Facultad de Ciencias Humanas y Sociales
Grado en Relaciones Internacionales

Trabajo Fin de Grado

Estudio del Bitcoin y el Blockchain como alternativa real al sistema monetario actual

Estudiante: Salvador Sánchez-Terán Manzanedo

Director: Luis Gaviria

Madrid, Mayo 2022

Índice de ilustraciones

Índice de Tablas

0. Resumen Ejecutivo

El sistema monetario actual se encuentra desafiado por el Blockchain y las Criptomonedas, que son soportadas por esta tecnología. La más conocida de ellas es Bitcoin; que se creó con el claro intento de dar una alternativa a la centralización predominante en el sistema financiero. No obstante; a pesar de que la gran utilidad de las soluciones que presenta la tecnología Blockchain y el furor que rodea a la criptomoneda Bitcoin; son muchos los factores que dificultan el desafío real de Bitcoin y el Blockchain al sistema financiero, especialmente a los Bancos Centrales.

En primer lugar, la mayoría de los Bancos Centrales como el Banco Central Europeo o la Reserva Federal han iniciado el desarrollo su propia divisa online. Entre otros motivos, para hacer frente a las alternativas que suponen las ciptomonedas. Otros como el Banco Central Chino ha impuesto fuerte restricciones a esta industria. No obstante, es inevitable que esta tecnología afecte al sector financiero; al igual que muchos otros; por eso es importante entender su origen, las motivaciones de su creación, los conceptos fundamentales de como funciona y sobretodo los factores principales que han imposibilitan a los primeros intentos de criptomoneda y Blockchain a representar una alternativa real y sostenible a los Bancos Centrales.

Palabras clave: Criptomoneda, Blockchain, proof of work; descentralización, eficiencia

Abstract

The current monetary system is challenged by the Blockchain and Cryptocurrencies, which are supported by this technology. The best known of these is Bitcoin; which was created with the clear intent of providing an alternative to the predominant centralization in the financial system. However; despite the great usefulness of the solutions presented by Blockchain technology and the furor surrounding the Bitcoin cryptocurrency; there are many factors that hinder the real challenge of Bitcoin and the Blockchain to the financial system, especially to Central Banks.

First of all, most Central Banks such as the European Central Bank or the Federal Reserve have initiated the development of their own online currency. Among other reasons, in order to face the alternatives of cyptocurrencies. Others, such as the Chinese Central Bank, have

imposed strong restrictions on this industry. However, it is inevitable that this technology will affect the financial sector; like many others; so it is important to understand its origin, the motivations for its creation, the fundamental concepts of how it works and above all the main factors that have prevented the first attempts of cryptocurrency and Blockchain to represent a real and sustainable alternative to the Central Banks.

Keywords: Cryptocurrency, Blockchain, proof of work; decentralization, efficiency.

1. Introducción

El mundo en el que vivimos se ve forzado a adaptarse a una tecnología que se desarrolla de manera exponencial; en apenas unas décadas se han desarrollado nuevas formas de almacenar, transmitir y configurar datos; entre estas formas destaca el Blockchain; una tecnología de almacenamiento de datos que desafía el orden establecido.

A pesar de que el día de ayer se parezca a nuestro día de hoy y al de mañana, la realidad es que en este mismo tiempo que vivimos se está produciendo quizás la revolución más vertiginosa de la historia del ser humano. Desde la creación del Internet en 1983; el mundo, y especialmente occidente, ha sufrido o se ha beneficiado de una rapidísima revolución tecnológica; apenas 40 años más tarde el mundo es notoriamente distinto en lo que respecta a la tecnológica. Tan rápido ha sido este cambio que la diferencia generacional de conocimientos técnicos es superlativa y con grandes consecuencias (Y. Hernandez, 2019).

No obstante, ahora estamos viviendo una segunda revolución tecnológica en varios aspectos; la digitalización de nuestra vida profesional y personal se esta acelerando; entre otros factores; principalmente por la pandemia; y mucha tecnología a la que hemos ido accediendo desde finales del sigo pasado está siendo revisada con el fin de mejorar deficiencias que presentaban.

El máximo exponente de este fenómeno es el llamado “Blockchain”. Esta es una tecnología que se puede explicar con mucho detalle y abarcando toda su complejidad, pero que de forma simplificada se puede decir que es una forma distinta de traspasar datos a la que prevalece actualmente. La propuesta de Blockchain es el traspaso de una forma descentralizada; donde la verificación del traspaso la hacen una red de ordenadores. Mientras que el sistema actual (centralizado) se rige por una tercera parte que goza del poder necesario para verificar la transacción.

La alternativa que simboliza Blockchain coge especialmente fuerza después de la crisis del 2008. Lo hace como soporte de Bitcoin una criptomoneda. No obstante, Blockchain es más amplio que Bitcoin; nace por ciertos motivos y tiene muchos más usos, que abarcaremos más adelante. Pero es importante saber que detrás del famoso Bitcoin hay una tecnología mucho más amplia, con muchísima utilidad: desde la posibilidad de reducir o eliminar los

fraudes electorales hasta revolucionar la industria alimenticia permitiendo un mayor rastreo del origen y trayectoria de los alimentos.

De entre todos los usos que se le puede dar al Blockchain nosotros nos centraremos en su impacto en las instituciones Financieras, especialmente en los Bancos Centrales. Esto se debe a que es el sector donde el Blockchain supone un mayor valor de mercado (Statista, 2020)

Por tanto, está claro que Blockchain es una nueva tecnología que desafía a un sistema anterior. Esta alternativa presenta varias ventajas al igual que ciertos inconvenientes, que estudiaremos más adelante. Además, tiene infinidad de usos y por tanto de impacto. Las oportunidades que presenta Blockchain son bien conocidas y son muchas las empresas e instituciones que están estudiando o implementando su uso. Solo en 2021 el gasto mundial destinado a buscar soluciones con Blockchain alcanzo 6,6 Mil millones de dólares americanos (Statista, 2022). Otro dato que refleja el creciente interés en esta tecnología es el aumento de la financiación de capital riesgo en empresas emergentes de blockchain en todo el mundo en los últimos 6 años: en 2016 esta financiación era de 0,8 miles de millones de $; mientras que en 2021 ascendía ha 2,6 miles de millones de $. Por tanto, es extremadamente útil familiarizarse con esta nueva tecnología, porque si no o hace ya, en un futuro muy próximo tendrá un impacto en nuestras vidas; y no solo a través del sector bancario.

1.1 Objetivo

El objetivo de este trabajo es analizar que repercusiones tendría sustituir la economía centralizada en torno a Bancos Centrales por la descentralizada que propone la tecnología Blockchain. Para ello estudiaremos el impacto que tiene esta tecnología en la industria económica, concretamente su impacto en los Bancos Centrales.

1.2 Metodología

Este trabajo nace de una conversación que tuve hace un año, donde un amigo afirmaba contundentemente que la economía iría mejor sin los Bancos Centrales y usando monedas como Bitcoin que están descentralizadas. Para ello comenzó a enumerar una larga lista de errores de los Bancos Centrales y otra lista pareja de las virtudes del Bitcoin y Blockchain.

Me pareció un tema sumamente interesante y complejo. Creo que existe cierto consenso entorno a la existencia de errores de los Bancos Centrales. Estoy de acuerdo en que comenten fallos; el propio Bitcoin se creo con el propósito de hacer frente a las instituciones financieras que había defraudado a los ciudadanos; y en gran medida causado la crisis del 2008.

No obstante, dudo que evidenciar los errores de un modelo, automáticamente valide el modelo contrario. Creo que Bitcoin y Blockchain están viviendo unos años de fuerte crecimiento; en parte por su valor, que lo tienen, pero también por una ilusión desmedida. Es decir, creo que la percepción del ser humano, en general, actualmente, esta castigando en exceso la economía centralizada (Bancos Centrales) y recompensando también en exceso a la descentralizada (Bitcoin). Con este debate abierto me propongo analizar que alternativa propone realmente Blockchain a los Bancos Centrales y que ventajas he inconvenientes esta supone.

Para ello investigaré entre una amplia red de documentos sobre este tema; dado que no se trata de medir la opinión pública no será necesario encuestas.

1.3 Revisión bibliográfica

La bibliografía del presente trabajo de investigación tiene como pilar el libro de *El Patrón del Oro del Bitcoin* de Saifedean Ammous (Deusto, 2018), que tiene como principal idea explicar las deficiencias de los Bancos Centrales y exponer las soluciones que aporta adoptar el Bitcoin como moneda.

Asimismo, la investigación del proyecto se ha realizado tanto en páginas oficiales (por ejemplo, El Banco Central Europeo, Reserva Federal como en artículos científicos y de opinión de grandes medios de comunicación nacionales (La Vanguardia, La Razón) e internacionales (Washington Post, Forbes).

1.4 Estructura

Esta investigación se divide en tres grandes partes. Primero entenderemos que es el Blockchain y el Bitcoin. Imprescindible familiarizarnos con estos conceptos tan disruptivos. Para ello estudiaremos de es lo que son técnicamente, su origen, la motivación de su creación y en que ha derivado.

Una vez tengamos un cierto grado de entendimiento sobre estos conceptos podremos estudiar que impacto han tenido en las economías y los Bancos Centrales. Nos centraremos en el Banco Central Europeo, en la Reserva Federal de Estados Unidos y en el Banco Popular Chino. Una vez tengamos claro que supone esta tecnología y como ha impactado recientemente a los mayores Bancos Centrales del mundo, podremos entonces estudiar que consecuencias tendría un futuro con una economía descentralizada, y hasta que punto es posible.

Además de estas tres partes, este trabajo tiene, como es requerido, una Introducción, conclusión y Bibliografía.

2. ¿Qué son Criptomonedas y su tecnología: Blockchain?

2.1 Origen

2.1.1 70s – 2008

Para entender bien que representa el Bitcoin hay que entender su origen. Desde los años 80 surge un pequeño grupo de gente con conocimientos informáticos que abogan por un internet sin el control del Estado. Su pensamiento se alinea bastante a la corriente, predominantemente estadounidense, libertaria. Muchos estudios apuntan al desarrollo de este tipo de tecnología con los pensamientos más de extrema derecha de Estados Unidos (J. Baldwin, 2018).

La corriente libertaria es un movimiento político-filosófico que toma como principal valor la libertad individual. Son herederos del liberalismo desarrollado por el economista Adam Smith; o los filósofos John Stuart Mill y John Locke. Para ellos los humanos tenemos unos derechos inviolables entre los que están la libertad de expresión, religión, asociación,

igualdad ante la ley y la búsqueda de cada concepto personal de felicidad. El gobierno debe limitarse a garantizar estos derechos de los ciudadanos, y cada uno puede expresar sus derechos hasta que interfieran en los del siguiente. En resumen, son liberales clásicos que ponen el énfasis en la libertad individual y la limitación del gobierno para intervenir en la vida de sus ciudadanos (D. Boaz, 2009).

El origen de este movimiento se remonta a la década de los 70; hasta esa década la criptografía era principalmente usada y desarrollada como una nueva tecnología militar. Esto cambio cuando el gobierno de Estados Unidos publicó el "Data Encryption Standard" en 1977. La criptografía es la técnica que se ocupa de codificar mensajes para que no puedan ser interpretados por receptores no autorizados (G. Granados 2006). A partir de esta década la criptográfica se abre al público y se crea un pequeño movimiento que une los pensamientos del movimiento libertario con la nueva tecnología disponible critográfica. Este movimiento es conocido como "cryptopunks" o "crypto-anarchist" (S. Bandyopadhyay, 2018). Durante las dos últimas decadás del siglo XX este grupo se hizo cada vez más fuerte y fueron varios los intentos de hacer algo parecido a lo que hoy es Bitcoin.

En 1992 se publica el primer Crypto Anarchist manifesto; donde su autor Tim C. May define:

"...Tecnología informática que permite a individuos y grupos comunicarse... de forma totalmente anónima... intercambiar mensajes, llevar a cabo negocios y negociar contratos electrónicos sin conocer nunca el verdadero nombre, o la identidad legal, del otro... no rastreable, a través de un amplio redireccionamiento de paquetes encriptados"

2.1.2 2008 – 2011

En estos círculos de corriente libertaria es donde es creado Bitcoin; se tuvieron que juntar dos condiciones para que definitivamente fuese creado; la primera es la experiencia previa de dos décadas de experimentos y desarrollo tecnológico; la segunda es la crisis financiera del 2008. Las instituciones financieras de todo el mundo sufrieron grandes perdidas, movidas principalmente por la crisis de las "*subprime*"; un activo que termino siendo altamente arriesgado pero que fue permitido durante mucho tiempo por la avaricia de los ciudadanos y la avaricia e irresponsabilidad de las instituciones financieras (Wharton,

2021). El culmen de esta caída a la crisis fue la banca rota del banco americano Lehman Brothers el 15 de Septiembre de 2008. Un mes y medio más tarde un usuario de internet llamado Satoshi Nakamoto envía un correo a una lista de mails de cyberpunks. En este correo presenta Bitcoin al mundo. Explica lo que es; anuncia la página web de Bitcoin y presenta el "Bitcoin White Paper"; donde explica como funciona esta criptomoneda.

Satoshi Nakamoto, el autor o grupo de creadores de esta criptomoneda explica en el resumen de este documento la motivación de crear esta moneda:

"Una versión puramente peer-to-peer del dinero electrónico permitiría que los pagos en línea se enviaran directamente de una parte a otra sin pasar por una institución financiera. La firma digital es una parte de la solución, pero las principales ventajas se pierden si se sigue necesitando un tercero de confianza para evitar el doble gasto. Proponemos una solución al problema del doble gasto utilizando una red de pares."

Fuente: Bitcoin White Paper. Bitcoin.org

Esta iniciativa fue recibida con un modesto éxito, pero el suficiente para que en los años siguientes se desarrollase completamente la idea, con cada vez más personas participando; estos primeros usuarios eran principalmente gente con conocimientos informáticos que les atraía la idea de una moneda descentralizada. Pero todo esto cambio con el comienzo de la nueva década.

2.1.3 2011 – 2017

En 2011 el creador de Bitcoin desaparece completamente de Internet. Hasta entonces no había revelado su identidad, pero si participaba en foros, respondía dudas sobre Bitcoin, o hacía mejoras en su red. No obstante, sus intervenciones pararon al completo y desde entonces no se ha sabido nada de el. Esto se podía hacer porque Bitcoin al ser descentralizado no requiere de alguien que lo mantenga; se sustenta con la propia participación de sus usuarios.

No se sabe porque el creador de Bitcoin paró sus intervenciones al completo en este año; pero una de las posibles causas es que se pervirtió su idea "libertaria" de una divisa fuera

del control del gobierno y las instituciones financieras causantes de la crisis del 2008. Al contrario, Bitcoin amasó gran popularidad entre los negocios ilegales; pues aparentemente estaba fuera del control del gobierno y la policía. De esta forma Bitcoin pasaba a ser la manera preferente de pago en redes de venta de armas, esclavos y drogas.

La mas notoria de todas es "Silk Road". Un mercado negro online, creado por un programador americano llamado Ross Ulbricht. La web fue lanzada en febrero de 2011; usando Bitcoin como medio de pago; dos años más tarde, en 2013, la web fue cerrada por el Buró Federal de Investigaciones (FBI); y su creador fue arrestado (M C. Van Hout; T. Bingham, 2014).

A finales de ese mismo año, Bitcoin sufrió otro gran golpe. El 5 de diciembre el Banco Popular de China prohibía a las instituciones financieras de su país comerciar esta criptomoneda. Al prohibir comprar Bitcoin con la moneda estatal, el Yuan, restringía esencialmente su comercio. Esta fue la primera de varias restricciones que ha puesto China a Bitcoin (BBC, 2013).

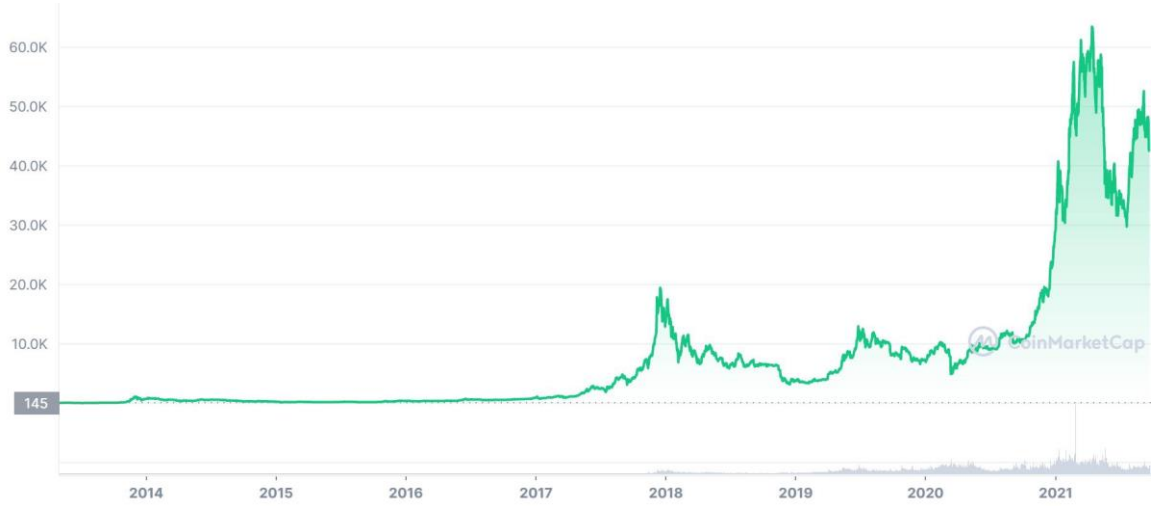
No obstante, a pesar de ser usado para actividades ilegales y empezar a ser restringido por grandes potencias económicas; el Bitcoin fue cogiendo fuerza hasta que a finales de la década formo parte de un gran movimiento especulativo.

2.1.4 2017 – Presente

A comienzos del 2017 el precio del Bitcoin superó la barrera de los 1.000$; y cerro el año con su máximo histórico hasta la fecha de $19,345.49 el 15 de diciembre (Investopedia, 2022). Tras alcanzar este máximo el precio cayo y se mantuvo relativamente estable hasta la pandemia COVID-19, tras la cual volvió a sufrir otra enorme subida.

Estos fuertes movimientos bursátiles generaron mucha incertidumbre acerca de que era este activo tan volátil; muchos inversores economistas, periodistas y hasta el Banco de Estonia han prevenido que puede tratarse de un esquema Ponzi. No obstante; según remarca el profesor de derecho de la Universidad de Chicago Eric Posner, para que sea un esquema Ponzi debe haber un componente de fraude, sin embargo, los agresivos movimientos de la cotización del Bitcoin se asemejan más a una ilusión colectiva.

Ilustración 1: Cotización Histórica del Bitcoin



Fuente: Coinmarketcap

2.2 Qué son

2.2.1 Bitcoin

Bitcoin esencialmente es una divisa. Pero que tiene muchas diferencias respecto al resto de monedas, que ahora explicaremos y además ha sido usada como un activo altamente especulativo; pero detrás de un activo altamente volátil, hay un proyecto más profundo de gobernanza monetaria y detrás de ese proyecto hay una tecnología revolucionaria que tiene más usos que Bitcoin. Entendamos primero que es Bitcoin.

Transacciones – Cómo se verifican las Bitcoins

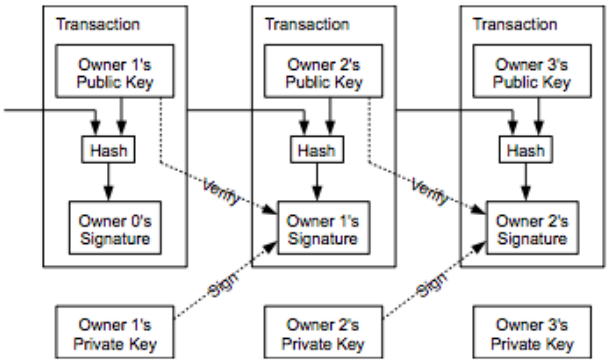
Si nos proponemos enviar dinero electrónico a otra persona; esencialmente la transacción cumplirá estos requisitos: Pongamos que Juan quiere enviar 1€ a María. El que envía el dinero dará la orden de envió; esta será recibido por una tercera entidad (en este caso nuestro Banco); que primero comprobará que Juan tiene 1€ en su cuenta; después procederá a enviar el euro a María. El problema de esto es que dependemos de una tercera entidad para realizar esta transacción; esto requiere que un cierto grado de confianza en la tercera entidad; que como hemos visto en los apartados anteriores; los creadores de estas criptomonedas no tenían; por eso proceden a diseñar un sistema de pago si la intervención de una tercera entidad.

Para realizan los siguientes cambios: las transacciones serán de conocimiento público; todo el mundo podrá observar los intercambios de moneda. Esto no quiere decir que el público sepa que individuos hacen las transacciones; pues recordemos que el objetivo principal es mantener la libertad individual al igual que su privacidad. Para ello cada individuo realizará las transacciones a través de una clave privada.

Una vez que abres las transacciones al ojo público, este público es el que debe verificar que la transacción se puede hacer. Es decir; el público tiene un registro completo de todas las transacciones hechas desde el origen. De este modo si Juan quiere enviar una moneda a María; será la red pública de usuarios quien rastree todas las transacciones anteriores hasta confirmar que efectivamente la "cuenta" de Juan tiene ese dinero para enviar. Es decir; lo que has hecho es traspasar la confianza de una tercera entidad a una red pública, manteniendo el anonimato.

Técnicamente esta transacción se realiza de esta forma: Bitcoin es una red de firmas digitales; sostenida por la tecnología Blockchain. Para hacer una transacción el propietario de una Bitcoin deberá firmar un *Hash* con la transacción anterior (del registro público de transacciones); añadiendo la clave del monedero del beneficiario de la acción junto con la moneda que quiere enviar.

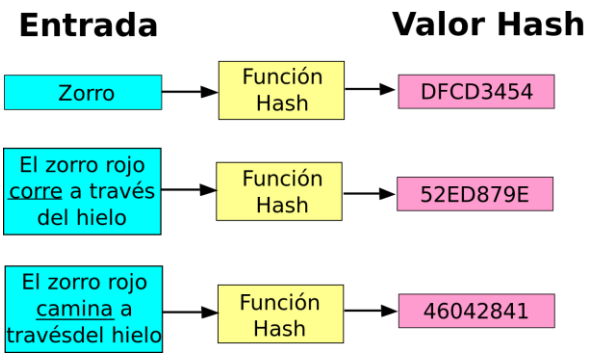
Ilustración 2: Sistema de firmas en transacciones de criptomonedas



Fuente: Bitcoin White Paper

El Hash es básicamente una fórmula que transforma unos inputs en unos outputs.

Ilustración 3: Función Hash



Fuente: FreeCodeCamp

Esta función Hash es la encargada de registrar la cantidad de dinero que se quiere enviar; a donde se quiere enviar y unirla a la última transacción para continuar el registro público de transacciones.

Bitcoin Mining: Cómo se crean las Bitcoins

Minar Bitcoin es el término con el que se conoce al proceso de creación de esta moneda y su puesta en circulación. Esto se consigue a través de unos ordenadores que resuelven una serie de problemas matemáticos. Cuando lo resuelven, proceden a descubrir un nuevo "bloque" que es añadido al Blockchain. Este bloque no es más que una estructura de datos. Digamos que es como una caja donde metes datos. El ordenador minero cuando consigue resolver el problema crea una nueva caja vacía donde se pueden meter datos. ¿Qué datos se meten? Las transacciones. Recordemos lo que hemos visto antes; el listado de transacciones públicas no es una lista tal cual; estas transacciones se agrupan en bloques; por tanto, el listado público es de bloques (cajas); donde dentro están las transacciones hechas.

Una vez que el minero crea el bloque; y este se llena de datos de transacciones; este bloque tendrá que ser validado; es decir; que la mayoría de los ordenadores mineros; comprueben el historial de transacciones públicas para verificar que las transacciones de este nuevo bloque pueden hacerse; si esto ocurre el bloque, entonces, será cerrado y pasará a formar parte del Blockchain.

Costes y beneficios de Minar

Los costes de minar son esencialmente tiempo de CPU y electricidad. Estos costes en el origen eran muy pocos, se podía minar con cualquier ordenador personal; no obstante, ahora los costes se han elevado mucho y solo se puede minar con grandes estructuras de ordenadores, que consumen grandes cantidades de energía.

Este consumo ha sido criticado por muchas corrientes medioambientalistas; al igual que muchos detractores del Bitcoin. También ha sido usado como pretexto para imponer restricciones al comercio y minería de la criptomoneda.

Los beneficios de minar Bitcoin provienen de dos fuentes. La primera es que la red Blockchain recompensa a los mineros otorgándoles monedas Bitcoin. El segundo incentivo es a través de tasas de transacción. Si el coste de validar las transacciones es mayor que el input recibido por el Blockchain, los mineros pueden cobrar una tasa.

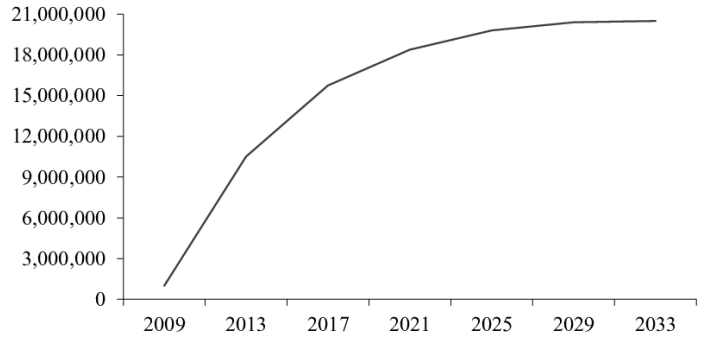
La primera tasa de cambio entre Bitcoin y Dólares se fundamento en el coste de producir una Bitcoin. Hasta el 5 de octubre de 2009, Bitcoin carecía de un valor real; fue entonces cuando en una casa de cambio llamada New Liberty Standard, se intercambió 1.309,03 BTC por 1 dólar. Esta tasa de cambio se estableció por el coste energético de minar una Bitcoin (R. Włodarczyk, 2021). Este intercambio establecía un valor por Bitcoin de 0,0008$ por Bitcoin. Hoy en día su precio oscila entre los 40.000$. (Bloomberg).

Bitcoin Halving – Cómo se regula la inflación de Bitcoin

Ya sabemos como se crea esta divisa y como se traspasa de forma segura y validada. Pero ¿Cómo se sostiene el valor? Si fuese un bien ilimitado carecería de valor alguno. Por eso está creado con un fin y un sistema que pretende garantizar su valor. Es decir, está creado para asemejarse a la producción del oro.

Existe un numero limitado de Bitcoins que pueden ser minadas (creadas y puestas en circulación). Este numero es 21 Millones; pero su creación es cada vez más costosa. Esto se debe a uno de los elementos más importantes del Bitcoin; que es el *Halving*. (en español: “reducir a la mitad”).

Ilustración 4: Evolución histórica y futura de creación de nuevas Bitcoin



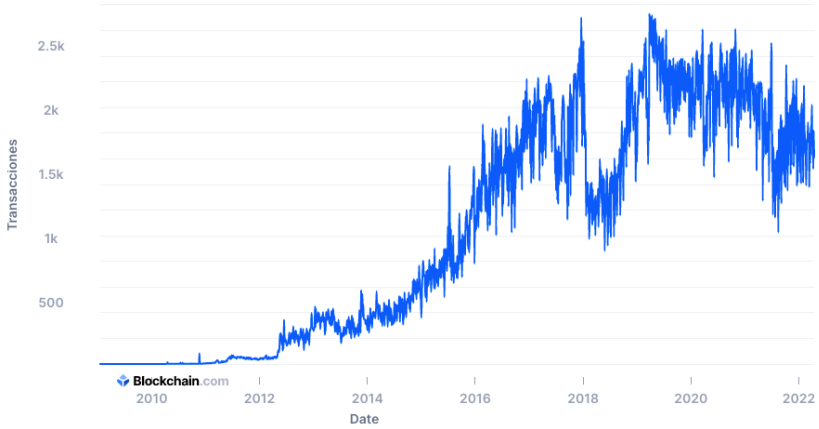
Fuente: Researchgate

Este sistema tiene como objetivo inducir inflación en el precio de la criptomoneda a partir de reducir el número de monedas puestas en circulación paulatinamente, consiguiendo así aumentar la demanda. Como hemos visto antes, los mineros los mineros gastan tiempo y energía en resolver problemas matemáticos; que al lograrlo crean bloques donde se almacenan transacciones, Estas transacciones deben ser validadas por nodos (ordenadores mineros y validadores o ordenadores que solo se dedican a validar). Una vez validados (al comprobar en el registro público de transacciones), el bloque de transacciones es cerrado y pasa a formar parte de la cadena Blockchain, que es el registro público de todas transacciones. En este punto se recompensa a los mineros del bloque con nuevas Bitcoins.

¿Cuántas BTC se les recompensa? He aquí la cuestión; al igual que la cantidad de oro es limitada, y la gran mayoría ya se comercializa; cada vez resulta mas difícil encontrar oro. Lo mismo pasa con Bitcoin, a mayor cantidad de BTC en circulación, más difícil es conseguir nuevas monedas.

Esta reducción se consigue con el *Having*. Esto significa que cada cierto tiempo se recompensa menos Bitcoins a los mineros. ¿Cuánto tiempo? Exactamente cada vez que se minen 210.000 bloques nuevos. Cada vez que eso pase, se reducirá a la mitad la recompensa. Desde su creación ha habido tres *Havings*. Es decir, desde su origen se han creado 630.000 bloques mínimo. El número de transacciones por bloque no es fijo, pero en los último ha oscilado entre 1.500 y 2.500 transacciones.

Ilustración 5: Media de transacciones por bloque



Fuente: Blockchain.com

Desde el origen de Bitcoin hasta el primer Having, la recompensa por Bloque minado eran 50 BTC. El día que esto sucedió se paso a recompensar 25 BTC por bloque, el segundo *Having* lo redujo a 12,5 y el tercero a 6,25. Al igual que el cuarto lo reducirá a 3,125. Si hacemos los cálculos podemos descubrir cuantas BTC mínimo hay en circulación.

Tabla 1: Tabla de Havings

Having	Fecha	Bloques	Recompensa BTC/Bloque	BTC	Acumulativo
	Enero 2009	210.000	50	10.500.000	10.500.000
1º	28-11-2012	210.000	25	5.250.000	15.750.000
2º	09-07-2016	210.000	12,5	2.625.000	18.375.000
3º	11-05-2020	210.000	6,25	1.312.500	19.687.500
4º	2024*	210.000	3,125	656.250	20.343.750

*estimado

Fuente: Elaboración propia

A pesar de que cada vez se recompensan menos Bitcoins, el valor que reciben los mineros es mayor, pues cada moneda está más valorada, al ajustar la oferta. Otro efecto que tiene es el aumento del coste de minar, con el paso del tiempo, los mineros menos potentes se ven incapacitados a ejecutar los cada vez más difíciles problemas matemáticos necesarios para minar, al igual que hacer frente a su coste energético y registrar la cada vez más larga lista de transacciones.

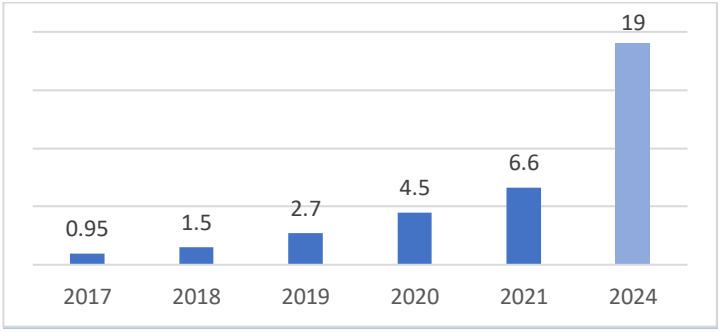
Se estima que la última Bitcoin será minada en 2140. En ese momento el beneficio de recompensa en Bitcoins para los mineros será suprimido y se quedará el beneficio de las tasas de transacción; es decir cobraran por validar las transacciones entre usuarios. Esto permitirá que los mineros mantengan incentivos para operar la red y que Bitcoin perdure.

2.2.2 Blockchain

Blockchain es la tecnología que permite descentralizar Bitcoin y otras criptomonedas. Gran parte de su funcionamiento lo hemos visto al analizar como opera Bitcoin, no obstante, no es una tecnología cuyo uso es exclusivo de criptomonedas. Aunque la descentralización monetaria es donde ha cobrado más fuerza, también ha servido para darla a conocer; y recientemente se está empezando a investigar su aplicación en varias áreas.

Cada vez se es más reconocido el valor que aporta Blockchain. El incremento de inversiones en esta tecnología no ha parado de crecer en los últimos años, según los últimos datos de *Statista*, el dinero global destinado a encontrar soluciones con esta tecnología ha aumentado un 284,2% de 2017 a 2019. Y se prevé un crecimiento de 703,7% hasta el 2024.

Ilustración 6: Gasto mundial en soluciones de Blockchain. (Miles de Millones de dólares)



Fuente: Statista

Blockchain básicamente es una base de datos; pero en vez de guardar los datos una persona lo guardan varias. La principal ventaja de esto es que garantiza una mayor seguridad de almacenamiento al ser más difícil de alterar la base de datos, o al menos no se requiere depositar la confianza de resguardar los datos en un tercero.

La forma que tiene Blockchain de almacenar esta información es como vimos con las transacciones de Bitcoin. Se recoge la información en grupo, posicionándola en bloques, que pueden tener diversas capacidades de almacenamiento. Estos bloques están unidos entre ellos formando una cadena de bloques. El mayor logro de esta tecnología es conseguir que los datos sean registrados dificultando o haciendo nula su posibilidad de edición.

Las bases de datos centrales, en ingles Centralized database (CDB); por el contrario organizan su información en tablas. Estas bases de datos están situadas en una sola ubicación; con un ordenador. Estos sitemas son usados por universidades, instituciones o empresas; que dan claves a sus usuarios y se les permite acceso a los datos de la entidad a través de sus ordenadores centrales.

Es importante distinguir el modelo descentralizado que propone Blockchain respecto a otro tipo las bases de datos distribuidas (DDB). Este tipo de almacenaje no es descentralizado, pero almacena la información en varios ordenadores en vez de uno. Estos ordenadores pueden estar en varias ubicaciones o en la misma. La principal diferencia entre *Distributed Databes* y Blockchain, es que en la primera depositas la confianza en varias terceras entidades (con sus respectivos ordenadores) y en Blockchain no se deposita en una o varias terceras entidades sino en una red de ordenadores. (P. Lake, 2013).

Uno de las grandes ventajas de Blockchain es su seguridad. Resulta más difícil hackear la información que se almacena en una Blockchain que en la de una base de datos centralizada. Aunque hay varios matices; la red Blockchain al depositar la confianza en una red de ordenadores, es más segura cuando más ordenadores haya; pro lo tanto, al origen de una red de Blockchain sería más fácil hackearla. En el caso de las bases de datos centralizadas; el nivel de exposición a hackeos depende de la seguridad que tenga cada sitema; pero con el constante desarrollo de métodos de robo informático; siempre están expuestos, y se reduce a una batalla constante en el tiempo. Por el camino; constantemente hay casos de robos. Según varias fuentes gubernamentales la pandemia ha incrementado notablemente los ciberataques. Según el *National Cyber Security Center* de Suiza (NCSC);

los ciberataques a compañías incrementaron hasta 350 en junio de 2020; desde la media de los años pasados de entre 100 y 150.

La subida del trabajo desde casa se atribuyó a la pandemia de coronavirus, ya que las personas que trabajan en casa carecen del mismo nivel de protección intrínseca y de medidas disuasorias que las que se encuentran en un entorno laboral.

3. Bancos centrales

3.1 Respuesta Banco Central Europeo

Aunque el Bitcoin y otras criptomonedas se están extendiendo, el BCE está presionando a sus ciudadanos para que prefieran el euro digital. A pesar de que no está listo para su uso todavía, el BCE ha iniciado un esfuerzo de relaciones públicas. El banco central todavía está en las primeras fases de las pruebas con dinero virtual dentro de la institución, y se espera que un prototipo esté listo como muy pronto a finales de 2023.
Sin embargo, los esfuerzos del BCE se han visto frustrados por los gigantes de Internet, que están inventando nuevos métodos de pago basados en activos digitales que podrían revolucionar la forma en que el ciudadano de a pie realiza cada vez más transacciones en línea. Diem, un plan desarrollado por Facebook y otras 25 empresas, podría empezar a funcionar en Estados Unidos este año.

"El valor de los criptoactivos es ahora mayor que el valor de los activos titulizados antes de la crisis financiera mundial [en 2008]", dijo Fabio Panetta, miembro del Comité Ejecutivo del BCE, en una gira europea para promover el mensaje del banco central. "Si no satisfacemos esta demanda, otro lo hará".

Sin embargo, los banqueros centrales se enfrentan a una difícil tarea para conseguir el apoyo popular. Según encuestas realizadas en el Reino Unido y Alemania, a la mayoría de los encuestados no les gusta la idea de las monedas virtuales con respaldo público, citando el temor a las escuchas del gobierno y las dudas sobre los beneficios que ofrecerían.

Panetta ha realizado una gira informal el año pasado para ayudar a cambiar la opinión pública ante estas incertidumbres. Recientemente hizo presentaciones sobre la importancia

de una moneda digital respaldada por el banco central en Madrid y Helsinki antes de venir a Bruselas.

Su discurso abarca desde el establecimiento de una garantía pública para la moneda hasta la advertencia sobre los peligros de que las empresas de Internet acaparen el negocio de los pagos aprovechando las criptodivisas.

"Si estos dos desarrollos colisionan, los mercados financieros globales pueden verse perturbados y los servicios de pago tradicionales pueden verse desplazados", dijo. Un euro digital proporcionaría a los ciudadanos un acceso constante a un depósito de valor fiable, algo que una empresa tecnológica en quiebra no podría hacer, afirma.

El Parlamento Europeo fue algo más que una simple parada en la gira de Panetta. También instó al poder legislativo de la UE a tener un papel en la promulgación del euro digital como ley.

"Como colegisladores, desempeñarán un papel fundamental en cualquier modificación del marco jurídico de la UE que pueda ser necesaria para implantar el euro digital", dijo.

La ley aún está lejos de ser propuesta por la Comisión Europea. La idea no se menciona en el calendario legislativo para el próximo año, y su personal sigue debatiendo con el BCE diversas dificultades jurídicas sobre cómo proceder. Aunque se desconoce el contenido del proyecto de ley, funcionarios familiarizados con el tema dijeron que lo más probable es que aborde problemas políticos como la privacidad de los pagos.

La gente aprecia la privacidad que proporciona el efectivo, según una encuesta realizada por el Banco Central Europeo el año pasado. El euro digital ofrecería cierta privacidad, pero ese anonimato total también permitiría a los delincuentes utilizar la moneda virtual para blanquear dinero negro. Es casi seguro que los legisladores tendrán que encontrar el equilibrio adecuado para satisfacer a ambas partes del debate político.

Lo que resulta evidente es que la implantación del euro digital no requerirá ninguna revisión de los tratados de la UE, lo que supondría una empresa de gran envergadura que requeriría unanimidad y referendos en algunos países. En su lugar, lo más probable es que

se aplique mediante una norma que requiera la aprobación de una mayoría cualificada de los países miembros.

También será fundamental que los comerciantes acepten la moneda virtual como dinero legal. Es poco probable que este punto se incluya en el proyecto de ley porque puede aplicarse a nivel nacional para garantizar que la extensión digital del euro tenga la misma legitimidad y fiabilidad que las monedas y los billetes.

No obstante, las instituciones de la Unión Europea temen quedarse atrás; tal como dijo Panetta: "Si la gente no obtiene servicios digitales de nosotros en diez años, los obtendrá de otros". Por tanto, en Europa se sabe cual es el camino, pero se muestran de momento reticentes a ir rápido.

3.2 Respuesta Reserva Federal

La FED publicó el documento "*Money and Payments: The US Dollar in the Age of Digital Transformation*" a comienzos de año, para analizar cómo podría fortalecer el sistema de pagos nacional una posible moneda digital del banco central (CBDC) o "*Central Bank Digital Currency*".

Posibles beneficios de una CBDC estadounidense:

- Satisfacer las futuras necesidades y demandas de servicios de pago: Según la Reserva Federal, un CBDC estadounidense respondería de forma segura a las necesidades y expectativas de los servicios de pago, proporcionando al público en general un amplio acceso al dinero digital libre de riesgo de crédito y de liquidez.

- Mejoras en los pagos transfronterizos: un CBDC los mejoraría mediante la introducción de nuevas tecnologías, la simplificación de los métodos de distribución y la ampliación de la colaboración e interoperabilidad entre jurisdicciones. Sin embargo, la consecución de estos beneficios potenciales requerirá una amplia cooperación internacional.

- Podría fortalecer el dólar; pues en un mundo en el que los países extranjeros y las uniones monetarias pueden introducir sus propios CBDC, lo que podría llevar a una caída en el uso

del dólar, un CBDC estadounidense podría ayudar a preservar el papel internacional del dólar.

- Promover la inclusión financiera, en particular para los hogares y comunidades económicamente vulnerables, proporcionando acceso a los pagos digitales, permitiendo el pago de impuestos de forma rápida y rentable, y permitiendo la entrega rápida y rentable de los salarios, las devoluciones de impuestos y otros pagos federales, entre otros beneficios.

A continuación, se exponen algunos de los riesgos potenciales y consideraciones políticas:

- Una CBDC estadounidense podría alterar fundamentalmente la estructura del sistema financiero de Estados Unidos, afectando a las funciones y obligaciones del sector privado y del banco central. Una CBDC estadounidense ampliamente disponible, por ejemplo, sería una alternativa cercana al dinero de los bancos comerciales. Este efecto de sustitución podría disminuir la cantidad total de depósitos en el sistema bancario, reduciendo la disponibilidad de crédito y aumentando potencialmente los precios del crédito para las familias y las empresas. Un CBDC que pague intereses podría provocar el abandono de otras inversiones de bajo riesgo como los fondos de inversión del mercado monetario, los pagarés del Tesoro y otros valores a corto plazo. Para las empresas y los gobiernos, el alejamiento de estos otros activos de bajo riesgo podría restringir la disponibilidad de crédito o elevar los precios de este.

- Seguridad y estabilidad del sistema financiero: Una CBDC estadounidense podría repercutir en la seguridad y la estabilidad del sistema financiero, ya que la capacidad de convertir rápidamente otros tipos de dinero, como los depósitos de los bancos comerciales, en CBDC podría hacer que las corridas de las empresas financieras fueran más posibles o graves. En caso de pánico financiero, los mecanismos tradicionales, como la supervisión prudencial, el seguro de depósitos del gobierno y el acceso a la liquidez del banco central, podrían no ser suficientes para evitar retiradas masivas de depósitos de bancos comerciales en CBDC.

- Privacidad del consumidor: Una CBDC de propósito general recopilaría información sobre las transacciones financieras de los usuarios de la misma manera que lo hacen ahora los bancos comerciales y el dinero no bancario. En el modelo de CBDC intermediado

propuesto por la FED, los intermediarios resolverían los problemas de privacidad utilizando sus herramientas actuales.

- Prevención de los delitos financieros: Las instituciones financieras deben seguir un estricto conjunto de normas para prevenir el blanqueo de capitales y la financiación del terrorismo, incluyendo la diligencia debida con los clientes, el mantenimiento de registros y las obligaciones de información. Cualquier CBDC en Estados Unidos tendría que construirse de manera que apoye el cumplimiento de estas normas mediante la participación de socios del sector privado con procesos establecidos para garantizar el cumplimiento.

- Ciberseguridad y resistencia operativa: Las amenazas a los sistemas de pago existentes, como las interrupciones operativas y las amenazas a la ciberseguridad, también se aplicarían a un CBDC estadounidense. Cualquier infraestructura dedicada a un CBDC estadounidense tendría que ser resistente a tales amenazas, y los gestores de la infraestructura del CBDC estadounidense tendrían que permanecer atentos a medida que los malos actores despliegan métodos y estrategias cada vez más sofisticados. En la actualidad, muchos pagos digitales no están disponibles durante las catástrofes naturales u otras interrupciones importantes, lo que obliga a las poblaciones afectadas a depender de las transacciones en efectivo en persona. Los bancos centrales están investigando si los métodos de pago CBDC fuera de línea son prácticos.

- Eficacia de la aplicación de la política monetaria: La Reserva Federal controla el nivel del tipo de los fondos federales y otros tipos de interés a corto plazo principalmente a través de la fijación de los tipos administrados por la Reserva Federal bajo el actual régimen de política monetaria de "amplias reservas". En este contexto, la creación de un CBDC estadounidense podría repercutir en la aplicación de la política monetaria y el control de los tipos de interés al afectar a la oferta de reservas en el sector bancario. El nivel y la volatilidad de la demanda pública de una CBDC estadounidense que no devenga intereses pueden ser comparables a otros factores que actualmente afectan a la cantidad de reservas en el sistema bancario, como los cambios en la moneda física o los acuerdos de recompra a un día, en el caso de una CBDC estadounidense que no devenga intereses. En esta situación, una caída de la CBDC estadounidense unida a un aumento de las reservas aumentaría con toda probabilidad las reservas y no tendría ningún efecto sobre el tipo de los fondos federales.

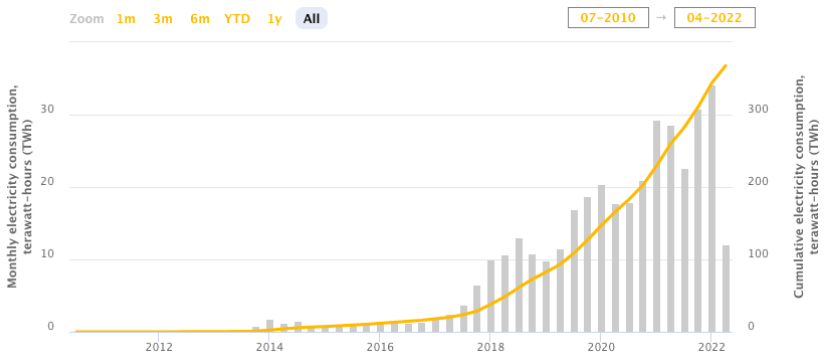
3.3 **Respuesta Banco Popular Chino**

A finales del año pasado China ha declarado ilegal toda actividad con estos instrumentos de pago digitales (The New York Times), por considerarlos una amenaza para la seguridad nacional y los "bienes del pueblo". El veto, declarado por el Banco Popular de China y una docena de instituciones gubernamentales, no es del todo nuevo; lo que sí es nuevo es su carácter categórico y su alcance, ambos mayores que las prohibiciones anteriores.

China, que había sido uno de los mercados más importantes para estas monedas digitales, ha declarado que establecerá "nuevos procedimientos" para luchar contra las amenazas que suponen las criptodivisas (El Economista). El Banco Popular afirma que el aumento del uso de las criptodivisas ha perturbado el "orden económico y financiero" y ha provocado un aumento de las actividades delictivas, como "el blanqueo de dinero, la recaudación ilegal de fondos, el fraude y las estafas piramidales". Precisan que quienes desobedezcan la prohibición serán examinados por su posible culpabilidad penal.

Además, se cerrarán gradualmente las minas de criptodivisas y no se permitirá el funcionamiento de otras nuevas. China era uno de los países más importantes del mundo para este tipo de negocios, debido a sus bajos costes de electricidad, entre otros factores. Según el Índice de Consumo de Electricidad del Bitcoin de Cambridge el Bitcoin, acapara el 0,65% del consumo global de electricidad (Universidad of Cambridge).

Ilustración 7: Consumo total de electricidad de Bitcoins



Fuente: Universidad of Cambridge

El anuncio del viernes se suma a la presión de China sobre las criptodivisas, que comenzó en 2017 y se ha intensificado últimamente. Las autoridades chinas prohibieron varias plataformas nacionales de intercambio de criptomonedas en 2017. El Banco Popular, el

banco central del país, dijo en 2019 que limitaría el acceso a los sitios web que proporcionaban criptodivisas. La nueva prohibición forma parte de un paquete de medidas destinadas, por un lado, a proteger el medio ambiente (el minado de criptodivisas en ordenadores consume mucha electricidad y emite mucho CO2) y, por otro, a una dura campaña para aumentar el control estatal sobre la economía y limitar los riesgos excesivos en el sistema financiero.

Una primera advertencia llegó en mayo del año pasado, cuando los reguladores declararon que cualquiera que realizara transacciones con criptodivisas no estaría protegido, y que los bancos y las empresas de pago no podrían ofrecer a sus clientes ninguna transacción con criptodivisas. Sin embargo, en aquel momento no tenían poder para vetar transacciones individuales, algo que ahora se incluye en el nuevo decreto. Los usuarios simplemente habían migrado por Internet desde las plataformas y bancos nacionales a los operadores internacionales. Las plataformas extranjeras ya no podrán prestar sus servicios a los clientes chinos.

Varias provincias chinas han prohibido la minería de bitcoins en sus jurisdicciones, alegando el elevado uso de electricidad en un año en el que China sufre escasez de energía. La Comisión Nacional de Desarrollo, encargada de la planificación económica, puso fin de las operaciones de minería en el país, citando la necesidad de cumplir los objetivos de neutralidad de carbono como una de las razones del cierre; pues Pekín prometeque alcanzará la neutralidad en 2060 (France 24).

4. Bitcoin como alternativa a la Centralización

4.1 La vulnerabilidad e ineficacia de la tecnología Bitcoin

La red Bitcoin destaca por su resistencia, estabilidad y escalabilidad. Además, las tecnologías de cadena de bloques y de libro mayor distribuido se están convirtiendo rápidamente en estándares de la industria para los activos digitales y otras aplicaciones. Todavía no se ha descubierto todo el potencial de estas tecnologías.

La idea de la prueba de trabajo (*prove of work*), que es fundamental para el sistema Bitcoin, se considera a menudo ineficiente y lenta, con una tasa de transacciones de sólo siete a diez

transacciones por segundo. Esto se traduce en un prolongado tiempo de procesamiento de las transacciones. A modo de ejemplo: Se cree que la red de Visa es capaz de procesar 24.000 transacciones por segundo (Avoca, 2021, p.4), lo que implica que la escalabilidad y la eficiencia de los sistemas de pago centralizados tradicionales bien diseñados son bastante menos limitadas.

Las redes de precios lentas y opacas han atraído en el pasado a los operadores de algoritmos depredadores, y por ello están sujetas a las tensiones del mercado. El Bitcoin también ha sido objetivo de las empresas de comercio de alta frecuencia. La red de Bitcoin es especialmente susceptible, ya que se basa en un único mecanismo de seguridad que los expertos consideran obsoleto debido a los avances informáticos. Bitcoin emplea el algoritmo de hash seguro (SHA), que tiene más de dos décadas de antigüedad. El Departamento de Defensa de EE.UU. y varias grandes empresas informáticas, como Microsoft, consideraron que el estándar SHA-1 era inadecuado para la ciberseguridad, por lo que se dejó de utilizar a principios de la década de 2010. En un entorno de computación cuántica, los investigadores temen que la tecnología sea incapaz de seguir el ritmo. Es difícil entender cómo podría actualizarse la tecnología de seguridad principal para resistir las dificultades de futuros desarrollos técnicos por parte de otros en ausencia de una administración legitimada centralmente.

Desde hace tiempo, se ha observado otra vulnerabilidad técnica de carácter conceptual en la red Bitcoin. Es vulnerable al llamado ataque del 51 por ciento, que se produce cuando mineros malintencionados obtienen el control de más del 51 por ciento de la tasa de hash de la red, lo que les permite emitir monedas dos veces. Aunque la gran red de 1.000 nodos de Bitcoin la hace menos vulnerable a un asalto del 51 por ciento en teoría, en 2014 se habría producido una concentración preocupante: En el transcurso de un período de 24 horas en junio de 2014, el pool de minería GHash.IO tuvo una participación de alrededor del 55 por ciento del hashrate de Bitcoin. Aunque la participación de GHash.IO en el hashrate de la red se había reducido a poco más del 38% un mes después, la perspectiva de que un solo minero o pool de minería recuperara el control persistía. GHash.IO aceptó voluntariamente mantener su cuota de mercado por debajo del 40%.

4.2 Bitcoin no es un tipo de dinero.

Nakamoto (2008) presentó a Bitcoin como beneficioso para la sociedad debido a su función de pago, aunque sus razones de apoyo eran todavía un poco confusas en ese momento. En cualquier caso, ahora hay un acuerdo generalizado en que Bitcoin no consigue su objetivo inicial de convertirse en dinero. Bitcoin es demasiado volátil para servir como unidad de cuenta, método de pago o depósito de valor. Además, la tecnología es demasiado lenta y costosa para competir con los métodos de pago y las monedas existentes. Es difícil y costoso incentivar el mantenimiento del sistema sin una autoridad central. Debido a los largos retrasos en la liquidación y a las elevadas tasas de transacción (que ahora oscilan entre 2,5 y 4 dólares por transacción), los minoristas aún no aceptan Bitcoin como modo de pago fuera de los nichos. Como resultado, el modelo de negocio de Bitcoin como método de pago a nivel mundial es inverosímil.

El Salvador intentó hacer realidad la visión de Nakamoto (2008) a mayor escala introduciendo el Bitcoin como segunda moneda legal junto al dólar estadounidense el 7 de septiembre de 2021. La introducción fue difícil, debido a la falta de adopción generalizada del nuevo método de pago. El valor de cambio del Bitcoin se desplomó un 15% el día del lanzamiento, seguido de manifestaciones contra el presidente Bukele.

Mientras tanto, el presidente Bukele ha anunciado nuevos planes para promover el uso de Bitcoin y la minería en El Salvador, incluyendo la creación de una nueva ciudad centrada en la criptodivisa. La financiación de la construcción y el mantenimiento de la "Ciudad Bitcoin" se basaría en nuevos bonos Bitcoin, con la energía necesaria procedente de un volcán cercano.

4.3. Bitcoin no parece ser una inversión a largo plazo.

Uno de los argumentos más frecuentes entre los defensores de Bitcoin es que la oferta restringida de Bitcoin protegería a los inversores contra la inflación, mientras que el dinero fiduciario, que puede ser duplicado a capricho, perderá valor con el tiempo.
Incluso si Bitcoin se convirtiera en el nuevo dinero global, su supuesta "oferta monetaria" fija parecería ser un defecto tras un examen más detallado: el mundo se vería abocado a una trampa de deflación en una economía en auge. El descenso de los precios de los bienes y servicios lleva a los individuos a posponer las compras menos esenciales hacia el futuro

durante un periodo deflacionario. Individualmente, esto está bien, pero la demanda agregada se resiente, frenando la economía.

Los que defienden el oro como herramienta contra la inflación y los que abrazan el Bitcoin por la misma razón- deberían recordar por qué se abolió el patrón oro. Mientras que la fijación del oro puede dar protección contra la inflación, también aumenta la posibilidad de deflación, como se mencionó anteriormente: Tras años de dura recesión, deflación e inestabilidad financiera, las principales monedas abandonaron la fijación del oro en 1931.

Del mismo modo, después de la Segunda Guerra Mundial, el patrón oro indirecto del sistema monetario de Bretton Woods se derrumbó. En ese momento, las monedas ya no estaban directamente vinculadas al oro, sino al dólar estadounidense (a una paridad fija de 35 dólares por onza de oro). El fracaso se debió a la incapacidad de Estados Unidos de mantener el dinero lo suficientemente ajustado como para que la paridad del oro fuera creíble y, al mismo tiempo, proporcionar la liquidez adecuada a la economía internacional, que estaba en rápido crecimiento.

Sin embargo, la analogía con el oro que se utiliza a menudo se queda corta por razones más fundamentales. Según Taleb (2021), el oro se ha utilizado como depósito de valor, activo de inversión y moneda de reserva durante milenios antes de convertirse en un depósito de valor, un activo de inversión o una moneda de reserva. Además, no se degrada con el tiempo y mantiene su valor incluso en condiciones mundiales caóticas o degenerativas, como catástrofes naturales o un colapso a corto o largo plazo de la infraestructura eléctrica o digital.

Por último, el argumento de que el dinero fiduciario de los bancos centrales modernos no tiene valor intrínseco fracasa porque, al abandonar el patrón oro, los órganos de gobierno y los bancos centrales han implementado mandatos claramente definidos, garantías legales y acuerdos estructurales y de proceso (autonomía y préstamos garantizados) que les permiten soltar el freno del oro sin perder estabilidad.

Por último, pero no por ello menos importante, la alternativa al dinero fiduciario de los bancos centrales para el Bitcoin como depósito de valor es la financiación de proyectos económicos reales a través de capital y/o deuda que sirvan a las necesidades de la sociedad y generen un flujo de caja que permita mantener rendimientos positivos, anclando el valor

de los activos de inversión en su productividad real. La preocupación por la estabilidad de determinadas monedas fiduciarias puede expresarse adecuadamente invirtiendo en acciones, materias primas, bienes inmuebles, capital humano y otros activos productivos. El dinero fíat no está respaldado por "nada" que no sean decenas de billones de dólares en crédito privado, el imperio de la ley y la fuerza del Estado, implantado a su vez en un sistema estatal.

Algunos también han sugerido que el aumento del valor de Bitcoin es atribuible a la política de bajos tipos de interés de los bancos centrales. Estos factores obligarían a los inversores a buscar ingresos, que presumiblemente proporciona el Bitcoin, una especie de mercancía digital capaz de escapar a las restricciones financieras. Aunque el deseo de obtener altos rendimientos nominales y reales, así como el descontento con la realidad en muchas naciones avanzadas, es comprensible y justo, no debería utilizarse como excusa para invertir dinero en activos de alto riesgo. Si los bancos centrales fijan unos tipos de interés nominales excesivamente bajos, que no están bien justificados por las implicaciones de la política monetaria, los inversores deberían tratar de financiar activos reales con valor a largo plazo por una contribución demostrada a las necesidades de la sociedad, al tiempo que apoyan a los responsables políticos que se comprometen a tomar medidas para apoyar el crecimiento económico real y, en consecuencia, las tasas reales de rendimiento del capital social de la economía.

4.4 **Creciente preocupación por la viabilidad de Bitcoin a largo plazo**

Bitcoin no es competitivo para los pagos legales ya que es ineficiente e inadecuado como método de pago. Bitcoin tampoco tiene un valor inherente y no produce flujo de caja ni dividendos. Como resultado, el valor de mercado de Bitcoin depende únicamente de las conjeturas. Este auge del mercado sólo puede durar lo que dure la fe de la comunidad de Bitcoin en los beneficios declarados de Bitcoin como método de pago o que el valor del mercado siga subiendo indefinidamente. Como resultado, si todavía hay un alguien que cree que puede vender a un mejor precio más adelante, el valor crece. Sin embargo, "con el tiempo, uno se queda nadie después que piense igual. Por tanto, a largo plazo, el entusiasmo de Bitcoin no es suficiente

4.5. El fantasma de la libertad

Como hemos visto, desde sus orígenes, Bitcoin tuvo motivos políticos, especialmente libertarios. Ya en su creación, Satoshi Nakamoto, vio sus motivos cuestionados; en la lista de correo en la que público su idea le argumentaban:

- *You will not find a solution to political problems in cryptography.*

- Yes, but we can win a major battle in the arms race and gain a new territory of freedom for several years. (Satoshi)

Fuente: Metzdowd

A pesar de sus defectos económicos, la misión de Bitcoin sigue siendo liberar a la gente de la autoridad gubernamental y de las instituciones centralizadas que hacen mal uso de su poder. La estructura descentralizada de Bitcoin ofrece la liberación individual y la eventual democratización del sistema monetario (2021). Sin embargo, incluso en el caso de Bitcoin, se necesitan regulaciones; de lo contrario, reinaría el caos y la ley del más fuerte. El hecho de que la economía y los mercados financieros en las economías de mercado desarrolladas se apoyen en instituciones centrales y nodos distribuidos con jerarquías internas (empresas) y dentro de unas reglas establecidas ha sido reconocido desde hace tiempo en la literatura económica. Las empresas y los contratos incompletos pueden ayudar a hacer frente a la incertidumbre y a la complejidad, al tiempo que reducen los costes de las transacciones, pero están lejos de ser ideales en ausencia de una tecnología adecuada. El Bitcoin busca generar normas mecanicistas, que no son una respuesta aceptable para un entorno dinámico. Como resultado, el esfuerzo más reciente y ambicioso de hacer de Bitcoin un método de pago necesariamente socavó sus valores libertarios, incluyendo el objetivo clave de Nakamoto de evitar los intermediarios centrales de pago.

Bitcoin tampoco es tan democrático como su comunidad pudo creer, al menos en los primeros días, sino que está moldeado por intereses financieros y accionistas poderosos, así como por el riesgo de concentración, dada su dependencia de unas pocas entidades, como los monederos de custodia y los intercambios. El grueso de las direcciones, el 75 por

ciento, apenas posee más del 0,2 por ciento del mercado; los cien primeros accionistas de Bitcoin poseen más que los 38 millones inferiores juntos (Dunn, 2021)

Por último, Bitcoin presenta una imagen de un sistema de pago global que no depende de las autoridades nacionales para cruzar las fronteras, a diferencia de las transacciones transfronterizas tradicionales. La gente podría transmitir dinero a cualquier persona con un monedero Bitcoin de forma gratuita y sin restricciones. Este punto de vista pasa por alto el hecho de que el elevado coste de los pagos transfronterizos tradicionales es atribuible en parte a los gastos de gestión del riesgo de mercado y de liquidez, así como a las obligaciones legales de lucha contra el blanqueo de capitales y la financiación del terrorismo. Sin embargo, sólo el sector financiero regulado se ve afectado por los gastos de cumplimiento de estas normas, así como por los preparativos para los riesgos legales y de tipo de cambio. El hecho de que ciertas transacciones de bitcoin, como las de tipo peer-to-peer, hayan conseguido evitarlo totalmente hasta ahora se debe a una laguna normativa más que a un avance técnico. Sin embargo, no se puede negar que el coste, la puntualidad, la transparencia y la inclusividad de los pagos transfronterizos podrían mejorar.

4.6 El uso de Bitcoin para fines nefastos

Bitcoin ha demostrado ser un método de pago viable para fines ilegales. La manipulación del mercado y las operaciones dudosas de los operadores de intercambio deben distinguirse de su uso para el blanqueo de dinero, el tráfico de drogas, la financiación del terrorismo y la extorsión y el rescate, por debajo del radar de las fuerzas del orden y los organismos reguladores.

Por el lado de la oferta, Dunn (2021) esboza una larga lista de operaciones dudosas y de manipulación del mercado que han caracterizado la historia de Bitcoin. La bolsa Mt Gox, que albergaba alrededor del 70% del comercio de Bitcoin, impulsó el boom inicial en 2013. La bolsa quebró tras perder 650.000 Bitcoins de sus consumidores.

El bitcoin también se utiliza a menudo para financiar operaciones ilegales. Los usos más comunes incluyen el tráfico de drogas, el lavado de dinero, la financiación del terrorismo y la extorsión. Sin embargo, dado que las transacciones nunca desaparecen de la cadena de bloques, la configuración de Bitcoin puede ayudar a la investigación forense a identificar

operaciones delictivas. Aunque esto puede permitir la recuperación de parte del rescate pagado, como ha demostrado el Departamento de Justicia de EE.UU. en los últimos años, sigue siendo un proceso difícil, largo y desigual.

4.7 La red Bitcoin tiene un importante coste privado y social.

Cuanto mayores sean los riesgos y los costes para las personas invertidas y la sociedad en su conjunto, más durará el boom y más dinero entrará en el sistema hasta que la música se detenga. Los diferentes tipos de costes sociales de la red Bitcoin son a menudo malinterpretados en la discusión. Piense en las siguientes cuestiones:

Bitcoin tiene considerables costes privados en forma de uso de energía y hardware de la red Bitcoin. Si es cierto que Bitcoin acabará siendo insostenible y dejará de existir, y que no habrá aportado valor a la sociedad más que promesas efímeras de beneficios especulativos que al final se verán defraudados, entonces estos gastos privados habrán supuesto una pérdida neta para la sociedad. Independientemente de las posibles externalidades negativas del uso de la energía, este razonamiento persiste.

Es discutible que las externalidades negativas del uso de la energía estén adecuadamente tasadas a través de los impuestos. El arbitraje geográfico en la minería de Bitcoin conducirá a una mayor concentración de la minería en las regiones en las que esto sea menos frecuente, permitiendo que las externalidades negativas se internalicen sin serlo.

Algunos han afirmado que la minería de Bitcoin debería realizarse en lugares donde la energía es casi gratuita, lo que se traduce en la ausencia de emisiones de CO2. El Salvador, por ejemplo, planea construir una "Ciudad Bitcoin" cerca de un volcán y aprovechar su energía. Del mismo modo, el suministro de energía geotérmica barata de Islandia atrajo a las empresas mineras durante mucho tiempo - hasta que su corporación nacional de energía decidió en diciembre de 2021 restringir la electricidad a los nuevos mineros de Bitcoin (Cointelegraph, 2021). ¿Por qué cualquier otra empresa que haga un uso intensivo de la energía, con límites geográficos a priori restringidos, se vería atraída por una solución tan sencilla? Además, el uso de energía de la red Bitcoin está inversamente relacionado con el coste de la electricidad. Esto implica que si las granjas de minería se trasladan en gran número a lugares donde la energía es más barata, la lógica del método de prueba de trabajo dicta que para un precio dado de Bitcoin, se gastará más energía en la minería.

Los inversores en Bitcoin piensan que el alto coste social de Bitcoin y su valor social neto negativo se compensan actualmente con los beneficios especulativos actuales y futuros. Los beneficios puramente especulativos, por otro lado, no son una base sostenible para las subidas de precios, y la factura de los gastos privados de la red Bitcoin se acabará pagando. Una vez que la música haya dejado de sonar y el valor de Bitcoin haya caído en picado, se deberá pagar la totalidad del coste social.

El daño social será un gran componente adicional de los eventuales costes sociales, ya que muchas personas descubrirán que han perdido sus fondos ganados con esfuerzo en beneficio de los mejores inversores de Bitcoin que compraron barato y vendieron caro. Los que perdieron dinero, especialmente los inversores minoristas que colocaron estúpidamente una parte sustancial de sus ahorros en la cesta de las criptomonedas, no apreciarán la transferencia masiva de beneficios a su costa, y cuestionarán el funcionamiento de la sociedad que permitió que se produjera tal injusticia. Mientras que las superestrellas del sistema pueden retirarse de los focos, el consenso público y la confianza sufren otro golpe. La reacción de la sociedad será más intensa cuanto mayor sea el valor de mercado que se ha quemado.

En general, las naciones tendrán que amortizar el consumo de energía acumulado (incluyendo las externalidades negativas no valoradas), los costes de inversión en hardware, el capital humano acumulado del ecosistema Bitcoin, el esfuerzo acumulado y una saludable dosis de acuerdo social en algún momento. Además, al ofrecer un método de pago ilegítimo, la red Bitcoin habrá apoyado mientras tanto la actividad criminal. Todos estos gastos son aproximadamente proporcionales a la capitalización de mercado que alcanzará Bitcoin, y también están influidos por la duración total del ciclo de Bitcoin. A partir de estos datos, concluye que Bitcoin es una competencia de suma negativa para la sociedad, mucho peor que una estafa Ponzi.

5. Conclusiones

La viabilidad a largo plazo de Bitcoin, como se ha discutido en otros lugares está en duda. Es difícil encontrar razones convincentes para su viabilidad como medio de comercio o forma de inversión. El coste social neto del ciclo de vida de Bitcoin será bastante elevado

si finalmente se hunde. Y cuanto más grande sea, más durará y mayor será la capitalización máxima del mercado de Bitcoin.

Los costes sociales brutos y netos de Bitcoin serán iguales en ausencia de una contribución positiva a la sociedad, e incluirán el consumo de energía y el uso de hardware de la red Bitcoin, así como el capital humano y técnico que habrá que amortizar. Lo que no se puede medir es el daño social que se producirá cuando los inversores habituales descubran que sus inversiones han sido destruidas, mientras que algunos de los primeros inversores que salieron antes de que la música dejara de sonar se han beneficiado a su costa.

Los políticos públicos han sido lentos a la hora de manejar todos los problemas de Bitcoin. A pesar de que su uso para pagos ilícitos se descubrió muy pronto, la lentitud en la implementación y aplicación global de las normas ALD/CFT para los pagos basados en Bitcoin ha socavado los enormes esfuerzos realizados para prevenir los pagos ilícitos a través de las industrias reguladas, permitiendo a los actores criminales aprovecharse del arbitraje regulatorio. Además, Bitcoin se ha convertido en una clase de activo en la que cualquiera puede invertir fácilmente y que "parece un valor, nada como un valor y grazna como un valor, pero no está regulado como un valor" y, lo que es más importante, que carece de una contribución subyacente plausible a la sociedad que justifique su valoración, gracias en parte a la generosidad de las autoridades públicas.

Tras comprobar que el valor social de Bitcoin es perjudicial, numerosos gobiernos han tomado o pretenden tomar duras medidas contra él. Además, las autoridades de las economías occidentales más sofisticadas han tomado medidas importantes para combatir el uso de Bitcoin con fines ilegales, pero el uso no intermediario de la red Bitcoin sigue sin verse afectado por las actividades de los reguladores. Como resultado, se necesitan más medidas reguladoras para combatir adecuadamente todos los tipos de transferencias delictivas de Bitcoin. Independientemente del carácter único de Bitcoin, la premisa de "la misma función, los mismos peligros, las mismas regulaciones" debe aplicarse de manera uniforme si se quiere que los esfuerzos mundiales contra los pagos ilegales sean efectivos.

Los legisladores y las autoridades deben ser cautelosos para no contribuir a un resurgimiento de los flujos de inversión en Bitcoin, lo que aumentará la capitalización del mercado de la criptodivisa y el tamaño del coste social acumulado final de la red. Varios cambios de este tipo se produjeron en el año 2021, y el aumento de los precios de Bitcoin

en noviembre de 2021 se debe probablemente a las entradas de inversión ayudadas por dichas iniciativas. La revelación de que los ETFs de bitcoin basados en futuros estarían (o podrían) no estar prohibidos, o la nueva legislación alemana al respecto, que entra en vigor el 1 de julio de 2022 y permite a los inversores institucionales participar en criptoactivos, se citan como impulsores de la dinámica del precio de Bitcoin en otoño de 2021.

Por último, pero no menos importante, las preocupaciones sobre la viabilidad a largo plazo de Bitcoin y los costes sociales asociados no niegan las virtudes de DLT, blockchain y las finanzas descentralizadas como métodos tecnológicos novedosos. Lo que no está claro es si las criptomonedas que no son stablecoins (o tokens no fungibles que reflejan la propiedad de otros activos) pueden servir como vehículo de inversión viable. Estas sospechas son especialmente altas en el caso de Bitcoin, debido a su dependencia del ineficiente concepto de prueba de trabajo y a su escaso rendimiento como método de pago.

6. Bibliografía

Ammous, S. (2018). The Bitcoin Standard: The Decentralized Alternative to Central Banking. Deusto.

Aparicio, L. (2021). Euro digital: El BCE quiere ser tu otro banco | Negocios | EL PAÍS. El País. elpais.com. Retrieved March 15, 2022, from https://elpais.com/economia/2021-08-20/el-bce-quiere-ser-tu-otro-banco.html

Avoca Global Advisors (2021), "Bitcoin: a trojan horse", wcg avoca 14 Oct 2021, available: https://www.linkedin.com/posts/activity-6854411140617818112-NpKx

Baldwin , J. (2018). In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism. Palgrave. https://www.nature.com/articles/s41599-018-0065-0.pdf.

Blockchain. (2022). n-transactions-per-block. Blockchain.Com; www.blockchain.com. https://www.blockchain.com/charts/n-transactions-per-block

Boaz, D. (2009). libertarianism | Definition, Philosophy, Examples, History, & Facts. Encyclopedia Britannica; www.britannica.com. https://www.britannica.com/topic/libertarianism-politics

Braue, D. (2014). Bitcoin confidence game is a Ponzi scheme for the 21st century | ZDNet. ZDNet; www.zdnet.com. https://www.zdnet.com/article/bitcoin-confidence-game-is-a-ponzi-scheme-for-the-21st-century/

Clinch, M. (2014). Roubini launches stinging attack on bitcoin. CNBC; www.cnbc.com. https://www.cnbc.com/2014/03/10/nches-stinging-attack-on-bitcoin.html

Cointelegraph (2021), "Iceland cuts power to new Bitcoin miners", 8 Dec 2021, https://cointelegraph.com/news/iceland-cuts-power-to-new-bitcoin-miners.

Dunn, W (2021), "Bitcoin's gold rush was always an illusion", in: The New statesman, 20 July 2021, https://www.newstatesman.com/business/finance/2021/07/bitcoins-gold-rush-was-always-illusion

Edwards, J. (2022). Bitcoin's Price History. Investopedia; www.investopedia.com. https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp

elEconomista. (2021). El yuan digital es una amenaza para el bitcoin y para el reinado del dólar: www.eleconomista.es. Retrieved March 29, 2022, from https://www.eleconomista.es/mercados-cotizaciones/noticias/11153954/04/21/El-yuan-digital-es-una-amenaza-para-el-bitcoin-y-para-el-reinado-del-dolar-Puede-cambiarlo-todo.html

European Central Bank. (2022, March 30). Un euro digital que responda a las necesidades del público: encontrar el equilibrio adecuado. European Central Bank. www.ecb.europa.eu. Retrieved May 2, 2022, from https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220330_1~f9fa9a6137.es.html

Farber, M. (2017). This Billionaire Just Called Bitcoin a “Pyramid Scheme.” Fortune; fortune.com. https://fortune.com/2017/07/27/howard-marks-bitcoin-pyramid-scheme/

Gil, P. C. (2006). Introducción a la Criptografía.

Hernandez, Y; (2019). "The Technology Gap Across Generations: How Social Media Affects the Youth Vote," Political Analysis: Vol. 20 , Article 1. https://scholarship.shu.edu/pa/vol20/iss1/1/#:~:text=While%20the%20accusations%20generations%20make,generational%20gaps%20in%20American%20history.

Kelion, L. (2013). Bitcoin sinks after China restricts yuan exchanges - BBC News. BBC News; www.bbc.com. https://www.bbc.com/news/technology-25428866

Lake, Peter (2013). Concise Guide to Databases: A Practical Introduction. New York City: Springer. p. 37. ISBN 978-1447156000.

Lowry, J. (2020). MD5 vs SHA-1 vs SHA-2 - Which is the Most Secure Encryption Hash and How to Check Them. freeCodeCamp.Org; www.freecodecamp.org. https://www.freecodecamp.org/news/md5-vs-sha-1-vs-sha-2-which-is-the-most-secure-encryption-hash-and-how-to-check-them/

May, T. C. (n.d.). The Crypto Anarchist Manifesto . Netcom. Retrieved March 7, 2022, from https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html

Metzdowd. (2008). Bitcoin P2P e-cash paper. Metzdowd; www.metzdowd.com. https://www.metzdowd.com/pipermail/cryptography/2008-November/014823.html

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org. https://bitcoin.org/bitcoin.pdf

Ossinger, J. (2022). Bloomberg - Are you a robot? Bloomberg - Are You a Robot?; www.bloomberg.com. https://www.bloomberg.com/news/articles/2022-04-18/bitcoin-falls-to-lowest-in-a-month-as-risk-aversion-takes-toll

Posner, E. (2013). "Fool's Gold: Bitcoin is a Ponzi scheme—the Internet's favorite currency will collapse". Slate.

ResearchGate. (2021). Figure 1. Total number of Bitcoins in circulation over time from 2009... Figure 1. Total Number of Bitcoins in Circulation over Time from 2009...; www.researchgate.net. https://www.researchgate.net/figure/Total-number-of-Bitcoins-in-circulation-over-time-from-2009-to-2033-Source-based-on-Nian_fig1_350727702

Rincon, A. (2020). China se compromete en la ONU a alcanzar la neutralidad de carbono en 2060. France 24. www.france24.com. Retrieved February 21, 2022, from https://www.france24.com/es/20200923-china-neutralidad-carbono-cambio-climatico

Statista. (2022). Global spending on blockchain solutions 2024. Statista. www.statista.com. Retrieved January 14, 2022, from https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/#:~:text=Global%20blockchain%20solutions%20spending%202017%2D2024&text=In%202021%2C%20global%20spending%20on,billion%20U.S.%20dollars%20by%202024

Swissinfo. (2020). Jump in cyber attacks during Covid-19 confinement. SWI Swissinfo.Ch; www.swissinfo.ch. https://www.swissinfo.ch/eng/jump-in-cyber-attacks-during-covid-19-confinement/45818794

Tabuchi, H. (2022) After Chinese Ban, Cryptocurrency Mining Got Worse for Climate - The New York Times. China Banished Cryptocurrencies. Now, 'Mining' Is Even Dirtier. www.nytimes.com. Retrieved April 18, 2022, from https://www.nytimes.com/2022/02/25/climate/bitcoin-china-energy-pollution.html

Taleb, N (2021), "Bitcoin, currencies, and fragility", published online: 22 Jul 2021: https://www.tandfonline.com/doi/full/10.1080/14697688.2021.1952702?scroll=top&needAccess=true

The Federal Reserve. (2022) Money and Payments: The U.S.Dollar in the Age of Digital Transformation. Board of Governors of the Federal Reserve System (U.S.).

Ummelas, O; Seputyte, M. (2014). "Bitcoin 'Ponzi' Concern Sparks Warning From Estonia Bank". bloomberg.com. Bloomber.

University of Cambridge. (2022). Cambridge Bitcoin Electricity Consumption Index (CBECI). Cambridge Bitcoin Electricity Consumption Index (CBECI). ccaf.io. Retrieved April 2, 2022, from https://ccaf.io/cbeci/index

USA Government. (1977). Data Encryption Standard. National Institute of Standards and Technology. https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf

Van Hout, M.C; Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading.International Journal of Drug Policy. Volume 25, Issue 2. Pages 183-189.

Włodarczyk, R. W. (2021). Blockchain as a determinant of bitcoin value. The Review of Economics, Finance & Investments, 1(1). https://doi.org/10.53752/refi.2020.1.10

Yilmaz, B. (2021). Victimizing the Borrowers: Predatory Lending's Role in the Subprime Mortgage Crisis. Knowledge at Wharton; knowledge.wharton.upenn.edu. https://knowledge.wharton.upenn.edu/article/victimizing-the-borrowers-predatory-lendings-role-in-the-subprime-mortgage-crisis/