Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

Facultad de Filosofía y Letras

TRABAJO FIN DE GRADO

GRADO EN FILOSOFÍA

PROTOCOLO BITCOIN Y TECNOLOGÍA BLOCKCHAIN: ¿HACIA UN MUNDO CRYPTO?

Autor: Marlon Cárdenas Chamaya

Tutor: Armando Menéndez Viso

Oviedo, 05 de julio de 2022

Índice

Resumen: En este trabajo, estudiaremos los orígenes y el desarrollo de una novedosa tecnología que ha comparecido con gran ímpetu en el mundo digital. Se trata de la tecnología blockchain, nacida a partir del proyecto de la criptodivisa Bitcoin por Satoshi Nakamoto. Se exhibirá el funcionamiento de la tecnología, sus genialidades, y sus peligros, en sus distintas aplicaciones en tres partes diferenciadas. Primeramente, estudiaremos la tecnología fundamental que ha permitido el desarrollo de blockchain, a saber, las redes *Peer-to-Peer*. Segundamente, se estudiará a fondo la llegada del protocolo Bitcoin a partir de la tecnología *Peer-to-Peer* en conjunción con la criptografía. Terceramente, se expondrá aplicaciones alternativas de la tecnología, sus éxitos y fracasos. En fin, se terminará el trabajo con una breve conclusión.

Palabras clave: Bitcoin, blockchain, *Peer-to-Peer*, Satoshi Nakamoto, criptografía

Introducción

Durante la primera década del presente siglo, se ha ido fraguando en el seno de la tecnología digital una invención que consiguió conjugar un tipo de sistema de computadoras junto a la criptografía digital más potente, dando lugar a una divisa digital que por vez primera en la breve pero implacable era digital es funcional. Muchos de los más entusiastas tecnológicos no tardaron en equiparar este acontecimiento con la misma invención de Internet; otros no veían en esta tecnología nada diferente a una innovación más en la inagotable fuente digital. Lo cierto es que su desarrollo ulterior así como las posibilidades que ofrecía en diversos campos digitales en virtud de sus particularidades, convinieron a la perfección para despertar el interés de los agentes sociales y económicos más diversos: desde las empresas tecnológicas y personalidades más poderosas, hasta los usuarios más cercanos a la red virtual. Nacía así el protocolo Bitcoin junto a su mejor fruto, la tecnología blockchain; y parecía abrirse con él un nuevo mundo que Internet aún no había explorado. Un mundo sin injerencia externa de ningún tipo; un mundo funcional sin requerimientos centrales; un mundo garante de la seguridad a partir de su propia estructura interna: el mundo *Crypto*.

El protocolo Bitcoin logró servirse de una tan prolífica como potente tecnología de redes conocida como redes P2P o red de pares o entre iguales. Este tipo de sistema de redes brindaba una serie de ventajas para el intercambio de información digital y escondía en su propia concepción un anhelo deseado por muchos: la supresión de un servidor central que coordine al resto de clientes. Internet tendría que escribir aún numerosas páginas en el nuevo capítulo que se inauguraba con la revolución digital, pero el germen de su aplicación descentralizada, independiente de autoridades reguladoras preestablecidas, y en donde cada computadora sería al mismo tiempo usuario y servidor, amo y esclavo, había sido ya plantado.

Habría que esperar aún unos años, hasta noviembre de 2008, para que un conjunto de criptógrafos, matemáticos y programadores aunados bajo el pseudónimo de Satoshi Nakamoto clavase la bandera libertaria de Gadsden en el aún por recorrer mundo digital, y se anunciase un nuevo sistema de dinero electrónico basado en el modelo de red P2P

en conjunción con la cartografía, que no requeriría de terceras entidades que validasen los distintos intercambios de información. Surgía de este modo el protocolo Bitcoin y los libertarios de todos los países, persuadidos por su particular arenga del "*Dont* (sic) *tread on me*", creían vislumbrar un mundo nuevo liberado de las cadenas del Estado y de sus instituciones reguladoras. Pero, una vez más, las tecnologías rebasan por completo sus fines iniciales y acaban por plantear innúmeras rutas alternativas sobre las que es preciso reflexionar de un modo crítico. Tal vez, el entusiasmo inicial por un lado, y el fuerte rechazo por otro, que se ha ido levantando en ciertos sectores sociales a medida que el protocolo Bitcoin y otras aplicaciones de la tecnología blockchain penetraban en la cotidianidad, deba ser aplacado por una mirada filosófica omniabarcante que arroje algo de luz para una comprensión más justa de los medios y los fines del proyecto Crypto.

Esta tecnología, además, ha colmado su primera función efectiva de actuar como moneda digital, y se piensan ya multitud de aplicaciones en las que el cifrado y la individualización de lo que por naturaleza es replicable, juegan un papel clave. Muchas son las vertientes que se van trazando y, aunque solo hubiese una ínfima porción de verdad en las comparativas de esta tecnología con la invención de internet, esto ya merecería toda nuestra atención. Una tecnología tal que no solo pretende sino que también puede, al menos en potencia, inmiscuirse de una forma total en nuestro modo de relacionarnos con el otro, soportando nuestras transacciones económicas, modificando nuestro modo de concebir la virtualidad, o aligerando nuestras maquinarias burocráticas que parecen no haber evolucionado un ápice desde que monsieur Sans-délai calculase en quince los días necesarios para resolver sus asuntos administrativos.

En este trabajo de investigación, estudiaremos la tecnología blockchain y sus diferentes aplicaciones tanto económicas, con las criptomonedas; artísticas, con los novísimos NFTs; como cuasi-ontológicas, con la ambiciosísima empresa del Metaverso. Para ello es necesario entender, al menos de una manera superficial, cómo funciona

propiamente la tecnología blockchain en la que se sustenta Bitcoin y las miles de criptomonedas posteriormente desarrolladas[1].

Parte I. El recorrido hacia el mundo *Crypto*

1. Sistemas *Peer-to-Peer*

En el tortuoso camino de la problematización filosófica sobre las innúmeras cosas que atraviesan nuestra existencia en el mundo, el primer paso ha de ser siempre la aprehensión —o al menos, el intento— de lo que son tales cosas, sus relaciones entre ellas, con nosotros, y con el mundo. En el caso de los objetos tecnológicos, antes incluso de que podamos establecer las diferentes relaciones, tal aprehensión debe pasar necesariamente por comprender su funcionamiento interno. Descubrir esta organización interna de los diferentes objetos, nos será de gran utilidad luego para poder entrever las potencias que entrañan los objetos tecnológicos. En este sentido, nos resulta preciso estudiar primero la tecnología sobre la que se apoya la tecnología blockchain del protocolo Bitcoin y, consecuentemente, las posteriores aplicaciones de blockchain en diferentes campos. Esta tecnología informática no es otra que la arquitectura de red P2P.

Los sistemas P2P (por sus siglas en inglés, *peer-to-peer* traducido como "entre iguales" o "entre pares") son una forma de arquitectura de redes de ordenadores que se constituyen como un sistema distribuido, descentralizado, y autoorganizado. Se dice que es una arquitectura distribuida porque todas las computadoras que forman los *peers* o nodos del sistema comparten la carga de trabajo en la red. Se dice que es un sistema descentralizado porque no depende de un servidor central para su funcionamiento, sino de los distintos *peers* del sistema. Se dice, finalmente, que es un sistema autoorganizado porque actúa autónomamente, respondiendo solo al protocolo sobre el que se haya construido el sistema.

[1] A fecha de catorce de abril, la plataforma virtual de seguimiento de precios para criptoactivos CoinMarketCap cifra en 18886 las criptodivisas. Como es presumible, la gran parte de estos activos no presenta ningún, o prácticamente ningún volumen de trading. Visto en: https://coinmarketcap.com/

Podemos intuir ya las grandes posibilidades que dibujan estos principios de diseño sobre los que fueron concebidos los sistemas P2P, y que los distinguen radicalmente del modelo de sistemas cliente-servidor: mientras estos se estructuran a partir de la coordinación centralizada por un servidor, aquellos establecen la cooperación entre iguales sin necesidad de mecanismos de control. Las ideas de descentralización y autoorganización conformarían, como veremos, las piedras sobre las que Satoshi Nakamoto edificaría su iglesia del sistema monetario descentralizado y autoorganizado.

Pero todavía harían falta unos cuantos años hasta que Nakamoto aprovechase estos rasgos esenciales de descentralización y autoorganización de las redes P2P en su aplicación para las divisas. Esto no significa, sin embargo, que la arquitectura de red P2P estuviese desaprovechada, esperando ansiosa alguna idea genial que desplegase verdaderamente todo su ser. Las redes P2P, lejos de ser una novedad en el mundo digital, han acompañado desde sus orígenes al otro gran tipo de arquitectura digital, a saber, la de cliente-servidor, en la noble tarea de difundir internet al público masivo. Asimismo, su forma descentralizada llamó poderosamente la atención de ingenieros, técnicos, y expertos informáticos en general, desde el mismo momento de su concepción. La aplicación efectiva de estos sistemas, en un mundo donde el protocolo World Wide Web fundamentado en la arquitectura cliente-servidor comenzaba igualmente a masificarse, se circunscribía entonces mayormente al intercambio de archivos incurriendo con frecuencia en infracciones a derechos de autor; y en menor medida a su uso en la telefonía basada en Internet, y en la construcción de diferentes sistemas distribuidos.

Comoquiera que la popularidad de los sistemas P2P acrecentaba hasta el punto de superar el tráfico Web, los trabajos académicos y artículos de expertos informáticos interesados en indagar este potencial comenzaban a multiplicarse. Toda esta información y conocimiento desperdigados parecían exigir una sintetización o, al menos, una recopilación y ordenación. Así, en el año 2005, los prominentes profesores informáticos Klaus Wehrle y Ralf Steinmetz emprenderían esta exigente tarea en su obra *Peer-to-Peer Systems and Applications*.

2. La enciclopedia informática P2P

La obra *Peer-to-Peer Systems and Applications* (2005) de los reputados informáticos alemanes Klaus Wehrle y Ralf Steinmetz ha de ser considerada sin duda como un gran hito en el recorrido hacia el mundo blockchain, toda vez que impulsó de manera determinante el desarrollo de los sistemas P2P y demostró por vez primera todo el potencial que abrigaba en su ser.

Debido a los muchos y valiosos trabajos de investigación que se habían realizado durante los primeros años del nuevo siglo, los autores creyeron improrrogable ofrecer una perspectiva general sobre el campo P2P y sus aplicaciones, así como una clasificación de los diferentes territorios de investigación que brotaban de él. Asimismo, había que definir de un modo preciso lo que significaba el "Paradigma *Peer-to-Peer*" y precisar de este modo el alcance completo de la tecnología. Hasta ese momento, la asociación de los sistemas P2P con su uso para la piratería a través de las populares aplicaciones de Napster y Gnutella, limitaban una comprensión más profunda y ambiciosa de la tecnología. Finalmente, Wehrle y Steinmetz actuaron en esta obra también como editores y recopiladores de todas estas investigaciones sobre el campo P2P que se hallaban dispersas en la academia, facilitando su enseñanza y difusión.

La obra consta de diez partes diferenciadas según criterios puramente técnicos sobre el funcionamiento de los sistemas P2P, así como por sus aplicaciones en diferentes sectores, sumando un total de treinta y dos capítulos. Es, pues, una obra más bien técnica en la que, sin embargo, dos capítulos se nos presentan como interesantes para nuestros propósitos. Por un lado, la primera parte, titulada "Peer-to-Peer: Notion, Areas, History and Future", consigue en unas pocas páginas introducirnos de modo excelente la tecnología P2P, presentándonos por vez primera una definición sistemática de la tecnología, así como un repaso a su evolución desde los tempranos sistemas P2P y a las áreas de uso. La parte quinta, por otro lado, exhibe de manera directa el gran interés de los autores en un rasgo concreto de la tecnología, a saber, "el fascinante tema de la autoorganización" (Steinmetz & Wehrle, 2005, p. 3) o autonomía de los sistemas P2P. Exploremos brevemente, pues, estas páginas.

3. “¿De qué trata esto del *Peer-to-Peer*?”

De un modo directo y casi informal, Steinmetz y Wehrle abren su obra con la pregunta más pertinente posible: ¿de qué trata esto del *Peer-to-Peer*? Los autores consideran el paradigma *Peer-to-Peer* de comunicación en Internet como la herramienta indicada para superar los desafíos que iría poniendo sobre la mesa la comunicación digital. Estos desafíos son sintetizados en tres principales, a saber, el problema de la escalabilidad; el problema de la seguridad y fiabilidad; y el problema de la flexibilidad y calidad del servicio. Primeramente, el problema de la escalabilidad se refiere al problema de un sistema informático de satisfacer una creciente demanda de recursos como el ancho de banda, la capacidad de almacenamiento, o el poder computacional, a medida que el número de usuarios de una aplicación aumenta. Segundamente, el problema de la seguridad y fiabilidad se refiere a la capacidad de un sistema para defenderse ante los ciberataques. Asimismo, el anonimato y la resistencia a la censura son dos características de cada vez mayor importancia a la hora de navegar en la red. Terceramente, el problema de la flexibilidad y la calidad de servicio se refiere en general a la capacidad de los sistemas para ir adaptándose a medida que evolución las tecnologías informáticas (Steinmetz & Wehrle, 2005, pp. 9, 10).

Ante estos problemas esbozados, cabe señalar hasta qué punto diferentes aplicaciones basadas en sistemas P2P han proporcionado una salvaguarda efectiva. Si mentamos el problema de la escalabilidad, podemos afirmar que los sistemas P2P son escalables por diseño, y esto sin perjuicio de que sistemas basados en arquitecturas clientes-servidor sean igualmente escalables. La gran diferencia es que en la arquitectura de redes entre pares, cada par es al mismo tiempo un servidor en potencia, sorteando de esta manera el fenómeno del “cuello de botella” que se puede dar en sistemas centralizados donde los servidores necesarios para el funcionamiento del sistema aumentan linealmente con el número de clientes. Además, este esencial rasgo de escalabilidad es complementado por la descentralización del sistema, merced a lo cual cada nodo se apoya solamente en información local y restringida para completar su funcionamiento.

Ocurre algo similar si atendemos a la cuestión de la seguridad: los sistemas basados en la arquitectura cliente-servidor son tremendamente vulnerables a los ciberataques, en particular, los tan conocidos como perniciosos ataques de denegación de servicio distribuido o DDoS. Este tipo de ataque cibernético consiste en provocar un incesante tráfico web de manera artificial mediante redes de *bots* hasta saturar los servidores centrales de una red, ralentizándolos o directamente *crashéandolos*. Los sistemas P2P son en cambio muy resistentes a estos ataques por, una vez más, su mismo diseño descentralizado. Un ataque exitoso a una red P2P debería, pues, vulnerar simultáneamente una gran proporción de los nodos de esa red, algo que en la práctica se torna demasiado costoso.

Cabe mencionar finalmente, a título de ejemplo sobre el anonimato y la lucha contra la censura, el celebérrimo caso de Julian Assange y su portal web WikiLeaks. El portal del activista australiano se ha dedicado desde el año 2006 a filtrar información muy sensible en materia de derechos humanos, tanto de empresas y personalidades relevantes, como de gobiernos de superpotencias mundiales. En este último caso, son por todos conocidas las filtraciones realizadas por la web sobre los crímenes de guerra perpetuados a principios de siglo por Estados Unidos en la Guerra de Irak y la Guerra de Afganistán, entre los que se encuentran el asesinato de doce periodistas que no presentaban ninguna amenaza, o los cientos de casos de torturas, violaciones, y asesinatos a población civil. Todas estas valiosísimas informaciones difícilmente podrían haber visto la luz si WikiLeaks no hubiese contado con la capacidad de proteger el anonimato de sus informantes, merced a aplicaciones diversas entre las que destaca Freenet, una red de distribución de información descentralizada basada en redes P2P.

4. *Peer-to-Peer* frente a *Cloud computing*

Los sistemas P2P, pese a las numerosas posibilidades que ofrecían, no cumplieron con las augurios más optimistas predicados por los chamanes informáticos de principios de siglo que conjeturaron un “cambio de paradigma [en Internet] de la coordinación hacia

la cooperación, de la centralización a la descentralización, del control a los incentivos" (Steinmetz & Wehrle, 2005, p. 12). Con todo, es fácilmente rastreable la enorme influencia que este tipo de red y sus investigaciones concomitantes han tenido en el desarrollo de diversos sistemas informáticos. Aplicaciones de comunicación como Skype fueron diseñadas en virtud de este tipo de redes; otras aplicaciones de *streaming* de música, como es el caso de Spotify, hicieron uso igualmente en sus orígenes de sistemas híbridos que combinaban servidores que centralizan los datos con sistemas P2P que los almacenan distribuidos a través de los diferentes *peers*.

Lo cierto es que resultaba difícil hasta para los mejores ingenieros informáticos del momento predecir la inapelable apuesta de Internet por los sistemas centralizados basados en el modelo *cloud computing*, o como ha sido traducido, computación en la nube. Esta tecnología, verdaderamente interesante pero que para los propósitos de esta investigación solo repasaremos de un modo somero, ha monopolizado durante la última década todas las aplicaciones dentro de Internet.

La computación en la nube se fundamenta en la tecnología de la virtualización. Esta tecnología consiste en la creación de un ordenador virtual, simulado y digital conocido como máquina virtual que funciona en tu computadora física, como el teléfono móvil, el ordenador de sobremesa, el portátil, etc. El modelo de la nube, en conjunción con la elevadísima y creciente demanda de Internet, arrostra una dificultad logística importante: y es que las infraestructuras que demanda este modelo, conocidas como centros de datos de hiperescala (HDCs, por sus siglas en inglés, *Hyperscale Data Centers*), son obras colosales de la ingeniería, tanto en software como en hardware[2], y que por lo mismo demandan un consumo energético, humano, y tecnológico igual de colosal. Finalmente, y como cabría conjeturar, las empresas que en Occidente acaparan los centros de datos de hiperescala son los punteros tecnológicos agrupados en el acrónimo GAFAM, estos son, Google, Amazon, Facebook, Apple y Microsoft.

[2] En este sentido, pueden llegar a ocupar una superficie de hasta cien mil metros cuadrados como es el caso del gigantesco centro de datos de hiperescala *Inner Mongolia Information Park* propiedad de China Telecom y que está situado, junto a otros HDCs, en Hohhot. Visto en: https://www.vertiv.com/en-emea/about/news-and-insights/articles/educational-articles/what-is-a-hyperscale-data-center/

Pero incluso ante este nuevo escenario en el que Internet se decantaría finalmente por el modelo de la nube, los sistemas P2P todavía no habrían dicho su última palabra. En este sentido, los reputados ingenieros informáticos Anne-Marie Kermarrec y François Taïan, cuya materia de estudio se centra en los sistemas distribuidos y redes P2P, han señalado cómo los complejísimos algoritmos sobre los que fueron diseñadas las distintas aplicaciones P2P pueden ser útiles para aportar esa escalabilidad por diseño a los sistemas basados en la nube. Su argumento se sostiene sobre un principio de complejidad: los sistemas distribuidos como las redes P2P requieren de complejísimos algoritmos que le permitan escalar, y que pueden ser traspasados a los sistemas centralizados como la nube que a medida que crecen tienden a distribuirse, y de este modo mejorar aún más su eficiencia (Kermarrec & Taïani, 2015).

En cualquier caso, el protocolo *Peer-to-Peer* no iba a quedarse relegado a distintos nichos *geeks* del Internet, o a su uso primigenio y un tanto vulgar del *filesharing*, traducido en la práctica en la piratería. Y además de constituir el esqueleto de multitud de aplicaciones importantísimas en la historia digital como las que hemos repasado, *Peer-to-Peer* estaba destinado a convertirse en un elemento esencial en la fundación y el éxito del protocolo Bitcoin y todo el desarrollo c*rypto* ulterior. Satoshi Nakamoto nos daba la bienvenida, de este modo, al mundo *Crypto*.

Parte II. El advenimiento del protocolo Bitcoin

5. Satoshi de Tokio

En el principio conectó Internet los servidores y las computadoras. Y la red estaba desordenada y vacía, y los recuerdos de un mundo desconectado estaban sobre la faz del ayer, y el Espíritu de Internet se movía sobre la faz del mañana. Sucedieron los días e Internet continuaba poblando su mundo virtual de prodigios sin igual. Un futuro esperanzador parecía abrirse paso. La red virtual se expandía inexorable, y la idea de un espacio en el que ser verdaderamente libres se grababa sobre las mientes de sus más fervientes adeptos. Pero las Tinieblas acechaban y, sin conmiseración alguna, cercaron la

red virtual y comenzaron a inundar sus territorios. El pecado original de la regularización pesaba sobre el mundo libérrimo de la virtualidad. La red ansiaba la llegada de aquel capaz de desafiar y vencer de una vez por todas las Tinieblas. La red ansiaba el advenimiento de su Mesías.

El 1 de noviembre de 2008, Satoshi Nakamoto envío un mensaje a la lista de correos especializado en criptografía llamada *metzdowd*[3] en el que anunciaba un nuevo sistema de dinero electrónico basado puramente en redes *Peer-to-Peer*. En este famoso w*hite paper* o monografía titulado *Bitcoin: A Peer-to-Peer Electronic Cash System*, Nakamoto expone de manera concisa los aspectos técnicos que presenta su nueva moneda digital, así como el objeto principal de su creación: prescindir de terceros de confianza. "Lo que se necesita es un sistema de pago electrónico basado en pruebas criptográficas en lugar de confianza, permitiendo así que dos partes interesadas realicen transacciones directamente sin necesidad de una tercera parte de confianza" (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, p. 1).

Con la presentación de la novedosa tecnología blockchain se sentaron por fin las bases de una divisa digital descentralizada que, a diferencia de todos los intentos anteriores, funcionaba. El 3 de enero de 2009, Nakamoto ejecutó su protocolo con el minado del primer bloque conocido como el Bloque génesis, dando inicio a la primera criptodivisa de la historia: Bitcoin. Días después, Nakamoto realizó la primera transacción al enviar 10 BTC[4] a Hal Finney, criptógrafo que mostró genuino interés en la Bitcoin desde sus inicios llegando colaborar activamente en la mejora del software. En octubre de ese mismo año, un usuario de Bitcoin consiguió vender por primera vez bitcoins[5] por dinero, cambiando 5050 BTC por 5,02 USD, y estableciendo así a Bitcoin como un bien de mercado. Tuvieron que pasar unos meses, hasta el 22 de mayo de 2010, para que Bitcoin fuese usado ahora como medio de intercambio cuando un programador

[3] La lista de correos sigue ofreciendo sus servicios a todo aquel interesado en la criptografía como herramienta política para fortalecer la privacidad y seguridad de los usuarios en el mundo digital en su página web: https://www.metzdowd.com/mailman/listinfo/cryptography

[4] La abreviatura de la criptodivisa de Bitcoin es "BTC".

[5] Por convención, se distingue "Bitcoin" como el protocolo general planteado por Nakamoto, de "bitcoin" como la criptodivisa en funcionamiento una vez ejercitado el protocolo.

de Florida pagó 10000 BTC a otro usuario a cambio de dos pizzas de la famosa multinacional estadounidense Papa John's por valor de 40 USD[6].

Bitcoin continuaría a lo largo de los años siguientes su periplo como divisa virtual en un ascenso meteórico de su valor, alternado con fuertes desplomes: en febrero de 2011 alcanza la paridad con el dólar; en octubre de 2012, el Banco Central Europeo califica Bitcoin como una amenaza para el sistema financiero tradicional por su falta total de regularización; en noviembre de 2013, el precio de un bitcoin iguala al de una onza de oro; en octubre de 2021, Bitcoin alcanza su máximo histórico hasta la fecha llegando a valer 66000 USD; finalmente, en mayo de 2022, desciende por debajo de los 27000 USD representando una caída de más del más del 50% en siete meses[7].

Así las cosas, la volatilidad de Bitcoin se nos presenta de un modo tan claro y distinto como su relevancia tecnológica. A lo largo de estos años, Bitcoin ha tenido que enfrentarse en una guerra abierta contra gobiernos enteros, como es el caso de China, y contra entidades bancarias supranacionales, como es el caso del Banco Central Europeo. En la mayoría de los casos, los poderes antagonistas se han visto obligados a readaptarse, lanzando sus propias criptodivisas o buscando los usos más favorables de la tecnología blockchain. Lo cierto es que Satoshi Nakamoto, esa entidad cuasi-etérea, virtual, del que se desconoce hasta el número de cuerpos que habita, ha sacudido unos aparatos por naturaleza reaccionarios. Nakamoto ha preguntado a los Estados y Bancos Centrales que rigen la economía mundial por la validez de su autoridad absoluta; y su invención ha obligado a obtener una respuesta.

[6] Hoy en día, esta fecha es celebrada por los más fervientes *crypto-bros* pidiendo pizza a domicilio, mostrando sus criptodivisas, y expresando su apoyo a la tecnología crypto en tus redes sociales en una efeméride que se ha bautizado como *Bitcoin Pizza Day*.

[7] Una infografía muy completa de los acontecimientos más relevantes de las criptomonedas puede ser consultado en la página oficial de la Oficina de Seguridad del Internauta en https://www.osi.es/es/campanas/criptomonedas/historia-criptomonedas

6. El protocolo Bitcoin de Nakamoto

El funcionamiento de la tecnología blockchain podría sintetizarse en la fórmula *Peer-to-Peer* más criptografía informática. El resultado de esta conjunción es la de un libro mayor distribuido que almacena información de las diferentes transacciones económicas, entendidas en sentido amplio[8], que se dan en una red blockchain entre todos sus usuarios, y que se protege de posibles vulneraciones internas o externas a partir su propio funcionamiento descentralizado y criptográfico. La idea que vertebra, pues, todo el mundo de las cripto-cosas no es otra que la idea de descentralización desde su propia estructura técnica. Pero tomemos ahora el protocolo Bitcoin presentado por Satoshi Nakamoto en su *whitepaper* como ejemplo paradigmático para explicar el funcionamiento de la tecnología blockchain en una aplicación donde, de hecho, está funcionando.

El dinero digital antes de que Nakamoto presentase su proyecto de Bitcoin ya existía con más o menos éxito en forma de cadenas de firmas digitales. Esto es, un usuario transfiere la moneda firmando digitalmente una secuencia numérica codificada a partir de la transacción previa, y la clave pública del siguiente beneficiario. Su funcionamiento, sin embargo, se topaba con el problema que acecha a cualquier moneda digital conocido como *double-spending* o doble gasto. Y es que el beneficiario de la moneda no tiene forma de comprobar que la moneda digital que le ha sido transferida no ha sido gastada ya en otra transacción. La solución común a este problema es establecer la institución de una autoridad central que tenga acceso al registro de todas las transacciones realizadas por los usuarios de la moneda. De esta forma, en una transacción cualquiera, la institución central responsable comprobaría el historial de transacciones del usuario constatando si efectivamente el usuario tiene la moneda que dice tener, y daría el visto bueno o no. Esta solución es insatisfactoria para Nakamoto, toda vez que el futuro de esa moneda depende en su totalidad de la compañía que gestiona dicha moneda. En este modelo, cada

[8] Decimos "en un sentido amplio" porque estas transacciones de, en esencia, información, no están circunscritas al dinero digital (este es el caso de las criptomonedas), sino que también se pueden dar en contratos laborales o de intercambio de activos de cualquier tipo (los s*mart contracts*) o en la posesión de activos digitales tokenizados (el caso del criptoarte y los NFTs).

transacción debe necesariamente pasar a través del organismo central para poder comprobar su validez, tal y como sucede con los bancos.

La única forma de superar el problema del doble gasto es, como hemos visto, conociendo todas las transacciones realizadas por el dueño de la moneda. Para que esta solución sea posible sin la necesidad de instituciones centrales o terceros de confianza, propone Nakamoto, "las transacciones deben ser públicamente anunciadas, y necesitamos un sistema para que los participantes convengan en una única historia del orden en el que fueron recibidos" (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, p. 2).

Las diferentes transacciones T_1, T_2, T_x… que ocurren simultáneamente en una ventana de tiempo determinada son, entonces, públicamente anunciadas. Los usuarios de esa red blockchain pueden comprobar que dichas transacciones sean viables, pues el historial completo de todas las transacciones realizadas es igualmente público. Las transacciones verificadas son ahora agrupadas en bloques diferentes. Una vez agrupas un número de transacciones válidas que complete el peso establecido por diseño en un bloque[9], este es codificado en una secuencia numérica conocida como hash, que funciona como una marca de tiempo y que también incluye al bloque anterior. Posteriormente, este hash es compartido a todos los miembros de la red que la asumen y añaden a la cadena de bloques principal para tener el mismo registro de transacciones, y se pasa a trabajar en el siguiente bloque. Es posible afirmar, así, que la moneda BTC no es más que este registro completo de todas las transacciones que se han dado en su red.

Podemos preguntarnos con acierto por qué razón los usuarios de una red blockchain elegirían un bloque sobre otro igualmente válido, o cómo definir qué cadena de bloques es la auténtica si se puede dar el caso en el que lleguen bloques distintos a la

[9] En el caso de Bitcoin, cada bloque puede agrupar aproximadamente un total de dos mil transacciones en un peso de un megabyte.

cadena[10]. Una posible solución a esto podría ser realizando una votación entre todos los usuarios de la red para decidir la cadena válida. Esta opción corre el gravísimo riesgo de sufrir una *sybil attack*, en la que un usuario malicioso infecta la red con multitud de computadoras virtuales creadas por él a partir de IPs falsas. El reto de crear consenso sin necesidad de terceros de confianza ni de votaciones virtuales se nos muestra ahora como uno titánico, y es en esta solución donde el protocolo Bitcoin es realmente revolucionario, potente, aunque también controvertido. Nakamoto, pues, tuvo la genial idea de utilizar *proof-of-work*, o prueba de trabajo, para construir su protocolo.

7. La genial idea de la prueba de trabajo

La idea de la prueba de trabajo es sin lugar a dudas el cemento que mantiene unido toda la estructura de la tecnología blockchain. Originalmente, la idea fue expuesta por Adam Back ya en 1997 en su trabajo llamado *Hashcash – A Denial of Service Counter-Measure*, y tenía como objetivo regular el abuso desmedido de recursos virtuales, especialmente los provocados por los *remailers*, una suerte de *spammers*[11] del momento.

El ingenioso programa *hashcash* permitía construir un token utilizando una pequeña parte de la potencia computacional de la CPU. Una vez hacemos abstracción del precio de venta pagado para la obtención de nuestros dispositivos inteligentes, como un teléfono móvil, una televisión, o un ordenador; la potencia computacional que exige su uso puede parecer gratuito. Nada más lejos de la verdad: el poder computacional no es gratuito, y si bien en la microescala del uso privado su coste puede ser más o menos baladí, en una escala mayor el gasto energético que exige se traduce en un consumo eléctrico que ha de ser pagado[12]. En este sentido, el token producido requería de un

[10] El intercambio de información en Internet no se produce a una velocidad universalmente constante debido a infinidad de factores, como puedan ser la conexión de la red, interferencias, el propio equipo, etc. De este modo, puede suceder que dos usuarios completen un bloque y lo anuncien públicamente, pero por este desfase temporal, a unos usuarios le llegue un bloque y a otros, otro; dando lugar así a registros de transacciones diferentes.

[11] Un *spammer* es una persona o programa informático que envía y reenvía de forma masiva correo basura, no deseado.

[12] El coste que aquí importa es el coste de la electricidad en dinero pero, en realidad, una perspectiva más amplia observa también que, como cualquier proceso que necesita de electricidad, se paga adicionalmente en contaminación ambiental.

pequeñísimo coste por el gasto energético que, en la pequeña escala del uso privado de enviar un par de correos a su destinatario, resultaba totalmente asumible. Sin embargo, en una escala mayor de enviar correos masivamente, bien por spam o para realizar un ataque DoS, suponía ya un gran primer obstáculo que podía disuadir aquellas amenazas. Esta misma genial idea es tomada por Nakamoto, sintetizada bajo el rótulo de p*roof-of-work*, y empleada no con menos ingenio en su proyecto de criptomoneda.

En el caso de Bitcoin, el algoritmo de hash utilizado es el SHA-256 (por sus siglas en inglés, *Secure Hash Algorithm*). Este algoritmo codifica cualquier input de datos, como pueda ser una fotografía, códigos informáticos que expresen un contrato, un bloque, etc., en una secuencia de números aparentemente aleatorios (256 bits en el caso del algoritmo SHA-256). La particularidad que posee este tipo de algoritmos, y lo que les proporciona también una gran seguridad, es que los mismos datos son siempre codificados en la misma secuencia de números, mas la alteración de un solo bit de información en los datos iniciales nos dará un código hash completamente distinto.

El input en Bitcoin, vemos ahora, será nuestro bloque que agrupa todas las transacciones ya verificadas que suceden durante una ventana de tiempo determinada, más un valor numérico que podremos ir cambiando. El "puzle" consiste en modificar ese valor numérico hasta que el algoritmo nos devuelva una secuencia de números, el código de hash, que comience con una cantidad determinada de ceros[13]. La única forma en la práctica de resolver este puzle es probando infinidad de valores numéricos hasta dar con la solución. No existe como tal un acertijo que resolver. Una vez obtenido ese valor numérico, el usuario podrá añadir ese bloque al registro general o libro mayor, y hará público su descubrimiento al resto de usuarios que, tras la verificación de su validez, añadirá igualmente ese bloque a sus cadenas. Este proceso es conocido como minado de bloque, y el usuario que resuelve el puzle, como minero[14]. Los mineros de bitcoin, cabe

[13] La dificultad de este acertijo es dinámica, esto es, varía según la potencia computacional que tenga la red para que sea resuelto en un tiempo prefijado en el propio código que, en el caso de Bitcoin, es de unos diez minutos.

[14] La metáfora es aún más rica si se tiene en cuenta que Bitcoin sueña con llegar a ser una suerte de oro digital, toda vez que, como aquella, existe un límite que puede ser minado. Se confía que a partir de esta escasez se alcance una estabilidad en su valor.

señalar, no invierten su poder computacional de manera altruista, sino que cada bloque que se agrega a la cadena de registros tiene asociado una recompensa: el minero que encuentre la solución tendrá el derecho a incluir una transacción especial en su bloque asignada a él como forma de pago por su trabajo, que consiste en una cantidad de bitcoins, y comisiones a medida que la cadena se alargue.

8. La controvertida idea de la prueba de trabajo

La aplicación de la idea de prueba de trabajo tiene un envés no tan agradable que acompaña a su genialidad. El método de minado digital en Bitcoin, como hemos visto, exige un enorme gasto energético, pero este mismo gasto posibilita el ansiado consenso por diseño, y confiere al sistema su gran seguridad. Como mencionamos con anterioridad, un pequeño cambio en algún bit de información del input que introduzcamos al algoritmo nos devolverá un código totalmente distinto. A su vez, cada bloque de la cadena de bloques está conectado con el posterior, por lo que la modificación de un bloque compromete todos los bloques ulteriores que deben ser nuevamente minados. Las redes blockchain, adicionalmente, se rigen por el criterio de la cadena más larga: así, la cadena que acumule el mayor número de bloques es la única válida, toda vez que es la que más poder computacional a través de pruebas de trabajo ha invertido.

Este criterio permite salvar el posible problema de que dos mineros encuentren la solución para sus bloques en el mismo instante de tiempo: una transacción podría ir a parar a cadenas de bloques distintos, y podría registrarse dos veces. Los miembros de la red mantendrán el bloque que le hubiese llegado, y continuarán con el minado del siguiente bloque. Llegará un momento en el que un minero encuentre la solución al siguiente bloque, lo registre y junte a su cadena, dando como resultado la cadena más larga y siendo, por tanto, esta la nueva cadena válida. La potencia computacional invertida en el bloque de la cadena huérfana queda, sencillamente, desechada; y el minero que la hubiese descubierto, sin recompensa.

Pero aún más importante, la preferencia por la cadena más larga, por la cadena que más prueba de trabajo acumula, otorga a la tecnología blockchain además de una poderosa barrera de seguridad, la posibilidad de crear consenso. En este sentido, si un usuario malicioso intentase vulnerar el sistema cambiando algún valor de un bloque, tendría que estar igualmente dispuesto a minar, gastando potencia computacional, todos los bloques que comprometiese así como los nuevos bloques que los usuarios honestos continuasen minando y añadiendo a la cadena más larga. Se alcanza un punto en el que sencillamente este gasto computacional extraordinario no es viable. El ritmo de minado necesario para superar a la cadena más larga que necesitaría un atacante para validar su vulneración deberá, pues, ser superior al resto de la red que trabaja honestamente. Para que esto suceda, el atacante debería contar con al menos el 51% total del poder computacional de la red blockchain entera. Algo, como podemos intuir, tan costoso que no llega a ser rentable. Mas, si aún este caso se diese, Nakamoto prevé que "el ambicioso atacante debería elegir si utilizar su potencia computacional para defraudar a gente robándole sus pagos, o generar nuevas monedas" (Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, p. 4). El atacante verá más beneficioso jugar bajo las reglas del juego y utilizar su poder computacional para minar nuevos bloques con su correspondiente recompensa. No cabrían dudas entre los usuarios de la red blockchain acerca de la validez de las transacciones reflejadas en la cadena de bloques.

En cualquier caso, este gran prodigio de la ciberseguridad; esta garantía de seguridad y prácticamente inmutabilidad de la cadena que brota no de ninguna institución u organismo central, sino de la misma naturaleza, del propio código del sistema que conjuga exitosamente informática, matemática y criptografía, se sustenta sobre un gasto energético sin parangón. Cuando presentamos el mecanismo de la prueba de trabajo, en su primer planteamiento casi inocente de medida contra el *spam*, advertimos ya que la potencia computacional ha de ser pagada no solo con dinero, sino con contaminación ambiental. Una de las estimaciones más fiables realizada por la Universidad de Cambridge situó el consumo anual de la red de Bitcoin en unos 125 TWh[15], equivalente

[15] La estimación data de junio del año pasado. A fecha de hoy, este consumo estimado se sitúa en 92 TWh. Este sensible descenso del gasto eléctrico en un 33% puede ser explicado por una siempre

al doble del consumo de toda Grecia. Si Bitcoin fuese un país, ocuparía el puesto número treinta en la escala de los más consumidores (QuantumFracture, 2021).

El uso de las distintas tecnologías informáticas no se pone nunca en cuestión: su llegada, implementación, y vertiginoso desarrollo ha cambiado para siempre nuestra forma de relacionarnos con el mundo, y lo ha cambiado a mejor. Sin embargo, en el desarrollo y la aplicación de las tecnologías que nos vienen es ineludible escrutar con una mirada crítica cuáles son los derroteros que nos abren. Resulta fácilmente previsible que la tecnología blockchain tendrá una importancia fundamental en nuestras vidas en un futuro próximo. Pero no en todas sus formas. La seguridad que confieren, y esa maravilla técnica de la *inmutabilidad*[16]encontrará sin lugar a dudas un gran espacio en ámbitos administrativos, burocráticos, y contractuales en general. La descentralización de su uso y su particular forma de construir consenso en base a su propio funcionamiento, permitirá construir alternativas a organismos centrales a la hora de decidir qué hacer con nuestro dinero. Su novedad y las grandes expectativas que dibuja encontrará, en fin, a igual de grandes especuladores que verán en su triunfo una victoria para sus bolsillos.

Parte III. Aplicaciones alternativas de blockchain

9. La expansión de blockchain

La tecnología blockchain diseñada con notable éxito para su aplicación como criptodivisa, ha traspasado ya desde temprano estos límites y se ha situado como una ventajosa herramienta en otros campos. Esta versatilidad para bañar otros espacios para los que no fue inicialmente concebida, y el ímpetu con el que ha pretendido cambiar la forma en la que nos relacionamos en el mundo digital, nos muestra sin duda una potencia y viveza resaltables. No es novedad para ningún filósofo, siempre atento a las cosas del mundo, constatar que nada de lo que el hombre construye, inventa o ingenia, se lo arroga

constante mejora en la eficiencia del minado pero, aún más importante, es la severa caída que están sufriendo las cripto-cosas. (Consultado en: https://ccaf.io/cbeci/index)

[16] Un notable economista especializado en Bitcoin y las redes blockchain se maravillaba ante lo *eterno* de esta tecnología, y afirma advirtiéndonos antes de que no le gusta mentar cuestiones metafísicas: "El libro mayor de transacciones de Bitcoin debe ser el único conjunto de hechos objetivos en el mundo" (Ammous, The Bitcoin Standard, 2018, p. 192). Nos parece ahora natural las razones por las que no le gusta traer a colación "cuestiones metafísicas".

para sí; y difícilmente no encontrará otro como él una motivación, un ejemplo, o una inspiración en sus acciones. En el caso que aquí nos compete, blockchain ha demostrado tener gran potencial para ser muy útil con otras aplicaciones, aunque también su éxito ha servido a especuladores y avariciosos de todo el globo para sus propósitos. Estudiemos, brevemente, los campos en los que más expectativas ha despertado.

Un rasgo muy valioso de blockchain que hemos estudiado es que es capaz de crear escasez digital. En el mundo digital, todo es replicable *ad infinitum* de un modo perfecto. Una imagen, un texto, un sonido no son en la virtualidad nada más que un conjunto de unos y ceros. Todo el valor que se ha generado ha sido siempre merced a organismos centrales que son sólidas, compactas, tangibles. Así, nadie de nosotros en su sano juicio pagaría ni un céntimo de euro por una imagen de *La Gioconda* en Internet que puedo obtener gratuitamente con una simple búsqueda. Nadie pagaría tampoco por unos tokens virtuales que no valen nada, a menos que estos tokens estén sostenidos por un organismo central, como puede ser una empresa de videojuegos, que regularice que esos tokens darán ciertas ventajas en su programa. No existía en Internet, en un sentido estricto, valor de las cosas virtuales por ser virtuales. Y con razón, pues solo un insensato podría pagar por algo que todos los demás consiguen gratis.

Otro rasgo de blockchain que también ha generado gran interés es el de su seguridad e inmutabilidad. Estas grandes ventajas se han planteado y desarrollado ya en los conocidos como *smart contracts*. Los *smart contracts* o contratos inteligentes consisten en códigos informáticos, o scripts, que a la manera de una aplicación o programa informático, almacenan comandos y órdenes. El uso, pues, para aligerar los aparatos burocráticos parece evidente. Es probable que en un futuro próximo los contratos laborales, de propiedad, o hasta las votaciones, utilicen la tecnología blockchain para garantizar su seguridad.

10. Criptoarte y NFTs

El *Nyan Cat* es un vídeo animado en *pixel art* de un gato espacial que va dejando un reguero de arcoíris a medida que navega el ciberespacio. Está reproducido en bucle durante unos tres minutos y treinta segundos, y se convirtió en meme de Internet hace una

década. A comienzos del año pasado, su NFT fue vendido por unos 600000$. El vídeo seguirá estando accesible para cualquiera que quiera verlo.

Los *Non Fungible Tokens* o NFTs son la aplicación directa de la tecnología blockchain en el mundo del arte. En su traducción literal, obtenemos que las NFTs son tokens no fungibles. Los bienes fungibles, como el dinero, son cosas reemplazables que se agotan en su uso. Una moneda de un euro es totalmente reemplazable por otra moneda de un euro. Una obra de arte, en cambio, es un bien no fungible pues es única, y aunque existan copias de ella, fotografías, escaneos digitales, etc. siempre existirá el objeto original a partir del que ha sido fabricado. Esto, en el mundo digital, como hemos visto, no es posible. O parecía no serlo hasta que blockchain trató de conseguirlo.

Del mismo modo que la tecnología blockchain ha permitido crear criptodivisas cuyo valor radica en que su libro mayor o historial de transacciones resulta inalterable, en el mundo del arte ha posibilitado la creación de ficheros igual de inamovibles que acreditan la posesión de un bien digital. En un caso práctico, un artista digital podrá individualizar su obra, o crear una escasez de un número determinado a partir de NFTs. Estos NFTs, que no son más que ficheros de metadatos, pueden ser comercializados y vendidos, sellando así el intercambio. El comprador se quedaría con ese fichero que indicaría que esa obra determinada de la que solo hay cinco ejemplares, es suya. Todo este proceso, al igual que con las criptomonedas, ocurriría de manera descentralizada, sin necesidad de casas de arte que, junto a una comisión, asegurasen el proceso. A su vez, blockchain mantendría un registro de ese NFT comprado y, en caso de que fuese revendido, el autor original continuaría ganando ingresos por su obra. De esta forma, nos puede parecer que la aplicación de blockchain en el mundo del arte proporciona al artista una mayor independencia sobre su obra, y le permite rentabilizarla de manera más efectiva.

La aplicación de blockchain en el criptoarte, en obras digitales de cualquier tipo, o en videojuegos, ha sido sin duda una de las aplicaciones más flagrantemente especulativas que ha tenido. En ninguno de esos casos, ha existido otro interés más allá

del especulativo, y su promoción para captar a nuevos usuarios que mantuviesen la rueda ha llegado a ser embarazoso. En el caso de una obra digital, bien sea una imagen, un sonido, o un vídeo, la posesión de un NFT no te asegura ni la autoría de la obra, ni su exclusividad: solamente te proporciona un fichero que indica que posees el NFT de esa obra. Mas cualquier otro usuario de Internet que quisiese ver esa imagen, escuchar ese audio, o reproducir ese *Nyan Cat*, podrá hacerlo. El valor de los NFTs, hace un año por las nubes, hoy se encuentran bajo tierra. Y no se puede olvidar nunca las vidas que ha arruinado de incontables personas, y toda la contaminación inútil que ha generado.

Conclusión

La llegada de la tecnología blockchain merced al ingenio de Nakamoto en su proyecto Bitcoin, no ha dejado indiferente a nadie. Lo que en un principio parecía un experimento más entre un nicho de *geeks* informáticos, ha hecho levantar la vista de organismos mundiales, bancos centrales, gobiernos y naciones. Ante este choque, no se ha tardado en crearse dos frentes, los *crypto-bros* y los *crypto-haters* que de una forma fundamentalista defienden sus posturas. Resulta perentorio para cualquiera que desee comprender el alcance de las nuevas tecnologías, estudiar con sobriedad sus ventajas, sus peligros, y sus inconvenientes para las sociedades en su conjunto.

En este trabajo, se ha intentado estudiar a fondo esta tecnología y sus diferentes aplicaciones, para entender mejor cuál puede ser el futuro que construya. Una de las tareas más nobles de la Filosofía es precisamente tratar calmar las revueltas aguas de la realidad, aportando esos recursos conceptuales que permitan su comprensión y asimilación. Descubrimos, no obstante, una vez más, que las respuestas definitivas no solo comprometen de manera total al que las da como si estuviese dotado de omnisciencia, sino que tampoco son siempre necesarias. Nos contentamos con haber iniciado una investigación que no puede terminar aquí, pues ha levantado nuevas cuestiones.

Bibliografía

1. Alizart, M. (2020). *Criptocomunismo.* Buenos Aires: Ediciones La Cebra.
2. Ammous, S. (2018). *El Patrón Bitcoin.* Barcelona: Deusto.
3. Ammous, S. (2018). *The Bitcoin Standard.* New Jersey: Wiley.
4. Assange, J., Appelbaum, J., Müller-Maguhn, A., & Zimmermann, J. (2012). *Cypherpunks: La libertad y el futuro de Internet.* Barcelona: Deusto.
5. Back, A. (2002). *Hashcash - A Denial of Service Counter-Measure.* Obtenido de hashcash.org: http://www.hashcash.org/papers/hashcash.pdf
6. de Larra, M. (2022). *Vuelva usted mañana.* Obtenido de Biblioteca Virtual Miguel de Cervantes: https://www.cervantesvirtual.com/obra-visor/vuelva-usted-manana--0/html/ff7a5caa-82b1-11df-acc7-002185ce6064_2.html
7. Dot CSV. (23 de Mayo de 2021). Hoy sí vas a entender qué es el blockchain - (Bitcoin, Cryptos, NFTs y más) [Vídeo]. YouTube. Obtenido de https://www.youtube.com/watch?v=V9Kr2SujqHw&t=1162s&ab_channel=Dot CSV
8. European Central Bank. (2012). *Virtual Currency Schemes.* Frankfurt: EuroSystem.
9. Golumbia, D. (2016). *The Politics of Bitcoin.* Minneapolis: University of Minnesota Press.
10. Kermarrec, A. M., & Taïani, F. (2015). Want to scale in centralized systems? Think P2P. *Journal of Internet Services and Applications*(16). Obtenido de https://jisajournal.springeropen.com/articles/10.1186/s13174-015-0029-1
11. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Obtenido de Bitcoin.org: https://bitcoin.org/en/bitcoin-paper
12. Nakamoto, S. (2008). *Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario.* Obtenido de Bitcoin.org: https://bitcoin.org/en/bitcoin-paper
13. Pérez-Solà, C., & Herrera-Joancomartí, J. (2014). Bitcoins y el problema de los generales bizantinos. *RECSI 2014*.

14. QuantumFracture. (27 de Junio de 2021). ¿Es Bitcoin un atentado contra el Medio Ambiente? | Criptomonedas y Contaminación [Vídeo]. YouTube. Obtenido de https://www.youtube.com/watch?v=H_djHCQSl0A&t=618s&ab_channel=QuantumFracture

15. QuantumFracture. (30 de Mayo de 2021). Han comprado el NFT de este vídeo por 4533,83€ | El criptoarte y los NFTs explicados [Vídeo]. YouTube. Obtenido de https://www.youtube.com/watch?v=YKRpRmnIN_g&ab_channel=QuantumFracture

16. QuantumFracture. (23 de Mayo de 2021). Por qué el dinero no vale nada (y por qué las criptomonedas podrían sustituirlo) [Vídeo]. YouTube. Obtenido de https://www.youtube.com/watch?v=pqEidVW9da0&ab_channel=QuantumFracture

17. Steinmetz, R., & Wehrle, K. (2005). *Peer-to-Peer Systems and Applications.* Berlín: Springer.

18. Swan, M., & De Filippi, P. (2017). Toward a Philosophy of Blockchain: a Symposium. *Metaphilosophy*.

19. University of Cambridge. (2022). *Cambridge Bitcoin Electricity Consumption Index*. Obtenido de The Cambridge Centre for Alternative Finance: https://ccaf.io/cbeci/index

20. W. Chohan, U. (2022). *A History of Bitcoin.* Obtenido de SSRN: https://ssrn.com/abstract=3047875