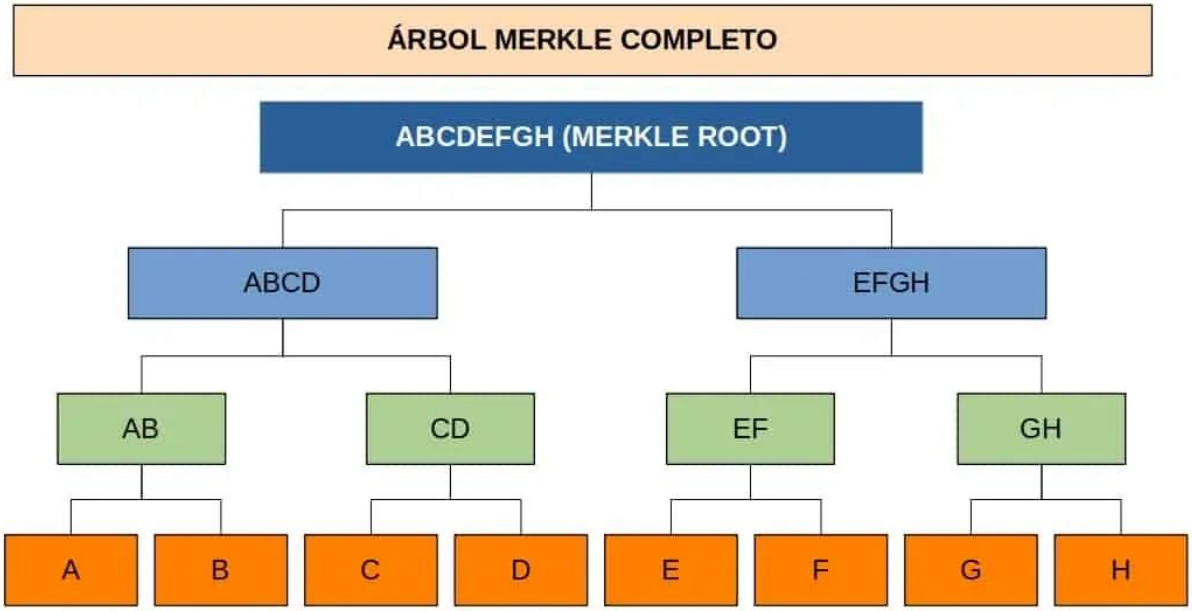
2.2.1.4. Creación de un bloque:

Los nodos que ejecutan el software de minería codifican y agrupan las transacciones verificadas en un nuevo bloque. El tamaño del bloque está limitado para asegurar que pueda ser propagado rápidamente por la red. (Bit2me Academy, 2023a)

Cada bloque contiene un encabezado con información sobre el bloque, como la marca de tiempo, el *hash* del bloque anterior y la raíz del árbol de Merkle. El árbol de Merkle es una estructura de datos que se utiliza para verificar la integridad de las transacciones en un bloque, parecido a un rastro digital para poder seguir el camino que han ido haciendo las criptomonedas. La raíz del árbol de Merkle es un resumen criptográfico de todas las transacciones en el bloque. (Netflix & Hoffmann, 2020)

En la siguiente ilustración podemos ver un ejemplo gráfico de cómo se puede rastrear el camino previamente recorrido por esa información:

Ilustración 5: Árbol de Merkle



(Bit2me Academy, 2023)

2.2.1.5. Minería del bloque:

Los nodos de minería compiten para resolver un complejo problema matemático.

El problema matemático se llama función *hash* y se utiliza para garantizar la seguridad de la cadena de bloques, el primer nodo en resolver el problema recibe el derecho de agregar el nuevo bloque a la cadena de bloques. A cambio de su trabajo, el nodo de minería recibe una recompensa en criptomonedas. (Bit2me Academy, 2023a)

2.2.1.6. Adición del bloque a la cadena:

El bloque válido se agrega al final de la cadena de bloques.

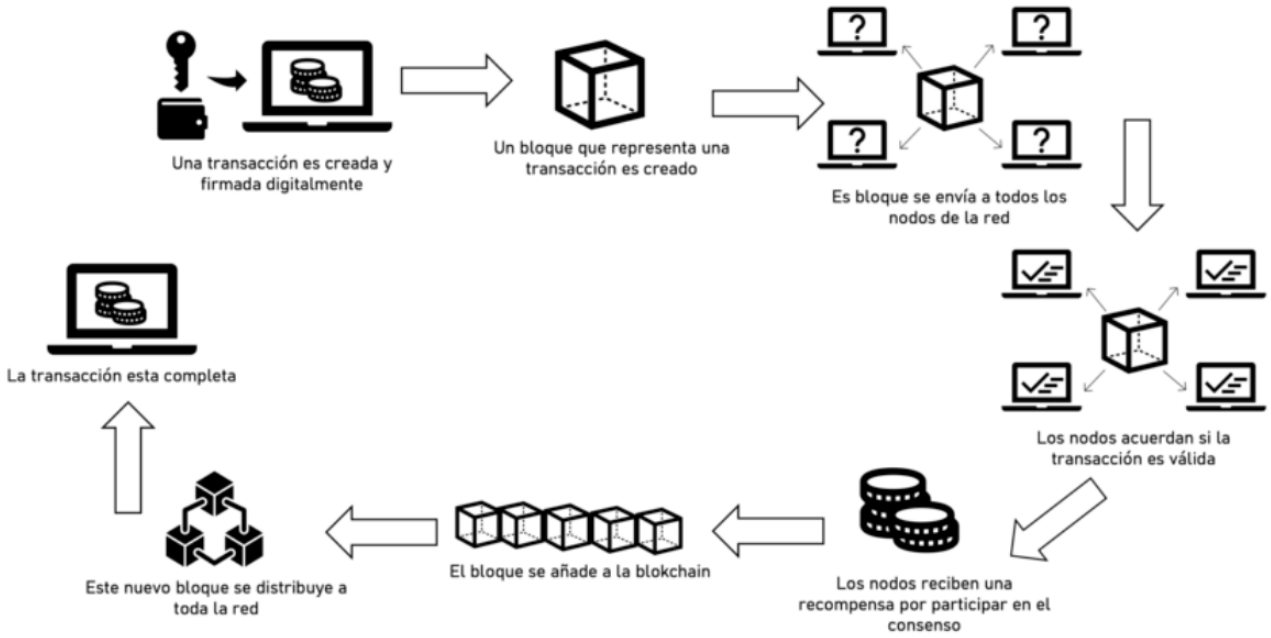
Todas las copias de la cadena de bloques en la red se actualizan para reflejar el nuevo bloque. Cuando esto sucede, la adición del nuevo bloque a la cadena se denomina consenso. (Bit2me Academy, 2023a)

2.2.1.7. Confirmación de la transacción:

Una vez que el bloque se agrega a la cadena de bloques, la transacción se considera completa y confirmada solo faltando la transferencia de las criptomonedas del remitente al destinatario.

El número de confirmaciones necesarias para que una transacción se considere completa puede variar según la red en la que se opere. Lo más habitual para cantidades estándar de criptomonedas es entre 3 y 6 confirmaciones por nodos aleatorios, pero en transacciones en las que el valor transferido es elevado el número de confirmaciones requeridas puede aumentar. (Bit2me Academy, 2023a)

Ilustración 6: Funcionamiento de la ***blockchain****.*



Fuente: (Aldeco-Perez & Rajsbaum, 2022)

2.3 Tipos de *Blockchain*.

La tecnología *blockchain* surgió de la mano de Bitcoin, pero como toda innovación tecnológica, a medida que se desarrolla surgen nuevas vertientes que aprovechan esos avances tecnológicos y se adaptan a necesidades más específicas. Tras Bitcoin, considerada una red pública, surgieron otros tipos de redes ya operativos en la actualidad. (Observatorio *Blockchain*, 2023)

Para entender sus diferencias y similitudes se van a explicar los distintos tipos de *blockchain* actuales:

2.3.1 *Blockchain* pública.

Una de las características más destacadas de la *blockchain* pública es su naturaleza abierta y accesible. Cualquier persona puede descargar el software necesario para convertirse en un nodo de la red y participar en la validación de transacciones. Esto significa que no hay restricciones para unirse a la red y que todos los datos registrados en ella son visibles para cualquier persona en tiempo real. (Observatorio *Blockchain*, 2023)

Otro aspecto fundamental es la transparencia y la inmutabilidad de los datos, esto es debido a que es una red distribuida, la responsabilidad y el control está distribuido en los nodos de la red, sin existir un servidor central. Todas las transacciones realizadas en la cadena de bloques pública son registradas de manera permanente en bloques que se enlazan entre sí mediante criptografía. (CEU Digital & Monteverde, 2019)

Una vez que se ha validado una transacción y se ha agregado a un bloque, es prácticamente imposible modificarla o eliminarla sin el consenso de la mayoría de los participantes en la red, lo que garantiza la integridad de la información almacenada en la cadena de bloques.

Además, la seguridad es una característica clave de la *blockchain* pública, ya que utiliza algoritmos criptográficos para proteger los datos y garantizar la autenticidad de las transacciones. Cada nodo de la red tiene una copia completa del libro mayor distribuido, lo que hace que sea extremadamente difícil para un atacante comprometer la red o alterar los datos sin ser detectado. (Observatorio *Blockchain*, 2023)

Ejemplos destacados de *blockchain* pública incluyen Bitcoin y Ethereum. Bitcoin fue la primera implementación exitosa de una red pública, diseñada principalmente como una red para transferir valor de manera peer-to-peer sin necesidad de intermediarios.

Ethereum, o Solana, por otro lado, son unas plataformas más versátiles que permiten la ejecución de contratos inteligentes y el desarrollo de aplicaciones descentralizadas (dApps) sobre su red. Además, son mucho más escalables debido a su sistema de validación "*Proof of Stake*", que reduce ligeramente la seguridad en la validación de información, pero aumenta exponencialmente la rapidez en las operaciones, además de ser mucho más beneficioso para el medio ambiente, ya que consume mucha menos energía. (CEU Digital & Monteverde, 2019)

Estas dos últimas redes, son más programables que Bitcoin. Por la naturaleza de su código, Bitcoin es una red más compleja de evolucionar, es por eso por lo que los desarrolladores independientes deciden priorizar la innovación de nuevas funcionalidades públicas en estas nuevas redes.

La gobernanza es un aspecto muy valorado dentro del mundo *blockchain*. Ethereum y Solana son dos redes que otorgan un mayor grado de gobernanza a sus usuarios, permitiéndoles participar en votaciones que deciden el rumbo a seguir por parte de la red, aportando un grado de descentralización más. (CEU Digital & Monteverde, 2019)

2.3.2 *Blockchain* privada.

La *blockchain* privada es una versión de la tecnología que restringe el acceso y la participación a un grupo específico de usuarios autorizados. A diferencia de la *blockchain* pública, donde cualquiera puede unirse y participar en la red, en una red privada se requieren permisos para acceder y realizar transacciones.

Una de las características principales de la red privada es su control centralizado. En lugar de depender de una red descentralizada de nodos anónimos como en la pública, en una cadena de bloques privada, una entidad centralizada, como una empresa, supervisa y controla la operación de la red. Esto significa que la empresa tiene el poder de decisión sobre quién puede unirse a la red, qué transacciones se pueden realizar y quién puede acceder a los datos almacenados en la cadena de bloques. (Cointelegraph, s. f.)

Además, la velocidad y la escalabilidad suelen ser mejores en una red privada en comparación con una pública. Dado que la red está controlada por un grupo selecto de nodos, se pueden implementar medidas para mejorar el rendimiento y la eficiencia de la red, como algoritmos de consenso optimizados y capacidades de procesamiento mejoradas. (Cointelegraph, s. f.)

2.3.3 *Blockchain* consorcio.

La *blockchain* de consorcio, también conocida como autorizada o permisionada. Es un tipo de red que combina características de la pública y privada. En una *blockchain* de consorcio, la participación y el acceso a la red están restringidos a un grupo específico de participantes autorizados, generalmente organizaciones que forman un consorcio o una asociación.

Una de las características clave de la red de consorcio es su naturaleza compartida entre un grupo selecto de participantes. A diferencia de la red pública, donde cualquier persona puede unirse y participar en ella, en una red de consorcio, los participantes son conocidos y verificados. Esto permite una mayor confianza entre los miembros del consorcio, ya que se conocen entre sí y han sido previamente aprobados para participar en la red. (Cointelegraph, s. f.)

Otro aspecto importante es la distribución del control y la gobernanza. Aunque la red puede estar descentralizada en términos de participantes, el control y la administración de la *blockchain* de consorcio suelen estar centralizados en manos de los miembros del consorcio. Esto significa que las decisiones sobre cambios en el protocolo, actualizaciones de software y políticas de gobierno son tomadas por consenso entre los participantes autorizados.

La *blockchain* de consorcio también ofrece beneficios similares a los de la privada, como mayor privacidad y confidencialidad de los datos.

Se utiliza principalmente en entornos empresariales donde se requiere colaboración entre un grupo selecto de organizaciones. (Cointelegraph, s. f.)

2.3.4 *Blockchain* híbrido.

La *blockchain* híbrida es un tipo de sistema que combina características de la pública y privada en una sola red. Esta combinación permite a los usuarios tener acceso a funcionalidades tanto de las redes públicas como de las privadas, adaptándose así a una amplia gama de aplicaciones y casos de uso.

Una de las características principales de la *blockchain* híbrida es su flexibilidad en cuanto a la gestión de permisos y la visibilidad de los datos. Por ejemplo, puede haber áreas de la red que son completamente públicas, donde cualquier persona puede acceder y participar en la red, mientras que otras áreas pueden estar restringidas a un grupo específico de usuarios autorizados. Esta capacidad de personalización permite a las organizaciones adaptar la red a sus necesidades específicas, combinando la transparencia y la accesibilidad de una pública con la privacidad y la seguridad de una privada. (Observatorio *Blockchain*, 2023)

Otro aspecto importante de la *blockchain* híbrida es su capacidad para integrar múltiples protocolos de consenso. Esto significa que la red puede utilizar diferentes algoritmos de consenso en diferentes partes de la red según sea necesario. Por ejemplo, se puede implementar un protocolo de consenso de prueba de trabajo (PoW) en las áreas públicas de la red para garantizar la seguridad y la resistencia a la censura, mientras que se utiliza un protocolo de consenso de prueba de participación (PoS) en las áreas privadas de la red para mejorar la eficiencia y el rendimiento.

Además, la *blockchain* híbrida puede facilitar la interoperabilidad entre diferentes sistemas. Al actuar como un puente entre redes públicas y privadas, la híbrida permite a los usuarios transferir activos y datos entre diferentes redes de forma segura y eficiente.

Este tipo de red puede ser usada por entidades bancarias como plataforma de comunicación con sus clientes, ofreciéndoles acceso a su información, pero privándoles el acceso a la del resto de clientes o de la propia entidad. Esto haría las aplicaciones móviles para usuarios mucho más seguras. (Observatorio *Blockchain*, 2023)

2.3.5 *Blockchain* autorizado

La naturaleza es muy similar a la de los sistemas híbridos, una de las características clave de la *blockchain* autorizada es su control centralizado. Aunque la red puede estar descentralizada en términos de distribución geográfica de los nodos, el control y la administración de la red están en manos de una entidad centralizada, como una organización, empresa o consorcio.

Esto significa que la entidad tiene la capacidad de decidir quién puede unirse a la red, qué transacciones se pueden realizar y qué datos se pueden almacenar en la cadena de bloques.

La diferencia con la híbrida radica en que mientras que esta combina características de las redes públicas y privadas para ofrecer flexibilidad y adaptabilidad, la *blockchain* autorizada se centra en restringir el acceso y la participación a un grupo selecto de usuarios autorizados, proporcionando un mayor control sobre la red y los datos. (Observatorio *Blockchain*, 2023)

(III) ANÁLISIS DE LAS SOLUCIONES.

3.1 Solución frente a la ineficiencia en las transferencias.

Esta tecnología ha demostrado ser una solución prometedora para abordar los desafíos de eficiencia y confiabilidad en las transferencias financieras. Uno de los aspectos más destacados es la drástica reducción en la ratio de error en comparación con los métodos de transferencia convencionales. Mientras que en las transferencias bancarias nacionales la tasa de error ronda el 0,05%, y en las internacionales puede llegar al 0,1%, en la *blockchain*, esta ratio por transferencia es mucho menor, oscilando entre un 0,01% y 0,001%, lo que representa una mejora de entre 10 y 100 veces en la precisión de las transacciones. (Glassnode, s. f.)

Las cualidades de la cadena de bloques que hacen posible la reducción drástica del número de errores son las siguientes:

Inmutabilidad. La red utiliza una estructura de datos inmutable y distribuida, donde cada transacción se registra en bloques enlazados criptográficamente. Una vez que se ha validado una transacción y se ha añadido a un bloque, se vuelve prácticamente imposible modificarla o eliminarla sin el consenso de la mayoría de los participantes de la red. Esta característica asegura la integridad de los datos y reduce significativamente la posibilidad de errores en las transacciones. (CEU Digital & Monteverde, 2019)

Automatización mediante contratos inteligentes. La tecnología permite la ejecución de contratos inteligentes en redes como Ethereum o Solana. estos son programas informáticos que se ejecutan automáticamente cuando se cumplen ciertas condiciones predefinidas. Los contratos inteligentes pueden automatizar una amplia gama de procesos financieros, incluidas las transferencias de fondos. Al eliminar la necesidad de intermediarios y procesos manuales, los contratos inteligentes reducen los errores humanos y agilizan el proceso de transferencia de fondos.

Transparencia y trazabilidad: Cada transacción en una red *blockchain* es transparente y auditable para todos los participantes de la red. Esto significa que los usuarios pueden verificar fácilmente el historial de una transacción y rastrear su origen y destino. La transparencia y la trazabilidad de las transacciones ayudan a prevenir el fraude y aumentan la confianza entre los participantes de la red, lo que contribuye a la reducción de errores en las transferencias financieras. Esta cualidad también aportaría una agilidad necesaria en casos de estafas o fraudes, ya que su rastreo sería mucho más fácil.

En la actualidad cuando una estafa sucede, la manera que tienen los estafadores de no ser rastreados es mover el dinero de manera continua entre cuentas en diferentes países, llegando a hacerlo en miles de ocasiones, aprovechando las distintas jurisprudencias. Esto es imposible vía *blockchain*, pues solo las tarifas a pagar por la inmediatez de la transacción harían desaparecer el “botín” conseguido por los piratas de la red. (CEU Digital & Monteverde, 2019)

3.2 Solución frente a las brechas de seguridad.

Las brechas de seguridad en el sistema financiero tradicional representan una preocupación significativa, ya que pueden resultar en pérdidas financieras, robo de identidad y falta de confianza por parte de los usuarios. La tecnología ofrece varias soluciones para abordar estas vulnerabilidades y minimizar los riesgos asociados.

Las características de *blockchain* que suponen un avance en términos de seguridad y como se aplican se explicarán a continuación.

La *blockchain* utiliza algoritmos de criptografía avanzada para proteger la integridad y la confidencialidad de los datos. Cada transacción en la red está protegida por una firma digital única, que garantiza su autenticidad y evita la falsificación o la manipulación. Además, la encriptación de extremo a extremo asegura que solo los participantes autorizados puedan acceder a la información, lo que reduce el riesgo de acceso no autorizado y robo de datos. (Nakamoto, 2008)

En el sistema financiero tradicional, los usuarios deben confiar en terceros, como bancos y procesadores de pagos, para almacenar y proteger sus datos financieros. Esto crea una dependencia de terceros y aumenta el riesgo de brechas de seguridad debido a errores humanos, fallos del sistema y acciones malintencionadas, elementos inexistentes en la *blockchain*. (CEPYME, 2023)

Otra cualidad de la tecnología *blockchain* es la distribución de sus nodos y la descentralización del poder de validación. La mayoría de las redes utilizan un sistema descentralizado de consenso, donde las transacciones son validadas y registradas por una red de nodos distribuidos en lugar de depender de una autoridad central. (Nakamoto, 2008)

En el sistema financiero tradicional, los datos financieros están centralizados en servidores controlados por instituciones financieras. Esto hace que los datos sean más susceptibles a ataques cibernéticos, ya que un solo punto de acceso puede comprometer grandes cantidades de información. (CEPYME, 2023)

Este enfoque descentralizado hace que sea mucho más difícil para los hackers comprometer la red, ya que tendrían que controlar la mayoría de los nodos para realizar cambios maliciosos. Además, la distribución geográfica de los nodos aumenta la resistencia a ataques cibernéticos y garantiza la continuidad del sistema incluso en caso de fallas o ataques dirigidos. (Nakamoto, 2008)

La inmutabilidad de la red nos aporta la norma que dicta que, una vez que se ha registrado una transacción en el tecnológico libro contable, se vuelve prácticamente imposible modificar o eliminar sin el consenso de la mayoría de los participantes de la red. Esto significa que los registros de transacciones son inmutables y transparentes, lo que ayuda a prevenir el fraude y la manipulación de datos. Los usuarios pueden confiar en la integridad de la información almacenada en la cadena de bloques, lo que aumenta la confianza y la seguridad en el sistema financiero.

El sistema de identificación habitual en las redes *blockchain* puede proporcionar soluciones de identidad digital y autenticación más seguras mediante el uso de firmas digitales y claves criptográficas. Los usuarios pueden tener control sobre su identidad y acceder a servicios financieros de manera segura sin comprometer su información personal. Esto ayuda a

prevenir el robo de identidad y otros tipos de fraudes relacionados con la autenticación de usuarios en el sistema financiero.

A pesar de que no están presentes en la red de Bitcoin, Los contratos inteligentes son programas informáticos autoejecutables que se activan automáticamente cuando se cumplen ciertas condiciones predefinidas. Estos contratos pueden automatizar procesos financieros complejos y garantizar que se cumplan las condiciones acordadas de manera segura y transparente. Al eliminar la necesidad de intermediarios y procesos manuales, los contratos inteligentes reducen los errores humanos y los riesgos de fraude en el sistema financiero. (Buterin, 2014)

A diferencia de lo que sucede en la ejecución de un "*Smart contract*", muchos procesos en el sistema financiero tradicional son innecesariamente manuales y dependen de la intervención humana, lo que aumenta el riesgo de errores y fraudes. Los datos pueden ser mal introducidos o manipulados durante el proceso manual, lo que puede resultar en brechas de seguridad. (Buterin, 2014)

3.3 Solución frente a la tardanza transaccional.

A diferencia de los métodos convencionales de transferencia de fondos que dependen de intermediarios, como bancos y sistemas de pago, la *blockchain* ofrece un enfoque descentralizado y transparente para realizar transacciones financieras. Esta tecnología minimiza la tardanza transaccional debido a algunas características que la diferencian de las entidades bancarias tradicionales.

Estas cualidades son las siguientes:

Velocidad de procesamiento. Se suele utilizar como argumento en contra de esta tecnología que los tiempos de procesamiento son de varios minutos, comparándose con el popular Bizum, pero la homogeneidad que aporta es clave para solventar estos problemas, ya que esos pocos minutos que tarda al transferir una cantidad X a una billetera de otro usuario de tu región, son los mismos necesarios para transferir esa misma cantidad a un usuario de la otra punta del planeta. (Mit Media Lab, 2021)

Las transacciones se verifican y se registran en bloques de forma descentralizada, lo que elimina la necesidad de intermediarios y reduce significativamente el tiempo necesario para completar una transacción. Esto es especialmente beneficioso en el caso de transferencias internacionales, donde las transacciones pueden tardar días en completarse debido a la participación de múltiples intermediarios. En la *blockchain*, las transacciones pueden procesarse de manera casi instantánea, lo que reduce drásticamente el riesgo de errores y retrasos.

Los sistemas financieros tradicionales a menudo implican múltiples intermediarios, como bancos, instituciones financieras y sistemas de compensación, cada uno de los cuales puede introducir retrasos en el proceso de transacción. En contraste, la tecnología *blockchain* elimina la necesidad de intermediarios al permitir que las transacciones se realicen de igual a igual directamente entre las partes involucradas. Esto reduce significativamente el tiempo necesario para completar una transacción. (Nakamoto, 2008)

Las redes *blockchain* operan de manera continua, las 24 horas del día y los 7 días de la semana, sin importar las zonas horarias. Esto significa que las transacciones pueden procesarse

y confirmarse en cualquier momento, lo que elimina las restricciones de tiempo asociadas con los sistemas financieros tradicionales, donde los procesos pueden retrasarse durante los fines de semana o días festivos.

Puede que sorprenda leer que, por ejemplo, BTC cotiza de manera ininterrumpida, por lo que no hay horarios de apertura ni de cierre.

Esto se debe a que las criptomonedas fueron concebidas como activos descentralizados. Su compraventa no se efectúa en un único mercado concreto como ocurre con las acciones o los futuros. En vez de esto, se negocian en múltiples "*Exchange*" que están activos de lunes a domingo a cualquier hora. Además, también es posible intercambiar Bitcoin entre dos usuarios de forma totalmente privada sin ningún intermediario. (Mit Media Lab, 2021)

Todo esto permite que, de manera automática y auto regulada por el mercado, la tecnología esté operativa todos los días del año a todas horas, ya que depende de que haya validadores la confirmación de transacciones, algo presente a todas horas debido a las recompensas que reciben. (Narula, 2021)

3.4 Solución frente a la aparición de comisionistas.

En el mundo actual, las transferencias de dinero son una parte esencial de nuestras vidas. Ya sea para enviar pagos a familiares y amigos, realizar compras online o transferir ahorros, las opciones para mover nuestro dinero son diversas. Entre las opciones más populares se encuentran las transferencias bancarias tradicionales y las transferencias a través de la tecnología *blockchain*.

A continuación, se exponen las diferencias entre las dos opciones mencionadas desde el punto de vista del emisor de efectivo, receptor y del comisionista o intermediario que hace posible la transferencia.

Las comisiones por transferencias existen por diversas razones:

En el sistema bancario tradicional, las comisiones sirven para cubrir los costes operativos de los bancos, que incluyen el mantenimiento de la infraestructura tecnológica, el pago del personal y la gestión de riesgos. Además, las comisiones también generan beneficios para las entidades financieras.

En las operaciones *blockchain*, las comisiones se destinan principalmente a incentivar a los mineros o validadores que participan en la red. Estos nodos de la red se encargan de verificar y validar las transacciones, asegurando la seguridad, la inmutabilidad y el buen funcionamiento de la cadena de bloques. Sin la existencia de estas comisiones, la red podría ser vulnerable a ataques y fraudes. (Godoy, 2024).

Las comisiones bancarias se suelen deducir directamente de la cuenta del emisor de la transferencia, aunque en algunos casos pueden compartirse con el receptor. El método de pago varía según el banco y la entidad receptora, pudiendo realizarse mediante cargos en cuenta, extracciones en cajero automático o incluso pagos en efectivo.

En las transferencias *blockchain*, las comisiones se pagan en la criptomoneda nativa de la red utilizada para la transacción. Por ejemplo, en el caso de Bitcoin, las comisiones se pagan en BTC, mientras que en Ethereum se utilizan ETH. Los usuarios deben disponer de estas criptomonedas en sus carteras digitales para poder cubrir las tarifas antes de iniciar la transferencia. (Godoy, 2024)

En general, el emisor de la transferencia es quien asume el pago de las comisiones, tanto en el sistema bancario tradicional como en las transferencias *blockchain*. Sin embargo, en algunos casos excepcionales, las comisiones pueden ser compartidas entre el emisor y el receptor, o incluso ser asumidas en su totalidad por el receptor.

En el sistema bancario tradicional, las comisiones por transferencias son cobradas por los bancos, que actúan como intermediarios en el proceso. Estas comisiones pueden variar según diversos factores, como el tipo de cuenta, el importe de la transferencia, el país de destino y la urgencia de la transacción. Los bancos suelen establecer tarifas fijas, comisiones porcentuales o una combinación de ambas para cubrir sus costes operativos, obtener beneficios y mantener su infraestructura. (Godoy, 2023).

En el caso de las transferencias *blockchain*, las comisiones no se cobran a través de intermediarios, sino que son pagadas directamente por los usuarios a la red. Estas comisiones, generalmente denominadas "tarifas" o "*fees*", se calculan mediante un algoritmo y se destinan a incentivar a los mineros o validadores que se encargan de verificar y añadir las transacciones

a la cadena de bloques. De esta manera, se garantiza la seguridad, la inmutabilidad y el buen funcionamiento de la red descentralizada.

En el sistema bancario tradicional, las comisiones por transferencias suelen ser más altas para las transacciones internacionales o de grandes cantidades. Además, las comisiones pueden variar significativamente según el país o región de origen y destino de la transferencia. Esto se debe a los diferentes costes operativos, las regulaciones financieras y los tipos de cambio existentes en cada región. (Godoy, 2023).

En el caso de las transferencias *blockchain*, las comisiones por transacción suelen ser más bajas que las bancarias, especialmente para pequeñas cantidades. Las comisiones pueden variar ligeramente según la red *blockchain* utilizada y la congestión de esta en un momento determinado. Sin embargo, no están sujetas a diferencias geográficas. Es decir, un usuario enviará la misma cantidad de comisión por una transferencia a cualquier parte del mundo, independientemente de su ubicación. (Godoy, 2024).

El siguiente cuadro diferencia y compara de manera visual las dos vías, en función del tipo de transferencia que se desea realizar:

Característica	**Comisiones bancarias**	**Comisiones *blockchain***
Comisionista	Intermediarios (bancos)	Red descentralizada (pagadas a validadores)
Pago	Varía (fijas, porcentuales, híbridas)	Criptomoneda nativa de la red según urgencia
Paga	Emisor (o compartido)	Emisor
Motivo	Costes operativos, beneficios, infraestructura	Incentivar seguridad y funcionamiento
Cantidad/Ubicación	Más altas para internacionales/grandes cantidades, varían por región	Más bajas, no varían por ubicación

La principal ventaja que muestra el uso de *blockchain* es la nula variabilidad en cuanto a los diversos factores que pueden determinar una transacción. (IBM, 2024).

3.5 Solución frente a la opacidad del sector.

La tecnología *blockchain* ofrece soluciones innovadoras para abordar el problema de opacidad

La característica fundamental de esta tecnología, que permite que se minimice este problema es su capacidad para crear registros transparentes y permanentes de transacciones. Cada transacción se registra en bloques enlazados de manera cronológica, formando una cadena inmutable. (CEU Digital & Monteverde, 2019).

El funcionamiento es semejante al que tendría una cámara acorazada de máxima seguridad, pero cuyas cajas son anónimas y transparentes. Solo siendo disponibles si se cuenta con la frase semilla personal, privada e intransferible. (CEU Digital & Monteverde, 2019)

Esto significa que cualquier persona puede acceder y verificar las transacciones pasadas, lo que aumenta la transparencia en el proceso. Al eliminar la opacidad, los usuarios pueden comprender mejor las tarifas y los costos asociados con las transacciones internacionales. (CEU Digital & Monteverde, 2019)

Cómo ya se comentó con anterioridad, con la eliminación de intermediarios y una mayor transparencia en las transacciones, se pueden reducir drásticamente los costos asociados con las transferencias internacionales de dinero.

En lugar de pagar altas comisiones a empresas remesadoras, los usuarios pueden beneficiarse de tarifas mucho más bajas o incluso inexistentes al utilizar plataformas basadas en la cadena de bloques para realizar transferencias de fondos.

3.6 Estado actual y próximos pasos a seguir.

La tecnología *Blockchain* ha irrumpido en el panorama financiero como una solución innovadora con el potencial de revolucionar los sistemas tradicionales. Sin embargo, a pesar de su irrupción, su adopción a gran escala se enfrenta a una serie de desafíos y obstáculos que deben abordarse cuidadosamente para garantizar su éxito a largo plazo.

1. Escalabilidad y eficiencia:

Las redes, especialmente aquellas basadas en mecanismos de consenso de Prueba de Trabajo (PoW), pueden presentar limitaciones de escalabilidad en cuanto a la velocidad y el volumen de transacciones que pueden procesar. Esto se traduce en cuellos de botella y congestión, especialmente en escenarios de alta demanda, lo que afecta la experiencia del usuario y la eficiencia general del sistema. (Bit2me Academy, 2023c)

Una posible solución para este obstáculo serían las soluciones de capa 2. Implementar soluciones de segunda capa, como "Lightning Network" para Bitcoin o "Polygon" para Ethereum, que permiten procesar transacciones fuera de la cadena principal, mejorando la escalabilidad y reduciendo los costes.

2. Consumo de energía:

Los mecanismos de consenso como PoW demandan una gran cantidad de energía computacional para validar transacciones y asegurar la red. Este alto consumo energético ha generado críticas por su impacto ambiental y la sostenibilidad a largo plazo de la tecnología.

Esto sería contrarrestado por la optimización de los protocolos existentes, o con la creación de nuevos protocolos que requieran menos energía para validar transacciones. Además, esta energía tendría un menor impacto si se consiguiese y se promoviese el uso de fuentes de energía renovables. (Bit2me Academy, 2023c)

3. Regulación y cumplimiento:

El marco regulatorio y legal en torno a la tecnología *Blockchain* aún se encuentra en desarrollo en la mayoría de las jurisdicciones. La falta de claridad y lineamientos específicos genera incertidumbre para las empresas e instituciones financieras que buscan implementar soluciones incluyendo esta tecnología, dificultando su adopción generalizada.

Establecer un diálogo abierto y colaborativo con los reguladores y legisladores para desarrollar marcos regulatorios claros y adaptables a la tecnología sería una manera de mitigar los efectos negativos de esta situación. (Netflix & Hoffmann, 2020)

4. Privacidad y protección de datos:

Si bien la cadena de bloques ofrece un alto nivel de seguridad e inmutabilidad de los datos, también surgen preocupaciones en torno a la privacidad y protección de datos personales. Es crucial establecer mecanismos robustos para garantizar la confidencialidad de la información sensible y cumplir con las regulaciones de protección de datos. (Netflix & Hoffmann, 2020)

5. Interoperabilidad:

La existencia de diferentes plataformas con sus propios protocolos y formatos de datos dificulta la interoperabilidad entre ellas. Esta fragmentación limita la comunicación y el intercambio de información entre distintos sistemas, lo que podría obstaculizar la adopción generalizada de la tecnología.

Fomentar el desarrollo y la adopción de estándares comunes para la comunicación e interoperabilidad entre diferentes plataformas *Blockchain*, sería un punto clave en la adopción y desarrollo de esta tecnología. (Netflix & Hoffmann, 2020)

6. Aceptación y adopción por parte del usuario:

La adopción generalizada de *Blockchain* requiere un cambio significativo en el comportamiento y las preferencias de los usuarios. Se deben desarrollar interfaces amigables y fáciles de usar para que la tecnología sea accesible a un público amplio y fomentar su confianza en sus beneficios.

Implementar programas de educación y divulgación para aumentar la comprensión y confianza del público en la tecnología, así como desarrollar interfaces amigables y fáciles de usar que hagan que la red sea accesible y atractiva para un público amplio, ayudaría a que esta tecnología fuese adoptada por la población con mayor rapidez. (Bit2me Academy, 2023a)

7. Talento y capacitación:

La implementación y gestión de soluciones tecnológicas requiere personal con conocimientos técnicos especializados en criptografía, desarrollo de software y seguridad de redes. La escasez de talento capacitado en estas áreas podría obstaculizar la adopción de la tecnología en el sector financiero. (Buterin, 2014)

Fomentar la educación y capacitación en universidades y centros de formación para crear una fuerza laboral especializada en *Blockchain* sería una posible solución a este problema.

8. Gobernanza y gestión de redes:

Las redes *Blockchain* descentralizadas presentan desafíos en cuanto a la gobernanza y la toma de decisiones. Es necesario establecer mecanismos claros para la gestión de la red, la resolución de conflictos y la adaptación a cambios tecnológicos futuros.

9. Riesgos de seguridad:

Si bien esta tecnología ofrece un alto nivel de seguridad general, las redes y los sistemas asociados aún pueden ser vulnerables a ataques cibernéticos y hackeos. Es crucial implementar medidas de seguridad robustas y protocolos de gestión de riesgos para proteger los activos y la integridad de los datos.

Realizar auditorías y pruebas de seguridad regulares para identificar y mitigar vulnerabilidades en las redes y sistemas *Blockchain* harían que el público general y las grandes empresas confiasen más en estos sistemas. (CEU Digital & Monteverde, 2019)

10. Impacto en el empleo:

La automatización de procesos mediante contratos inteligentes y la disrupción de modelos de negocio tradicionales podrían generar impactos en el empleo en el sector financiero. Se deben considerar estrategias para mitigar estos efectos y reorientar la fuerza laboral hacia nuevas oportunidades en el entorno. (Puig, 2023)

Brindar oportunidades de reentrenamiento y capacitación a los trabajadores afectados por la automatización. Además de fomentar la creación de nuevos empleos en áreas como desarrollo de software, seguridad de redes y análisis de datos, hará que este efecto se mitigue.

3.7 Estudio acerca del potencial mercado.

Para saber el potencial del mercado más general en España, se ha elaborado una encuesta de 11 preguntas, cuyo objetivo era segmentar la situación actual en cuanto a conocimiento y adopción de esta tecnología por edades y sexos.

La intención principal es comprobar si realmente la población está desinformada o lo que existe es un desinterés general acerca de estos emergentes sistemas. Con la encuesta se pretende identificar las barreras y preocupaciones que impiden una mayor adopción de esta tecnología, así como evaluar el interés y la necesidad de educación sobre esta tecnología en el sistema educativo.

A través de esta investigación, se busca obtener una visión clara sobre cómo la sociedad española está interactuando con la cadena de bloques y qué medidas podrían fomentar una comprensión y adopción más amplia y efectiva.

Antes de mostrar y sacar conclusiones sobre los resultados obtenidos se va a explicar cada cuestión y sus posibles respuestas, clasificándolas en distintos segmentos del mercado.

La encuesta se ha difundido vía redes sociales y mediante grupos de whatsapp y se ha obtenido una muestra de 138 encuestados.

Los segmentos que se han definido son tres: Desconocedores, Informados apáticos y Entusiastas *Blockchain*.

Se clasificará como “Desconocedores” a aquellos que no sepan nada o casi nada sobre estos términos y/o su situación actual.

Se clasificará como “Informados apáticos” a aquellos que conozcan esta tecnología, sepan de su utilidad, pero no presenten un gran interés en sus aplicaciones o en usarla en el día a día.

Se clasificará como “Entusiastas *Blockchain*” a aquellos conocedores de la tecnología, pero además siendo usuarios asiduos de sus aplicaciones o utilidad.

3.7.1 Análisis de las Preguntas y respuestas de la encuesta.

Las dos primeras preguntas son únicamente para poder segmentar la población y sacar conclusiones posteriormente.

Pregunta número 1

“Indique su sexo”

La primera cuestión es acerca del sexo del encuestado, estableciendo como opciones el sexo masculino, el femenino y una tercera opción en caso de que el encuestado no se sienta identificado con ninguno.

Pregunta número 2.

” Indique su rango de edad”

La segunda cuestión es sobre la edad del encuestado, se establecen 3 franjas de edad. La primera franja será la de menores de 26 años, se llamará a este segmento de encuestados la población “joven”. Este segmento nació y creció en la era digitalizada. Se considera que su familiarización con la tecnología debería ser avanzada.

La segunda franja de edad será la población entre 26 y 45 años, este segmento serán los “adultos jóvenes”, que no nacieron en la era digital, pero si vieron cómo se desarrollaba mientras aun eran jóvenes, por lo que se considera que su familiarización con las nuevas tecnologías debería ser moderada.

La tercera franja de edad será la población mayor de 45 años, los “adultos mayores”, que no nacieron en la era digital y su evolución la vivieron siendo ya adultos jóvenes, por lo que se considera que su familiarización con estas nuevas tecnologías debería ser baja

Pregunta número 3

“¿Estás familiarizado o conoces la tecnología *blockchain* o las crypto divisas?”

Sí, estoy muy familiarizado.

Sí, tengo un conocimiento básico.

No, no las conozco ni se nada acerca de ello.

Esta pregunta es fundamental para establecer una base de conocimiento sobre la tecnología *blockchain* entre los encuestados. La familiaridad con la tecnología puede influir en la comprensión y percepción de las preguntas posteriores sobre su adopción y potencial.

Permite segmentar a los encuestados en función de su nivel de conocimiento inicial sobre *blockchain*, lo que ayuda a contextualizar sus respuestas posteriores y entender cómo se relacionan con su comprensión de la tecnología.

Pregunta número 4

“¿Has utilizado alguna vez una aplicación o plataforma que utilice *blockchain*?”

Sí, a título personal

Sí, en el ámbito profesional

No, nunca he utilizado ninguna aplicación que utilice *blockchain*.

Esta pregunta busca explorar la experiencia práctica de los encuestados con la tecnología *blockchain*, y si han tenido la oportunidad de interactuar con ella en aplicaciones o plataformas reales.

Proporciona información sobre el grado de adopción y experiencia de los encuestados con la tecnología *blockchain* en el ámbito práctico, lo que puede influir en su percepción y opinión sobre su utilidad y efectividad.

Pregunta número 5

“¿Qué nivel de confianza tienes en la seguridad y transparencia de las transacciones realizadas mediante *blockchain*?”

Muy alto

Neutral

Muy bajo

Esta pregunta explora la percepción de los encuestados sobre la seguridad y transparencia inherentes a las transacciones *blockchain*, aspectos fundamentales de su funcionamiento.

Permite evaluar la confianza de los encuestados en la tecnología *blockchain* como medio seguro y transparente para realizar transacciones, lo que puede afectar su disposición a adoptarla en sus actividades financieras y comerciales.

Pregunta número 6

"¿Crees que la tecnología *blockchain* tiene el potencial de transformar sectores como la banca en España?"

Sí, tiene un gran potencial.

Sí, pero su impacto será limitado.

No, no creo que tenga mucho impacto.

No estoy seguro/a.

Esta pregunta busca explorar la percepción de los encuestados sobre el potencial transformador de la tecnología *blockchain* en sectores clave de la sociedad española.

Proporciona información sobre la visión de los encuestados respecto a cómo la tecnología *blockchain* puede impactar en sectores fundamentales de la economía y la administración pública, lo que puede influir en su apoyo a iniciativas de adopción de *blockchain* en estos ámbitos.

Pregunta número 7

"¿Qué uso crees que tiene la tecnología *blockchain* en la sociedad española?"

Facilitar transacciones

financieras seguras.

Mejorar la trazabilidad.

Aumentar la transparencia.

Agilizar trámites administrativos.

Todas las anteriores.

Ninguna de las anteriores

Esta pregunta busca explorar la percepción de los encuestados sobre los posibles usos y aplicaciones de la tecnología *blockchain* en la sociedad española.

Proporciona información valiosa sobre la comprensión y visión de los encuestados sobre cómo la tecnología *blockchain* puede ser aplicada en diversos sectores y situaciones en España, lo que puede ayudar a identificar áreas de interés y potencial desarrollo.

Pregunta número 8

"¿Qué preocupaciones tendrías al utilizar tecnología *blockchain* en tu vida cotidiana?"

Privacidad y protección de datos

personales.

Seguridad de las transacciones.

Riesgo de ciberataques.

Complejidad en su uso.

Ninguna preocupación.

Esta pregunta permite comprender las preocupaciones y percepciones de los encuestados sobre los posibles riesgos o desafíos asociados con la adopción de la tecnología *blockchain* en su día a día, lo que puede ayudar a abordar estas preocupaciones con anticipación en futuras implementaciones.

Pregunta número 9

"¿Cuáles crees que son los principales obstáculos para una mayor adopción de la tecnología *blockchain* en la sociedad española?"

Falta de información y educación sobre *blockchain*.

Barreras regulatorias y legales.

Desconfianza en la tecnología.

Costes de implementación.

Otro…

Esta pregunta busca identificar las percepciones de los encuestados sobre los obstáculos que podrían limitar la adopción generalizada de la tecnología *blockchain* en España.

Proporciona información crucial sobre las barreras percibidas por los encuestados para la adopción de *blockchain*, lo que puede ayudar a identificar áreas de mejora y enfoque para promover su adopción en la sociedad española.

Pregunta número 10

"¿Qué opinas sobre la regulación de las criptomonedas y otros usos de la tecnología *blockchain* por parte del gobierno español?"

Debería ser más estricta.

Debería ser más flexible.

La regulación actual es adecuada.

No debería regularse en absoluto.

No estoy seguro/a.

Esta pregunta busca explorar las opiniones y actitudes de los encuestados hacia la regulación gubernamental de las criptomonedas y la tecnología *blockchain* en España.

Proporciona información sobre la percepción de los encuestados sobre la necesidad y la eficacia de la regulación gubernamental en el ámbito de las criptomonedas y la tecnología *blockchain*, lo que puede influir en el desarrollo futuro de políticas y normativas en este campo.

Pregunta número 11

"¿Consideras que la educación sobre tecnología *blockchain* debería ser parte del sistema educativo español?"

Sí, desde la educación primaria.

Sí, pero solo a nivel secundario y/o

universitario.

No estoy seguro/a.

No, creo que no es necesario.

Otro…

Esta pregunta indaga sobre la opinión de los encuestados sobre la integración de la educación sobre tecnología *blockchain* en el sistema educativo español.

Permite entender la percepción de los encuestados sobre la importancia de incluir la educación sobre tecnología *blockchain* en el currículo educativo, lo que puede influir en el apoyo a iniciativas de educación y formación en este ámbito.

3.7.2 Resultados de la encuesta.

Para su análisis se descargarán los resultados en un libro de EXCEL y se utilizarán tablas dinámicas para sacar conclusiones.

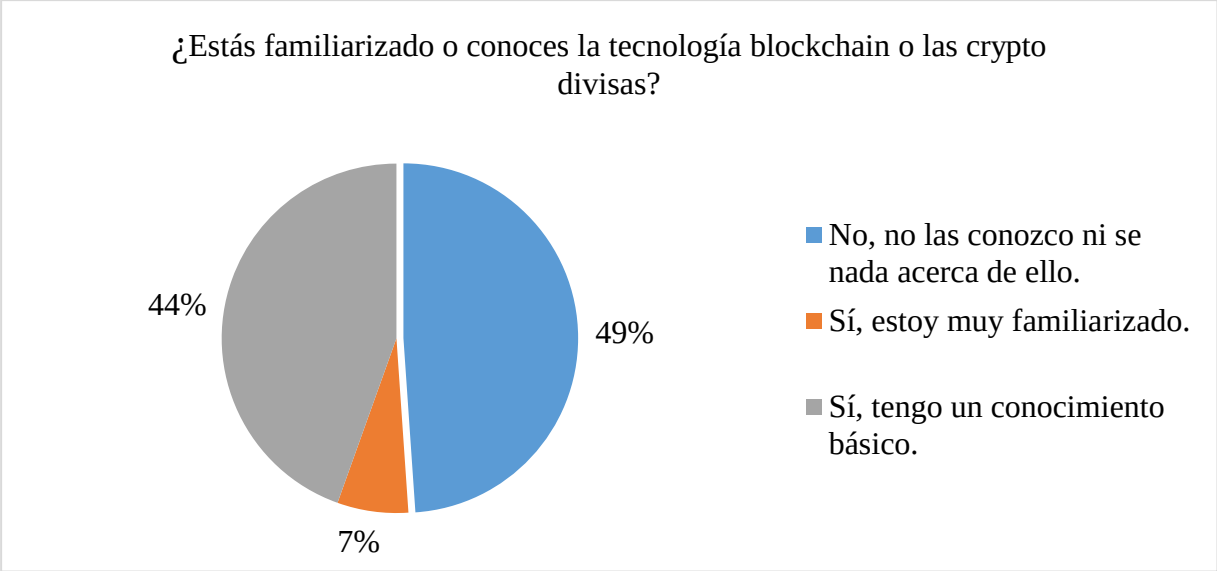
Preguntas 1 y 2.

En cuanto al sexo de los encuestados, se ha conseguido obtener respuestas de 60 hombres (43,5%) y de 78 mujeres (56,5%), un resultado muy similar, que era la intención del experimento, obtener una cantidad de respuestas muy similar en cuanto al sexo del encuestado.

Los rangos de edad han tenido una mayor diferencia en cuanto a los encuestados. La mayoría de los encuestados han sido "jóvenes", un 67,9%, seguido de "adultos mayores" conformando un 22,6% y por último los "adultos jóvenes" siendo el 9,5% restante.

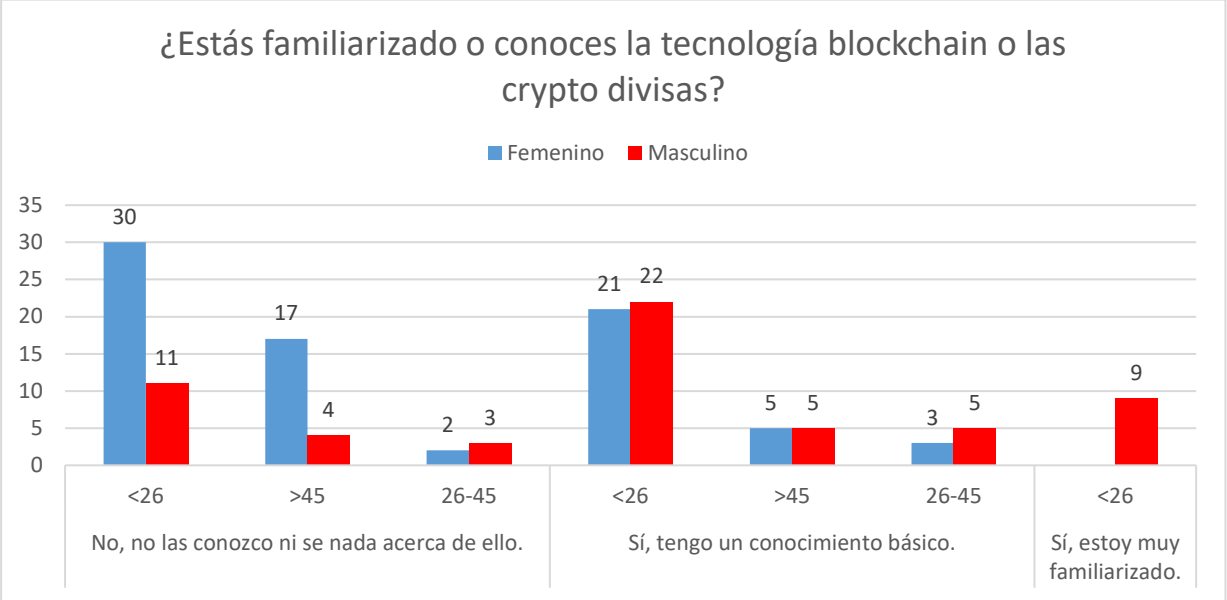
Pregunta 3.

Ilustración 7: Gráfico circular pregunta 3



Fuente: Elaboración propia en base a los resultados de la encuesta realizada.

Ilustración 8: Resultados pregunta 3



Fuente: Elaboración propia en base a los resultados de la encuesta realizada.

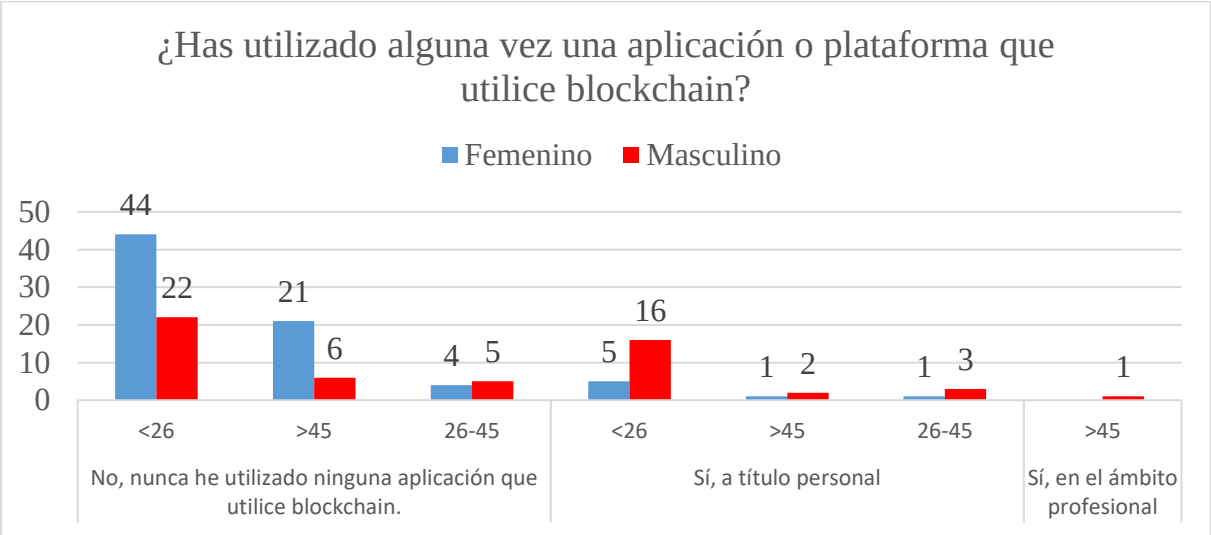
Los resultados se han filtrado por cada respuesta, posteriormente por el rango de edad que ocupan y por último por el sexo del encuestado.

La encuesta revela que la tecnología *blockchain* y las criptomonedas aún son relativamente desconocidas para la población, aunque existe un interés creciente, especialmente entre los jóvenes. Si bien el 51% de los encuestados ha oído hablar de estos conceptos, solo el 6,6% posee un conocimiento profundo. Las mujeres y los mayores de 45 años son los grupos que menos familiaridad presentan.

Esto muestra claramente una oportunidad de mercado, para que la tecnología alcance su máximo potencial, se recomienda que las empresas e instituciones inviertan en iniciativas educativas que aumenten la comprensión del público sobre *blockchain*.

Pregunta 4.

Ilustración 9: Resultados pregunta 4

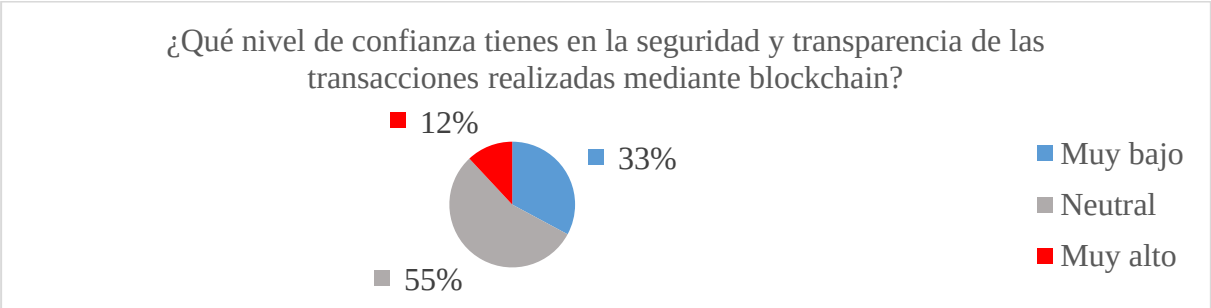


Fuente: Elaboración propia en base a los resultados de la encuesta realizada.

Estos resultados revelan que la mayoría de los encuestados nunca han utilizado una aplicación o plataforma que utilice *blockchain*. Sin embargo, un porcentaje significativo de ellos indicó haberlo hecho a título personal, mientras que un número mucho menor lo ha hecho en el ámbito profesional. Esto sugiere que, aunque la adopción de aplicaciones *blockchain* es aún limitada, hay un interés y una participación significativos, especialmente a nivel personal entre los jóvenes.

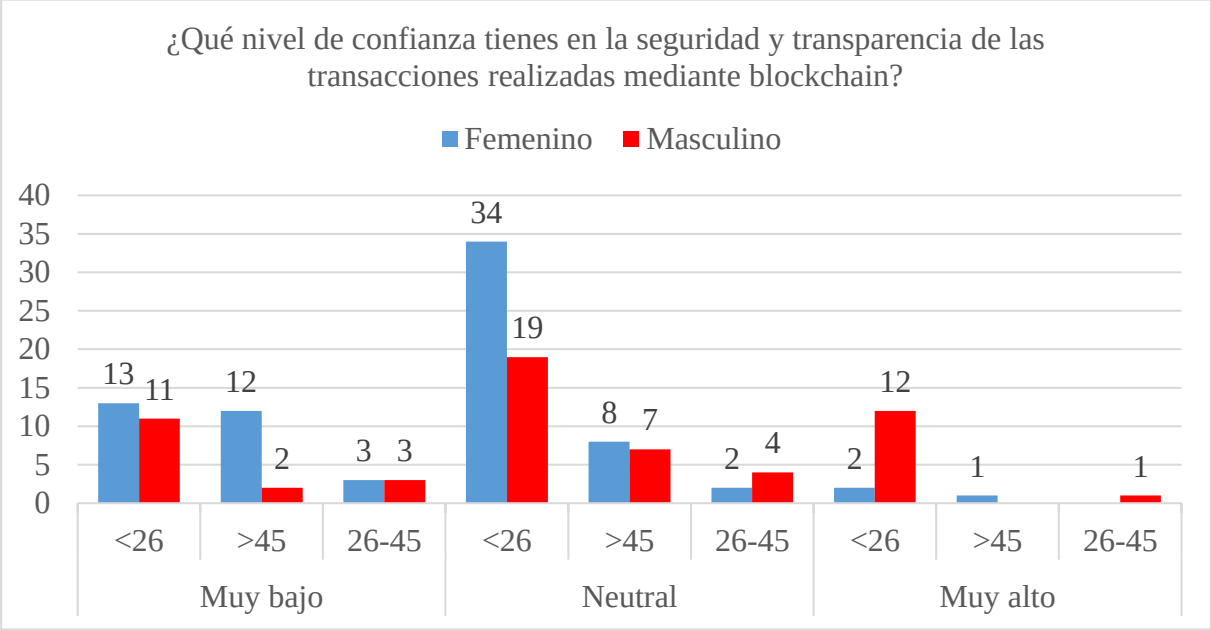
Pregunta 5.

Ilustración 10: Resultados pregunta 5



Fuente: Elaboración propia en base a los resultados de la encuesta realizada.

Ilustración 11: Resultados pregunta 5



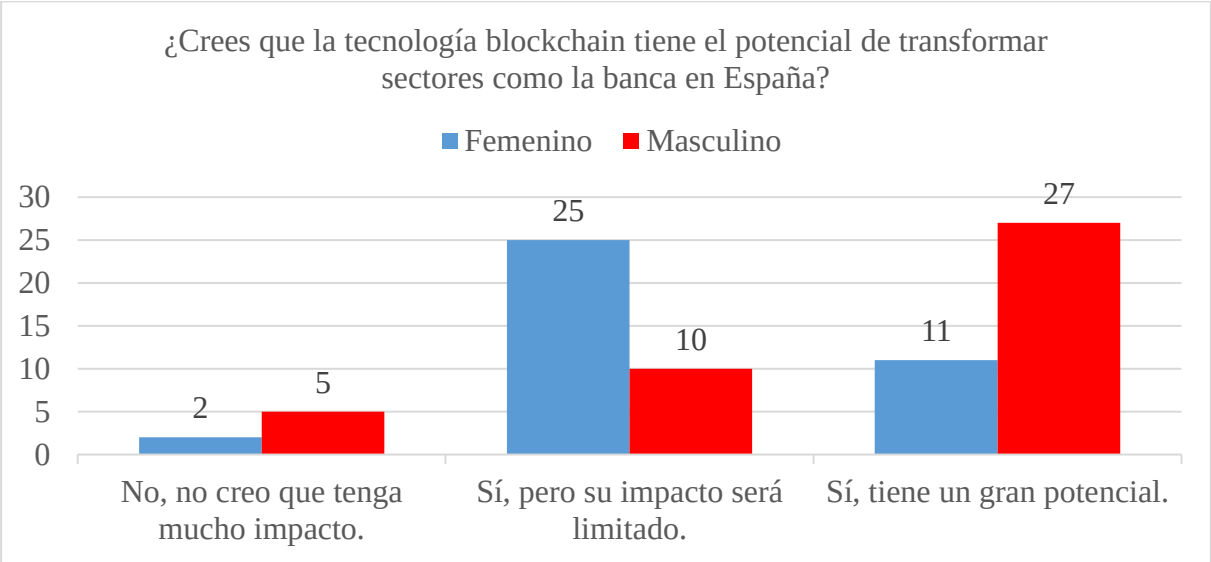
Fuente: Elaboración propia en base a los resultados de la encuesta realizada.

Estos resultados indican que la población no se cree o no conoce realmente las características de la *blockchain*, uno de los puntos revolucionarios en esta nueva industria es su transparencia y seguridad en su naturaleza. La gran mayoría es neutral en este aspecto, pero casi un tercio de la población considera su grado de confianza como “Muy bajo”, ligeramente más mujeres que hombres. Siendo altamente confiados en este aspecto los hombres jóvenes.

En conclusión, los hombres son ligeramente más propensos que las mujeres a expresar un alto nivel de confianza en la seguridad y transparencia de las transacciones *blockchain*. para aumentar aún más la confianza en la tecnología *blockchain*, es importante que se siga trabajando en la mejora de la seguridad y la transparencia de las transacciones.

Pregunta 6.

Ilustración 12: Resultados pregunta 6



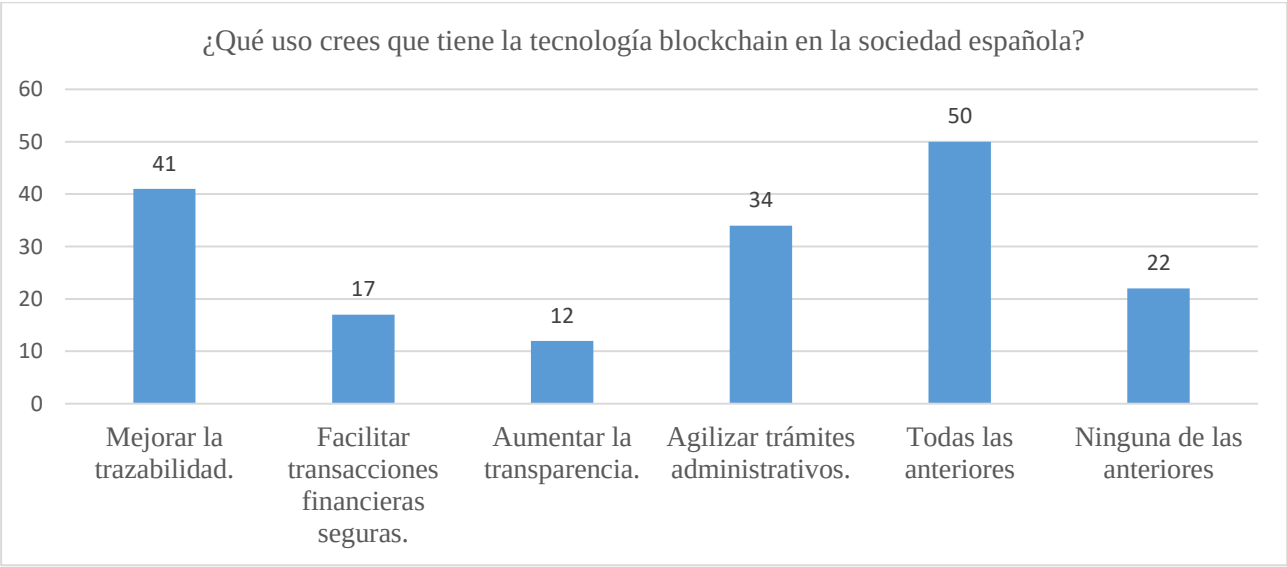
Fuente: Elaboración propia en base a los resultados de la encuesta realizada.

Para este gráfico se han excluido los encuestados que se han abstenido de responder. Los resultados obtenidos muestran que existe una pequeña brecha de género entre los encuestados, ya que las mujeres son mucho más moderadas en sus pensamientos acerca del potencial, como ya se ha visto con anterioridad los hombres tienen mucha más confianza en esta tecnología.

Además, se observa que una porción muy pequeña de la población no cree que esta tecnología pueda crear un gran cambio en el sector bancario español.

Pregunta 7.

Ilustración 13: Respuestas pregunta 7



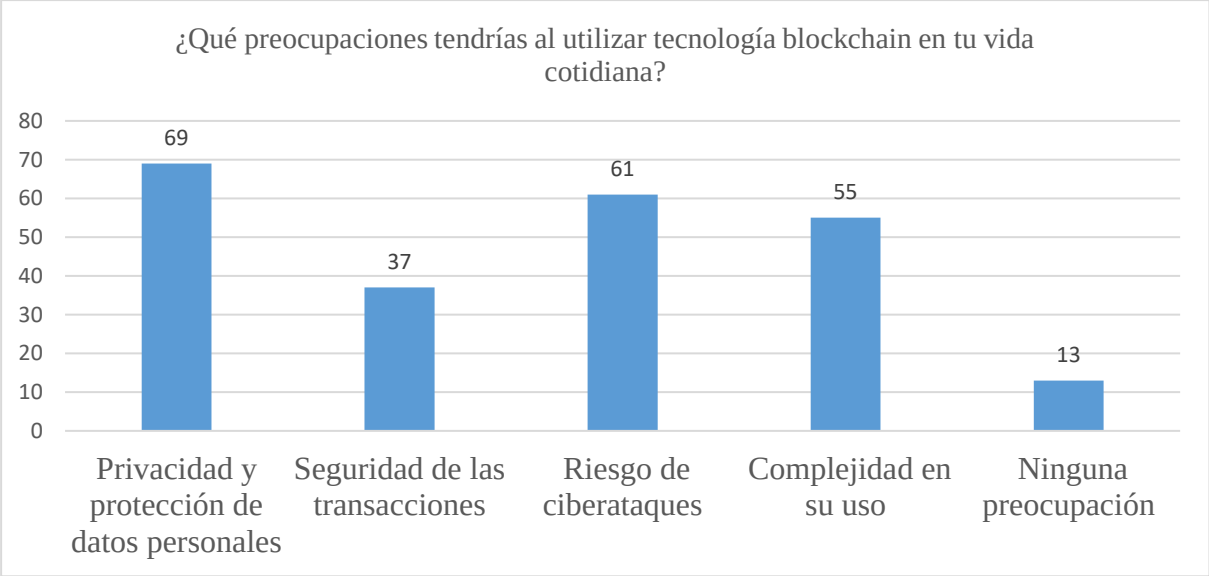
Fuente: Elaboración propia en base a los resultados de la encuesta realizada.

Estos resultados muestran que hay una percepción generalizada entre los encuestados sobre los diversos usos y beneficios de la tecnología *blockchain* en la sociedad española. La opción "Todas las anteriores" fue la más seleccionada, lo que indica que la mayoría de los encuestados reconocen el potencial de la tecnología para facilitar transacciones financieras seguras, mejorar la trazabilidad, aumentar la transparencia y agilizar trámites administrativos. Sin embargo, también es notable que un número significativo de encuestados seleccionaron "Ninguna de las anteriores", lo que sugiere que aún existe un segmento de la población que no ve claros los beneficios de la tecnología *blockchain* en la sociedad española, o que puede haber falta de comprensión sobre sus aplicaciones específicas.

En esta cuestión los resultados no se han segmentado por sexo y edad al considerarse suficientemente parejos para su estudio. Siendo más relevante la cantidad de respuestas obtenidas de cada opción.

Pregunta 8.

Ilustración 14: Resultados pregunta 8



Fuente: Elaboración propia en base a los resultados de la encuesta realizada.

Los resultados de la encuesta revelan una percepción generalizada entre los encuestados sobre los diversos usos y beneficios de la tecnología *blockchain* en la sociedad española. La mayoría reconoce su potencial para facilitar transacciones financieras seguras, mejorar la trazabilidad, aumentar la transparencia y agilizar trámites administrativos.

Sin embargo, también hay preocupaciones significativas, especialmente en torno a la privacidad y protección de datos personales, el riesgo de ciberataques y la complejidad en su uso. Estas preocupaciones subrayan la necesidad de una mayor educación y comprensión sobre cómo la tecnología *blockchain* aborda estos desafíos y cómo los usuarios pueden beneficiarse de su implementación adecuada. Es crucial abordar estas preocupaciones para promover una adopción más amplia y efectiva de la tecnología *blockchain* en la sociedad española.

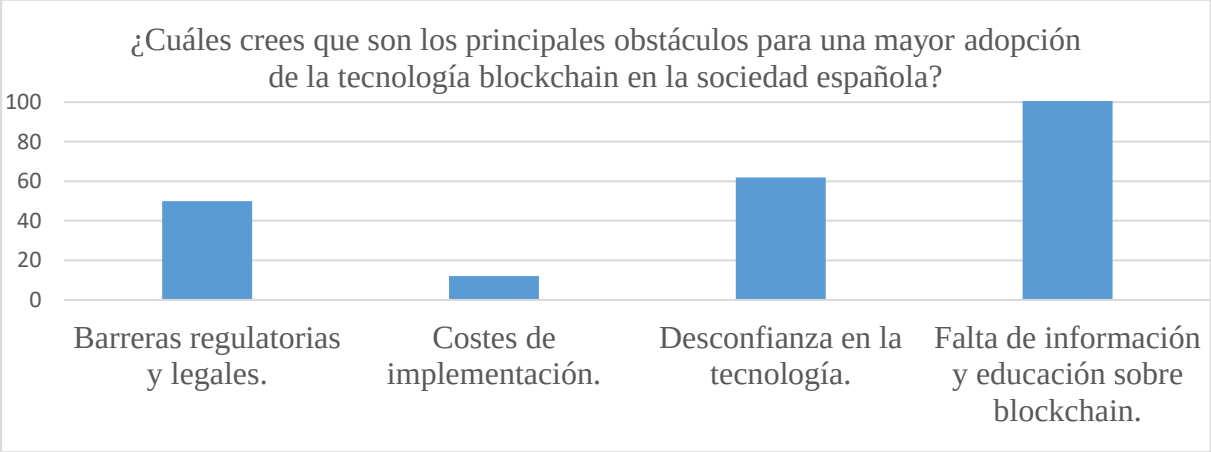
Aunque estas preocupaciones pueden parecer contradictorias con las características prometedoras de la tecnología *blockchain*, también subrayan la importancia de una

comprensión clara y una comunicación efectiva sobre cómo *blockchain* aborda estas preocupaciones y cómo los usuarios pueden beneficiarse de su implementación adecuada.

En esta cuestión los resultados no se han segmentado por sexo y edad al considerarse suficientemente parejos para su estudio. Siendo más relevante la cantidad de respuestas obtenidas de cada opción.

Pregunta 9.

Ilustración 15: Resultados pregunta 9



Fuente: Elaboración propia en base a los resultados de la encuesta realizada.

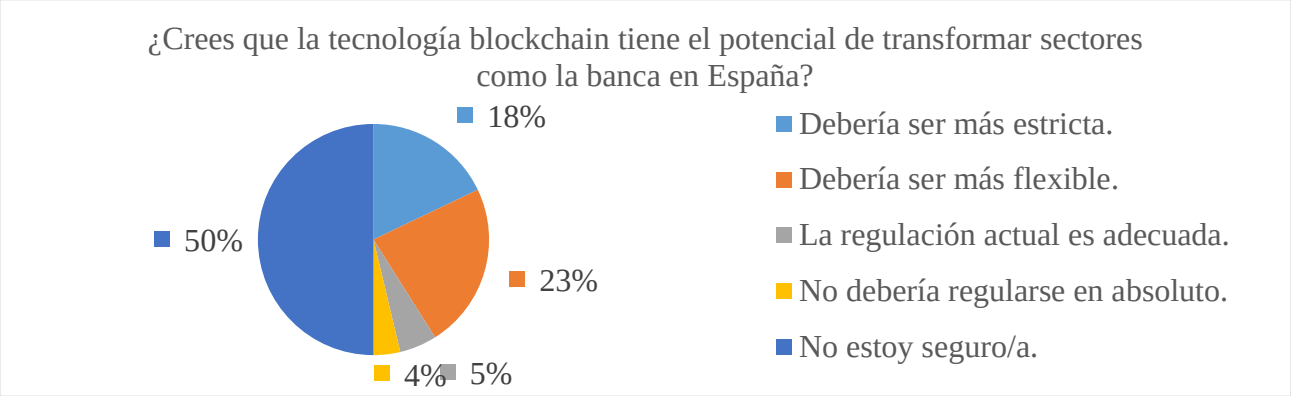
Los principales obstáculos para una mayor adopción de la tecnología *blockchain* en la sociedad española son multifacéticos. La falta de información y educación sobre *blockchain* es citada como la barrera más significativa, con un amplio consenso entre los encuestados. Esto destaca la necesidad de campañas educativas y programas de sensibilización para aumentar la comprensión pública sobre el potencial y los beneficios de la tecnología *blockchain*.

Además, las barreras regulatorias y legales, así como la desconfianza en la tecnología, también se identifican como obstáculos importantes. Estos desafíos subrayan la necesidad de un marco normativo claro y favorable, así como la importancia de generar confianza y credibilidad en la tecnología *blockchain* a través de casos de uso exitosos y transparencia en su implementación.

Los costes de implementación también se mencionan como un obstáculo, aunque en menor medida. Esto sugiere que, si bien los aspectos financieros pueden ser una preocupación, la falta de conocimiento y confianza en la tecnología son barreras más significativas que deben abordarse para fomentar una adopción más amplia de la tecnología *blockchain* en la sociedad española.

Pregunta 10.

Ilustración 16: Resultados pregunta 10



Fuente: Elaboración propia en base a los resultados de la encuesta realizada.

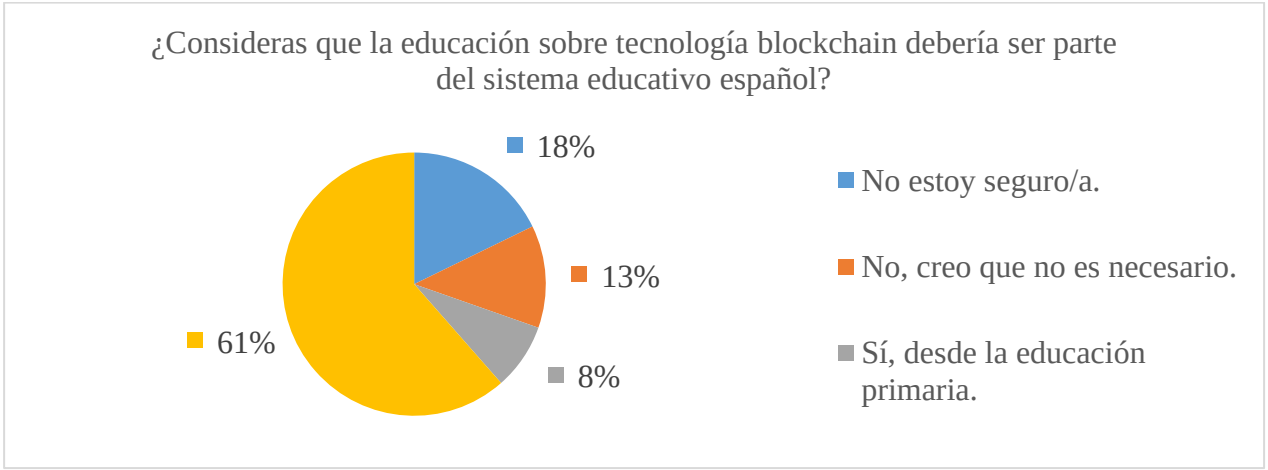
Los resultados muestran una división de opiniones entre los encuestados sobre la regulación de las criptomonedas y otros usos de la tecnología *blockchain* por parte del gobierno español. Una parte considerable de los encuestados expresó incertidumbre, lo que sugiere una falta de consenso o conocimiento sobre el tema.

Por otro lado, existe un grupo ligeramente mayor de encuestados que consideran que la regulación debería ser más flexible en lugar de estricta. Esta postura puede reflejar una inclinación hacia un enfoque más permisivo que permita la innovación y el desarrollo de nuevas aplicaciones de *blockchain* y criptomonedas en España.

Sin embargo, también hay una cantidad significativa de encuestados que opinan que la regulación debería ser más estricta. Esto puede deberse a preocupaciones sobre posibles riesgos asociados con el uso de criptomonedas, como el lavado de dinero, la evasión fiscal o la financiación del terrorismo, que podrían requerir medidas regulatorias más estrictas para mitigarlos.

Pregunta 11.

Ilustración 17: Resultados pregunta 11



Fuente: Elaboración propia en base a los resultados de la encuesta realizada.

Los resultados reflejan una amplia aceptación de la idea de incluir la educación sobre tecnología *blockchain* en el sistema educativo español, aunque con matices en cuanto a cuándo y cómo se debería integrar. La mayoría de los encuestados están a favor de incorporar la educación sobre *blockchain* en el nivel secundario y/o universitario, lo que sugiere el reconocimiento de la importancia de esta tecnología en el panorama actual y futuro.

Sin embargo, también hay un grupo significativo de encuestados que no están seguros o que no creen que sea necesario incluir la educación sobre *blockchain* en el sistema educativo. Esto puede reflejar la necesidad de más información y discusión sobre los beneficios y las implicaciones de integrar la tecnología *blockchain* en la educación, así como posibles desafíos y limitaciones asociadas con su implementación.

Los resultados de la encuesta revelan que un gran segmento de la población, aproximadamente el 50%, mayoritariamente compuesto por los adultos de más edad, sigue siendo desconocedora de la tecnología *blockchain*, sin tener conocimiento ni haber utilizado aplicaciones relacionadas.

Un grupo considerable sobre el 35%, tiene un conocimiento básico y puede haber interactuado con *blockchain* en algún grado, pero no muestra un gran interés activo, que serían los “Informados apáticos”.

Finalmente, un grupo más pequeño pero significativo que sería el 15% restante, está bien informado y es entusiasta, reconociendo el valor de la tecnología *blockchain* y apoyando su integración en el sistema educativo. Estos resultados subrayan la necesidad de mayor educación y sensibilización sobre *blockchain* para aumentar la adopción y confianza en esta tecnología emergente.

(III) CONCLUSIONES.

En el presente Trabajo de Fin de Grado, se ha realizado una inmersión profunda en la tecnología *blockchain* y su potencial para revolucionar el panorama financiero español. Tras un análisis detallado de los conceptos fundamentales, la historia y los orígenes de la criptografía, el funcionamiento y las aplicaciones de la tecnología, se ha explorado en profundidad cómo esta tecnología puede abordar las deficiencias existentes en el sistema financiero actual. Se ha destacado la capacidad de *blockchain* para optimizar la eficiencia de los procesos financieros, reduciendo costes y agilizando trámites. La transparencia inherente a esta tecnología permite un mayor control y trazabilidad de las transacciones, combatiendo el fraude y generando confianza entre los participantes. La seguridad robusta que ofrecen las redes basadas en criptografía y consenso distribuido, protegen los datos financieros de manera inigualable. Además, *blockchain* tiene el potencial de promover la inclusión financiera, brindando acceso a servicios financieros a sectores tradicionalmente excluidos.

Tras lo anterior, se expusieron posibles retos que la implantación y adopción de esta tecnología ya está confrontando y se cree que confrontará en el futuro, siendo visible que ni mucho menos estas aplicaciones están en un nivel de madurez elevado, abriendo la puerta a la posibilidad de que nunca sean adoptadas.

Para evaluar el nivel de conocimiento y familiaridad de la población española con *blockchain*, se diseñó y ejecutó una encuesta a una muestra significativa de 138 individuos. Los resultados obtenidos revelaron que, si bien existe un segmento poblacional considerable que aún no está familiarizado con la tecnología, también hay un número considerable de personas que la reconocen y comprenden sus beneficios potenciales.

A la luz del análisis realizado y los resultados de la encuesta, se puede afirmar con rotundidad que la tecnología *blockchain* posee un potencial transformador sin precedentes para el sector financiero español. Su implementación estratégica puede conducir a la creación de un sistema financiero más eficiente, transparente, seguro e inclusivo, beneficiando tanto a las entidades financieras como a los usuarios finales.

Sin embargo, para materializar este potencial transformador, es fundamental abordar ciertos desafíos. Es necesario aumentar significativamente la inversión en investigación y desarrollo de *blockchain*. La colaboración entre el sector público y privado es crucial para establecer estándares y regulaciones claras que propicien un entorno operativo seguro.

La educación y formación en torno a la cadena de bloques son otros pilares fundamentales para impulsar su adopción. De confiar en su utilidad, se deben desarrollar programas educativos dirigidos a profesionales del sector financiero, permitiéndoles adquirir las competencias necesarias para aprovechar al máximo las capacidades de esta tecnología.

Es imperativo fomentar el desarrollo de aplicaciones prácticas y adaptadas a las necesidades específicas del sector financiero español. Estas aplicaciones deben abordar los problemas y desafíos más acuciantes que enfrenta el sistema actual, optimizando procesos, mejorando la transparencia y reforzando la seguridad.

Sensibilizar y educar a la población es otro punto imprescindible para tener en cuenta. Implementar campañas de sensibilización y educación para aumentar el conocimiento y la comprensión de la tecnología entre la población española, generando confianza y promoviendo su adopción responsable.

(V) BIBLIOGRAFÍA.

Aldeco-Perez, R., & Rajsbaum, S. (2022). ¿Qué es *Blockchain*? *ResearchGate*. https://www.researchgate.net/publication/366570202_Que_es_*Blockchain*

Asociación Española de Banca. (s. f.). *Estadísticas de la zona euro - Asociación Española de Banca*. https://www.aebanca.es/estadisticas-de-la-zona-euro/

Asociación Española de Banca. (2024, 4 noviembre). *Informe 2023 - Asociación Española de Banca*. https://www.aebanca.es/asamblea-aeb/pdf/informe

Banco de España. (2022). *La lucha contra la falsificación*. Recuperado 22 de abril de 2024, de https://www.bde.es/wbe/es/areas-actuacion/billetes-monedas/lucha-contra-falsificacion/

Bit2me Academy. (2023a, marzo 31). ¿Cómo funciona la Cadena de Bloques (*Blockchain*) ?- Bit2Me Academy. *Bit2Me Academy*. Recuperado 23 de abril de 2024, de https://academy.bit2me.com/como-funciona-*blockchain*-cadena-de-bloques/

Bit2me Academy. (2023b, abril 6). ¿Qué es un Árbol Merkle? *Bit2Me Academy*. Recuperado 23 de abril de 2024, de https://academy.bit2me.com/que-es-un-arbol-merkle/

Bit2me Academy. (2023c, mayo 17). Escalabilidad de Bitcoin: Bitcoin para 7000 millones de personas. *Bit2Me Academy*. Recuperado 13 de mayo de 2024, de https://academy.bit2me.com/que-es-escalabilidad-de-bitcoin/

BIZUM. (2024, 10 enero). *¿Cuál es el importe máximo Bizum?* Bizum. Recuperado 22 de abril de 2024, de https://bizum.es/blog/importe-maximo-bizum/

blockchain.info. (2024). *Blockchain Explorer - Bitcoin Tracker & more | Blockchain.com*. Recuperado 22 de abril de 2024, de https://*blockchain*.info/

Buterin, V. (2014). *WHitepaper Ethereum* [Comunicado de prensa].

CEPYME. (2023). *Indicador CEPYME sobre la situación de las pymes 2ºTri2023 – Cepyme*. Recuperado 25 de abril de 2024, de https://cepyme.es/indicador-cepyme-sobre-la-situacion-de-las-pymes-2otri2023/

CEU Digital, & Monteverde, C. (2019, 18 enero). *Blockchain y su aplicación en el ámbito financiero* [Vídeo]. YouTube. Recuperado 23 de abril de 2024, de https://www.youtube.com/watch?v=lkO168P39Z0

Chaum. (1989). *Advances in Cryptology - CRYPTO '89: Proceedings*. Springer.

Cointelegraph. (s. f.). *A beginner's guide to the different types of blockchain networks*. Recuperado 23 de abril de 2024, de https://es.cointelegraph.com/learn/a-beginners-guide-to-the-different-types-of-*blockchain*-networks

Deloitte. (s. f.-a). *Blockchain & Digital assets*. Deloitte United States. Recuperado 25 de abril de 2024, de https://www2.deloitte.com/us/en/pages/about-deloitte/solutions/*blockchain*-and-digital-assets.html

Deloitte. (s. f.-b). *Blockchain & Digital assets*. Deloitte United States. Recuperado 7 de mayo de 2024, de https://www2.deloitte.com/us/en/pages/about-deloitte/solutions/*blockchain*-and-digital-assets.html

Glassnode. (s. f.). *Glassnode - On-chain market intelligence*. https://glassnode.com/

Godoy, G. (2023, 18 noviembre). Criptomonedas: ¿una solución para las remesas entre España y Latinoamérica? *Cointelegraph*. Recuperado 13 de mayo de 2024, de https://es.cointelegraph.com/news/cryptocurrencies-a-solution-for-remittances-between-spain-and-latin-america

Godoy, G. (2024, 27 marzo). Bancos, fintechs y cripto: ¿El futuro de las remesas? *Cointelegraph*. Recuperado 13 de mayo de 2024, de https://es.cointelegraph.com/news/banks-fintechs-and-crypto-the-future-of-remittances

Gutiérrez, H., Gutiérrez, H., & Gutiérrez, H. (2023, 6 octubre). Las reclamaciones por fraude de los clientes ante el Banco de España se duplicaron en 2022. *Cinco Días*. https://cincodias.elpais.com/companias/2023-10-06/las-reclamaciones-por-fraude-de-los-clientes-ante-el-banco-de-espana-se-duplicaron-en-2022.html

Haber, & Stornetta, W. (1991). *Journal of Cryptology*. https://doi.org/10.1007/BF00196791

IBM. (2024). *Beneficios de blockchain - IBM Blockchain | IBM*. Recuperado 13 de mayo de 2024, de https://www.ibm.com/es-es/topics/benefits-of-*blockchain*

Kriptomat. (s. f.). *¿Qué es una billetera de blockchain y cómo funciona?* Recuperado 23 de abril de 2024, de https://kriptomat.io/es/*blockchain*/que-es-billetera-de-blockchaina/

Ministerio de Industria. (2023). *Ministerio de Industria y Turismo - Marco estratégico en política de PYME*. Recuperado 22 de abril de 2024, de https://industria.gob.es/es-es/servicios/paginas/marco-estrategico-politica-pyme.aspx

Mit Media Lab. (2021, 23 mayo). *The Limits to Blockchain Scalability*. Recuperado 8 de mayo de 2024, de https://vitalik.eth.limo/general/2021/05/23/scaling.html

Nakamoto. (2008, 31 octubre). *Bitcoin Whitepaper*. metzdowd.com. Recuperado 23 de abril de 2024, de https://bitcoin.org/bitcoin.pdf

Narula. (2021). *Blockchain technology for beginners: A comprehensive guide to understanding, evaluating, and implementing blockchain solutions.*

Netflix, & Hoffmann, T. (2020). *CRYPTOPIA: Bitcoin, Blockchains and the Future of the Internet. Torsten Hoffmann* [Vídeo]. YouTube. Recuperado 23 de abril de 2024, de https://www.youtube.com/watch?v=Y2qe3hFeQ5g

Observatorio *Blockchain*. (2023, 3 noviembre). *Los 3 principales tipos de redes Blockchain - Hypernifty Academy*. Recuperado 23 de abril de 2024, de https://observatorioblockchain.com/hypernifty/redes-*blockchain*-tipos/

Público. (2023, 9 septiembre). *¿Altas comisiones al enviar dinero? Cuidado con esta tasa*. Consumo - Público. Recuperado 22 de abril de 2024, de https://www.publico.es/ahorro-consumo-responsable/envio-dinero-altas-comisiones/

Puig, A. T. (2023, 10 mayo). *El impacto de la tecnología Blockchain en el tejido empresarial - Mel - Management & eLearning*. Mel - Management & eLearning. https://blogs.uoc.edu/mel/es/el-impacto-de-la-tecnologia-*blockchain*-en-el-tejido-empresarial/

Saleem, E. (2023, 23 noviembre). The M2 and Bitcoin Connection: Unravelling the Ties Between Money Supply and Digital Gold. *Medium*. https://medium.com/@eemansaleem/the-m2-and-bitcoin-connection-unravelling-the-ties-between-money-supply-and-digital-gold-0051bcb1752f

Szabo, N. S. (1996). *Nick Szabo -- Smart Contracts: Building Blocks for Digital Markets*. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

World Economic Forum. (s. f.). *WEF Blockchain Toolkit*. WORLD ECONOMIC FORUM. Recuperado 13 de mayo de 2024, de https://widgets.weforum.org/*blockchain*-toolkit/introduction/index.html