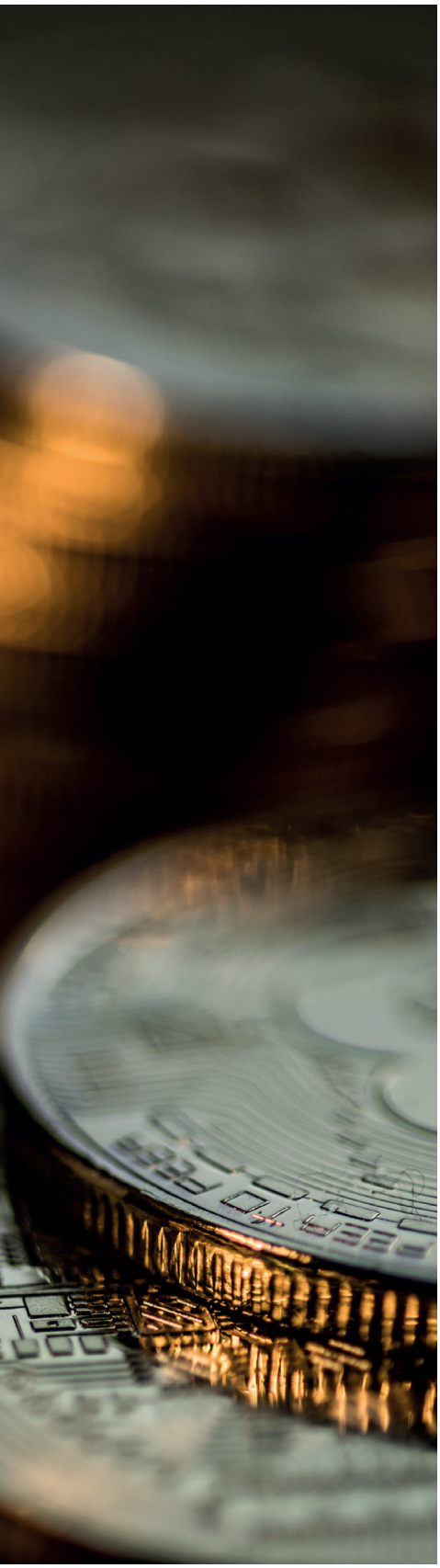
ISSN 2215-5910
Caso de estudio

ISSN 2215-5910
Caso de estudio



LIBRO BLANCO EXTENDIDO DE BITCOIN. ADAPTADO AL REGLAMENTO MICA

EXTENDED BITCOIN WHITE PAPER. ADAPTED TO EU MICA REGULATION

Recibido: 16 Octubre, 2023 • Revisado: 30 Noviembre, 2023 • Aceptado: 13 Diciembre, 2023

Javier Maestre Rodríguez,
Juan Ignacio Ibañez y Nancy Quirós Aguilar

RESUMEN

La aparición de Bitcoin en el año 2009 ha impactado a diferentes sectores, tales como el financiero, tecnológico, político, educativo, regulatorio, entre otros, y más de una década después, todavía no contamos con un consenso acerca de su naturaleza. Es por esta razón, que el ámbito regulatorio enfrenta grandes retos, ya que debe encontrar la forma de no obstaculizar el auge innovativo de la nueva tecnología Bitcoin. Los requerimientos del reglamento MiCA representan uno de los primeros enfoques regulatorios que han surgido y surgirán a nivel mundial. Así que, los autores de este documento, de forma voluntaria, han decidido redactar "El Libro Blanco Extendido de Bitcoin" de acuerdo con las normativas de MiCA y brindarlo a la comunidad, para que así Bitcoin sea el primer criptoactivo en cumplir con dichas disposiciones y que tales requerimientos no sean un impedimento para su uso.

Palabras clave: Bitcoin, regulación, criptoactivo, tecnología, minería, prueba de trabajo.

ABSTRACT

The emergence of Bitcoin in 2009 has had an impact on various sectors, including the financial, technological, political, educational, regulatory, and others. More than a decade later, we still do not have a consensus about its nature. For this reason, the regulatory brand faces significant challenges, as it must find a way to not hinder the innovative rise of the new Bitcoin technology. The requirements of the MiCA regulation represent one of the first regulatory approaches that have emerged and will continue to emerge worldwide. Therefore, the authors of this document have voluntarily decided to draft the "Extended White Paper of Bitcoin" in accordance with MiCA regulations and offer it to the community. This way, Bitcoin can become the first cryptoasset to comply with these provisions, so these requirements will not be an impediment to its use.

Keywords: Bitcoin, regulation, cryptoasset, technology, mining, proof of work.

Javier Maestre es Abogado especializado en Internet y nuevas tecnologías, empezó a escribir y trabajar en temas de Bitcoin y criptoactivos en el año 2013. Profesor del Máster de Formación Permanente y Alta Especialización en Asesoría Fiscal de la Escuela de Práctica Jurídica de la Universidad Complutense.

Juan Ignacio Ibañez es Chief of Staff de la DLT Science Foundation, Administrador del Centro de Tecnología Blockchain del University College London, docente de Blockchain y Criptomonedas de la Universidad Católica Argentina, Investigador en blockchain y sustentabilidad en la Universidad Católica de Córdoba. Abogado especializado en análisis económico del derecho.

Nancy Quirós Aguilar. PhD in Physics, MSc in Digital Currencies. Instructora del curso "Bitcoin y los criptoactivos" que imparte LEAD University de Costa Rica. Vicepresidenta de la Asociación Bitcoin Costa Rica (AsoBitcoin CR). Su interés se enfoca en el estudio del impacto político y económico de Bitcoin en la sociedad desde una perspectiva filosófica.

MOTIVACIÓN

Los integrantes del movimiento *cypherpunk*[1], que inspira Bitcoin, no estaban exentos de una cierta paranoia, como muestra el hecho de que quien o quienes lo concibieron [Bitcoin] se cuidaron mucho de permanecer en el anonimato, así como la obsesión que evidencia su diseño por los eventuales puntos de fallo.

No hay que llegar a la paranoia *cypherpunk* para discernir que los actuales Estados tienen a Bitcoin en el punto de mira, dado que supone una seria amenaza al latrocinio en que se ha convertido lo que eufemísticamente denominan "política monetaria".

Pero a pesar de la tiranía en la que, en aras del bien común y el interés general, se están convirtiendo nuestras democracias, hay cosas que se antojan todavía difíciles, como, por ejemplo, que haya una prohibición directa de tener contacto alguno con Bitcoin y su tecnología. No pueden decir "prohíbo bitcoin"; tienen que ser más sutiles.

En Estados Unidos habría quien arguyera en su favor la 2ª enmienda y el derecho a portar armas, pues no falta quien lo ve desde esa perspectiva. O también podría considerarse que su naturaleza de código informático haga que esté amparado por la proscripción de la censura y Libertad de expresión. En España, por ejemplo, el derecho fundamental "a la producción y creación literaria, artística, científica y técnica" consagrado en el art. 19 de la Constitución[2], podría ser empleado para amparar Bitcoin ya que es un *software*, por lo tanto, una creación de índole científico y técnico.

Como se indica, si se quiere mantener un mínimo de coherencia que sustente el castillo de naipes sobre el que andan, han de ser más precavidos e ir por otro camino. Una de las estrategias a las que se suele echar mano en situaciones como éstas consiste en crear una categoría, por artificial y arbitraria que sea (véase el caso del concepto de *"security"*[3]) y regularla. Esa es la punta de lanza. La categoría ya la tenemos: criptoactivo, en la que bitcoin entra, aunque sea con calzador y admitiendo barco como animal acuático.

Por razones cuya explicación sería demasiado extensa para este acto, hay quienes consideramos, como los que presentamos este trabajo, que Bitcoin necesitará un Libro Blanco que cumpla las previsiones del MiCA[4] para que pueda ser admitido a cotización. Mucha gente puede pensar: "a mí eso me da igual". Pero se considera que no es una actitud honesta ni razonable: los bitcoiners no pueden ser un grupo exclusivo, los bitcoiners deben aspirar a que todas las personas puedan beneficiarse de este avance tecnológico. Y eso pasa, de momento, porque la gente pueda entrar y salir del *fiat*[5] al Bitcoin de forma fácil y sencilla y que puedan experimentar ambas opciones.

Este proyecto viene a decir a los reguladores que Bitcoin será el primer criptoactivo en cumplir con los requerimientos del Reglamento MiCA y, lo más importante, que todas las modificaciones y ampliaciones normativas que se avecinan (porque con certeza vendrán), van a contar con un ejército de individuos que, como los autores de este documento, harán efectivo el cumplimiento de las ocurrencias legislativas que se antojen, al objeto de que la mayor cantidad de gente posible tenga la opción de elegir; la posibilidad de aspirar a un grado mayor de Libertad.

CUMPLIMIENTO DE DEBERES DE INFORMACIÓN DEL ART. 6.3 Y 6.4[6]

En cumplimiento de lo indicado en el Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo,

[1] El movimiento cypherpunk emergió a finales de los años 80 y fue conformado por un grupo de activistas expertos en ciencia computacional, matemática, filosofía y política quienes tenían por objetivo resguardar las libertades individuales, también la anonimidad, privacidad en línea por medio del uso de criptografía. Eric Hughes. "A Cypherpunk's Manifesto". Consultado el 29 de Noviembre de 2023. https://www.activism.net/cypherpunk/manifesto.html.

[2] David Vila-Viñas, "Derecho a la ciencia. Libertad de investigación, acceso, participación y promoción de la ciencia en el ordenamiento español," Universidad de Zaragoza, 2020, https://e-revistas.uc3m.es/index.php/DYL/article/download/6110/4479/.

[3] El análisis de los criptoactivos bajo la categoría de security (valores negociables e instrumentos financieros) ha sido motivo de enorme controversia en distintos países, sobre todo Estados Unidos, donde el *Security and Exchange Commission (SEC)* ha demandado a reconocidas casas de intercambio bajo el incumplimiento de la normativa relacionada con este tipo de instrumentos financieros. Sin embargo, al día de redacción de este documento, no existe una clara definición acerca de qué corresponde como security en el caso de los criptoactivos. Javier Maestre, "To be security or not to be. That's the question". Consultado el 29 de noviembre de 2023, https://maestreabogados.com/to-be-security-or-not-to-be-thats-the-question/

[4] MiCA: Markets in CryptoAssets. Marco regulatorio de la Unión Europea para los criptoactivos y mercados asociados. Se puede encontar en: https://eur-lex.europa.eu/eli/reg/2023/1114/oj

[5] El dinero fiat o fiat se refiere al dinero emitido por los bancos centrales de los distintos países o sus respectivas autoridades monetarias y no tiene respaldo por dinero mercancía.

[6] Página 69 del "Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos", https://eur-lex.europa.eu/eli/reg/2023/1114/oj

de 31 de mayo de 2023, relativo a los mercados de criptoactivos (MiCA)[7], se informa de que:

- Artículo 6.3: Este libro blanco de criptoactivos no ha sido aprobado por ninguna autoridad competente de ningún Estado miembro de la Unión Europea. El oferente del criptoactivo, la persona que solicite la admisión a negociación, el operador de la plataforma de negociación, o cualquier otra persona que haga uso del presente documento, según el caso, es el único responsable del contenido de este libro blanco de criptoactivos.
- Artículo 6.4:
  a) el criptoactivo puede perder su valor total o parcialmente;
  b) el criptoactivo puede no ser siempre negociable;
  c) el criptoactivo puede no ser líquido;
  d) cuando la oferta pública se refiera a una ficha de consumo, esa ficha puede no ser canjeable por el bien o servicio prometido en el libro blanco de criptoactivos, especialmente en caso de fracasar o interrumpirse el proyecto de criptoactivos;
  e) el criptoactivo no está cubierto por los sistemas de indemnización de los inversores con arreglo a la Directiva 97/9/CE del Parlamento Europeo y del Consejo;
  f) el criptoactivo no está cubierto por los sistemas de garantía de depósitos con arreglo a la Directiva 2014/49/UE.

DECLARACIÓN PARA EL CUMPLIMIENTO DEL ART. 6.6[8]

En cumplimiento de lo indicado en el art. 6.6, el órgano de dirección del oferente, la persona que solicite la admisión a negociación o el operador de la plataforma de negociación declara que, según el leal saber y entender del órgano de dirección, la información presentada en el libro blanco de criptoactivos es imparcial, clara y no engañosa y el libro blanco de criptoactivos no incurre en ninguna omisión que pueda afectar a su contenido.

RESUMEN PARA EL CUMPLIMIENTO DEL ART. 6.7[9]

Bitcoin fue, usando la terminología del Reglamento, el primer criptoactivo de la historia y ha estado plenamente operativo desde el año 2009. Nació como un *software* libre, de código abierto, que cualquier persona puede utilizar, reproducir y modificar sin restricción alguna impuesta por sus autores. El *White Paper* (Libro Blanco) original del proyecto se encuentra accesible en el enlace de esta nota[10]. En el presente documento se hará referencia a Bitcoin (con mayúsculas) para designar al sistema compuesto por la red de ordenadores y el *software* necesario para su funcionamiento, mientras que bitcoin (en minúsculas) se usará para referirse a las unidades, *token* o fichas que se crean automáticamente como recompensa por la validación de operaciones en el contexto de un mecanismo de consenso, mediante la utilización del mecanismo conocido como Prueba de Trabajo (PoW, por sus siglas en inglés, *Proof of Work*).

En cumplimiento de lo indicado en el art. 6.7, se efectúa un resumen sobre diversos aspectos del criptoactivo.

a) Oferta pública[11]: A diferencia de otros proyectos, en el caso de Bitcoin, no hubo una venta inicial o preminado por parte del emisor[12], puesto que Bitcoin no tiene emisor, en el sentido que se indica en el Reglamento, ya que no existe persona o empresa que haya emitido, emita o vaya a

[7] Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos, https://eur-lex.europa.eu/eli/reg/2023/1114/oj

[8] Página 70 del "Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos", https://eur-lex.europa.eu/eli/reg/2023/1114/oj

[9] Art. 6.7. "El libro blanco de criptoactivos contendrá un resumen, insertado después de la declaración a que se refiere el apartado 6, que proporcionará, de forma **sucinta y sin tecnicismos**, **información** relevante acerca de la **oferta pública** del criptoactivo o de **su admisión prevista a negociación**. El resumen será fácil de comprender y se presentará y aparecerá en un formato claro y completo, utilizando caracteres de tamaño legible. El resumen del libro blanco de criptoactivos ofrecerá información adecuada sobre las **características del criptoactivo** en cuestión a fin de que los potenciales titulares puedan tomar una decisión fundada."

[10] Satoshi Nakamoto, "Bitcoin: Un sistema de efectivo electrónico peer-to-peer," bitcoin.org, https://bitcoin.org/bitcoin.pdf.

[11] El art. 3 define "**oferta pública**" como "una comunicación a personas, de cualquier forma y por cualquier medio, que presenta información suficiente sobre los términos de la oferta y los criptoactivos que se ofertan de modo que permite a potenciales titulares decidir si adquieren dichos criptoactivos". Y el término **oferente** se define como "la persona física o jurídica, u otra empresa, o el emisor, que oferta al público criptoactivos".

[12] El artículo 3 define al **emisor** como "una **persona física o jurídica u otra empresa que emite** criptoactivos". Por su parte, el Considerando 20 indica que "Los emisores de criptoactivos son las **entidades** que **controlan la creación** de criptoactivos."

emitir o controle la creación de los criptoactivos de la red. Desde que el software se encontró disponible y la red comenzó a funcionar, la emisión de nuevas unidades del criptoactivo se realiza de forma automática como parte del funcionamiento del mecanismo de consenso. [a completar, en su caso, por el oferente]

b) Su **admisión prevista a negociación**. Bitcoin lleva muchos años siendo admitido a cotización en innumerables plataformas de intercambio, al menos desde octubre del año 2009[13]. Al ser el primer criptoactivo de la historia, fue también el primero en ser admitido a negociación en los mercados, por lo que es de esperar que siga siendo así. [a completar, en su caso, por el oferente o solicitante a negociación]

Igualmente, en cumplimiento de lo indicado en el art. 6.7 del Reglamento, se advierte de que:

a) el resumen debe leerse a modo de introducción del libro blanco de criptoactivos;

b) el potencial titular debe basar su decisión de compra del criptoactivo en el contenido de la totalidad del libro blanco de criptoactivos, y no únicamente en el resumen;

c) la oferta pública del criptoactivo no constituye una oferta o invitación para la adquisición de instrumentos financieros, que únicamente puede hacerse mediante un folleto u otro documento de oferta en virtud del Derecho nacional aplicable;

d) el libro blanco de criptoactivos no constituye un folleto a tenor del Reglamento (UE) 2017/1129 del Parlamento Europeo y del Consejo[14] ni ningún otro tipo de documento de oferta en virtud del Derecho de la Unión o nacional.

Parte A: Información sobre el oferente o la persona que solicite la admisión a negociación
[a completar por el oferente/solicitante]

1. Nombre:
2. Forma jurídica:
3. Domicilio social y sede social, si fueran diferentes:
4. Fecha de inscripción en el registro:
5. Identificador de entidad jurídica u otro identificador exigido en virtud del Derecho nacional aplicable (NIF):
6. Varios:
   a. Número de teléfono de contacto:
   b. dirección de correo electrónico:
   c. número de días en los que un inversor que se ponga en contacto recibirá una respuesta:
7. En su caso, el nombre de la empresa matriz:
8. Identidad, dirección profesional y funciones de las personas que son miembros del órgano de dirección de la empresa:
9. Actividad empresarial o profesional del oferente o de la persona que solicite la admisión a negociación y, en su caso, su empresa matriz.
10. La situación financiera, en los tres últimos años, del oferente o de la persona que solicite la admisión a negociación o, en caso de que el oferente o la persona que solicite la admisión a negociación no haya estado establecido durante los tres últimos años, su situación financiera desde la fecha de su inscripción en el registro. La situación financiera se evaluará sobre la base de una exposición fiel de la evolución y los resultados de la actividad empresarial del oferente o la persona que solicite la admisión a negociación, y de su situación, para cada año y período intermedio sobre los que se deba presentar información financiera histórica, con las causas de los cambios importantes. La exposición consistirá en un análisis equilibrado y exhaustivo de la evolución y los resultados del negocio del oferente o la persona que solicite la admisión a negociación y de su situación, que sea coherente con la magnitud y la complejidad de la misma.

[13] - "Línea del tiempo de Bitcoin", Dinero Sin Reglas, https://dinerosinreglas.com/linea-del-tiempo-de-bitcoin/.
- "2009 Exchange Rate," New Liberty Standard, https://web.archive.org/web/20131102222638/http://www.newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate, consultado el 18 de octubre de 2023.

[14] Reglamento (UE) 2017/1129 del Parlamento Europeo y del Consejo, de 14 de junio de 2017, sobre el folleto que debe publicarse en caso de oferta pública o admisión a cotización de valores en un mercado regulado y por el que se deroga la Directiva 2003/71/CE (DO L 168 de 30.6.2017, p. 12).

Parte B: Información sobre el emisor, cuando difiera del oferente o la persona que solicite la admisión a negociación

1. **Nombre**: Bitcoin no tiene emisor, ni identificable ni no identificable. Las unidades de bitcoin se crean automáticamente como recompensa por la validación de operaciones en el contexto de un mecanismo de consenso.
2. **Forma jurídica**: No procede.
3. **Domicilio social y sede social, si fueran diferentes**: No procede.
4. **Fecha de inscripción en el registro**: No procede
5. **Identificador de entidad jurídica u otro identificador exigido en virtud del Derecho nacional aplicable (NIF)**: No procede
6. **En su caso, el nombre de la empresa matriz**: No procede.
7. **Identidad, dirección profesional y funciones de las personas que son miembros del órgano de dirección del emisor**: No procede.
8. **Actividad empresarial o profesional del emisor y, en su caso, su empresa matriz**: No procede.

Parte C: Información sobre el operador de la plataforma de negociación en los casos en que elabore el libro blanco de criptoactivos
[a completar por el operador de la plataforma]

1. Nombre.
2. Forma jurídica.
3. Domicilio social y sede social, si fueran diferentes.
4. Fecha de inscripción en el registro.
5. Identificador de entidad jurídica u otro identificador exigido en virtud del Derecho nacional aplicable.
6. En su caso, el nombre de la empresa matriz.
7. Motivo por el que dicho operador elaboró el libro blanco de criptoactivos:
8. Identidad, dirección profesional y funciones de las personas que son miembros del órgano de dirección del operador.
9. Actividad empresarial o profesional del operador y, en su caso, su empresa matriz.

Parte D: Información sobre el proyecto de criptoactivos

1. **Identificación del proyecto de criptoactivo:**
   a. **Denominación del proyecto de criptoactivos**: "Bitcoin: A Peer-to-Peer Electronic Cash System".
   b. **Denominación de los criptoactivos**: bitcoin y satoshi (la cien millonésima parte de un bitcoin).
   c. **Forma abreviada o ticker:** BTC
2. **Breve descripción del proyecto de criptoactivos**[15]:

   En síntesis, Bitcoin es un protocolo para la transmisión de valor entre pares (*peer-to-peer*, en inglés), sin la necesidad de un tercero de confianza, que posibilita la aparición, por primera vez en la historia, de un activo digital escaso.

   De acuerdo con el *White Paper* (Libro Blanco) original cuyo/s autor/es se identifica/n con el pseudónimo "Satoshi Nakamoto", mencionado en la nota 4, Bitcoin es un protocolo que permite el almacenamiento y la transmisión de valor sin la necesidad de participación de intermediarios o terceros de confianza, ya que las transacciones o intercambios se realizan entre pares y una vez realizadas tienen el carácter de irreversibles.

   Bitcoin hace uso de un sistema de firmas digitales. El marco habitual de monedas basadas en firmas digitales proporciona un control estricto de la propiedad basado en registros de transacciones centralizados, a cargo de terceros de confianza, que garanticen la unicidad de las transacciones y eviten el doble gasto. Bitcoin ofrece una solución alternativa al problema del doble gasto sin necesidad de recurrir a elementos centrales de confianza, mediante una tecnología de registro distribuido (TRD), que permite la aparición, por primera vez en la historia, de un activo digital real escaso.

   La red de Bitcoin está conformada por los nodos que ejecutan el *software* de Bitcoin, que es de código abierto y, por tanto, susceptible de poder ser modificado por cualquiera, y contempla las

[15] Redacción basada en gran medida en el "Abstract" del White Paper original mencionado en la nota 4.

reglas del protocolo a las que todos los usuarios se someten para recibir, verificar y transmitir transacciones. Además, almacenan el libro histórico de registro de transacciones y, en consecuencia, mantienen el registro distribuido.

Al no existir elementos de coordinación central en la red, el consenso de todos los nodos acerca del orden temporal de transacciones se produce a través de los nodos llamados "mineros", cuya función es organizar en grupos (bloques)[16] las transacciones que se van produciendo en la red, y agregarlos al libro de registro de transacciones o registro distribuido. Este proceso ocurre aproximadamente cada 10 minutos y se conoce como la Prueba de Trabajo, que es la forma en que Bitcoin resuelve el problema del doble gasto, y que será descrita en secciones posteriores.

La red marca la hora de las transacciones mediante el hash[17] de estas en una cadena continua de pruebas de trabajo[18], formando un registro que no se puede cambiar sin repetir el proceso de Prueba de Trabajo. La cadena más larga[19], no solo sirve como prueba de la secuencia de eventos presenciados, sino también de que proviene del grupo con mayor poder de cómputo o procesamiento[20]. Mientras la mayoría del poder de cómputo o procesamiento esté controlada por nodos que no cooperen para atacar la red, éstos generarán la cadena más larga y superarán a los eventuales atacantes. La propia red requiere una estructura mínima. Los mensajes se transmiten sobre la base del mayor esfuerzo, y los nodos pueden abandonar y volver a unirse a la red a voluntad, aceptando la cadena de pruebas de trabajo más larga como evidencia de lo que sucedió mientras estuvieron ausentes.

De esta forma, se propone un sistema para transacciones electrónicas sin depender de la confianza, con base en una red entre pares (*peer-to-peer*) que utiliza pruebas de trabajo para registrar un historial público de transacciones, integrantes del registro distribuido, que rápidamente se vuelve computacionalmente impracticable de cambiar si los nodos honestos controlan la mayoría del poder de cómputo. La red es robusta en su simplicidad no estructurada. Los nodos trabajan todos al mismo tiempo, con poca coordinación. No necesitan ser identificados, ya que los mensajes no se enrutan hacia ningún lugar en particular y tan solo necesitan ser entregados de la mejor manera posible. Los nodos pueden abandonar y volver a unirse a la red a voluntad, aceptando la cadena de pruebas de trabajo como evidencia de lo que sucedió mientras estuvieron ausentes. Los nodos hacen su elección con su potencia de procesamiento informático, expresando su aceptación de bloques válidos trabajando en su extensión y rechazando bloques inválidos al negarse a trabajar sobre ellos. Cualquier regla o incentivo necesario pueden ser implementados con este mecanismo de consenso.

3. **Datos de todas las personas físicas o jurídicas (incluida su dirección profesional o el domicilio de la empresa) que participen en la ejecución del proyecto de criptoactivos, como los asesores, el equipo de desarrollo y los proveedores de servicios de criptoactivos**: No procede. En la ejecución del proyecto participa una pluralidad indeterminada de personas, algunas anónimas y otras no, y con papeles o funciones muy variadas.

[16] Estructura de datos que contiene un conjunto de transacciones de bitcoin, información del bloque y metadata, entre la que se incluye el campo “nonce” usado para la Prueba de Trabajo y el identificador del bloque.

[17] **Hash**: función criptográfica que calcula sobre ciertos elementos de entrada (input) un valor de tamaño fijo, determinista y único. El elemento de salida se conoce como el "hash del input". Es inviable calcular el input a partir de su hash. Los identificadores o ID de los bloques son obtenidos por medio de cálculos de hashes. El ID de un bloque nuevo depende del ID del bloque precedente formando una cadena de hashes.

[18] A lo largo de este documento, el término “Prueba de Trabajo” ha sido empleado para hacer referencia al mecanismo de consenso utilizado en Bitcoin. También, se hace mención a “pruebas de trabajo” y por esta expresión se debe entender a la actividad (o trabajo en forma de cálculo de hashes) realizado por los mineros.

[19] Por “**cadena más larga**” nos referimos al libro de registro de transacciones con la mayor cantidad de prueba de trabajo representada por cálculos de hashes. En ocasiones, diferentes nodos pueden tener libros de registro con diferente prueba de trabajo (distinto número de bloques y dificultad). Con el fin de que la red llegue a un consenso con respecto al estado del libro de transacciones, convencionalmente los nodos eligen como válida la cadena con mayor cantidad de trabajo.

[20] El White Paper original habla de “the largest pool of CPU power”. Las siglas CPU se corresponden con la expresión “Central Processing Unit” (Unidad Central de Procesamiento).

4. **Cuando el proyecto de criptoactivos se refiera a fichas de consumo, características fundamentales de los bienes o servicios por desarrollar**. No procede, Bitcoin no es una ficha de consumo, si bien puede usarse su red para la creación de ese tipo de criptoactivos.
5. **Información sobre el proyecto de criptoactivos, especialmente las principales etapas pasadas y futuras del proyecto y, cuando proceda, los recursos ya asignados al proyecto**:

Etapas pasadas

El **31 de octubre de 2008**[21], Satoshi Nakamoto publicó el Libro Blanco (*White Paper*) original en una lista de correo de asuntos criptográficos[22] llamada *"The Cryptography Mailing List"*. Hoy en día, todavía es un misterio la persona o colectivo que se encuentra tras ese pseudónimo y existen numerosas y variopintas teorías al respecto[23].

El **9 de noviembre de 2008**, se registra el proyecto en la plataforma "SourceForge.net"[24], un sitio especializado en distribución de *software* de código abierto.

El **16 de noviembre de 2008** es la fecha más antigua de la que hay constancia del código informático de Bitcoin, según se indica en el foro de Bitcointalk.org[25].

El **3 de enero de 2009** se procede a la creación del bloque génesis[26] de Bitcoin por parte de Satoshi Nakamoto y la red empieza a funcionar.

El **9 de enero de 2009** se da a conocer la versión 0.1 del cliente de Bitcoin. Esta es la primera versión en Código Abierto (*Open Source*) del código de Bitcoin que incluye unas 30.000 líneas de código[27].

El **5 de octubre de 2009** es la primera fecha de la que se tiene constancia en que se haya establecido alguna tarifa o relación de cambio entre bitcoin y una moneda *fiat*, fijándola en 1 USD ($) = 1.309,03 BTC, utilizando una ecuación que incluye el coste de la electricidad para hacer funcionar un ordenador que genere 1 bitcoin[28].

Durante los años siguientes, se realizaron mejoras técnicas significativas en el protocolo de Bitcoin. Por ejemplo:

- En el año 2017, se implementó Segregated Witness (SegWit), una actualización que mejoró la capacidad de la red y la eficiencia de las transacciones. Además, se llevaron a cabo discusiones y debates sobre la escalabilidad y el tamaño de bloque de Bitcoin, de forma que en agosto de 2017, Bitcoin experimentó, entre otras muchas, la bifurcación (*fork*) que condujo a la creación de Bitcoin Cash (BCH). Esta bifurcación fue el resultado de diferencias en la visión de escalabilidad de Bitcoin y condujo a la creación de un criptoativo diferente basado en una cadena con bloques más grandes.
- En el año 2018 se propone Taproot y se implementa en el 2021. Esta actualización cambió el esquema de firma de transacciones de Bitcoin y representó un aumento en privacidad, escalabilidad y capacidad para añadir funcionalidades avanzadas que son de utilidad para implementaciones de capa superior como *Lightning Network*[29].
- En el año 2019 es propuesto Erlay e implementado en el 2022. Erlay es una actualización realizada con el fin de incrementar la eficiencia en el proceso de comunicación entre los nodos al reducir la necesidad de transmisión de información redundante, como consecuencia, disminuye el ancho de banda requerido para ejecutar un nodo.

[21] "Línea del tiempo de Bitcoin", Dinero Sin Reglas, https://dinerosinreglas.com/linea-del-tiempo-de-bitcoin/.

[22] - "Mensaje d e la lista de correo de criptografía de octubre de 2008," Metzdowd Cryptography Mailing List, https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html
- "Fragmento de la página web," https://archive.is/rMBtV#selection-65.90-65.119.

[23] "Satoshi Nakamoto," Wikipedia, https://en.wikipedia.org/wiki/Satoshi_Nakamoto

[24] "Proyecto Bitcoin en SourceForge," SourceForge, https://sourceforge.net/projects/bitcoin/.

[25] "Topic: Bitcoin source from November 2008", Bitcointalk, https://bitcointalk.org/index.php?topic=382374.0. 18 de octubre de 2023

[26] "Bloque en Mempool Space," Mempool Space, https://mempool.space/es/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

[27] "Topic: v0.1," Bitcointalk, https://bitcointalk.org/index.php?topic=68121.0, 18 de octubre de 2023.

[28] "2009 Exchange Rate," New Liberty Standard, https://web.archive.org/web/20221009200138/http://newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate, consultado el 18 de octubre de 2023

[29] Protocolo de interacción peer-to-peer con la capa principal o base, Bitcoin, que permite la creación de relaciones transaccionales entre partes (canales de pago) por medio de multifirmas, con el fin de enviar y recibir pagos bitcoin sin la necesidad que estos movimientos sean registrados en el libro de registro de transacciones de Bitcoin. La ventaja de Lightning Network es que permite a Bitcoin alcanzar escalabilidad (elevado número de transacciones por segundo).

Recursos asignados al proyecto Bitcoin

Bitcoin es una red distribuida, con una gran descentralización y no está respaldada por una entidad centralizada. No hay una entidad responsable que gestione los recursos asignados al proyecto. Entre estos recursos se puede diferenciar:

Recursos de hardware y computación. Los mineros que contribuyen a la generación de nuevos bloques, utilizando equipos informáticos, tiempo y capacidad de cómputo o procesamiento (que actualmente se traduce en energía). Por otro lado, los nodos validan dichos bloques, comprobando que cumplen las reglas del protocolo. Ambos son necesarios para el funcionamiento de la red. La potencia de cálculo de los equipos mineros de la red se encuentra en constante ascenso, habiendo superado en agosto de 2023 la cifra de 400 millones de TH/s[30], mientras que el número de nodos conectados a la red, en agosto de 2023, se estima en más de 45.000[31].

Recursos humanos. Existen numerosos desarrolladores de *software* que contribuyen a su mejora y seguridad, así como una comunidad activa de contribuyentes en todo el mundo. Las mejoras y actualizaciones del protocolo se proponen y debaten abiertamente a través del proceso de mejora de Bitcoin (Bitcoin Improvement Proposal, BIP)[32].

Recursos inmateriales. Proporcionados por los desarrolladores y participantes de la comunidad, tales como el *software* o código informático, que se encuentra en constante actualización y que suele ser publicado como código libre y abierto, así como la creación de otros elementos protegidos por las leyes de propiedad intelectual o industrial, como, por ejemplo, el logotipo usado mayormente y que fue licenciado de forma amplia por su autor en favor de la comunidad[33].

Etapas futuras

Desde que Bitcoin ha estado en funcionamiento, las unidades del criptoactivo se han ido creando automáticamente como recompensa por la validación de operaciones en el contexto del mecanismo de consenso diseñado en el protocolo. Inicialmente, durante los primeros 210.000 bloques, aproximadamente 4 años, los mineros recibían 50 bitcoins como recompensa. Al concluir este periodo, se produjo un recorte de los incentivos a la mitad (25 bitcoins) y así sucesivamente[34]. Así que, como parte de las etapas futuras por las que atravesará Bitcoin, tendremos estos recortes en el subsidio por bloque hasta que finalmente, alrededor del año 2140, nos encontraremos con un acercamiento asintótico a los 21 millones de bitcoins y finalizará la creación de nuevas unidades y los mineros serán recompensados únicamente con las comisiones por transacción.

Además, como ha sido expresado a lo largo de este documento, Bitcoin es un *software* descentralizado que se ejecuta en nodos ubicados por todo el mundo y que no son coordinados por ningún elemento central. Por lo tanto, no existe lo que se conoce como *road map* o planes futuros para Bitcoin. De lo que hay certeza es lo que ya está establecido por el protocolo, como fue mencionado en el párrafo anterior. Por esta razón, no es posible describir con claridad por qué otras etapas atravesarán la red en los próximos años.

Sin embargo, es posible para los participantes de la red de Bitcoin llegar a consensos acerca de mejoras en funcionalidad del *software* a través de propuestas realizadas por los desarrolladores. Estas propuestas de mejoras son de índole voluntario y no imperativo, es decir, aquellos nodos que ejecutan el *software* tienen la capacidad de aceptarlas o rechazarlas. Es importante resaltar que los cambios o actualizaciones en el *software* no han alterado, ni es previsible que lo hagan, la cantidad total de unidades en circulación ni el proceso de emisión de las mismas.

Los retos a los que se enfrenta Bitcoin en el futuro podrían sintetizarse en los siguientes:

Mejoras en la escalabilidad: El desafío de la escalabilidad continúa siendo uno de los principales enfoques del desarrollo de Bitcoin. Se están explorando

30 "Gráficos del hashrate en Blockchain.com," Blockchain.com, https://www.blockchain.com/explorer/charts/hash-rate, 18 octubre de 2023.

31 "Sitio web de Bitnodes," Bitnodes, https://bitnodes.io/, 18 octubre de 2023.

32 "Página sobre BIP en Bit2Me Academy," Bit2Me Academy, https://academy.bit2me.com/que-es-bip-bitcoin/, 18 de octubre de 2023.

33 "Topic: More Bitcoin logos, buttons, and also some other graphics," Bitcointalk, https://bitcointalk.org/index.php?topic=1631, 18 de octubre de 2023.
- Enlace al hilo en una versión más antigua donde figuran los logotipos creados: "Topic: More Bitcoin logos, buttons, and also some other graphics," Bitcointalk, https://web.archive.org/web/20130912111647/https://bitcointalk.org/index.php?topic=1631, 18 de octubre de 2023.

34 Evento conocido como “halving”

diferentes soluciones, como la implementación de la tecnología *Lightning Network*, que permite transacciones más rápidas y de menor coste fuera de la cadena principal de Bitcoin.

Mayor adopción e integración: Se espera que Bitcoin continúe siendo adoptado por más personas y empresas en todo el mundo. A medida que se mejora la infraestructura y se facilita la accesibilidad, se espera que aumente la adopción tanto como reserva de valor como medio de intercambio.

Regulación y marco legal: A medida que se incrementa el uso y adopción de Bitcoin y otros criptoactivos, es probable que se implementen más regulaciones y se establezcan marcos legales en diferentes jurisdicciones. La forma en que se desarrollen estas regulaciones y cómo afecten a Bitcoin sigue siendo un tema de discusión y atención.

Innovaciones tecnológicas: Dado que Bitcoin es una tecnología en constante evolución, es probable que se realicen más innovaciones y mejoras en el software y el protocolo. Esto puede incluir mejoras en la privacidad, seguridad y eficiencia de las transacciones. Este tipo de mejoras se lograrían a través de consenso de la red y son de carácter voluntario, como fue mencionado previamente.

Es importante tener en cuenta que el futuro de Bitcoin es incierto y está sujeto a diversos factores, como la adopción, la competencia de otros criptoactivos y los desarrollos tecnológicos en el campo de la criptografía. Sin embargo, hasta la fecha, Bitcoin ha demostrado ser un proyecto resiliente y sigue siendo uno de los criptoactivos más populares y reconocidos en todo el mundo.

6. **Cuando proceda, el uso previsto de todos los fondos u otros criptoactivos captados:**

   No procede. Bitcoin nunca ha captado fondos ni otros criptoactivos, ni está previsto que lo haga en el futuro.

Parte E: Información sobre la oferta pública de criptoactivos o su admisión a negociación

1. **Indicación de si el libro blanco de criptoactivos se refiere a una oferta pública de criptoactivos o a su admisión a negociación**.
   [a completar por el oferente/solicitante]
2. **Motivos de la oferta pública o de la solicitud de admisión a negociación.**
   [a completar por el oferente/solicitante]
3. **Cuando proceda, importe o cantidad que se pretende obtener a través de la oferta pública en fondos o en cualquier otro criptoactivo, incluidos, en su caso, los objetivos mínimos y máximos de suscripción establecidos para la oferta pública de criptoactivos, y si se acepta el exceso de suscripciones y cómo se asigna.**
   [a completar, en su caso, por el oferente]
4. **Precio de emisión del criptoactivo ofertado al público (en una moneda oficial o en cualquier otro criptoactivo), comisiones de subscripción aplicables o método que se seguirá para determinar el precio de oferta.**
   [a completar, en su caso, por el oferente]. En su caso, ver punto III del presente Libro Blanco "Resumen para el cumplimiento del art. 6.7".
5. **Cuando proceda, número total de criptoactivos que se ofertarán al público o admitirán a negociación.**

   En cuanto al número de criptoactivos admitidos a negociación, no hay ningún límite más allá de los criptoactivos que se generarán conforme al *White Paper* original mencionado en la nota 4 y que alcanzará la cifra aproximada de 21 millones de bitcoins (BTC). [En caso de oferta pública, completar por el oferente]
6. **Indicación de los potenciales titulares a los que se dirige la oferta pública de criptoactivos o la admisión a negociación de criptoactivos, incluida cualquier restricción en cuanto al tipo de titulares de tales criptoactivos.**
   [a completar por el oferente/solicitante]
7. **Aviso específico que indique que los compradores que participen en la oferta pública de criptoactivos podrán obtener un reembolso si no se alcanza, al término de la oferta pública, el objetivo mínimo de suscripción previsto, si ejercen el derecho de desistimiento previsto en el artículo 13, o si la oferta se cancela, así como una descripción detallada del plan de reembolso, incluido el plazo previsto en que se llevarán a cabo dichos reembolsos.**
   [a completar por el oferente/solicitante]

8. **Información sobre las distintas fases de la oferta pública de criptoactivos, incluida información sobre el precio de compra con descuento para los primeros compradores de criptoactivos (preventa pública). En caso de haber precios de compra con descuento para algunos compradores, explicación de por qué los precios de compra pueden ser diferentes, y descripción del efecto de ello en los otros inversores.**
[a completar por el oferente/solicitante]
9. **En el caso de las ofertas limitadas en el tiempo, período de suscripción durante el cual estará abierta la oferta pública.**
[a completar por el oferente/solicitante]
10. **Mecanismos para salvaguardar los fondos u otros criptoactivos a que se refiere el artículo 10 durante la oferta pública limitada en el tiempo o durante el período de desistimiento.**
[a completar por el oferente/solicitante]
11. **Medios de pago para adquirir los criptoactivos ofertados y métodos de transferencia del valor a los compradores cuando estos tengan derecho a obtener un reembolso.**
[a completar por el oferente/solicitante]
12. **En lo que respecta a las ofertas públicas, información sobre el derecho de desistimiento a que se refiere el artículo 13.**
[a completar por el oferente/solicitante]
13. **Información sobre las modalidades y el calendario de transferencia de los criptoactivos adquiridos a los titulares.**
[a completar por el oferente/solicitante]
14. **Información sobre los requisitos técnicos que ha de cumplir el comprador para poseer los criptoactivos.**

    El comprador deberá contar con un *wallet* o monedero[35] que sea compatible con el protocolo de Bitcoin si quiere poseer realmente sus criptoactivos, custodiar sus claves privadas y no depender de terceros para esa posesión efectiva. [a completar por el oferente/solicitante]
15. **En su caso, el nombre del proveedor de servicios de criptoactivos encargado de la colocación de los criptoactivos y forma de dicha colocación (sobre la base de un compromiso firme o sin él).**
[a completar por el oferente/solicitante]
16. **En su caso, nombre de la plataforma de negociación de criptoactivos en la que se solicita la admisión a negociación, e información sobre la forma en que los inversores pueden acceder a tales plataformas de negociación y los costes correspondientes.**
[a completar por el solicitante]
17. **Gastos relacionados con la oferta pública de criptoactivos**.
[a completar por el oferente/solicitante]
18. **Posibles conflictos de intereses de las personas que participen en la oferta pública o en la admisión a negociación que surjan en relación con la oferta o la admisión a negociación.**
[a completar por el oferente/solicitante]
19. **Derecho aplicable a la oferta pública de criptoactivos, así como órgano jurisdiccional competente.** [a completar por el oferente]

Parte F: Información sobre los criptoactivos

1. **El tipo de criptoactivo que se ofertará al público o respecto del cual se solicita la admisión a negociación.**

   De acuerdo con la taxonomía del Reglamento MiCA, Bitcoin entra dentro de la categoría de criptoactivos distintos de fichas referenciadas a activos o fichas de dinero electrónico.
2. **Descripción de las características, incluida la información necesaria para la clasificación del libro blanco de criptoactivos en el registro a que se refiere el artículo 109, tal como se especifique de conformidad con el apartado 8 de dicho artículo, y funcionalidades de los criptoactivos objeto de la oferta o admisión a negociación, incluida información sobre el momento en que se prevé que las funcionalidades estarán disponibles.**

   El apartado 8 del art. 109 indica que:

[35] *Software* que genera las llaves criptográficas asociadas con el bitcoin del usuario, permite crear y firmar transacciones. También establece comunicación con los nodos con el fin de propagar transacciones a través de la red, o bien, escuchar transacciones entrantes hacia las direcciones asociadas con su llave privada.

"La AEVM[36] elaborará proyectos de normas técnicas de regulación donde se concreten los datos necesarios para la clasificación, por tipo de criptoactivo, de los libros blancos de criptoactivos en el registro, incluidos los identificadores de entidad jurídica, y especificarán las disposiciones prácticas para garantizar que dichos datos puedan leerse en formato de lectura mecánica.

La AEVM presentará a la Comisión los proyectos de normas técnicas de regulación a que se refiere el párrafo primero a más tardar el 30 de junio de 2024.
Se delegan en la Comisión los poderes para completar el presente Reglamento adoptando las normas técnicas de regulación a que se refiere el párrafo primero del presente apartado de conformidad con los artículos 10 a 14 del Reglamento (UE) n.o 1095/2010."

Dado que todavía no se ha publicado la correspondiente norma técnica de regulación, no se puede completar este apartado.

Parte G: Información sobre los derechos y obligaciones vinculados a los criptoactivos

1. **Descripción de los derechos y obligaciones del comprador, en su caso, así como del procedimiento y las condiciones para el ejercicio de tales derechos.**

   Jurídicamente, Bitcoin no confiere ni establece derecho u obligación alguna. Las facultades de disposición y uso del criptoactivo son las derivadas de su código informático, conforme al *White Paper* original indicado en la nota 4 y el código informático de Bitcoin.

2. **Descripción de las condiciones en las que podrían modificarse los derechos y obligaciones.**

   Bitcoin es un *software* de código abierto, circunstancia que permite que pueda ser replicado y modificado, produciendo otras variantes[37]. Como un hecho histórico, es importante mencionar un suceso acontecido en el 2017 al que se ha denominado "*The Blocksize Wars*" (La Guerra del Tamaño de Bloques). Los usuarios de Bitcoin (desarrolladores, mineros, compañías y usuarios) mostraron tener diferencias irreconciliables acerca de cuál es el tamaño ideal de los bloques, ya que de este parámetro depende la escalabilidad de Bitcoin o la cantidad de transacciones por segundo (tps) que es capaz de procesar la red.

   Tales diferencias dividieron a la comunidad de Bitcoin en dos bandos: los *big blockers* (BB, los de bloques grandes), y los *small blockers* (SM, los de bloques pequeños). Los BB propusieron cambiar el *softwar*e y aumentar el tamaño de los bloques con el objetivo de incrementar la escalabilidad y que de esta forma Bitcoin pudiera cumplir más eficazmente su función de medio de intercambio. Por otro lado, los SM se opusieron con vehemencia a esta idea porque tal cambio podría afectar la descentralización de la red, ya que el aumento del tamaño de los bloques provocaría un incremento del espacio requerido para almacenar el libro de transacciones o registro distribuido por parte de los nodos y, de esta forma, los usuarios que no tuvieran acceso a gran poder computacional se verían imposibilitados para ejecutar nodos.

   La Guerra del Tamaño de Bloques culmina con la división irreparable de la comunidad de Bitcoin y el surgimiento de otro criptoactivo. Los BB crearon su propia red a partir de Bitcoin a la que llamaron Bitcoin Cash (BCH) y aumentaron el tamaño de los bloques a 8 MegaBytes (MB), que ha ido incrementándose hasta los 32 MB. La red de Bitcoin, defendida por los SM, permaneció en 1 MB (sin embargo, debido a mejoras en el software, es posible que los bloques lleguen a tener un tamaño de hasta 4 MB). Este hecho describe lo que se conoce como un *hard fork*. Es interesante notar que Bitcoin Cash ha quedado en la irrelevancia, ya que el mercado, en líneas generales, ha rechazado su propuesta de valor. Por otro lado, la red de Bitcoin ha resuelto su problema de escalabilidad con implementaciones como Lightning Network.

[36] AEVM: Autoridad Europea de Valores y Mercados.

[37] Más información sobre las diferentes bifurcaciones *(forks)* que ha sufrido Bitcoin, dando lugar a otros proyectos puede consultarse en: "Mapa de bifurcaciones importantes de Bitcoin," Visual Capitalist, https://www.visualcapitalist.com/major-bitcoin-forks-subway-map, 18 de octubre de 2023.

A partir de este acontecimiento, es importante resaltar que si alguien considera que Bitcoin tiene alguna deficiencia, puede tomar el código, hacer los cambios que crea pertinentes y crear una copia de Bitcoin con diferentes parámetros. No obstante, lo relevante para definir a Bitcoin como tal es que los usuarios acepten las reglas que se proponen. Por lo tanto, los efectos de red son indispensables para concluir que las propiedades de Bitcoin son inalterables. Por esta razón, la descentralización e inmutabilidad de las reglas del protocolo dependen también del rechazo de los usuarios a cambios unilaterales por usuarios o entes que deseen proponer versiones alternativas al protocolo de Bitcoin generalmente aceptado. Cuanta mayor descentralización se produzca en el funcionamiento de la red, más sólida y robusta se convierte.

3. **Cuando proceda, información sobre las futuras ofertas públicas de criptoactivos del emisor y el número de criptoactivos conservados por el propio emisor.**

   Bitcoin nunca ha realizado ni realizará una oferta pública de adquisición, ni preminado, ni ninguna otra operación similar, dado que, como se ha explicado, carece de la figura del emisor, tal y como se define en el Reglamento.

4. **Cuando la oferta pública de criptoactivos o su admisión a negociación se refiera a fichas de consumo, información sobre la calidad y cantidad de bienes o servicios a los que dan acceso las fichas de consumo.**

   No procede.

5. **Cuando la oferta pública de criptoactivos o su admisión a negociación se refiera a fichas de consumo, información sobre la forma en que pueden canjearse las fichas de consumo por los bienes o servicios a los que correspondan.**

   No procede.

6. **Cuando no se solicite la admisión a negociación, información sobre cómo y dónde podrán adquirirse o venderse los criptoactivos después de la oferta pública.**

   Las unidades del criptoactivo podrán adquirirse o venderse libremente, sin más restricciones que las derivadas de la aplicación de la normativa en vigor.

7. **Restricciones aplicables a la transferibilidad de los criptoactivos ofertados o admitidos a negociación.**

   Las restricciones a la transferibilidad son las derivadas de su código informático, en síntesis, la principal restricción es no incurrir en doble gasto.

8. **Cuando se disponga de protocolos para criptoactivos en lo relacionado con el aumento o la disminución de su oferta en respuesta a cambios en la demanda, una descripción del funcionamiento de dichos protocolos.**

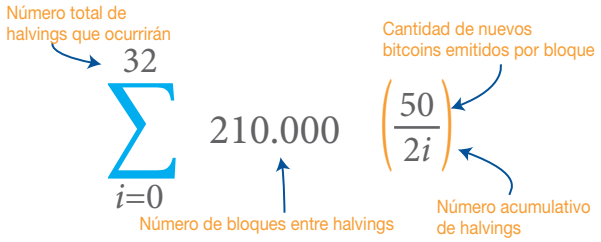
   No existe un mecanismo para variar la oferta en respuesta a cambios en la demanda. La generación de nuevas unidades de bitcoins está definida en el código informático de la red. Cada bloque de transacciones generado incluye una transacción que remunera al nodo que ha minado o generado el bloque. Cada 210.000 bloques generados, el número de unidades nuevas de bitcoin se divide a la mitad en un proceso conocido como "*halving*"[38], de forma que no pueden existir más de 21 millones de unidades, en concreto, la cantidad máxima de unidades será la de 2.099.999.997.690.000 de satoshis (la cienmillonésima parte de un bitcoin).

Los cálculos correspondientes se efectúan conforme a la siguiente fórmula[39] mostrada en la Figura 1 junto con una breve anotación del significado de cada término:

[38] Jameson Lopp, "How is the 21 Million Bitcoin Cap Defined and Enforced?" Blog de Jameson Lopp, https://blog.lopp.net/how-is-the-21-million-bitcoin-cap-defined-and-enforced/, 19 de octubre de 2023.

[39] -Jameson Lopp, "¿Cómo podrán existir 21 millones de Bitcoins? Jameson Lopp lo explica," CriptoNoticias,. https://www.criptonoticias.com/tecnologia/como-podran-existir-21-millones-bitcoins-jameson-lopp-explica/, 19 de octubre de 2023.

FIGURA 1. EXPRESIÓN MATEMÁTICA QUE DESCRIBE EL LÍMITE HACIA EL QUE TIENDE LA CANTIDAD TOTAL DE BITCOIN



Fuente: Imagen tomada de Jameson Lopp, "How is the 21 Million Bitcoin Cap Defined and Enforced?" Blog de Jameson Lopp, https://blog.lopp.net/how-is-the-21-million-bitcoin-cap-defined-and-enforced/

Aunque la fórmula anterior define al "*halving*" número 32 como el final de la emisión de bitcoins, según el código fuente de bitcoin no es exactamente así. El *halving* número 32 define que a partir de ese momento, la emisión de bitcoins será tan pequeña que sobrepasará el límite de 8 decimales, lo que implica que no podrá ser expresado dentro de la contabilidad de Bitcoin con los parámetros actuales.

A pesar de ello, los *halvings* continuarán hasta llegar al número 63, según muestra el propio código fuente, sobre la línea 1072.

9. **Cuando proceda, descripción de los sistemas de protección que protejan el valor de los criptoactivos y de los sistemas de indemnización.**

   No procede.

10. **Derecho aplicable a los criptoactivos, así como órgano jurisdiccional competente.**

    Al ser Bitcoin, en síntesis, un *software* libre, de código abierto, disponible para cualquier persona en cualquier parte del mundo, no se puede decir que haya un derecho nacional concreto aplicable al criptoactivo que genera la utilización del *software* aludido. De igual manera, no hay un "órgano jurisdiccional competente" específico. Si surge un conflicto a resolver en sede judicial, habrá que estar a las normas procesales de la sede del órgano jurisdiccional que conozca el asunto y los materiales que éste considere aplicables.

Parte H: Información sobre la tecnología subyacente

1. **Información sobre la tecnología utilizada, incluida la tecnología de registro distribuido, los protocolos y las normas técnicas utilizadas.**

   Bitcoin hace uso de numerosas tecnologías anteriores, tal y como se describe en el *White Paper* original[40]. En este artículo enlazado[41] se puede acceder a un compendio de las diferentes tecnologías que usa Bitcoin.

2. **Cuando proceda, mecanismo de consenso.**

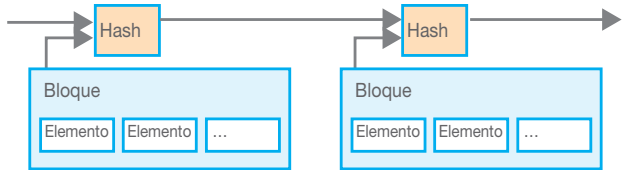
   El mecanismo de consenso está explicado en los puntos 3 y 4 del *White Paper* original de Bitcoin y, en síntesis, consiste en la creación de un servidor de marcas o sellos de tiempo utilizando el mecanismo de Prueba de Trabajo. Una representación de un servidor de marcas o sellos de tiempo se muestra en la Figura 2, de la forma en que fue presentado por Nakamoto. La función de la Prueba de Trabajo consiste en ordenar temporalmente las transacciones ocurridas en la red. La participación de los denominados mineros es de vital importancia para lograr este objetivo. Los mineros compiten entre sí con el fin de proponer el estado más actualizado del libro de transacciones o registro distribuido. La competencia se basa en encontrar un identificador (hash del bloque) para el bloque consecutivo del libro. El minero que logre realizar la tarea (o el trabajo) de encontrar el identificador antes que los demás mineros, se atribuye la capacidad de indicarle a los nodos el bloque que deberán agregar en su libro o registro. Es así como la red de nodos llega a un consenso sin la presencia de intermediarios ni terceros de confianza. Si por la red se propagan transacciones que representen un doble gasto, los mineros solamente escogerán una a la hora de crear su bloque, así que, eventualmente, solamente una de estas transacciones será agregada al libro de registro. Por el trabajo realizado para encontrar el identificador del bloque, los mineros son recompensados con nuevas unidades del criptoactivo.

[40] Satoshi Nakamoto, "Bitcoin: Un sistema de efectivo electrónico peer-to-peer," bitcoin.org, https://bitcoin.org/bitcoin.pdf

[41] Rishi Sidhu, "Exploring Bitcoin's History," Medium, https://medium.com/coinmonks/exploring-bitcoins-history-ecbf1c59952c, 19 de octubre de 2023.

Desde una perspectiva un poco más técnica, la Prueba de trabajo opera de la siguiente forma: un servidor de marcas de tiempo funciona al realizar el hash de un bloque de datos a ser fechados y publicándolo ampliamente, tal y como se haría en un periódico o en una publicación de Usenet. La marca de tiempo prueba que el dato, obviamente, debió de haber existido en ese momento para poder incluirse dentro del *hash*. Cada marca de tiempo incluye en su *hash* la marca de tiempo previa, formando una cadena, de modo que cada marca de tiempo adicional refuerza las anteriores.

FIGURA 2. ILUSTRACIÓN DE UN SERVIDOR DE MARCAS O SELLOS DE TIEMPO



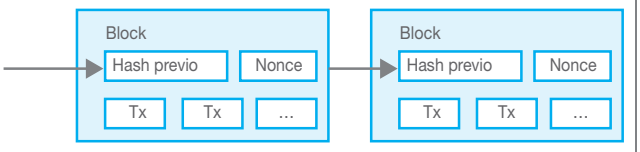
Fuente: Satoshi Nakamoto, "Bitcoin: Un sistema de efectivo electrónico peer-to-peer," bitcoin.org https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf

Para implementar un servicio distribuido de marcas de tiempo en un entorno de relaciones entre pares (*peer-to-peer*), se necesita utilizar un sistema de prueba de trabajo similar al Hashcash de Adam Back[42], en vez de usar una publicación en un periódico o en Usenet.

La prueba de trabajo consiste en buscar un valor de un campo denominado "nonce" ("*number used once*") que, al ser sometido, junto con los otros campos que integran el bloque, al cálculo de un *hash*, como con SHA-256, el resultado del hash comience con un cierto número de bits con valor cero. El trabajo promedio requerido es exponencial en la cantidad de bits de valor cero necesarios y puede ser verificado ejecutando un único hash. El *White Paper* original de Bitcoin representa esta idea por medio de la Figura 3.

Una vez que se ha invertido el esfuerzo de computación necesario para que cumpla con la prueba de trabajo, el bloque no puede ser modificado sin volver a realizar el trabajo. A medida que se encadenan bloques posteriores a este, el trabajo necesario para cambiar el bloque incluiría volver a hacer todos los bloques posteriores a él.

FIGURA 3. ILUSTRACIÓN DE LA FORMA EN LA QUE SE UTILIZA EL SERVIDOR DE MARCAS DE TIEMPO EN LA PRUEBA DE TRABAJO DE BITCOIN



Fuente: Satoshi Nakamoto, "Bitcoin: Un sistema de efectivo electrónico peer-to-peer," bitcoin.org https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf

La prueba de trabajo también resuelve el problema de determinar la representación en el proceso de decisión por mayoría. Si esta mayoría se basara en un voto por dirección IP, podría ser alterada por alguien capaz de asignar muchas direcciones IP. La prueba de trabajo equivale esencialmente a "una-CPU-un-voto"[43]. La decisión de la mayoría es representada por la cadena más larga, la cual posee la prueba de trabajo con mayor esfuerzo invertido.

Si la mayoría del poder de computación está controlada por nodos honestos, la cadena honesta crecerá más rápido y dejará atrás a cualquier otra cadena que esté compitiendo. Para modificar un bloque en el pasado, un atacante tendría que rehacer la prueba de trabajo del bloque y de todos los bloques posteriores, y luego alcanzar y superar el trabajo de los nodos honestos. La probabilidad de que un atacante más lento pueda alcanzar a la cadena con mayor cantidad de trabajo que cotidianamente se refiere como la "más larga", disminuye exponencialmente a medida que más bloques subsecuentes se van incorporando.

Para compensar el crecimiento de la velocidad de funcionamiento del hardware y la eventual variabilidad en el tiempo del interés por ejecutar

[42] Adam Back, "Hashcash: A Denial of Service Counter-Measure" (Cambridge, Reino Unido: Adam Back, 2002), http://www.hashcash.org/papers/hashcash.pdf, 19 de octubre de 2023.

[43] Hoy en día, la cantidad de poder computacional necesaria para la prueba de trabajo es enorme, por lo tanto, desde un punto de vista práctico es imposible realizarla con ordenadores personales clásicos.

nodos, la dificultad de la prueba de trabajo es determinada por una media móvil con el objetivo de conseguir un determinado promedio de nº de bloques por hora. Si estos se generan demasiado rápido, la dificultad se incrementa.

3. **Mecanismos de incentivo para asegurar las operaciones y comisiones aplicables, en su caso.**

   El mecanismo de incentivo está explicado en el punto 6 del *White Paper* original.

   Por convención, la primera transacción en el bloque es una transacción especial que genera nuevas unidades del criptoactivo, cuyo dueño es el creador del bloque. Esto agrega un incentivo para que los nodos apoyen a la red, y provee una forma inicial de distribuir y poner en circulación las unidades del criptoactivo, dado que no hay una autoridad para crearlas. Esta adición estable de una cantidad constante de nuevas unidades es análoga a los mineros de oro que gastan recursos para ponerlo en circulación. En nuestro caso, los recursos son el tiempo de procesamiento informático[44] y el consumo de electricidad.

   El incentivo también puede establecerse con los costes de transacción. Si el valor de salida de una transacción es menor que la entrada, la diferencia será una tarifa de transacción que se añadirá al valor del incentivo del bloque que la contiene. Una vez que un número predeterminado de unidades han entrado en circulación, el incentivo puede evolucionar enteramente a tarifas de transacción y estar completamente libres de inflación.

   El incentivo también puede ayudar a animar a los nodos a mantenerse honestos. Si un atacante egoísta es capaz de reunir más poder computacional que todos los nodos honestos, éste tendría que elegir entre utilizarlo para defraudar a la gente robando sus pagos, o usarlo para generar nuevas unidades. Debería encontrar más rentable jugar siguiendo las reglas, ya que éstas lo favorecerán con más unidades nuevas que a todos los demás nodos, en lugar de socavar el sistema y la validez de su propia riqueza.

4. **Cuando los criptoactivos se emitan, transfieran y almacenen utilizando tecnología de registro distribuido gestionada por el emisor, el oferente o por un tercero que actúe por cuenta de ellos, descripción detallada del funcionamiento de dicha tecnología de registro distribuido**:

   Si hay una persona, ya sea emisor, oferente o tercero que gestione la tecnología de registro distribuido, entonces no nos encontramos ante una tecnología de registro distribuido, sino ante una tecnología de registro, en mayor o menor medida, centralizado. Bitcoin utiliza una tecnología de registro distribuido realmente, por lo que no hay ninguna persona, ni emisor, ni oferente o tercero que la gestione.

5. **Información sobre el resultado de la auditoría de la tecnología utilizada, en caso de haberse llevado a cabo tal auditoría.**

   No procede.

Parte I: Información sobre los riesgos

1. **Descripción de los riesgos asociados a la oferta pública de criptoactivos o su admisión a negociación.**

   No hay riesgos específicos relacionados con la oferta pública y/o admisión a negociación de bitcoin diferentes a los de cualquier otro criptoactivo y que se reseñan a continuación.

2. **Descripción de los riesgos asociados al emisor, si difiere del oferente o la persona que solicite la admisión a negociación.**

   Como se ha indicado en el punto III del presente documento "Resumen para el cumplimiento del art. 6.7", en el caso de Bitcoin no existe emisor, ni conocido ni desconocido, en el sentido que se indica en el Reglamento. Desde que el software se encontró disponible y la red comenzó a funcionar, la emisión o creación de nuevas unidades del criptoactivo se lleva a cabo automáticamente como recompensa por la validación de operaciones en el contexto del mecanismo de consenso utilizado. En consecuencia, al no haber emisor, no puede hablarse de la existencia de riesgos asociados a dicha figura.

[44] El *Whiter Paper* original habla de "CPU time".

3. **Descripción de los riesgos asociados a los criptoactivos.**

   Es preciso tener en cuenta que las operaciones con criptoactivos presentan una serie de riesgos de los que se debe ser consciente, mencionados, entre otros documentos, en la **Circular 1/2022, de 10 de enero, de la Comisión Nacional del Mercado de Valores de España**[45], relativa a la publicidad sobre criptoactivos presentados como objeto de inversión, tales como los que se indican aquí[46].

   [Si se hace uso de este documento en jurisdicciones distintas a la española, sería conveniente adaptar este apartado al territorio a considerar]

   Producto de inversión de alto riesgo

   1. El valor de las inversiones y el rendimiento obtenido de las mismas puede experimentar significativas variaciones al alza y a la baja, pudiendo perderse la totalidad del importe invertido.
   2. Las inversiones en proyectos en etapas tempranas suponen un alto nivel de riesgo, por lo que resulta necesario entender adecuadamente su modelo de negocio.
   3. Los criptoactivos no están cubiertos por mecanismos de protección al cliente como el Fondo de Garantía de Depósitos o el Fondo de Garantía de Inversores.
   4. Los precios de los criptoactivos se constituyen en ausencia de mecanismos que aseguren su correcta formación, como los presentes en los mercados regulados de valores.
   5. Muchos criptoactivos pueden verse carentes de la liquidez necesaria para poder deshacer una inversión sin sufrir pérdidas significativas, dado que su circulación entre inversores, tanto minoristas como profesionales, puede ser muy limitada.

   Puede consultar igualmente el comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión en la URL: https://www.cnmv.es/Portal/verDoc.axd?t=%7Be14ce903-5161-4316-a480-eb1916b85084%7D

   Así como el Comunicado conjunto del Banco de España, la CNMV y la DG de Seguros sobre la advertencia de los reguladores financieros europeos en relación con los riesgos de los criptoactivos en la URL: https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/22/presbe2022_19.pdf

4. **Descripción de los riesgos asociados a la ejecución del proyecto. Riesgos legales.**
   1. La aceptación de los criptoactivos como medio de cambio es aún muy limitada y no existe obligación legal de aceptarlos.
   2. Cuando el proveedor de servicios no se encuentra localizado en un país de la Unión Europea la resolución de cualquier conflicto podría resultar costosa y quedar fuera del ámbito de competencia de las autoridades españolas o europeas.
   3. Cuando el inversor no disponga de los criptoactivos, estando en monederos digitales (*wallets*) del proveedor de servicios, y sin acceso a las claves privadas de los mismos, usted debe ser consciente de esa circunstancia y de los riesgos que conlleva, debiendo cerciorarse de los derechos que le confiere el prestador de los servicios.
5. **Descripción de los riesgos asociados a la tecnología utilizada, así como de las medidas de atenuación, en su caso.**
   1. Las tecnologías de registros distribuidos se encuentran todavía en un estadio temprano de maduración, habiendo sido muchas de estas redes creadas recientemente, por lo que, pueden no estar suficientemente probadas y existir fallos significativos en su funcionamiento y seguridad.
   2. El registro de las transacciones en las redes basadas en tecnologías de registros distribuidos funciona a través de protocolos de consenso que pueden ser susceptibles a ataques que intenten modificar dicho registro y, en caso de tener éxito estos ataques, no existiría un registro alternativo que respalde dichas

[45] Boletín Oficial del Estado, número 14, 17 de enero de 2022, páginas 4106-4116, https://www.boe.es/eli/es/cir/2022/01/10/1, 19 de octubre de 2023.

[46] Texto a continuación, hasta el punto 5, extraído de la normativa de la CNMV

transacciones ni por tanto a los saldos correspondientes a las claves públicas, pudiéndose perder la totalidad de los criptoactivos.

3. Las facilidades de anonimato que pueden aportar los criptoactivos los convierten en un objetivo para los ciberdelincuentes, ya que en el caso de robar credenciales o claves privadas pueden transferir los criptoactivos a direcciones que dificulten o impidan su recuperación.
4. La custodia de los criptoactivos supone una responsabilidad muy relevante ya que pueden perderse en su totalidad en el caso de robo o pérdida de las claves privadas.

6. Información sobre los principales efectos adversos sobre el clima y otros efectos adversos relacionados con el medio ambiente del mecanismo de consenso utilizado para emitir el criptoactivo.

El art. 6.1.j) del Reglamento indica que el Libro Blanco deberá contener información sobre los principales efectos adversos sobre el clima y otros efectos adversos relacionados con el medio ambiente del mecanismo de consenso utilizado para emitir el criptoactivo.[47] Sin embargo, en el anexo I[48] no se menciona nada al respecto, por lo que, para cumplir con las previsiones del art. 6.1.j) se hace necesario una breve referencia a la cuestión del clima y otros efectos adversos relacionados con el medio ambiente.

Toda actividad humana involucra efectos sobre el medio ambiente. Bitcoin, sin embargo, posee la particularidad de que una gran variedad de esos efectos son positivos. El principal de estos efectos positivos sobre el clima y el medio ambiente es el efecto descarbonizador del minado de Bitcoin, mediante dos mecanismos: la promoción de la penetración de las energías renovables a través de esquemas de consumo energético flexible, y la conversión de gas metano a dióxido de carbono a través de la mitigación de la ventilación de gas y del quemado en antorcha.

Entre eventuales efectos negativos de Bitcoin sobre el medio ambiente se cuentan simplemente aquellos comunes a todos los centros de cómputos y a la gran mayoría de las industrias: un efecto muy localizado de contaminación sonora generado por los grandes centros de cómputos ("granjas") en donde se está realizando la parte fundamental del consenso, i.e. el minado. Asimismo, si eventualmente se produce algún periodo en que el precio del bitcoin suba exponencialmente y la tecnología de minado ("ASICs") mejore rápidamente, podría producirse un estadio temporal con cierto grado de producción de residuos electrónicos. Ello sería, empero, temporal. En todo caso, estos impactos negativos son comunes a muchas industrias, e.g. los centros de cómputos en general, y pueden ser abordados desde la perspectiva de la regulación general.

Al discutirse el impacto de Bitcoin en el medio ambiente, sin embargo, el principal objeto de discusión es el impacto climático, dado por el consumo de energía y la emisión de gases de efecto invernadero. Este impacto es con frecuencia un impacto positivo para el medio ambiente, debido a que el minado de Bitcoin puede contribuir a la rentabilidad –y, por ende, a la penetración– de las fuentes renovables en las redes energéticas y a la neutralización de emisiones de gas metano de otras industrias. Esto implica un potencial para que el minado de Bitcoin sea carbono-negativo.

Esta sección desarrolla estos factores, cubriendo cuatro aristas:

1. La magnitud de las emisiones de alcance 2 de la red Bitcoin.[49]
2. La complementariedad de Bitcoin con las energías renovables variables.

[47] Nótese que el mecanismo de consenso no se utiliza "para emitir" el criptoactivo, sino para, justamente, alcanzar el consenso. En un criptoactivo, la emisión o acuñado puede darse durante el proceso que deriva en el consenso, o no darse. En el caso de Bitcoin, la gran mayoría de las unidades del criptoactivo (más de 19 millones sobre un total de 21) ya han sido emitidas, y las restantes se emitirán durante los restantes 120 años aproximadamente. Sin embargo, el mecanismo de consenso continuará operando más allá de este límite temporal al margen de que haya o no emisión. Sin embargo, sí es cierto que el "subsidio" de bloque que lleva a la emisión de bitcoin puede estimular un mayor minado que el que habría en su ausencia.

[48] Donde, supuestamente, se recogen con mayor detalle los "elementos de información para el libro blanco de criptoactivos relativo a criptoactivos distintos de fichas referenciadas a activos o fichas de dinero electrónico". Anexo I: Página 150 del "Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos", https://eur-lex.europa.eu/eli/reg/2023/1114/oj

[49] Las emisiones de alcance 1 son aquellas producidas directamente por la maquinaria de la empresa, las emisiones de alcance 2 son aquellas producidas en la generación de la energía consumida por la empresa, y las emisiones de alcance 3 son aquellas producidas por los clientes y proveedores de una empresa. Recientemente, se ha propuesto el término de emisiones de alcance 4 para las emisiones "negativas" o "evitadas" (Dan Roarty, David Wheeler, "Huellas de carbono positivas: un marco climático favorable para inversores en renta variable", AllianceBernstein, https://www.alliancebernstein.com/library/huellas-de-carbono-positivas-un-marco-climatico-favorable-para-inversores-en-renta-variable.htm, 19 de octubre de 2023). Bitcoin no tiene emisiones significativas de alcance 1 ni 3.

3. La utilidad de Bitcoin para la neutralización de las emisiones de metano.
4. Los esquemas emergentes en el ecosistema Bitcoin para la decarbonización.

El consumo energético y la huella de carbono de Bitcoin son temas ampliamente debatidos y estimados de manera variada. La magnitud del consumo energético fluctúa entre estimaciones de 72 y 185 mil millones de kilovatios-hora por año, según la Oficina de Políticas de Ciencia y Tecnología de la Casa Blanca[50]. Estas variaciones se deben a la dificultad de determinar el *hardware* exacto utilizado en la minería de Bitcoin y la intensidad de carbono de las fuentes de energía utilizadas. Para abordar esta incertidumbre, se han propuesto dos enfoques principales: el enfoque "de arriba hacia abajo", que estima la proporción de los ingresos de los mineros gastados en electricidad, y el enfoque "de abajo hacia arriba", que estima el consumo de energía en función de la tasa de hash. En general, se prefiere este último enfoque debido a su mayor precisión.

En relación con la intensidad de carbono, existen métodos para calcularla basándose en la mezcla de la red según las direcciones IP de los grupos de minería, o utilizando datos proporcionados por los propios mineros. Sin embargo, ambos enfoques presentan limitaciones en términos de disponibilidad y confiabilidad de los datos. La utilización de direcciones IP para la atribución de la intensidad de carbono propia de la región puede exagerar las emisiones provenientes del minado, dado que ignora la baja intensidad de carbono del minado realizado detrás del medidor (un gran y creciente porcentaje del total) así como ubica a los mineros lejos de la fuente de energía (frecuentemente baja en carbono) y cerca del "*pool*" de minado (probablemente más alta en carbono). Por otra parte, tomar la intensidad de carbono de los mineros directamente implica las vulnerabilidades del auto-reportaje de datos, así como potenciales inconsistencias con el sistema de certificados de atributos energéticos. Por esta razón, para describir las emisiones de alcance 2 de la red Bitcoin se utiliza un rango de posibilidades. Empero, todo ello excluye las emisiones de alcance 4 de la red, que son negativas (véase más adelante).

El impacto ambiental de Bitcoin se ha comparado con países e industrias para tener una idea de su escala de consumo de energía. Los críticos suelen preferir la comparación con países, ya que esto destaca la magnitud del consumo de energía de Bitcoin. Sin embargo, probablemente sea más apropiada la comparación con industrias específicas, argumentando que muchas de estas industrias superan el consumo de energía de países enteros sin que se considere un problema. En este sentido, el minado de Bitcoin consume mucha menos energía que las industrias del oro, el cobre o el zinc.[51]

Otro aspecto para tener en cuenta es la elección de denominadores para representar la participación de Bitcoin en una magnitud global. Algunos proponen utilizar el consumo global de electricidad como denominador. Sin embargo, es más apropiado acudir al consumo global de energía, no electricidad, para tener en cuenta las eficiencias de conversión entre diferentes fuentes de energía, dado que Bitcoin utiliza una mezcla energética diferente al promedio de la red. Más adecuado aún es la propuesta de utilizar denominadores basados en las emisiones globales de CO_2 y gases de efecto invernadero (GEI), ya que el cambio climático está relacionado principalmente con las emisiones de gases de efecto invernadero y no tanto con el consumo de energía en sí. Debe tenerse siempre en cuenta que Bitcoin consume un determinado porcentaje de la electricidad global, pero que este porcentaje será menor para la energía global, y que será todavía menor para las emisiones globales de gases de efecto invernadero. Esto es porque Bitcoin es más eficiente en su consumo de energía que la industria promedio, y porque el consumo de energías bajas en carbono es proporcionalmente mayor que el de la industria promedio.

Por último, el impacto del consumo energético de la red Bitcoin sobre las emisiones de GEI depende del paradigma de contabilidad de carbono adoptado. Existen dos grandes formas de contabilidad de carbono: contabilidad atribucional y contabilidad marginal. La primera involucra atribuir la totalidad emisiones de una red a la totalidad de los consumidores de energía de esa red, asignando a cada uno una porción del total según un criterio, que puede ser un criterio igualitario

[50] OSTP, "Climate and energy implications of crypto-assets in the United States". Tech. rep. Washington, D.C.: White House Office of Science and Technology Policy (Sept. 2022). https://www.whitehouse.gov/ostp/news-updates/2022/09/08/fact-sheet-climate-and-energy-implications-of-crypto-assets-in-the-united-states/, 19 de octubre de 2023.

[51] Nic Carter, Ross Stevens. "Bitcoin Net Zero. Tech". rep. NYDIG (2021). https://nydig.com/bitcoin-net-zero, 19 de octubre de 2023.

u otro (como el porcentaje de certificados de atributos energéticos adquiridos). La segunda asigna la diferencia entre las emisiones posteriores y anteriores de una demanda adicional de energía a esa demanda adicional de energía. La primera tiene la ventaja de ser consistencia en el largo plazo y de que cumple el principio de que el todo debe ser igual a la suma de las partes. La segunda permite observar el efecto "antes y después" de la introducción del minado de Bitcoin, pero no cumple este principio e introduce implícitamente una serie de juicios de valor insostenibles de ser aplicada en el largo plazo. Entre ellos, esta segunda forma de contabilidad asigna a los consumidores más antiguos de energía mayor legitimidad que los consumidores más nuevos. Generalmente, los artículos críticos del consumo de energía de Bitcoin asumen, sin admitirlo explícitamente, una perspectiva marginalista, razón por la cual debe mantenerse cierto escepticismo ante artículos sensacionalistas críticos del mismo.[52]

En resumen, el impacto ambiental de Bitcoin, en términos de consumo de energía y huella de carbono de alcance 2, es un tema complejo y debatido, debiéndose evitar las afirmaciones simplistas y prohibicionistas. Existen diferentes metodologías y perspectivas para evaluar este impacto, lo que puede llevar a conclusiones divergentes. Sin embargo, es claro que la minería de Bitcoin presenta características únicas que la diferencian como comprador de energía y ofrece oportunidades de negocio en la convergencia de las industrias de energía y criptoactivos. Así, es más plausible, como se indicó antes, que el impacto de Bitcoin sea positivo para el medio ambiente, a que sea negativo, gracias a la creciente eficiencia de la actividad minera y el uso de fuentes de energía renovable.

Más allá del consumo de energía absoluto de Bitcoin, su impacto climático depende de dos factores: la cantidad de electricidad generada a partir de fuentes intensivas en carbono que consume, y la cantidad de fuentes intensivas en carbono que lleva a reemplazar con fuentes bajas en carbono. Este último factor es un producto de la especial complementariedad de Bitcoin con las energías renovables variables.

Las energías renovables variables presentan algunos problemas fundamentales. Concretamente, se encuentran problemas de intermitencia en la generación de energía y de imposibilidad de adaptar la oferta de energía a la demanda de energía. En este contexto, se añade la insuficiencia de las opciones de almacenamiento de energía. Si bien el almacenamiento puede mitigar la intermitencia y los desequilibrios en la generación, las tecnologías existentes aún presentan limitaciones en términos de capacidad, costo y eficiencia.

Además, la expansión de la capacidad de generación de energía renovable también enfrenta obstáculos debido a su costo asociado. Aunque los precios de las tecnologías renovables han disminuido en los últimos años, el proceso de expansión a gran escala aún puede resultar costoso y requerir inversiones significativas. Adicionalmente, a medida en que aumenta la contribución de las energías renovables variables a la red energética, mayores son la cantidad y duración de eventos de precios negativos, reduciendo mayormente su rentabilidad. A ello se agrega la volatilidad de los precios, tanto en la generación de energía como en los mercados energéticos. La variabilidad en los precios puede afectar la rentabilidad de los proyectos renovables y dificultar la planificación a largo plazo.

Para abordar estos desafíos, se requiere una mayor resiliencia de la red eléctrica, así como soluciones técnicas y regulatorias para optimizar la transmisión y evitar la congestión en los nodos de conexión. Además, se deben explorar opciones de almacenamiento de energía más eficientes y rentables, así como expansiones de capacidad que puedan adaptarse a las fluctuaciones en la generación de energía renovable. Es fundamental superar estos desafíos para lograr una transición exitosa hacia un sistema energético más sostenible y confiable.

En este contexto, la minería de Bitcoin presenta características únicas que la diferencian como comprador de energía y que pueden coadyuvar a superar los desafíos indicados. Los mineros de Bitcoin tienen flexibilidad de carga, lo que les permite activarse o desactivarse rápidamente y con costos mínimos. También son interrumpibles, lo que significa que pueden cambiar su salida inmediatamente sin perder el trabajo realizado. Además, la minería de Bitcoin es portátil y móvil, ya que no requiere inversiones significativas en activos fijos y el equipo es fácilmente transportable.

[52] Juan Ignacio Ibañez, Alexander Freier, "Don't Trust, Verify: Towards a Framework for the Greening of Bitcoin" (May 2, 2023). https://ssrn.com/abstract=4436607 or http://dx.doi.org/10.2139/ssrn.4436607

Esta movilidad les permite adaptarse a diferentes condiciones geográficas y climáticas.

La sensibilidad al precio es otra característica destacada de la minería de Bitcoin. Los mineros son altamente reactivos a los cambios en los precios de la energía debido a sus bajos costos operativos y la alta proporción de sus ingresos dedicados a la electricidad. Además, la industria minera de Bitcoin es escalable y puede adaptarse a diferentes escalas de operación, desde pequeñas operaciones en el hogar hasta grandes instalaciones industriales. La granularidad en el consumo de energía también es una ventaja, ya que los mineros pueden ajustar con precisión sus niveles de consumo, lo que les permite ser participantes flexibles en el mercado energético.

Es importante destacar que la minería de Bitcoin no compite directamente con otros consumidores de energía, ya que puede aprovechar energía ya generada y utilizar emisiones que de todos modos se habrían producido. Esto implica que el consumo de energía de la minería no necesariamente aumenta la generación de energía o las emisiones, lo que puede ser beneficioso desde el punto de vista ambiental.

En términos de modelos de negocio, la minería de Bitcoin ofrece diversas oportunidades en la intersección de las industrias de energía y criptoactivos. Algunos modelos incluyen la minería como demanda primaria, y otros la de último recurso. En ambos casos, los mineros pueden pagar más por la energía que lo que obtendrían los generadores de venderla a la red, lo que aumenta rentabilidad de la instalación de nuevas plantas de energía, y por ende las fomenta. Además, la disponibilidad de los mineros de Bitcoin, su capacidad para proporcionar una carga estable a largo plazo y su adaptabilidad a diferentes escalas hacen que sean atractivos para los vendedores de energía.

Por todas las facilidades antedichas, está creciendo el minado de Bitcoin con energías renovables, y específicamente con energías renovables variables. A medida en que aumenta la penetración renovable en las redes energéticas, los problemas de financiamiento, desbalances oferta-demanda y congestión de nodos, empeoran, implicando que existe una tendencia a una utilidad cada vez mayor del minado de Bitcoin en estos contextos. En paralelo, a medida en que el Bitcoin gana más adopción, se estabiliza su precio y se "comodifica" y abarata la producción de infraestructura de minado. Esto resulta en menores márgenes de ganancia para los mineros, lo cual aumenta su necesidad de contar con fuentes de energía baratas, exacerbando así la complementariedad entre el minado y las energías renovables variables con instancias de precios negativos. Por añadidura, todo esto toma aún mayor color con los episodios de "halvings" antedichos, que reducen las ganancias de los mineros y acentúan aún más esta complementariedad.[53]

Dado que el minado de Bitcoin aumenta la rentabilidad de la generación renovable, particularmente de la generación renovable variable como la energía solar y la energía eólica, estimula su penetración. A mayor rentabilidad de una actividad, más emprendimiento de dicha actividad. Una mayor generación de energía renovable implica una mayor generación de energía absoluta, lo cual abarata los costos de la energía para el consumidor. El abaratamiento de los costos de la energía implica una reducción de los márgenes de ganancia para los generadores de energía en general. Por ende, a medida que se mine más Bitcoin, es probable que haya una mayor penetración de energías renovables, y que simultáneamente esto *expulse* a generadores no renovables fuera del mercado por su menor rentabilidad. Así, el minado de Bitcoin puede tener un efecto descarbonizador a pesar de tener un alto consumo energético, porque por su efecto se reemplazan fuentes de energía no renovables con fuentes de energía renovables. Esto ya está ocurriendo en la actualidad, existiendo regiones en la que el minado de Bitcoin está reduciendo los precios para los consumidores finales de energía, así como bajando las emisiones totales de la red.[54]

El minado de Bitcoin ofrece una segunda vía de descarbonización: el minado con gas metano. La ventilación y el quemado de antorcha de gas metano implican una gran contribución al cambio climático, puesto que el gas metano tiene un forzamiento radiativo mucho mayor al dióxido de carbono. Los vertederos de basura son una fuente de gas metano, y también lo son los

[53] Juan Ignacio Ibañez, Alexander Freier, "Bitcoin's Carbon Footprint Revisited: Proof of Work Mining for Renewable Energy Expansion", (8 Agosto, 2023). Challenges, 14(3), 35 Disponible en: https://doi.org/10.3390/challe14030035/3/35

[54] Xinyi Luo, "Bitcoin Miners Offered Way to Cut Texas Electricity Usage to Help the Grid," Coindesk, 6 de diciembre 2022, https://www.coindesk.com/business/2022/12/06/texas-bitcoin-miners-are-offered-to-cut-electricity-usage-to-help-the-grid/, 19 de octubre 2023.

sitios de extracción de petróleo. En ambos casos, se libera metano a la atmósfera directamente (ventilación) o indirectamente (el metano es quemado en antorcha, pero la combustión es de baja eficiencia y una gran cantidad de metano es igualmente liberada).

Siendo el minado de Bitcoin una industria "hambrienta" de energía, que busca energía de precio cero o precio negativo (muchas empresas están dispuestas a pagar para que alguien consuma el gas metano en cuestión para reducir su impacto ambiental y los créditos de carbono o descrédito público que deben afrontar) y que es altamente agnóstico en lo geográfico, los mineros de Bitcoin pueden consumir este gas metano. Los esquemas de minado modular de Bitcoin utilizan modos de combustión de altísima eficiencia, en grado mucho mayor al quemado en antorcha, asegurando que casi la totalidad de las emisiones de gas metano es utilizada y reconvertida en emisiones de dióxido de carbono, de mucho menor forzamiento radiativo. Así, el minado de Bitcoin reemplaza emisiones de mayor potencial de calentamiento global por emisiones de menor potencial de calentamiento global, o mayores emisiones carbono-equivalentes por menores emisiones carbono-equivalentes. Esto es, otro efecto descarbonizador del minado de Bitcoin. Existe un creciente cuerpo de literatura apoyando estas afirmaciones.[55]

Finalmente, debe notarse que la industria del Bitcoin es una industria excepcionalmente consciente de su consumo energético, y excepcionalmente innovadora en el desarrollo de esquemas de mitigación de impacto ambiental, muy por encima de las demás industrias. En este contexto, los diversos actores de la industria del Bitcoin han desarrollado múltiples iniciativas para favorecer y estimular el minado "verde" aún más allá de las ya fuertes tendencias de la industria hacia el uso de energías renovables. Empresas y emprendedores en la industria del Bitcoin son sensibles a las demandas de la sociedad por una mayor descarbonización, por lo cual se han elaborado certificados de Bitcoin verde y esquemas de co-inversión de Bitcoin con minado renovable que aseguran un efecto carbono-negativo de la inversión en Bitcoin, garantizando un efecto medioambiental positivo.[56]

En resumen, las críticas al consumo energético de Bitcoin tienden a provenir de malentendidos de su impacto ambiental. La minería de Bitcoin puede desempeñar un papel importante en la transición global hacia la energía renovable y contribuir a la descarbonización de la energía. Su flexibilidad de carga, capacidad de adaptación, y la creciente tendencia hacia el uso de energías renovables para el minado de Bitcoin son factores clave en este proceso. A medida que la sociedad continúa exigiendo una mayor conciencia ambiental, es probable que veamos aún más innovación y por parte de la industria del Bitcoin para no solamente minimizar su huella de carbono, sino descarbonizar a otras industrias[57].

[55] J. Vázquez, DL. Crumbley. “Flared Gas puede reducir algunos riesgos en la criptominería, así como en las operaciones de petróleo y gas.” Riesgos 2022, 10, 127. https://doi.org/10.3390/risks10060127

[56] Juan Ignacio Ibañez, Alexander Freier, “Don’t Trust, Verify: Towards a Framework for the Greening of Bitcoin” (May 2, 2023). https://ssrn.com/abstract=4436607 or http://dx.doi.org/10.2139/ssrn.4436607

[57] En sentido análogo se pronuncia el informe de KPMG titulado “Bitcoin’s role in the ESG imperative”, elaborado por Brian Consolvo y Kirk Caron, "Bitcoin's role in the ESG imperative," KPMG, https://advisory.kpmg.us/articles/2023/bitcoin-role-esg-imperative.html, 19 de octubre 2023.

REFERENCIAS BIBLIOGRÁFICAS

Back, A. (2002). *Hashcash: A Denial of Service Counter-Measure*. Cambridge. http://www.hashcash.org/papers/hashcash.pdf

Banco de España. (2022). *Comunicado conjunto del Banco de España, la CNMV y la DG de Seguros sobre la advertencia de los reguladores financieros europeos en relación con los riesgos de los criptoactivos*. https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/NotasInformativas/22/presbe2022_19.pdf

Bit2Me Academy. (2023). *Página sobre BIP en Bit2Me Academy.* https://academy.bit2me.com/que-es-bip-bitcoin/

Bitcointalk. (2008). *Topic: Bitcoin source from November 2008*. https://bitcointalk.org/index.php?topic=382374.0.

Bitcointalk. (2010). *Topic: More Bitcoin logos, buttons, and also some other graphics*. https://bitcointalk.org/index.php?topic=1631

Bitcointalk. (2023). *Topic: More Bitcoin logos, buttons, and also some other graphics*. https://web.archive.org/web/20130912111647/https://bitcointalk.org/index.php?topic=1631

Bitcointalk. (2023). *Topic: v0.1.* https://bitcointalk.org/index.php?topic=68121.0

Bitnodes. (2023). *Sitio web de Bitnodes*. https://bitnodes.io/

Blockchain.com. (2023). *Gráficos del hashrate*. https://www.blockchain.com/explorer/charts/hash-rate

Boletín Oficial del Estado. (Enero, 2022). No. 14. Pp. 4106-4116. https://www.boe.es/eli/es/cir/2022/01/10/1

Carter, Nic. y Stevens, Ross. (2021). *Bitcoin Net Zero. Tech*. Rep. NYDIG. https://nydig.com/bitcoin-net-zero

Comisión Nacional del Mercado de Valores. (2023). *Comunicado conjunto de la CNMV y del Banco de España sobre el riesgo de las criptomonedas como inversión*. https://www.cnmv.es/Portal/verDoc.axd?t=%7Be14ce903-5161-4316-a480-eb1916b85084%7D

Consolvo, B. y Caron, K. (2023). *Bitcoin's role in the ESG imperative*. KPMG. https://advisory.kpmg.us/articles/2023/bitcoin-role-esg-imperative.html

Dinero Sin Reglas. (*s.f.*). Línea del tiempo de Bitcoin. https://dinerosinreglas.com/linea-del-tiempo-de-bitcoin/

Fragmento de la página web. (*s.f.*) https://archive.is/rMBtV#selection-65.90-65.119

https://www.whitehouse.gov/ostp/news-updates/2022/09/08/fact-sheet-climate-and-energy-implications-of-crypto-assets-in-the-united-states/

Hughes, E. (1993). A Cypherpunk's Manifesto. https://www.activism.net/cypherpunk/manifesto.html

Ibañez, J.I. y Freier, A. (2023). Bitcoin's Carbon Footprint Revisited: Proof of Work Mining for Renewable Energy Expansion. *Challenges,* 14(3), 35. https://doi.org/10.3390/challe14030035/3/35

Ibañez, J.I. y Freier, A. (2023). *Don't Trust, Verify: Towards a Framework for the Greening of Bitcoin*. http://dx.doi.org/10.2139/ssrn.4436607

Lopp, J. (2023). *How is the 21 Million Bitcoin Cap Defined and Enforced?" Blog de Jameson Lopp*. https://blog.lopp.net/how-is-the-21-million-bitcoin-cap-defined-and-enforced/

Lopp, J. (2023). *¿Cómo podrán existir 21 millones de Bitcoins? Jameson Lopp lo explica*. CriptoNoticias. https://www.criptonoticias.com/tecnologia/como-podran-existir-21-millones-bitcoins-jameson-lopp-explica/

Luo, Xinyi. (2022). *Bitcoin Miners Offered Way to Cut Texas Electricity Usage to Help the Grid. Coindesk*. https://www.coindesk.com/business/2022/12/06/texas-bitcoin-miners-are-offered-to-cut-electricity-usage-to-help-the-grid/

Maestre, J. (2023). *To be security or not to be. That's the question*. https://maestreabogados.com/to-be-security-or-not-to-be-thats-the-question/

Mempool Space. (*s.f.*). *Bloque en Mempool Space*. https://mempool.space/es/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Metzdowd Cryptography Mailing List. (2008). *Mensaje de la lista de correo de criptografía de octubre de 2008*. https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Nakamoto, S. (*s.f.*). *Bitcoin: Un sistema de efectivo electrónico peer-to-peer.* Bitcoin.org. https://bitcoin.org/bitcoin.pdf

New Liberty Standard. (2009). *2009 Exchange Rate*. https://web.archive.org/web/20131102222638/http://www.newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate

OSTP. (2022). *Climate and energy implications of crypto-assets in the United States*. Tech. rep. White House Office of Science and Technology Policy.

Proyecto Bitcoin en SourceForge. (*s.f.*). *SourceForge*. https://sourceforge.net/projects/bitcoin/

Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos. https://eur-lex.europa.eu/eli/reg/2023/1114/oj

Roarty, D. y Wheeler, D. (*s.f.*). *Huellas de carbono positivas: un marco climático favorable para inversores en renta variable*. AllianceBernstein. https://www.alliancebernstein.com/library/huellas-de-carbono-positivas-un-marco-climatico-favorable-para-inversores-en-renta-variable.htm

Sidhu, R. (*s.f.*). *Exploring Bitcoin's History*. Medium. https://medium.com/coinmonks/exploring-bitcoins-history-ecbf1c59952c

Vázquez, J. y Crumbley, DL. (2022). Flared Gas puede reducir algunos riesgos en la criptominería, así como en las operaciones de petróleo y gas. *Riesgos*, 10: 127. https://doi.org/10.3390/risks10060127

Vila-Viñas, D. (2020). *Derecho a la ciencia. Libertad de investigación, acceso, participación y promoción de la ciencia en el ordenamiento español*. https://e-revistas.uc3m.es/index.php/DYL/article/download/6110/4479/

Visual Capitalist. (*s.f.*). *Mapa de bifurcaciones importantes de Bitcoin*. https://www.visualcapitalist.com/major-bitcoin-forks-subway-map