Universidad Zaragoza
1542

Trabajo Fin de Grado

Tecnología blockchain: una propuesta de aplicación a la bolsa española

Autor

Saúl Ortega Martínez.

Director

Jose Luis Sarto Marzal.

Facultad de Economía y Empresa.

Curso 2021/2022.

Autor del trabajo: Saúl Ortega Martínez

Director del trabajo: Jose Luis Sarto Marzal

Título del trabajo: Tecnología Blockchain: una propuesta de aplicación a la bolsa española

Work title: Blockchain technology: a proposal for application to the Spanish stock market

Titulación: Grado en Finanzas y contabilidad

Resumen: Desde el auge de las criptomonedas en 2020, las palabras cadena de bloques están en boca de todos. Debido a mi interés personal y la población en general en ahondar en el término, en este trabajo se describirá la tecnología Blockchain. Por su inminente incorporación, es un tema del cual creo que todos deberíamos saber.

En este TFG se ofrece una explicación clara, pero completa, de qué es la cadena de bloques desde un marco teórico. Además, se expondrán las diferentes aplicaciones al sector financiero, demostrando que en el futuro estará mucho más extendida con una propuesta de aplicación al mercado de valores español y por qué puede revolucionar un área que ha permanecido con un procedimiento similar durante muchos años.

Abstract: Since the cryptocurrency boom in 2020, the words blockchain are on everyone's lips. Due to my personal interest and the general population in delving into the term, Blockchain technology will be described in this work. Due to its imminent incorporation, it is a topic that I think we should all know about.

This TFG offers a clear but complete explanation of what the blockchain is from a theoretical framework. In addition, the different applications to the financial sector will be exposed, demonstrating that in the future it will be much more widespread with a proposal for application to the Spanish stock market and why it can revolutionize an area that has remained with a similar procedure for many years.

Índice

1. Introducción 5

1.1. Motivaciones: 5

1.2. Objetivos: 5

1.3. Transcendencia: 6

1.4. Contenido y distribución: 6

2. Tecnología Blockchain: 8

2.1. ¿Qué es blockchain? 8

2.2. ¿Cuál es su origen? 8

2.3. ¿Cómo funciona? 10

2.4. Tipos de redes Blockchain 11

2.5. Barreras regulatorias a las que se enfrenta una red pública 13

2.6. Glosario de términos. 14

3. Aplicaciones de Blockchain a las finanzas 16

3.1. Criptomonedas 16

3.1.1. Características 17

3.1.2. Marco regulatorio internacional 17

3.1.3. Bitcoin 18

3.1.3.1. ¿En qué consiste el minado de Bitcoin? 19

3.1.3.2. Cómo realizar una transacción con Bitcoin 20

3.2. Smart contracts 21

4. Propuesta de aplicación a la bolsa española 22

5. Conclusiones 27

6. Bibliografía 28

Índice de figuras

Figura 2.2.1: Ejemplo de árbol de Merkle……...9

Figura 2.3.1: Pasos para explicar el funcionamiento de blockchain……...11

Figura 2.4.1: Tipos de redes Blockchain…….13

Figura 3.1.1: Criptomonedas más importantes por capitalización de mercado……...16

Figura 3.1.2.1: Mapa de los países que han prohibido las criptomonedas……..18

Figura 3.1.3.1: Evolución del precio de Bitcoin……..19

Figura 4.1: Esquema de funcionamiento actual de la bolsa española…….23

Figura 4.2: Esquema de funcionamiento de la propuesta de aplicación
de blockchain en la bolsa española……..24

1. Introducción

1.1. Motivaciones:

Desde el boom de las criptomonedas en 2020 me ha llamado mucho la atención este tipo de activos financieros, por lo que no he dejado de seguir el comportamiento de las diferentes criptos y tratar de conocer más acerca de ellas y su funcionamiento.

En mi búsqueda de información encontré que estas monedas descentralizadas se desarrollan principalmente con una tecnología denominada blockchain. Indudablemente, ambas se tratan de una gran revolución comparable a la llegada de internet y su aplicación es inminente en muchas áreas actuales, entre las que destacan la banca, política, legal, gubernamental…

Grandes empresas invierten importantes cantidades de recursos para adaptarse a esta nueva tecnología, sin embargo, no muchos conocen sus características ni posibilidades porque, como he podido comprobar, los estudios académicos o investigaciones son prácticamente inexistentes dificultando la disposición de esta información desde fuentes fiables.

Pero, sin lugar a duda, lo que me lanzó a elegir este tema para mi trabajo de fin de grado fue leer una noticia en la que se exponía que Rusia, podría evitar gran parte de las sanciones económicas impuestas por occidente mediante el pago de criptomonedas. Y es que la cadena de bloques no necesita un organismo central que valide las operaciones y por tanto, no hay ninguna institución que pueda evitar la realización de las transacciones. Esto marca un antes y un después en las finanzas mundiales.

Por todas las razones expuestas, en este trabajo busco aprender todos los aspectos relacionados con esta tecnología y ofrecer una definición lo más amplia y precisa posible para todo el público interesado en el tema.

1.2. Objetivos:

El objetivo principal de la realización de este trabajo fin de grado es aportar una información útil y completa sobre qué es la tecnología blockchain y aspectos relacionados con ella. Esto también se fundamenta en que, la falta de estudios o investigaciones

académicas no facilita el conocimiento haciendo que se tomen decisiones precipitadas con las que se incurre en pérdidas o no realizar inversiones muy rentables.

Por otro lado, explicar los usos que tiene la cadena de bloques en el área financiera tanto actuales como potenciales, para lo que se ha desarrollado una propuesta de aplicación a la bolsa española para demostrar su utilidad y versatilidad.

1.3. Transcendencia:

Este trabajo tiene tres tipos de trascendencia que explicaré a continuación:

Por un lado, quiero que tenga utilidad pública, es decir, que sirva de guía para aquellos interesados en aprender de esta tecnología, aportando conocimiento y reduciendo el sesgo de la información disponible en internet que deriva, en muchas ocasiones, en decisiones precipitadas o mal tomadas.

Por otro lado, me gustaría que la propuesta aportada no se limite al ámbito académico, sino que su aplicación pueda llegar a extenderse en un futuro. Ya que, considero que con el paso del tiempo en las bolsas mundiales se acabará implantando una iniciativa muy similar a la planteada. Blockchain es el futuro y su aplicación en todos los ámbitos actuales es solo cuestión de tiempo y más en el sector financiero, donde ya ha demostrado múltiples beneficios.

Finalmente, también quiero que incite a empresarios y emprendedores a que comiencen a incorporar la cadena de bloques a sus negocios, no solo por todas las bonanzas que se van a exponer, sino porque su planteamiento no es muy costoso hablando de tiempo.

1.4. Contenido y distribución:

El contenido del siguiente trabajo se distribuye en varias partes bien diferenciadas:

En un primer lugar, podemos encontrar la introducción, donde aparecerán las motivaciones que me han llevado a elegir este tema, los objetivos que busco alcanzar, la utilidad y trascendencia que espero obtener para el futuro y finalmente el contenido y distribución del trabajo.

La segunda parte se trata de un marco teórico en el que contextualizaré la tecnología Blockchain y donde podremos conocer su definición, origen, tipos …

Seguidamente se podrá encontrar las aplicaciones actuales al ámbito de las finanzas. Por un lado, las criptomonedas, con especial énfasis en Bitcoin, por ser la criptodivisa original y la principal en términos de capitalización de mercado. Por otro lado, también los contratos inteligentes.

En cuarto lugar, veremos la propuesta de aplicación a la bolsa española donde primeramente introduciré el sistema bursátil en la actualidad, para después explicar en detalle el diseño del nuevo funcionamiento destacando sus posibles ventajas e inconvenientes.

En la quinta parte, encontraremos las conclusiones donde apreciar una valoración global del trabajo.

Finalmente, en el apartado bibliográfico aparecerán todas las fuentes consultadas y utilizadas en la elaboración de este trabajo, agrupadas en libros, artículos y páginas web.

2. Tecnología Blockchain:

2.1. ¿Qué es blockchain?

(Davis, 2022) lo ha contextualizado como un libro mayor resistente a las manipulaciones para la transacción de activos digitales entre personas que no tienen por qué confiar entre ellas, ya que el protocolo de consenso garantiza la seguridad y veracidad de la información.

Por otra parte, (Preukschat, 2017) define blockchain como una base de datos distribuida entre muchos participantes, protegida criptográficamente y organizada en bloques de varias transacciones relacionadas entre sí matemáticamente.

Por último, (BBVA) sostiene que blockchain no solo es una base de datos, sino un conjunto de tecnologías que permiten la transmisión de un valor o un activo sin la necesidad de intermediación por parte de una autoridad monetaria ni otros terceros implicados.

A pesar de que estas definiciones no difieren mucho entre sí, cabe destacar que la información siempre es transparente, ya que cada ordenador conectado a la base de datos tiene una copia de toda la cadena y en ningún caso será posible editar o borrar nada validado y añadido previamente sin el permiso de toda la red. Cada ordenador participante es un bloque de la cadena y, por tanto, contiene: Un enlace al bloque anterior, la fecha de registro y los datos de la transacción (Allende López, 2018) y (Berenguer, 2017).

2.2. ¿Cuál es su origen?

Antiguamente, gobiernos e instituciones hacían uso de bases de datos para registrar transacciones e información, por ejemplo, conocer la propiedad de la tierra. Con este sistema siempre ha sido necesaria la supervisión y presencia de una entidad central a fin de gestionar el flujo de transacciones. Debido a la confianza que los usuarios depositan en este intermediario, podían intercambiar activos sin conocerse. La función de estos mediadores era aportar la confianza necesaria entre ambas partes y registrar la información oficialmente.

A partir de la crisis financiera de 2008, los bancos y grandes instituciones financieras pierden la confianza de la población en general, propiciándose un escenario idóneo para

el desarrollo de una tecnología que permita a los usuarios realizar transacciones sin la supervisión de un intermediario.

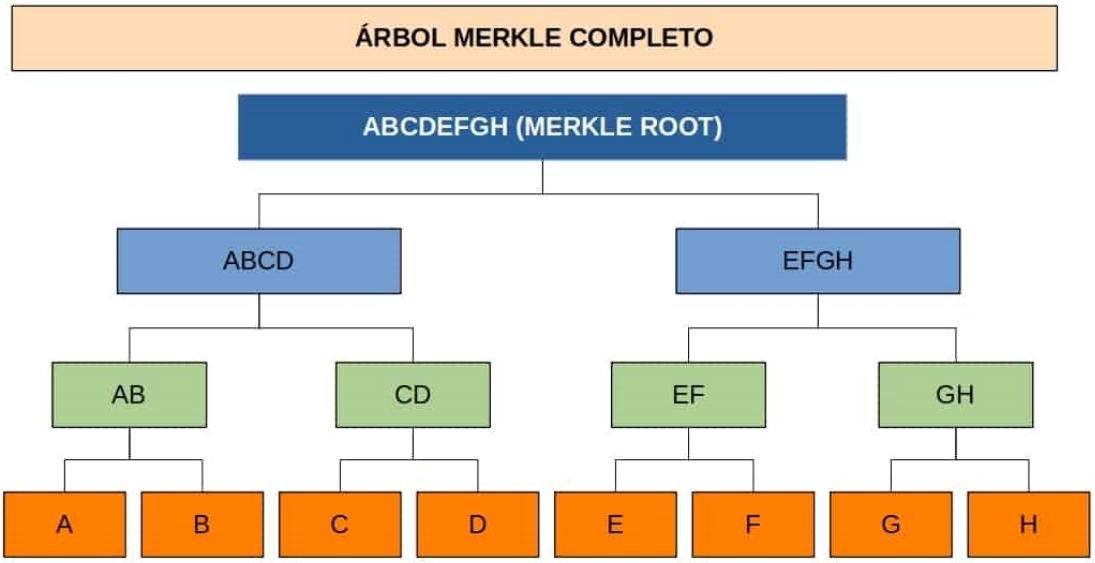
Aprovechando este momento de incertidumbre, una persona o grupo anónimo bajo el pseudónimo de Satoshi Nakamoto crearon un nuevo sistema de pago electrónico entre pares que empleaba una criptomoneda, llamada Bitcoin.

Así, surge una alternativa a estos registros ineficientes en tiempo y costes a pesar de los avances tecnológicos. Esta nueva opción sustituye al intermediario en su tarea de aportar legitimidad a las transacciones, gracias a su distribución y un sistema de algoritmos e incentivos denominado minería. (Binance,2021)

Sin embargo, a pesar de que Bitcoin es la primera aplicación práctica de esta tecnología, la base teórica es muy anterior. En 1991, los investigadores Haber y Stornetta querían diseñar una solución a la manipulación de los archivos digitales por lo que plantearon la primera cadena de bloques criptográficamente asegurada.

Este sistema almacenaba los documentos con un sello de tiempo, aunque en 1992 lo pusieron en funcionamiento incorporando al diseño árboles de Merkle. Su diseño en forma de árbol posibilitó que cada hoja pudiese almacenar información de forma más segura, ya que dependía a su vez de otras hojas.

Figura 2.2.1: Ejemplo de árbol de Merkle.



Fuente: Amano, 2019

La falta de éxito en la propuesta propició un abandono de la patente, que caducó en 2004.

En este mismo año, el informático Finney creó el sistema RPoW (Reusable Proof of Work – Prueba de trabajo reutilizable). A su vez, creó un token firmado criptográficamente y transferible entre personas. RPoW suponía la solución al doble gasto, registrando en un servidor confiable la propiedad de los tokens que permitía a cualquier usuario verificar su veracidad en tiempo real. (Amano, 2019)

Algunos expertos consideran este sistema como un prototipo y punto de partida para el diseño de la tecnología Blockchain.

2.3. ¿Cómo funciona?

Para explicar el funcionamiento de la cadena de bloques, vamos a basarnos en 6 pasos (Allende López, 2018)

Paso 0**:** Para formar parte de una blockchain, hay dos alternativas en función del tipo de red al que se quiera unir. Si se busca incorporar a una cadena pública, hay que descargarse una aplicación ya que cualquiera puede participar. O, por el contrario, para unirse a una cadena de bloques privada o federada es necesario acceder vía web, sin embargo, en estas redes hay unos nodos privilegiados que la administran y deciden quien puede ingresar.

Paso 1**:** Justo después de que los usuarios se conecten a la cadena, esta enviará la información de las transacciones que realice a los nodos inmediatamente anteriores y posteriores. Instantáneamente, cada nodo comprueba que la información recibida sea válida (Por ejemplo, el dinero enviado sea real o no haya sido gastado con anterioridad). En ese caso, cada nodo la añade a su base de transacciones o "pool" y la reenvía a los nodos a los que está conectado. Este proceso continúa hasta que un nodo recibe información ya almacenada previamente, la cual ignora.

Paso 2**:** Cada nodo introduce las transacciones que recibe en su pool, que puede diferir entre nodos debido al orden en el que cada uno ha recibido la información.

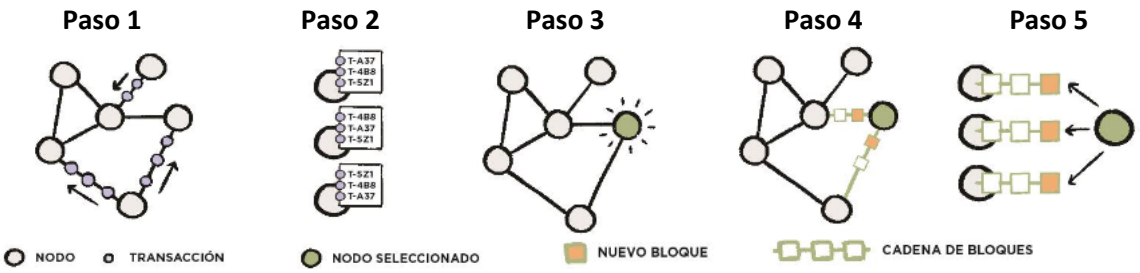
Paso 3**:** En cada proceso de validación, un nodo aleatorio es elegido para proponer un bloque. Este es el proceso más importante ya que es el que posibilita que las distintas partes no tengan la necesidad de confiar entre ellas. Esta decisión se conoce con el nombre de protocolo de consenso.

La cadena se va construyendo a medida que el nodo va añadiendo las transacciones registradas en su pool al final del bloque y enviando una nueva copia a la cadena con la que está conectado. El tamaño máximo de los bloques varía dependiendo el tipo de Blockchain, por lo que deben llenarse con un número limitado de transacciones.

Paso 4**:** El usuario elegido sugiere un nuevo bloque formado por las transacciones que ha ido registrando en su pool, este nuevo bloque debe ser enviado a los demás. Además, debe ser validado con un hash, es decir, un código alfanumérico obtenido a partir de toda la información almacenada en el bloque.

Paso 5**:** El bloque solo será aceptado por el sistema si contiene un hash válido. En caso afirmativo, el resto de los nodos verifican que las transacciones sean correctas y actualizan su copia de la cadena con la nueva versión que incluye el nuevo bloque.

Figura 2.3.1: Pasos para explicar el funcionamiento de blockchain



Fuente: Allende López (2018)

2.4. Tipos de redes Blockchain

Todas las redes están constituidas por un grupo de nodos que funcionan en un sistema peer-to-peer. Esto quiere decir que cada uno contiene una copia del registro compartido, que actualiza automáticamente. Partiendo de los puntos comunes, la mayoría de los autores sostiene que existen principalmente dos tipos de redes, las públicas y las privadas. No obstante, podemos exponer variaciones como son las híbridas y las de consorcio. (Parrondo, 2018).

Redes de blockchain públicas

Son aquellas redes en la que cualquier usuario de internet puede acceder y participar en los procesos como, por ejemplo, en la creación de bloques o en la validación. La seguridad de esta red se basa en la ejecución del protocolo de consenso y los usuarios pueden

interactuar de forma anónima. Además, se caracteriza por ser el único tipo puramente descentralizado y porque todas sus transacciones son totalmente transparentes.

Generalmente tiene asociado un token, de forma que se ofrece una pequeña parte de él como incentivo económico para participar en el protocolo de consenso. La gran participación en los procesos le hace ser una red más segura y confiable.

Redes de blockchain privadas

Son también conocidas como cadenas de bloques autorizadas y debido a sus particularidades son cerradas, restrictivas y centralizadas. Una sola organización administra y controla la red de forma individual, otorga permiso para participar, decide cuando ejecutar el protocolo de consenso y se encarga del mantenimiento.

Suele darse dentro de organismos o empresas, ya que solo los usuarios previamente autorizados pueden participar. Su funcionamiento es prácticamente el mismo que en las públicas, exceptuando las limitaciones al libre acceso, sin embargo, una ventaja de estas es que cuenta con una velocidad superior.

Redes de blockchain híbridas

Se trata de una combinación de las redes públicas y privadas. Al ser una solución mixta, las entidades a cargo pueden intercambiar una parte de la información completa a todos los usuarios y, que la otra, sea confidencial excepto para un grupo pre-escogido de usuarios. Este sistema es flexible ya que facilita el ingreso de los usuarios a una red privada, y que a su vez esta cuenta con varias públicas dentro.

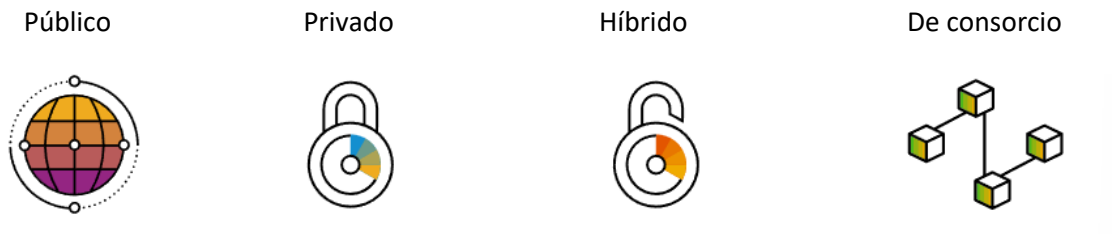
Este tipo de red se emplea para construir herramientas a nivel empresarial de código abierto. Además, debido a su seguridad, se ha extendido su uso en pagos transfronterizos confiables para la financiación y comercio.

Redes de blockchain de consorcio

Se trata de una variante parcialmente descentralizada en la que varias organizaciones administran la red. Este grupo de empresas, otorgan el derecho a participar en las transacciones o visualizar los datos.

Su uso se enfoca en el mundo empresarial en el que todos los participantes deben estar autorizados y comparten responsabilidad en cuanto al blockchain.

Figura 2.4.1: Tipos de redes Blockchain



Fuente: SAP

2.5. Barreras regulatorias a las que se enfrenta una red pública

Blockchain por definición debería generar confianza, pero como toda tecnología emergente, existen dudas acerca de su fiabilidad, seguridad o velocidad. Por otro lado, la falta de regulación no pasa desapercibida, mientras que algunos países empiezan a discutir sobre el tema, el panorama regulatorio está casi inexplorado. (PricewaterhouseCoopers).

En España, aún no se ha producido un ordenamiento jurídico al respecto y, que no esté regulado, suscita cierta incertidumbre. A pesar de los retos que supone las cadenas de bloques públicas que expondré a continuación, la legislación se acabará adaptando como ha sucedido con herramientas tecnológicas anteriores, es el ejemplo de internet. (Legerén-Molina, 2019).

Ausencia de dueño

De acuerdo con lo explicado anteriormente, una red blockchain es una base de datos descentralizada en la que los usuarios realizan transacciones sin la supervisión ni control de una autoridad. Esto sin duda constituye grandes ventajas, pero también un inconveniente: Como no hay una persona física ni jurídica que ostente la propiedad de la cadena, no hay una entidad a la que poder reclamar ni responsabilizar de los fallos del sistema como mal funcionamiento, hackeo, robos...

Límites en el registro

A pesar de que los registros son inmutables, tienen una serie de limitaciones entre las que cabe destacar: No se realiza de forma totalmente abierta, ya que hay restricciones en el acceso, en el cual no se puede incluir documentación, solo contiene un sello temporal.

Por tanto, la cadena de bloques no ejerce un control legal porque no tiene la capacidad de almacenar documentos que identifiquen al usuario. Esto, además, iría en contra de la esencia de blockchain porque el archivo de datos a efectos de identificación y jurídicos requiere de una entidad que supervise.

Identidad digital

A muchos usuarios de una cadena de bloques no les interesa que figure quienes son debido a que tampoco es necesario para ejecutar las transacciones porque prima que la operación se realice antes de quien lo hace.

2.6. Glosario de términos.

Para comprender mejor el potencial de esta tecnología y las explicaciones anteriores y posteriores, vamos a profundizar en algunos componentes fundamentales que han sido o van a ser nombrados a lo largo del trabajo (Allende López, 2018) y (BBVA).

Nodo

Se trata de un ordenador que utiliza un software concreto para almacenar y distribuir una copia actualizada en tiempo real de los datos de la cadena. Cada vez que un nuevo bloque se valida y añade a la cadena, el cambio se va añadiendo a las copias del resto de nodos.

Red entre pares (peer-to-peer)

Se trata de una red de nodos conectados entre sí en la que todos se comportan como iguales. Un ejemplo conocido es BitTorrent.

Bloques

Contiene un registro de todas las transacciones ejecutadas. Una vez validados se agregarán a la cadena a través de la distribución a todos los nodos de la red. Cada bloque que forma parte de la cadena está formado por:

1. Un código alfanumérico que enlaza con el bloque anterior y otro con el posterior.
2. Un paquete de transacciones.

Protocolo de consenso

Procedimiento mediante el cual se elige a un nodo para proponer un nuevo bloque, se trata de una selección aleatoria. El propósito de esta elección es evitar que haya un

responsable único en la proposición de bloques. Cualquier participante de la red puede ser elegido.

Hash

Es el código alfanumérico que se obtiene como resultado de la aplicación de una función matemática a unos datos concatenados. Este código encripta, entre otras cosas, número de bloque, las transacciones que contiene y la firma digital del proponente. Es la principal aportación a la seguridad de la cadena.

3. Aplicaciones de Blockchain a las finanzas

3.1. Criptomonedas

Desde un punto de vista técnico, las Criptomonedas son archivos, bits con datos cuyo objetivo es sustituir al dinero tradicional con todas sus funciones, aunque utilizando internet como medio de transmisión.

Mientras que financieramente, son un tipo de moneda virtual cuyas características le permiten aplicaciones universales más extendidas. Lo que las diferencia es que minimizan los problemas asociados a las reglas de escasez de la vida real. (Barroilhet, 2019).

Son emitidas de forma descentralizada y cambian de propietario usando criptografía para mantener la fidelidad, además de las tecnologías de registro o libros mayores que son actualizados constantemente por miles de ordenadores independientes para evitar su duplicidad.

Se calcula que existen en torno a 10.000 diferentes, algunas de ellas con único valor monetario y otras, en cambio, con propósito de realizar proyectos como la generación de contratos inteligentes, billeteras compartidas...

Figura 3.1.1: Criptomonedas más importantes por capitalización de mercado

#	Nombre	Símbolo	Precio (USD)	Cap. mercado
1	Bitcoin	BTC	38.341	730,36B $
2	Ethereum	ETH	2.827,41	341,41B $
3	Tether	USDT	1	83,16B $
4	BNB	BNB	387,19	63,24B $
5	USD Coin	USDC	1,0002	48,96B $
6	XRP	XRP	0,61769	29,75B $
7	Solana	SOL	87,076	29,13B $
8	Terra	LUNA	83,8694	28,87B $
9	Cardano	ADA	0,7923	26,77B $
10	TerraUSD	UST	1	18,63B $

Fuente: Investing.com, (03/05/2022)

3.1.1. Características

- No existen físicamente; ni en papel ni en metal. Son monedas puramente virtuales.
- No tiene vinculación con gobiernos o bancos centrales; Son monedas privadas. (Rangel, 2021)
- La red peer-to-peer en la que se desarrollan garantiza que las transacciones se realicen directamente entre los participantes, eliminando las comisiones e intermediarios características de los mercados tradicionales.
- La cadena de bloques en la que se almacenan los datos de las transacciones es inalterable, así que, una vez validada una operación, es imposible manipular el registro deshonestamente haciéndola una red altamente segura. (Gonzalo, 2021)

3.1.2. Marco regulatorio internacional

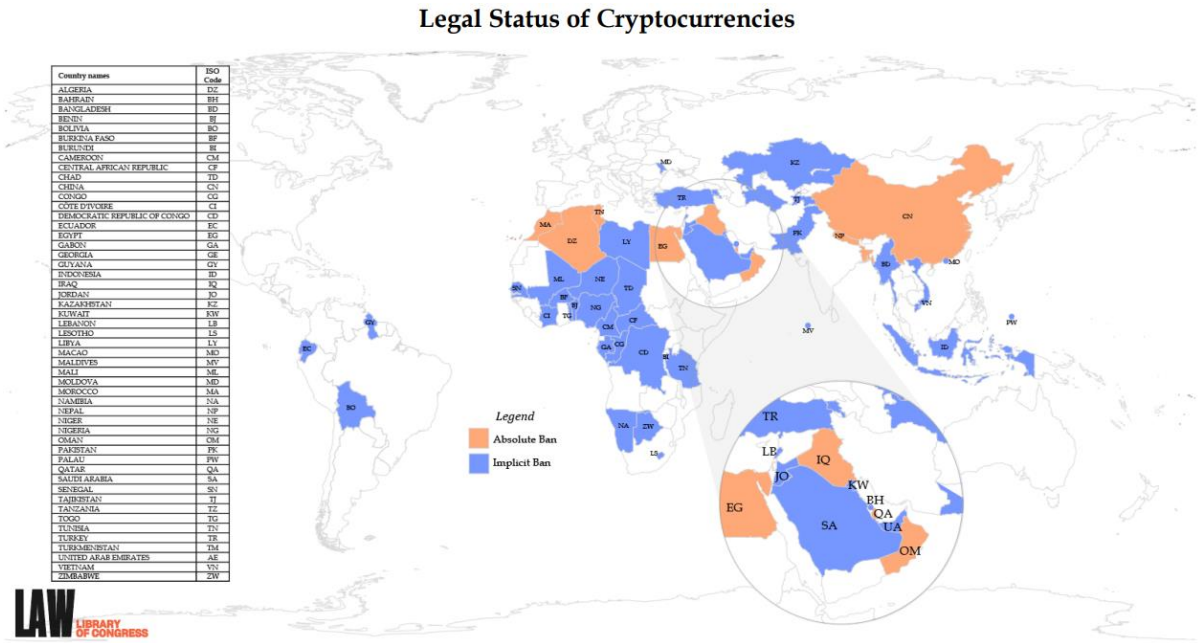
Frente a algunos países que tienen grandes equipos jurídicos trabajando para regular las criptomonedas, cabe destacar que ya hay 51 países que ya han prohibido las redes blockchain para la transmisión de divisas digitales.

Hay 9 países con una prohibición absoluta, que son: Argelia, Bangladesh, China, Egipto, Irak, Marruecos, Nepal, Qatar y Túnez. Los otros 42, mantienen limitaciones implícitas, esto es, prohíben a instituciones financieras negociar con criptodivisas u ofrecer servicios relacionados.

Estos países tratan de justificar su veto a través de investigaciones que sostienen que favorece la realización de actividad criminal como el blanqueo de capitales o la corrupción.

Frente a estas regulaciones restrictivas, encontramos el caso de El Salvador, que en la actualidad es el único país que ha adoptado una criptomoneda (Bitcoin) como moneda de curso legal, el pasado 7 de septiembre de 2021. (Global Legal Research Directorate, 2021).

Figura 3.1.2.1: Mapa de los países que han prohibido las criptomonedas



Fuente: Global Legal Research Directorate, 2021

3.1.3. Bitcoin

(Nakamoto, 2009) Se define como un sistema de dinero electrónico basado en la criptografía que permite a las distintas partes realizar transacciones sin necesidad de la intermediación de un tercero. Este es remplazado por una red entre pares donde se almacena un registro cronológico de las transacciones, evitando el problema del doble pago.

Se trata de la moneda virtual pionera por excelencia y tras su éxito, han ido apareciendo muchas otras. A pesar de esto, sigue siendo la protagonista indiscutible, ya que a fecha de 3 de mayo de 2022 acapara más del 40% del mercado de criptodivisas. Comenzó con un valor unitario de $0,06, hoy tiene un precio de $38.389,57.

Figura 3.1.3.1: Evolución del precio de Bitcoin

Fuente: investing, 2022

En el gráfico, que abarca los últimos 6 años, podemos apreciar un incremento notable en la segunda mitad del 2017, disparándose su valor de $2.737,4 el 1 de agosto hasta los $19.320 que finalmente alcanza, propiciándose un aumento de aproximadamente un 705%, es decir, que unos pocos meses multiplicó su precio por 7,05.

Posteriormente, debido a la pandemia, en marzo de 2020 su valor cayó hasta los $4.789, desde entonces comenzó un rally alcista que se pondría fin un poco más de un año más tarde cuando alcanza un nuevo pico en aproximadamente $63.512, lo que supone un aumento de un 1.326%. En agosto de 2021, alcanza el precio máximo histórico en $67.304 para comenzar una tendencia descendente en la que se mantiene hoy.

La capitalización de mercado a 3 de mayo de 2022 es de 730,36 billones de dólares, que es sumamente grande en comparación con la compañía de mayor capitalización bursátil en el mundo: Apple, que se alza con $2,57 billones.

Además, cuenta con un volumen diario de transacciones de más de 29 billones de dólares.

3.1.3.1. ¿En qué consiste el minado de Bitcoin?

El proceso de minado es un sistema de consenso distribuido en el que se validan y agrupan las transacciones pendientes de ser incluidas en la red blockchain. Esta actividad es la encargada de aportar seguridad además de hacer cumplir un orden cronológico.

Bitcoin utiliza un método de consenso denominado *Proof of Work*, en el que muchos ordenadores compiten por ser los primeros en resolver el problema matemático,

obteniendo el primero una recompensa en forma de la propia moneda. El premio varía en función de la dificultad que hay en la red en ese instante. Por tanto, los creadores de Bitcoin limitaron la actividad a 10 minutos, de forma que cuando la dificultad de la red está por encima o debajo de esta cantidad, el trabajo se redimensiona para ajustarse al tiempo establecido.

Para ser minero de Bitcoin necesitamos un equipo con una gran potencia computacional ya que la competencia en estos últimos años ha aumentado considerablemente y con ella la dificultad de ser el primero en hallar la solución. El problema matemático es siempre similar, sin embargo, algunas variables varían. Se resuelve probando números aleatorios hasta obtener el resultado. (Tromp, 2014)

Hoy en día la minería está en el punto de mira ya que es altamente contaminante. Esto se debe a la cantidad de energía necesaria para mantener ordenadores computacionalmente muy potentes trabajando las 24 horas del día. La actividad en su conjunto ha alcanzado un consumo el 10 de mayo de 2021 de 148 teravátios por hora, superior que países enteros como Argentina, que ese mismo día gastó 120 teravátios/hora.

Este elevado consumo abre un debate sobre el impacto que esta criptomoneda tiene sobre el medioambiente, afectando directamente al precio con caídas en su cotización. A raíz de estas bajadas, ya hay varias monedas digitales que se han propuesto reducir la huella que generan. (Blanco, 2021)

3.1.3.2. Cómo realizar una transacción con Bitcoin

Para enviar o recibir Bitcoin es necesario contar con una cartera digital o wallet.

Con su creación lo que realmente producimos es una serie de claves aritméticas, donde podemos distinguir entre públicas o privadas. La primera es similar a un sobre brindado en el que podemos introducir información y mandarlo con la certeza de que no va a ser abierto. Mientras que la segunda se asemeja a la combinación de una caja fuerte y nos permite administrar los bitcoins de forma total.

Además, Bitcoin utiliza las funciones hashes y firmas digitales dentro de cada transacción. Los hashes aportan el identificador de la transacción y además capas de seguridad en distintos elementos que forman la transacción.

Ejemplo: Ana desea enviar 0,01 BTC a Daniel, para lo que ambos abren sus respectivas carteras digitales. Cada una contiene una clave privada que cada uno de ellos conoce de forma personal, mientras que para la transacción Ana pide la dirección de destino.

Daniel genera una dirección, que se trata de una clave pública derivada de su clave privada y se la manda a Ana. Ella, prepara el envío especificando la cantidad y asumiendo una comisión de minería. En el momento que pulsa el botón de enviar, su monedero genera una transacción, la firma digitalmente y crea un identificador único utilizando la función Hash.

En pocos minutos la red Bitcoin ha procesado el envío y lo introduce en su historial contable. Así, Daniel dispone ya de sus BTC y podrá administrarlos haciendo uso de su clave privada, dando por concluida la transacción. (Preukschat, 2017)

3.2. Smart contracts

En español, contrato inteligente, se trata de una de las aplicaciones más relevantes sin contar con las criptomonedas. Su planteamiento se remonta a 1994, cuando Szabo afirmó que se podían almacenar acuerdos inteligentes en un libro mayor descentralizado.

En este formato, los contratos se pueden, mediante criptografía, convertirse a código, ser guardados y replicados en el sistema y supervisados por la red de dispositivos que ejecutan la cadena de bloques. (BBVA).

Define y especifica una serie de cláusulas para la realización de determinadas transacciones. Se diferencia de los contratos usuales en que estos, al estar incorporados en una cadena de bloques, su seguridad está garantizada y se ejecutan de forma autónoma. (Allende López, 2019)

Sus aplicaciones prácticas van desde la compra de un activo cuando su precio baja de cierta cantidad, por ejemplo, hasta establecer los términos y condiciones de un seguro de viaje, el cual se ejecuta de manera automática cuando un vuelo se retrasa por más de X horas.

4. Propuesta de aplicación a la bolsa española

En la actualidad, la mayoría de las negociaciones que se producen en el mercado financiero en España se llevan a cabo a través del Sistema de Interconexión Bursátil Español (SIBE), donde no solo se negocian acciones, también títulos de renta fija, warrants y otros productos…

El SIBE conecta en vivo las cuatro bolsas españolas: Madrid, Barcelona, Bilbao y Valencia. Este mercado funciona con órdenes y esta conexión, permite la existencia de un único libro de registro para cada valor.

Una orden es una instrucción o mandato a través de la cual un inversor expresa su interés de compra o venta de instrumentos financieros.

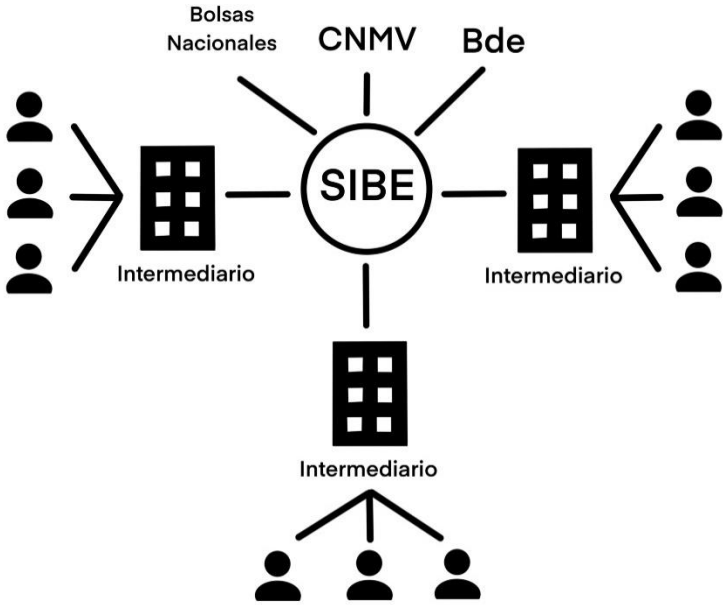
En el caso del mercado bursátil español, encontramos una limitación y es que solo pueden introducir y ejecutar órdenes en él los intermediarios que posean acciones de Bolsas y Mercados Españoles (BME), que integra las empresas que dirigen y gestionan las 4 bolsas nacionales. Es decir, deben ser miembros del propio mercado.

Además, podemos encontrar otras instituciones que velan por el buen funcionamiento de los mercados. Por un lado, la Comisión Nacional del Mercado de Valores (CNMV) supervisa y asegura un buen desempeño en la bolsa. También vigila los mercados financieros y garantiza la transparencia de las operaciones y fijación de precios libre.

Por otro lado, el Banco Central Europeo (BCE) y sus filiales, los bancos centrales nacionales, en concreto el español (Banco de España) supervisa los intermediarios financieros y bancos con un volumen de activo superior a los 30.000 millones de euros.

Por lo explicado recientemente, para que un inversor, por ejemplo, emita una orden de compra o venta de acciones en el mercado continuo, sigue el esquema que vemos en la imagen.

Figura 4.1: Esquema de funcionamiento actual de la bolsa española.



Fuente: Elaboración propia

Como podemos observar, antes de que la voluntad del usuario llegue al SIBE, debe pasar por intermediarios y, en el caso de que estos no participen en Bolsas y Mercados Españoles, se alarga la cadena.

Esto no solo hace que el proceso sea más lento, también más costoso. El importe de las comisiones asociadas a una operación bursátil tiene, a menudo, una incidencia significativa en la rentabilidad de la operación. Distinguimos dos grupos de gasto:

Costes del intermediario: Son los que le pagamos por la recepción, transmisión, ejecución y liquidación de la orden. Además, a estos se les añade las comisiones de administración y custodia.

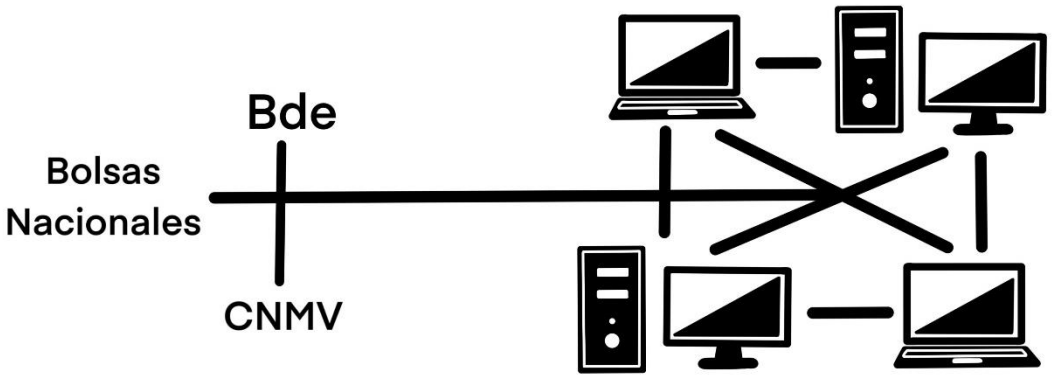
Cánones: Son gastos que cobran los mercados por la ejecución de la orden y la compensación y liquidación de valores y que los mediadores repercuten al cliente.

Con esta propuesta, se pretende, entre otras cosas, reducir el coste de la inversión al eliminar los intermediarios que negocian en cada transacción, lo que también permite disminuir el tiempo. (CNMV, 2011)

Para ello se plantea una red Blockchain de tipo híbrido ya que, por sus características, se trata del modelo más adecuado. Por un lado, necesitamos varias entidades que se hagan

cargo de la supervisión de la plataforma (Como CNMV, Banco de España o las 4 bolsas nacionales, que seguirán realizando sus tareas actuales) y a su vez intercambiar información confidencial entre ellos como la identidad de los compradores y vendedores. Por otro lado, aporta a los inversores facilidad para unirse a la red sin necesidad de permiso, es decir, es de código abierto.

Figura 4.2: Esquema de funcionamiento de la propuesta de aplicación de blockchain en la bolsa española.



Fuente: Elaboración propia

El proceso es el siguiente:

El primer paso antes de operar será identificarse ya que los dueños de las acciones tienen una serie de derechos como nuevos propietarios de la parte alícuota del capital social que les corresponde. El funcionamiento y naturaleza de la cadena de bloques aporta efectividad en la identificación de personas y activos, lo cual mejora el seguimiento de las personas y actividades realizadas. Este proceso no solo sería más rápido, sino que esta información será más segura y menos vulnerable a distorsiones o segmentación.

Una vez registrado, los inversores deciden comprar o vender una determinada acción. A través de contratos inteligentes, el comprador podrá seleccionar tipo y condición de ejecución y establecer un stop loss o take profit si lo desea. La orden se lanza a la red pública donde se cruzará con una de venta.

Cuando esto se produzca, los participantes de la red privada comprobarán que efectivamente que el vendedor es el propietario de los títulos comprobando la información alojada en la cadena de bloques y ejecutará un cambio en la propiedad. Para la liquidación,

la red privada hará participe a los nodos de la pública para que aporten potencia computacional añadiendo la información de la transacción en forma de bloque a la cadena. Además, les recompensará con un pequeño incentivo en forma monetaria aportada por el comprador, siendo está bastante inferior a las comisiones actuales. El proceso será similar al explicado anteriormente con el minado de Bitcoin.

Esta propuesta no está limitada a la compraventa, ya que también pretende facilitar operaciones relacionadas como es el pago de dividendos. Las empresas podrán ahorrar tiempo y dinero automatizando este proceso a través de Smart contracts. Estos consistirán en establecer pagos que se ejecuten de forma automática para pagar a los accionistas.

Por tanto, las características de la red planteada son las siguientes:

- De tipo híbrido.
- Código abierto.
- A cargo de entidades como la CNMV, Banco de España y las 4 bolsas nacionales (Madrid, Barcelona, Bilbao y Valencia).
- Con comisiones mínimas para incentivar el minado y consolidación de bloques.

Este cambio, de aplicarse, será uno de los mayores avances en la historia de la bolsa desde el paso al modelo moderno debido a que se transforma radicalmente todo el transcurso de las transacciones, prescindiendo prácticamente de los intermediarios. Los procesos se han descentralizado de forma que los nodos se encargan de la verificación de las transacciones aportando rapidez, seguridad, transparencia y bajos costes. Además, proporciona confianza entre las partes involucradas.

Beneficios:

- Este proceso de automatización del mercado permite recortar tanto tarifas como intermediarios, pero, a su vez, sin comprometer las garantías de los consumidores.
- También se facilita el cumplimiento normativo, facilitado por la homogeneización de procesos y mejora del ejercicio de supervisión financiera.
- Ofrece a los usuarios transparencia, información en vivo y gestión integrada en una única red.
- Cualquier persona puede participar en el mercado si se identifica debido a la descentralización del proceso.

Dependiendo el punto de vista, este último punto puede ser tanto positivo como negativo ya que permite, por ejemplo, a criminales convertirse en propietarios de las empresas con dinero ilícito del cual se desconoce la procedencia.

También presenta algunos inconvenientes como:

- Deberá contar con el apoyo de la Unión Europea, que deberá legalizar la iniciativa.
- Los intermediarios se opondrán rotundamente a ser eliminados.

Estas razones, pueden hacer que el proceso de cambio del modelo actual al propuesto sea largo y arduo.

- Privacidad: Las compraventas de los inversores no son 100% anónimas ya que en el proceso de validación de los bloques, los nodos de la red pública pueden conocer la existencia de la operación y el volumen operado.
- Inicialmente, puede tener menos velocidad si no se han unido aún nodos suficientes para registrar las transacciones.

A pesar de estos inconvenientes, con este modelo se ratifica la opinión de varios autores, como por ejemplo Preukschat, que afirman que los principales beneficiados de la tecnología Blockchain serán los consumidores.

5. Conclusiones

Uno de los principales objetivos del trabajo era conocer en profundidad la tecnología blockchain porque es un término desconocido ya que, generalmente, solo se ha oído hablar de criptomonedas. Esto, limita el desarrollo y uso de esta red a nivel usuario, ya que las empresas sí están destinando grandes cantidades de recursos para su desarrollo.

Blockchain es un sistema de registro ventajoso y revolucionario en comparación con todos los medios tradicionales. Además, permite eliminar los intermediarios de las transacciones, lo que se traduce en un ahorro en costes. El impacto de Blockchain aumenta día a día y cada vez podemos ver nuevas aplicaciones en todos los ámbitos, pero sin dudarlo, el sector más beneficiado es y será el financiero, más detallado en este trabajo.

Podemos concluir que su desarrollo avanza a pasos agigantados y es que, cada día podemos observar cómo aparecen nuevos proyectos y aún no somos capaces de cuantificar su alcance en el futuro. No obstante, también hay incógnitas que podrían limitarlo como son la falta de información disponible, el gran consumo energético o la incertidumbre de su regularización legal.

Sin embargo, el principal reto al que se enfrenta es el lento proceso de investigación e implementación de la cadena de bloques y el reemplazo de los medios tradicionales de forma progresiva y segura tanto para personas como empresas.

Finalmente, a pesar de las grandes ventajas que presenta esta tecnología, su puesta en funcionamiento debe ser escalonada. Al ser relativamente nueva, queda mucho para que podamos verla aplicada en empresas ya que, de momento, solo el sector privado está invirtiendo en esta tecnología. Por esto, sería más provechoso la colaboración con los gobiernos de forma que mientras las empresas desarrollan sus aplicaciones, los estados desarrollen una legislación que no las limite.

6. Bibliografía

Libros:

Preukschat, A, and Kuchkovsky, C. (2019): *Blockchain: La Revolución Industrial de Internet*. Editorial Planeta, Barcelona.

Parrondo, L. (2018): *Blockchain, Bitcoin Y Criptomonedas: Bases Conceptuales Y Aplicaciones Prácticas*. ACCID, Barcelona.

Champagne, P. (2014). *The book of Satoshi: the collected writings of bitcoin creator Satoshi Nakamoto.* E53 Publishing Llc.

Artículos:

Legerén-Molina, A. (2019): "Retos jurídicos que plantea la tecnología de la cadena de bloques. Aspectos legales de Blockchain". *Revista de derecho civil,* páginas 21-32.

Yahari Navarro, B. (2018): "Blockchain y sus aplicaciones". *Revista Universidad Católica Nuestra Señora de la Asunción,* páginas 4-5.

Barroilhet, A. (2019): "Criptomonedas, economía y derecho". *Revista Chilena de Derecho y tecnología,* Vol. 8, Nº 1, páginas 10-20.

Páginas web:

Global Legal Research Directorate (2021). Regulation of cryptocurrency around the world Albania, Algeria, Angola, Anguilla, Antigua and Barbuda, Argentina, Australia, Azerbaijan, Bahamas, Bahrain, Bangladesh, Belarus, Belgium… [online] Library of Congress, Washington, D.C, 2021. [10 may. 2022].

https://www.loc.gov/item/2021687419

BBVA. Claves para entender la tecnología 'blockchain'. [online] BBVA NOTICIAS, 2019. [10 mar. 2022].

https://www.bbva.com/es/claves-para-entender-la-tecnologia-blockchain/

Allende López, M. y Colina Unda, V. Blockchain. Cómo desarrollar confianza en entornos complejos para generar valor de impacto social. [online] Banco Iberoamericano de Desarrollo, 2018. [25 mar. 2022].

https://publications.iadb.org/es/blockchain-como-desarrollar-confianza-en-entornos-complejos-para-generar-valor-de-impacto-social

Davis, R. Blockchain Emerging Technology Offers Benefits for Some Applications but Faces Challenges. [online] United States Government Accountability Office, 2022. [15 mar. 2022].

https://www.gao.gov/assets/gao-22-104625.pdf

Berenguer, J. Blockchain la tecnología que está en boca de todos. [online] ANDBANK private bankers, 2017. [1 abr. 2022].

https://www.andbank.com/wp-content/uploads/2017/11/2017-10-27-que-es-el-Blockchain-Joan-Berenguer-ESP.pdf

Yukiteru Amano. Qué es un Árbol Merkle. [online] Bit2Me Academy, 2019. [5 abr. 2022].

https://academy.bit2me.com/que-es-un-arbol-merkle/

Binance. La Historia de Blockchain. [online] Binance Academy, 2021 [5 abr. 2021]

https://academy.binance.com/es/articles/history-of-blockchain

SAP. ¿Qué es la tecnología blockchain? [online] SAP insights. [20 mar. 2022].

https://www.sap.com/spain/insights/what-is-blockchain.html

PricewaterhouseCoopers. Blockchain ya está aquí. ¿Tienes claro tu próximo paso? [online] PwC. [25 abr. 2022].

https://www.pwc.es/es/digital/blockchain-proximo-paso.html

Investing. Bitcoin [online] [03 may. 2022].

https://es.investing.com/crypto/bitcoin

Gonzalo, M. Criptomonedas: cómo funcionan, cómo se crean y cómo tributan. [online] Newtral, 2021. [28 abr. 2022].

https://www.newtral.es/criptomonedas-como-funcionan-tributan/20210120/

Blanco Moro, V. La huella que deja el Bitcoin en el medio ambiente amenaza el futuro de la divisa. [online] www.eleconomista.es, 2021. [11 may. 2022].

https://www.eleconomista.es/mercados-cotizaciones/noticias/11242451/05/21/La-huella-que-deja-el-Bitcoin-en-el-medio-ambiente-amenaza-el-futuro-de-la-divisa.html

CNMV. Guía de órdenes de valores [online] Portal de publicaciones CNMV, 2011 [18 may. 2022].

https://www.cnmv.es/DocPortal/Publicaciones/Guias/ordenes.pdf

Nakamoto, S. Bitcoin: a Peer-to-Peer Electronic Cash System. [online] bitcoin.org, 2009 [10 may. 2022]

https://bitcoin.org/bitcoin.pdf.

Tromp, J. Cuckoo Cycle: a memory bound graph-theoretic proof-of-work. [online] eprint.iacr.org, 2014 [12 may. 2022]

https://eprint.iacr.org/2014/059.pdf.