INSTITUTO TECNOLÓGICO DE BUENOS AIRES – ITBA

MAESTRÍA EN DIRECCIÓN ESTATÉGICA Y TECNOLÓGICA

ESCUELA DE POSTGRADO

LA SUSTENTABILIDAD DE BITCOIN EN EL LARGO PLAZO

AUTOR: ANDREU, ANTONIO CARLOS (Leg. Nº 104406)

DIRECTOR DE TESIS: Almada, Jorge

CO-DIRECTOR: De Mendoça, Inés

TUTOR: Fahnle, Pablo Ariel

TESIS PRESENTADA PARA LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN DIRECCIÓN ESTRATÉGICA Y TECNOLÓGICA (ARGENTINA) Y MASTER EXECUTIVE EN DIRECCIÓN ESTRATÉGICA Y TECNOLÓGICA (ESPAÑA)

BUENOS AIRES

AÑO 2021

Agradecimientos

Quiero agradecer a mis profesores de la Maestría en Dirección Estratégica y Tecnológica por todo el apoyo que me han brindado durante dos años. Entre ellos, deseo destacar la predisposición de Diego Luzuriaga y de Jorge Almada enfocados en fomentar la culminación de la Maestría mediante el presente trabajo.

También deseo agradecer a mi tutor, Pablo Fahnle, por la ayuda brindada para hallar una visión holística del tema de estudio y encauzar el desarrollo de mi investigación.

Dedicatoria:

Este trabajo está dedicado a las personas que me han apoyado a realizarlo, pero también a quienes han sido parte de una formación académica, profesional y personal durante toda mi vida: familiares, amigos, compañeros, colegas y, especialmente, a mis padres

Índice Capítulos:

Índice de Cuadros:

Abstract:

El presente trabajo contiene un relevamiento exhaustivo de información relacionada con la criptomoneda Bitcoin (BTC). A partir de dicha información se han fundado argumentos que permiten sostener la hipótesis de que esta criptomoneda no es sustentable en el largo plazo. Para ello, se ha seguido una línea de razonamiento desde su génesis, basada en la cadena de bloques, hasta las amenazas que lo rodean en la actualidad.

En un primer lugar, se han destacado las cualidades de la tecnología Blockchain, sus usos en la actualidad y el infinito potencial que posee. Dentro de esta gama de aplicaciones para esta tecnología, se ha puesto foco en las criptomonedas y, particularmente, en Bitcoin, por ser la criptomoneda pionera y la que ha mantenido una marcada hegemonía durante más de una década de vida.

Al dirigir la mirada hacia Bitcoin, se ha contemplado que existen proyectos de criptomonedas con distintos objetivos, métodos y cualidades. Se ha visto que muchas criptomonedas alternativas a Bitcoin (o altcoins) logran superar debilidades inherentes a Bitcoin e incluso mejorar sus fortalezas.

Luego, se ha planteado analizar a Bitcoin desde diferentes puntos de vista. Para esto, se ha decidido examinarlo desde cuatro enfoques: un enfoque técnico con las vulnerabilidades a las que se halla expuesto, un enfoque desde las amenazas regulatorias y recaudatorias, un enfoque económico de su comportamiento en el mercado y un enfoque ecológico sobre su impacto en el medioambiente. En cada enfoque se ha podido apreciar que Bitcoin cuenta con debilidades incorregibles y amenazas externas que paulatinamente lo están llevando a un anunciado final.

Introducción:

Relevancia:

La tecnología Blockchain ha sido la última gran revolución tecnológica que ha experimentado la humanidad. Su abanico de posibilidades y funcionalidades la hace aplicable a casi cualquier industria conocida. Gobiernos, empresas y particulares están apostando actualmente a esta tecnología para potenciar sus actividades mediante el impulso que les brinda en eficiencia y confiabilidad. Blockchain se perfila para ser una herramienta fundamental a futuro en un mundo donde la confianza y la seguridad informática tienden a ser constantemente cuestionadas.

La aplicación de Blockchain específicamente a las criptomonedas ha revolucionado las finanzas globales. No solo la extensa variedad de criptomonedas existentes da fe de ello, sino también el alto grado de inversión que estos activos han adquirido en el último lustro. Estas inversiones son elevadas y continúan creciendo a tasas considerables, lo cual hace inevitable la necesidad de analizar este fenómeno y tomar su posicionamiento en el campo de la economía mundial con seriedad.

Si se habla de fuertes inversiones en criptomonedas, la estrella en escena es, sin lugar a dudas, Bitcoin (BTC), por popularidad, inversión en minado y capitalización de mercado.

Por lo expuesto, es importante analizar Bitcoin para poder vislumbrar el futuro que le depara y su sustentabilidad en el largo. El cuantioso nivel de inversión que posee y que se incrementa día tras día, la infraestructura que se ha desplegado en pro de su desarrollo y las externalidades negativas que ha ocasionado, evidencian la relevancia que ha adquirido Bitcoin y, por ello, el compromiso que se debe asumir para intentar estimar las posibilidades de su porvenir.

Definición y alcance del problema:

Es imprescindible ver la marcada diferencia existente entre Blockchain, las criptomonedas y Bitcoin particularmente. Para ello, es conveniente explorar brevemente los distintos usos de la tecnología Blockchain en una multiplicidad de rubros, para luego enfocarse en uno solo: las finanzas y, en especial, las criptomonedas.

Por otro lado, existe una variedad de criptomonedas con protocolos muy disímiles, por lo que es preferible dirigir el análisis a Bitcoin y a un número acotado de sus competidores para entender los atributos específicos de cada uno. El caso de Bitcoin es el más exitoso en la actualidad dentro del mundo de las criptomonedas y presenta dificultades dependiendo del ángulo del que se lo analice. Por esto, su caso se tiene que analizar desde distintos enfoques. Sin embargo, es imprescindible ver con claridad que

estos enfoques que son válidos para el caso de Bitcoin pueden no serlo para otras criptomonedas. Reconocer las diferencias entre Bitcoin y otros criptoactivos es fundamental para comprender que los caminos de cada uno probablemente diverjan en el tiempo.

Estado del conocimiento:

La tecnología Blockchain se inició y se ha popularizado mediante las criptomonedas y, en especial, Bitcoin. Se puede decir que Bitcoin ha sido el estandarte y la cara visible de Blockchain. El mundo ha conocido esta tecnología gracias a Bitcoin. Tanto es así, que mucha gente ajena a este entorno conoce lo que es Bitcoin, pero desconoce que esta criptomoneda se basa en la cadena de bloques. Incluso, en ciertas ocasiones, las personas sin una formación suficiente de la temática no ven con claridad la enorme distancia que existe entre los conceptos de "Blockchain" y "Criptomonedas". No obstante, una persona con un mínimo de conocimiento del medio y que interactúe con criptomonedas, seguramente jamás se vea inmersa en tal confusión.

De todas formas, cabe destacar que las criptomonedas, y en especial Bitcoin, han ganado popularidad dentro de los inversores financieros desde fines de 2017, cuando el 17 de diciembre de ese año alcanzó un precio de cotización en el mercado de más de USD 19.700, el máximo registrado desde su creación en 2009, hasta que en 2021 superara los USD 63.200. Desde ese pico en el precio en 2017, Bitcoin no ha dejado de ser el activo de referencia entre las criptomonedas; prueba de ello es que su MarketCap (o capitalización de mercado) durante el primer semestre de 2021 superó el billón millones de dólares[1]. Para tener idea de su magnitud, esto representa cerca de veinticinco veces las reservas del Banco Central de la República Argentina en ese mismo periodo. Es importante mencionar, también, que luego de estas fuertes alzas tanto el precio como la capitalización de mercado de Bitcoin sufrieron una corrección que retrajo el pecio en torno a los USD 30.000 y su MarketCap alrededor de los USD 600 millones.

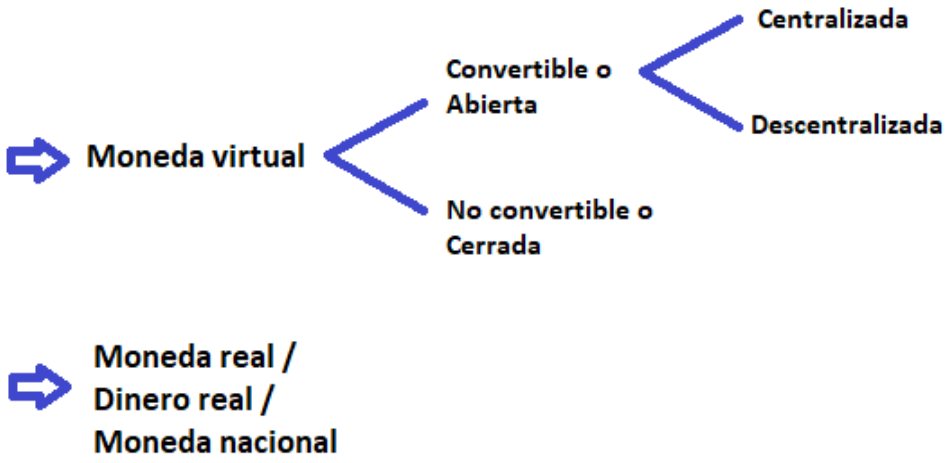
Existe divergencia de opiniones respecto de algunos conceptos en torno a estos activos. En efecto, según un informe del GAFI (Grupo de Acción Financiera Internacional) "*…se ha hecho evidente que carecemos de un vocabulario común que refleje con precisión las diferentes formas que las monedas virtuales pueden tomar*"[2]. En tal sentido, resulta conveniente definir con claridad los términos que identificarán a los distintos activos, a fin de reducir al máximo posible las confusiones semánticas que

[1] MarketCap.com, https://marketcap.com/coin/BTC (Recuperado en fecha 01/07/2021)
[2] Grupo de Acción Financiera Internacional, "Informe GAFI. Monedas virtuales. Definiciones claves y riesgos potenciales de LA/FT", 2014, (En línea) Disponible en: http://www.uaf.cl/asuntos/descargar.aspx?arid=961 (Recuperado en fecha 30/09/2020), p.4.

puedan surgir. Para ello, es oportuno hacer hincapié en la terminología que este informe del GAFI aplica. El informe bifurca su análisis en dos tipos de monedas: monedas virtuales y monedas reales (o monedas nacionales o dinero real –fiduciario–). Asimismo, relaciona el concepto de dinero electrónico únicamente con el dinero fiduciario y lo define como *"…una representación digital del dinero fiduciario usado electrónicamente para transferir valor denominado en dinero fiduciario. (…) es decir, transfiere electrónicamente un valor que tiene la condición de moneda de curso legal*"[3].

A su vez, hace mención del término de "moneda digital" e indica que puede generar confusiones dado que suele usarse tanto para monedas virtuales (dinero no fiduciario) como para dinero electrónico (dinero fiduciario), por lo que recomienda evitar su uso.

Para un mejor entendimiento y para evitar una transcripción demasiado extensa del informe del GAFI, se presenta el siguiente cuadro con las clasificaciones que realiza y, a continuación, las aclaraciones pertinentes:



Cuadro 0.1. Clasificación de monedas. Fuente de elaboración propia con base en el "Informe GAFI. Monedas virtuales. Definiciones claves y riesgos potenciales de LA/FT", 2014, (En línea) Disponible en: http://www.uaf.cl/asuntos/descargar.aspx?arid=961 (Recuperado en fecha 30/09/2020)

Tal como se puede apreciar en el cuadro, el GAFI propone una subclasificación dentro de las monedas virtuales entre "convertibles o abiertas" y "no convertibles o cerradas". La primera se refiere a que "*…tiene un valor equivalente en moneda real y puede ser intercambiada una y otra vez por dinero real*[4]". Por el contrario, la segunda clasificación *"…pretende ser específica de un dominio o mundo virtual*

[3] Grupo de Acción Financiera Internacional, "Informe GAFI. Monedas virtuales. Definiciones claves y riesgos potenciales de LA/FT", 2014, (En línea) Disponible en: http://www.uaf.cl/asuntos/descargar.aspx?arid=961 (Recuperado en fecha 30/09/2020), p.4.

[4] Grupo de Acción Financiera Internacional, "Informe GAFI. Monedas virtuales. Definiciones claves y riesgos potenciales de LA/FT", 2014, (En línea) Disponible en: http://www.uaf.cl/asuntos/descargar.aspx?arid=961 (Recuperado en fecha 30/09/2020), p.5.

particular, como los videojuegos (…) o Amazon.com, y en virtud de las normas que regulan su uso, no se puede cambiar por dinero real"[5]. En esta segunda clasificación, el GAFI hace una mención especial, destacando que "*…aunque en virtud de los términos establecidos por el administrador una moneda no convertible solo puede ser transferida oficialmente dentro de un entorno virtual específico, y aunque en ningún caso pueda ser convertible, es posible que pueda surgir un mercado negro secundario no oficial que proporcione una oportunidad de intercambiar la moneda virtual 'no convertible' por moneda fiduciaria u otra moneda virtual*"[6].

Otra apreciación que surge del cuadro es la subclasificación que existe dentro de las monedas convertibles. El Informe las subdivide entre centralizadas y descentralizadas. Según el GAFI, las monedas virtuales centralizadas *"…tienen una autoridad administrativa única (administrador), es decir, una tercera parte que controla el sistema. Un administrador emite la moneda, establece las normas pasa su utilización, mantiene un libro de contabilidad central de pago, y tiene autoridad para canjear la moneda (retirarla de circulación)"*.[7]

Dos aclaraciones importantes que deben hacerse sobre el cuadro son: en primer lugar, que el Informe indica que todas las monedas no convertibles o cerradas son de tipo centralizada; en segundo lugar, que hace una analogía entre monedas virtuales descentralizadas y las criptomonedas, es decir, para el GAFI las criptomonedas son monedas virtuales convertibles descentralizadas. A futuro, se tomará como referencia toda la terminología señalada por este informe, a excepción de esta última parte. Dado que el informe está fechado en el año 2014 y que han surgido nuevas criptomonedas desde entonces, no es válido decir que las criptomonedas son únicamente descentralizadas. El surgimiento de empresas que son mineras de criptomonedas propias (ej.: Crypto.com) y de Estados soberanos con intenciones de emitir sus propias criptomonedas (CBDC), hace que vincular a las criptomonedas como una moneda virtual exclusivamente descentralizada haya perdido vigencia. Además, la centralización puede también entenderse desde la concentración de los criptoactivos en pocos actores o en las jerarquías de los nodos de la red, entre otras.

La clasificación expuesta y sus aclaraciones pueden no tener límites del todo nítidos, pero dentro del gran espectro de monedas virtuales, echa luz suficiente para los objetivos a los que se apunta arribar.

---

[5] Grupo de Acción Financiera Internacional, "Informe GAFI. Monedas virtuales. Definiciones claves y riesgos potenciales de LA/FT", 2014, (En línea) Disponible en: http://www.uaf.cl/asuntos/descargar.aspx?arid=961 (Recuperado en fecha 30/09/2020), p.5.

[6] Grupo de Acción Financiera Internacional, "Informe GAFI. Monedas virtuales. Definiciones claves y riesgos potenciales de LA/FT", 2014, (En línea) Disponible en: http://www.uaf.cl/asuntos/descargar.aspx?arid=961 (Recuperado en fecha 30/09/2020), p.5.

[7] Grupo de Acción Financiera Internacional, "Informe GAFI. Monedas virtuales. Definiciones claves y riesgos potenciales de LA/FT", 2014, (En línea) Disponible en: http://www.uaf.cl/asuntos/descargar.aspx?arid=961 (Recuperado en fecha 30/09/2020), p.5.

Buscar precisión en los conceptos no es un aspecto menor, ya que actualmente entidades nacionales y supranacionales intentan legislar y regular las monedas virtuales. Y la existencia de tanta variedad de monedas virtuales con diferentes atributos, hace que estas intenciones impliquen una tarea sumamente compleja para los Estados. No obstante, el avance de los Estados sobre las monedas virtuales ha ido en aumento debido a cuestiones económicas, sociales y legales. El financiamiento del terrorismo, el lavado de activos, la evasión de impuestos y la incipiente pérdida de control sobre ciertos sectores de la economía, son algunos de los principales factores en los que los Estados se basan para manifestar la necesidad de regular e intervenir sobre las monedas virtuales.

Hipótesis:

En el presente trabajo se pretende demostrar que la criptomoneda estrella del mercado, Bitcoin, carece de sustentabilidad en el largo plazo. Se pretende evidenciar los problemas intrínsecos y extrínsecos que debilitan su subsistencia en el tiempo. A pesar del potencial de la tecnología Blockchain y de las criptomonedas en general, Bitcoin reviste características que la hacen vulnerable desde distintos enfoques.

Metodología

Se buscará demostrar la hipótesis planteada analizando la criptomoneda Bitcoin desde diferentes puntos de vista. En cada uno se verá que Bitcoin posee debilidades y amenazas que lo llevarán a su decadencia en el largo plazo. Se postularán dos capítulos para entender el potencial de Blockchain y las criptomonedas en general, así como lo que diferencia a Bitcoin y su situación en particular de otros protocolos de criptomonedas vigentes. Luego, se postularán cinco capítulos destinados cada uno a un enfoque distinto, a fin de demostrar las debilidades que Bitcoin padece y las amenazas que lo acechan.

La bibliografía utilizada tiene limitaciones. Dado que las criptomonedas están en plena expansión y que tienen fuertes implicancias socioeconómicas, el desarrollo teórico se encamina por detrás del práctico. Por ello, la bibliografía se encuentra generalmente en material muy reciente y en sitios web de actualidad.

Además, durante el trabajo se realizaron encuestas para conocer el nivel de conocimiento de un público heterogéneo sobre la temática en cuestión. También se han realizado entrevistas a profesionales afines a la materia.

Cuerpo Central

CAPÍTULO 1. La revolución de la tecnología Blockchain

Bitcoin es solo un elemento en la frondosa población de criptomonedas. A su vez, las criptomonedas son solo un elemento dentro del universo de posibilidades que brinda la tecnología Blockchain. El potencial que Blockchain poseía cuando surgió a modo de prueba con Bitcoin, ha sido explotado en distintas industrias y actividades económicas, sociales y gubernamentales. Este potencial que muchos sectores han estado aprovechando y desarrollando, no ha tocado su techo y en el horizonte se prevé que Blockchain tiene un futuro prometedor, incluso en funcionalidades que aún se desconocen. La tecnología Blockchain es la llave a un mundo por descubrir. El sitio de la empresa multinacional IBM define a Blockchain como "*…un libro mayor compartido e inmutable para registrar transacciones, rastrear activos y generar confianza*"[8]. Este registro se estructura en forma de bloques que se vinculan con los anteriores de forma cronológica, propiciando la inmutabilidad de la información contenida.

A pesar de las innumerables posibilidades que Blockchain habilita para el futuro, es conveniente revisar la incidencia actual de esta tecnología sobre diversas áreas de estudio y trabajo. Con esta revisión, se pretende contextualizar a las criptomonedas dentro de Blockchain y comprender que la prosperidad de Blockchain no guarda una correlación ineludible con la exclusiva subsistencia de las criptomonedas y que su aplicabilidad va más allá de estas.

El aprovechamiento de Blockchain

No es justo hablar únicamente del potencial de Blockchain, ya que actualmente esta tecnología ha dejado de ser una promesa para convertirse en una realidad en una extensa variedad de ámbitos: banca, industria de la moda, industria alimentaria, educación, salud, entre muchos otros.

En el presente existen muchas empresas abocadas a ofrecer servicios basados en tecnología Blockchain para optimizar los procesos de sus clientes. Estos clientes pueden ser tanto públicos como privados y provenientes de distintos sectores socioeconómicos. Para brindar un ejemplo de esto, el sitio e-Estonia cuenta el caso de la compañía Guardtime que, entre otros proyectos, ha incursionado en la industria vitivinícola de Australia. El sitio cuenta que "*La compañía Guardtime, empresa Blockchain líder en el mundo, se ha dispuesto a diseñar un sistema de autenticación de vinos en Australia, combinando la tecnología Blockchain KSI que provee a través de su plataforma de cadena de suministro con un 'tapón*

[8] Sitio Web Oficial de IBM, "¿Qué es la tecnología Blockchain?", (En línea) Disponible en: https://www.ibm.com/ar-es/topics/what-is-blockchain (Recuperado en fecha 15/12/2020)

digital', para prevenir fraudes y garantizar la integridad del vino"[9]. De esta manera, Blockchain proporciona un servicio anti-fraude sobre la procedencia del vino australiano. Así es como lo explica Chloe White del Departamento de Industria de Australia cuando dice que "*…el uso de la tecnología Blockchain puede proporcionar una solución de procedencia al fraude de alimentos y vinos…*"[10]. De igual manera, Bride Ohlsson, CEO de la plataforma Blockchain agrícola Geora explica que "*Las soluciones Blockchain también ofrecen beneficios significativos y ahorros de eficiencia para las industrias de certificación alimentaria y agrícola que actualmente dependen en gran medida de certificados basados en papel fácilmente falsificados…*"[11]

Pero esto es solo un vistazo a las aplicaciones de Blockchain. Fuera de la industria alimentaria, podemos también encontrar su instrumentación, por ejemplo, en la industria de la moda. Daniel Jiménez, columnista en Cointelegraph.com, afirma que "*…la Blockchain ya está encontrando su espacio para resolver problemas fundamentales como la débil cadena de suministro tradicional, transferencia de propiedades y hasta la identidad digital de las piezas elaboradas con la más fina seda*"[12]. Esta transformación en la industria de la moda es trascendental, ya que no solo asegura la calidad de los insumos y previene falsificaciones, sino que aporta un valor agregado a la logística de los productos.

Otro sector en el que hay empresas que proporcionan ventajas a través de la Blockchain es el bancario, en especial en el área de las garantías bancarias. La columnista Ting Peng de Cointelegraph.com, ha informado que "*…la plataforma blockchain ygon, que funciona con la nube pública de IBM, ha realizado con éxito su proyecto piloto (…) con los bancos australianos ANZ, el Banco del Commonwealth de Australia (CBA) y Westpac y un grupo de 20 empresas australianas. Se espera que los bancos emitan garantías bancarias en un solo día una vez que implementen Lygon, en comparación con las actuales garantías en papel que pueden tardar un mes*"[13]. La eficiencia y la reducción de tiempos que logra

[9] e-Estonia, "Estonian-founded Guardtime to build wine authentication system in Australia", 2019, Traducido, (En línea) Disponible en: https://e-estonia.com/guardtime-wine-authentication-system (Recuperado en fecha 17/12/2020)
[10] J. Wapperson, "La tecnología blockchain podría ayudar a combatir el fraude alimentario en Australia", 2020, (En línea) Disponible en: https://es.cointelegraph.com/news/blockchain-can-combat-australia-s-1-7b-food-and-wine-fraud-problem (Recuperado en fecha 03/01/2021)
[11] J. Wapperson, "La tecnología blockchain podría ayudar a combatir el fraude alimentario en Australia", 2020, (En línea) Disponible en: https://es.cointelegraph.com/news/blockchain-can-combat-australia-s-1-7b-food-and-wine-fraud-problem (Recuperado en fecha 03/01/2021)
[12] D. Jiménez, "¿Cómo se está utilizando la tecnología blockchain en la industria de la moda?", 2020, (En línea) Disponible en: https://es.cointelegraph.com/news/how-is-blockchain-tech-used-in-the-fashion-industry (Recuperado en fecha 03/01/2021)
[13] Ting Peng, "Una plataforma blockchain comercializa garantías bancarias digitales en Australia"; 2020, (En línea) Disponible en: https://es.cointelegraph.com/news/blockchain-platform-commercializes-digital-bank-guarantees-in-australia (Recuperado en fecha 03/01/2021)

Blockchain en esta cuestión es fundamental para las empresas que la utilicen, ya que obtienen una ventaja sobre sus competidores, inmersos en los tediosos tiempos convencionales.

Uno de los sectores que más provecho le puede sacar a Blockchain es el de la salud. En este sentido, aparece Estonia muy por delante de la mayoría de los demás países. Taavi Einaste, Jefe de Digital Healthcare en Nortal sostiene que "*Estonia, con uno de los gobiernos más "digitales" del mundo, se ha convertido en el primer país en utilizar la tecnología Blockchain en el cuidado de la salud a escala nacional. En 2016, la Estonian E-Health Foundation (...) lanzó un proyecto de desarrollo enfocado a salvaguardar los historiales clínicos de los pacientes usando la tecnología Blockchain archivando la actividad de los registros*"[14]. El acceso a historiales clínicos inalterables de manera rápida y transparente permite a los profesionales y las instituciones de la salud brindar un servicio más eficiente y más seguro a los pacientes.

Suele considerarse al sector de la salud como una de las áreas esenciales dentro de las actividades de un país, pero también aparece, en un rango similar, el sector de la educación. Ambos sectores son, en general, una prioridad para los Estados nacionales y estratos inferiores. Y no es menor la injerencia que ha tenido Blockchain también en la educación. Para Ylenia García de la Innovation and Entrepreneurship Business School comenta que "*...blockchain ha llegado al mundo de la educación para quedarse. Permitirá tener una gestión automatizada de calificaciones y exámenes, además de evitar cualquier tipo de fraude, como, por ejemplo, los cambios de notas y plagios*"[15]. Y agrega que "*...con la tecnología Blockchain se permitirá avalar las titulaciones de manera inmediata.*"[16]. Blockchain ofrece al ámbito educativo cambios que necesitaba con urgencia. La certificación de títulos y documentos oficiales con un sistema impermeable a falsificaciones y manipulaciones, el resguardo de la identidad de los alumnos, la posibilidad de tener un registro académico transparente e inalterable y la protección contra plagios, son avances revolucionarios para el ámbito educativo. Este progreso en la educación representa cambios positivos no solo a niveles nacionales, sino globales, dado que un alto grado de confiabilidad en el acceso a este tipo de información favorece a la integración al mundo de quienes la adopten; las certificaciones en el extranjero se reducirían si las equivalencias de formación académica no son puestas en tela de juicio.

[14] Taavi Einaste, "Blockchain and healthcare: the Estonian experience", 2018, Traducido, (En línea) Disponible en: https://nortal.com/blog/blockchain-healthcare-estonia (Recuperado en fecha 03/01/2021)
[15] Ylenia García, "Blockchain, la nueva tecnología aplicable en la educación", 2019, (En línea) Disponible en: https://www.iebschool.com/blog/tecnologia-blockchain-educacion-business-tech-finanzas (Recuperado en fecha 03/01/2021)
[16] Ylenia García, "Blockchain, la nueva tecnología aplicable en la educación", 2019, (En línea) Disponible en: https://www.iebschool.com/blog/tecnologia-blockchain-educacion-business-tech-finanzas (Recuperado en fecha 03/01/2021)

Si bien esta tecnología puede observarse desde las actividades que la utilizan, también puede cambiarse el enfoque hacia los actores que se encuentran sacándole provecho en la actualidad, ya que no son solo empresas las que la aplican, sino también los gobiernos y sus organismos.

La FDA (Food and Drug Administration) en Estados Unidos, encargada de proteger la salud pública a través del control sobre alimentos, vacunas, medicamentos, cosméticos, etc., ha comenzado a incursionar en la Blockchain a partir de los beneficios que ha visto que le pueden proporcionar para cumplir con sus funciones. Tommy Peterson, del portal FedTech, escribió que "*Cuando el virus del H1N1 comenzó un rebrote en 2017, los funcionarios de la FDA sabían que necesitaban una mejor manera de tener seguimiento de la información del brote, y desplegaron la tecnología Blockchain para que les asistiera en esta tarea*"[17]. Peterson agrega que "*La FDA también está investigando cómo utilizar la tecnología blockchain para rastrear y gestionar las amenazas a la seguridad alimentaria en el vasto y descentralizado sistema alimentario de la nación y aumentar la transparencia en la cadena de suministro farmacéutico*"[18]. He aquí una clara muestra de que la FDA ha tomado en serio los atributos de Blockchain y que pretende implementarla en sus funciones esenciales en materia alimentaria y sanitaria. En el mismo orden y basado en la información de Peterson, Husayn Hashim, escritor de Cointelegraph.com, afirma que "*El Departamento de Agricultura de los Estados Unidos (USDA) ya ha certificado a BeefChain, una compañía blockchain que rastrea la cadena de suministro de carne*"[19]. Este tipo de implementación es similar al caso de la industria vitivinícola en Australia y la autenticación del vino, lo que da cuenta de la proliferante aceptación de esta tecnología a nivel mundial.

A propósito de esta creciente aceptación global, en México se puede ver otra aplicación que los gobiernos le han dado a la Blockchain. José Colmenares, columnista en Criptonoticias.com, escribió sobre esto: "*El Instituto Nacional Electoral (INE) de México habilitará un sistema de voto electrónico que le permitirá a los mexicanos residentes en el extranjero participar en las elecciones del próximo año 2021. El sistema anunciado contará con una bitácora de registro basada en blockchain y, según el INE, asegura*

[17] T. Peterson, "Blockchain Makes Inroads at Federal Agencies", 2020, Traducido, (En línea) Disponible en: https://fedtechmagazine.com/article/2020/08/blockchain-makes-inroads-federal-agencies (Recuperado en fecha 02/02/2021)
[18] T. Peterson, "Blockchain Makes Inroads at Federal Agencies", 2020, Traducido, (En línea) Disponible en: https://fedtechmagazine.com/article/2020/08/blockchain-makes-inroads-federal-agencies (Recuperado en fecha 02/02/2021)
[19] H. Hashim, "Las agencias federales adoptan la tecnología blockchain por sus beneficios", 2020, (En línea) Disponible en: https://es.cointelegraph.com/news/federal-agencies-turning-to-blockchain-for-its-benefits (Recuperado en fecha 02/02/2021)

que el voto de cada persona sea secreto por medio de un cifrado criptográfico"[20]. Los sistemas de votación tienen con Blockchain la oportunidad de reflejar una transparencia sin precedentes, un atributo determinante para la legitimidad de los gobiernos electos.

Otro impacto fuerte que puede tener Blockchain en las instituciones gubernamentales se halla en la lucha contra la corrupción. Carlos Santiso, Director para la Innovación Digital Gubernamental del Development Bank of Latin America, afirma en un artículo que preparó para el Foro Económico Mundial, que "*Blockchain hace más dificultosa la corrupción ya que es un libro contable tecnologico distribuido, que puede certificar registros y transacciones – o bloques – sin usar una base de datos central y de una forma que no puede ser borrada, alterada o manipulada. Provee un nivel de integridad, seguridad y confiabilidad, sin precedentes, de la información que administra…*"[21]. Las posibilidades que brinda Blockchain para mitigar los efectos de la corrupción son para destacar por las nocivas consecuencias que tiene en los países donde está más presente y por lo extensivo de este problema a nivel mundial.

Siguiendo con esto, es remarcable mencionar que existen casos como el de Dinamarca, que elaboró un informe denominado "Código para la integridad", donde, entre otras cuestiones, vislumbra los posibles beneficios de Blockchain en la lucha contra la corrupción; algunos de los que menciona son: "*La reducción o eliminación de la necesidad de instituciones cuyo principal propósito sea la validación de transacciones, como bancos, registros de propiedad, contadores, (…) etc. La completa transparencia de toda la información en la Blockchain. El rápido y fácil acceso formal a un Documento de Identidad para todos. La íntegra trazabilidad de quién hace qué en la Blockchain*"[22]. Los beneficios son relevantes e implicarían un cambio profundo en el ámbito político, pero una resolución favorable en esta cuestión estará supeditada a la voluntad de los gobernantes y a la exigencia de mayor transparencia por parte de los gobernados.

Por lo expuesto, Blockchain ha generado una revolución en la industria, en la política y en los sectores más esenciales de la sociedad. Si bien existen muchos más usos para esta tecnología, como en la industria aseguradora, en los registros civiles o la seguridad privada, es dable destacar brevemente en un punto aparte a los *smartcontracts* o contratos inteligentes. Los mismos se basan en la Blockchain y están

[20] J. Colmenares, "México usará una blockchain para elecciones de gobernadores", 2020, (En línea) Disponible en: https://www.criptonoticias.com/gobierno/votaciones/mexico-usara-blockchain-elecciones-gobernadores (Recuperado en fecha 02/02/2021)
[21] C. Santiso, "Can blockchain help in the fight against corruption?", 2018, Traducido, (En línea) Disponible en: https://www.weforum.org/agenda/2018/03/will-blockchain-curb-corruption (Recuperado en fecha 02/02/2021)
[22] S. Sayers, "Code to integrity", 2019, Traducido, (En línea) Disponible en: https://um.dk/~/media/um/english-site/documents/news/code%20to%20integrity_enkeltsider_web.pdf?la=en (Recuperado en fecha 02/02/2021), p. 10.

generando una revolución dentro de esta revolución; que quizás logre un impacto similar al de las criptomonedas en el corto o mediano plazo.

Los Smartcontracts

Las primeras líneas del Whitepaper de Bitcoin expresan que los pagos en esta criptomoneda tenían la característica de que podían ser "*…enviados de un ente a otro sin tener que pasar por medio de una institución financiera*"[23], evitando el doble gasto ocasionado por la intervención de un tercero confiable. Se puede conjeturar que de forma implícita también buscaba escapar de las regulaciones convencionales a las cuales este tipo de entidades es sometido.

Los smartcontracts son una de las máximas promesas de la tecnología Blockchain y, a diferencia de Bitcoin, necesitan del aval y reconocimiento de las instituciones de la sociedad moderna.

Para bit2me Academy, un sitio especializado en Blockchain y criptomonedas, la principal característica de un contrato inteligente que lo diferencia de un clásico contrato, es que "*…un contrato inteligente es capaz de ejecutarse y hacerse cumplir por sí mismo, de manera autónoma y automática, sin intermediarios ni mediadores*"[24]. Es importante distinguir entre la necesidad de los smartcontracts de ser reconocidos y avalados por otras instituciones y la prescindencia de intermediarios para su concreción. Es decir, la creación de un contrato hasta la llegada de los smartcontracts, necesitaba de dos partes y un tercero confiable que diera fe, atestiguara o mediara, para concretar su rúbrica. En cambio, la creación de un contrato inteligente, solo necesita de las dos partes, pues la inmutabilidad y la imposibilidad de alterar los términos del contrato que Blockchain brinda, dejan sin efecto cualquier aporte que un tercero pudiera ofrecer en el pasado. Sin embargo, la firma del contrato no es lo mismo que los efectos que su ejecución puede producir. Es en este instante que los contratos requieren del aval de la sociedad frente a posibles litigios y reconocimiento de derechos de una parte por sobre otra cuando ocurra un conflicto.

Por lo dicho, puede entenderse que, en el caso de los smartcontracts, las regulaciones adecuadas podrían darle el impulso que necesitan para popularizarse y desplazar a los contratos físicos convencionales, susceptibles de manipulación y falsificación. No ocurriría de igual forma con Bitcoin y otras criptomonedas, dado que el impacto de regulaciones podría ser contraproducente al atentar principalmente contra el anonimato que brindan. Para los contratos inteligentes, esas regulaciones probablemente lleguen más temprano que tarde cuando su desarrollo alcance un nivel más avanzado. Jon

[23] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Traducido, (En línea) Disponible en: https://bitcoin.org/bitcoin.pdf (Recuperado en fecha 02/02/2021)
[24] Bit2me Academy, "Smart Contracts: ¿Qué son, cómo funcionan y qué aportan?", (En línea) Disponible en: https://academy.bit2me.com/que-son-los-smart-contracts (Recuperado en fecha 02/02/2021)

Martindale de DigitalTrends afirma que "*Por poderosos que los smartcontracts podrían ser, no están listos para remplazar los sistemas de confianza que existen hoy. (…) una transacción complicada utilizando smartcontracts requeriría múltiples contratos inteligentes vinculados entre sí para cubrir todos los escenarios posibles que podrían surgir como parte de esa transacción*"[25]. Si bien reconoce el potencial de esta herramienta, manifiesta que todavía no está lista para revolucionar el sistema de confianza que los contratos precisan.

La importancia de que se consolide el uso de smartcontracts está a la vista y radica en las ventajas que ofrece y que siempre están relacionadas con lo que Blockchain provee:

- *Velocidad*: La automatización en la ejecución de los procesos, los acelera y permite el ahorro de tiempo.
- *Autonomía*: Permite prescindir de intermediarios como abogados, escribanos, contadores.
- *Reducción de gastos*: Ahorro de intermediarios, papel, aranceles, apostillados.
- *Protección contra manipulaciones y falsificaciones*: Una vez en la Blockchain, los contratos inteligentes quedan inalterables en los bloques.

Estas ventajas de los smartcontracts son posibles debido a manejarse sobre Blockchain. Y aunque los contratos inteligentes sean una de las mayores promesas de esta tecnología, hay quienes encuentran otros usos provechosos para la cadena de bloques que aún son un boceto o una simple idea para el futuro.

Los beneficios futuros de Blockchain

Definitivamente, Blockchain es una herramienta de usos múltiples de la cual se siguen extrayendo beneficios e ideas día tras día. En este sentido, no hace falta más que repasar las ventajas que Blockchain provee y conectarlas a actividades que las puedan aprovechar para optimizar sus procesos. Para mencionar solo tres ejemplos factibles, estas actividades podrían ser: la actividad notarial, la industria eléctrica y los servicios de arrendamiento.

En el primero, guardando una estrecha relación con los smartcontracts, es evidente que el hecho de que la cadena de bloques sea inalterable y no permita la modificación de lo que en ella se registra, induce a pensar que los servicios de escribanos o notarios no serán necesarios en el futuro, al menos en lo que se refiere a contar con un tercero confiable.

[25] Jon Martindale, "What are Smart contracts?", 2018, Traducido, (En línea) Disponible en: https://www.digitaltrends.com/computing/what-are-smart-contracts (Recuperado en fecha 07/02/2021)

En el segundo ejemplo, vale citar al sitio Fin-Tech.es, que en 2016 comentaba sobre esta cuestión: "*…cada vez son más las casas o edificios que generan su propia electricidad con sistemas de energías renovables. Algunos usuarios se desconectan completamente de la red eléctrica, pero otros continúan conectados y, básicamente, utilizan la energía de la red cuando no generan suficiente energía con sus renovables y aportan energía a la red cuando generan mucha y tienen excedente. Para estos casos, algunos países han instaurado un sistema de compensación, entre los vatios aportados a la red y los consumidos, para realizar el cálculo de la factura energética, pero no es fácil llevar un control. Utilizando una blockchain, las casas y edificios, conectados entre sí a través de una red distribuida, podrían comprar energía a la red o vender sus excedentes dependiendo de sus necesidades en cada momento, sin necesidad de que ningún intermediario lleve el control. Todas las transacciones de pagos e intercambios de energía quedarían almacenadas en la blockchain y serían verificadas por los miembros de la red*"[26].

Finalmente, para el tercer ejemplo, también se puede encontrar una relación con los smartcontracts, dado que, un convenio de arrendamiento o alquiler es instrumentado con un contrato. La utilización de un contrato inteligente para locación permitiría la ejecución automatizada de este cuando la transacción sea acreditada. El uso de la Blockchain para este caso particular podría tener incidencia en empresas como Uber, Cabify o Airbnb, ya que la intervención de terceros sería prescindible para los usuarios.

Blockchain: la confianza que el mundo precisaba

Ha quedado clara la relevancia del Blockchain tanto en el presente como en el futuro de la sociedad. El poderoso nivel de confianza de la tecnología es el motivo principal por el que tantos actores sociales, económicos y políticos están detrás de su aplicación.

En todos los casos desarrollados se puede ver que la confianza es el mayor aporte de Blockchain. Si bien posee otras características que resaltan más en ciertas aplicaciones que en otras, en todo momento subyace la confianza. Esa confianza no existía en algunas actividades y la cadena de bloques apareció para incorporarla y darles impulso. Esta confianza sí existía en otras actividades, pero era imprescindible la presencia de un tercero confiable que diera fe de los hechos y que velara por el cumplimiento de los procesos; en este caso, Blockchain ha venido a tomar el lugar del tercero confiable, suprimiendo sus costos accesorios.

[26] Fin-Tech.es, "15 aplicaciones de la tecnología blockchain más allá de bitcoin", 2016, (En línea) Disponible en: https://www.fin-tech.es/2016/10/aplicaciones-de-la-tecnologia-blockchain.html (Recuperado en fecha 07/02/2021)

Blockchain es, definitivamente, una tendencia que crece en todos los niveles, en todas las regiones del mundo, en actividades económicas muy variadas y tanto en el ámbito privado como público. Sin embargo, luego de haber podido observar la revolución que la tecnología Blockchain viene generando en tantos aspectos, es inexorable reconocer que las criptomonedas han sido su piedra fundamental y las propulsoras de su despegue. Las criptomonedas nacieron gracias a Blockchain. Esta tecnología resolvió el clásico *problema de los generales bizantinos*, brindando la confianza requerida para que Bitcoin apareciera en escena y desechando la necesidad de una autoridad que avale las transacciones. Por ello, es necesario profundizar en los tipos de criptomonedas y sus atributos y darle un marco teórico adecuado para su análisis.

CAPÍTULO 2. Las criptomonedas y la prueba piloto de Blockchain

La puesta en marcha de la tecnología Blockchain se realizó mediante una criptomoneda: Bitcoin. Luego, otras criptomonedas fueron surgiendo, con distintas características cada una, pero casi siempre sobre Blockchain y apalancándose en las ventajas de sus registros confiables. A final de 2020, existían miles de criptomonedas, según la página web de MarketCap.com. Sin embargo, de la cuantiosa variedad de criptomonedas, menos de 60 de ellas poseían a esa fecha una capitalización de mercado superior a los 500 millones de dólares. Dentro de este conjunto con altos niveles de capitalización, existen distintos tipos de criptomonedas, con diferentes características, que apuntan a eliminar debilidades que Bitcoin posee o fortalecer las ventajas que ofrece; incluso existen otras con una mirada disruptiva que van más allá de lo que Nakamoto planteó en su Whitepaper. Por ello, es importante observar las similitudes que existen entre estas criptomonedas y Bitcoin, pero más importante aún es destacar las diferencias que existen entre ellas. Para eso, es necesario distinguir los atributos más importantes con los que cuentan.

Atributos de las criptomonedas

Las criptomonedas pueden tener distintos atributos. Ocurre que ciertas características son compartidas por algunas criptomonedas, pero no por otras. Incluso la calidad del atributo puede ser superior en una criptomoneda que en otras. Dentro de esta gama de atributos que pueden poseer las criptomonedas, los usuarios suelen preferir unas u otras en función de los beneficios que otorguen.

Asimismo, al tratarse de activos financieros, es lógico que aquellos que cuentan con las cualidades más distinguidas sean las que tengan mayor respaldo de los usuarios, lo cual se traduce en mayor MarketCap. Se da por sentado, entonces, que propiedades fuertes o excepcionales en una criptomoneda, conllevan una considerable capitalización de mercado, ya que atraen la atención de los usuarios. Por ello, es sensato enfocarse en criptomonedas que posean un fuerte MarketCap y en sus atributos particulares destacados. Con este criterio, se pueden encontrar los siguientes atributos que sobresalen por sobre otros:

Anonimato – Rastreabilidad: Esta es una de las cualidades que más interesan en el ambiente de las criptomonedas y de las más ponderadas con la aparición de Bitcoin. El anonimato consiste en la condición de que un usuario pueda ocultar su identidad al tiempo que acumula criptomonedas y realiza transacciones en el sistema.

Un punto importante a tener en cuenta es que, si bien el anonimato implica que la identidad de una persona es desconocida, en el ambiente de las criptomonedas los usuarios usan seudónimos. Es decir, si pudiera averiguarse la identidad de una persona detrás de un seudónimo, todas las interacciones que esta

persona hubiese tenido dentro de la red, quedarían expuestas. Incluso, si se pudiera obtener la identidad real de un seudónimo, podría facilitar la obtención de identidades de otros usuarios que hubiesen transaccionado con la primera.

El grado de anonimato no es un tema que deba tomarse a la ligera en este ambiente, ya que, al existir una transparencia de registros, conocer las transacciones y las criptomonedas que una persona real posee, podría ponerla en riesgo de ataques fuera del mundo virtual. Si bien es un hecho que muchos usuarios pretendan escapar a controles de instituciones formales, es importante considerar que el anonimato permite protegerlos de amenazas en la vida real.

A partir de estos riesgos evidentes, uno de los métodos más desarrollados ha sido el de los mixing services o servicios de mezcla, pero la necesidad de confiar en que estos no conserven registros de las transacciones y que no exijan un registro de identidad, no los hace del todo eficaces. Además, suelen tener costos, lo que los hace menos atractivos: el mayor anonimato pasa a ser un costo más. Incluso un servicio de mezcla en serie no puede considerarse del todo eficaz si las cantidades arrojasen ciertos patrones que pudieran permitir su rastreabilidad. Por otro lado, los servicios de mezcla poseen una mala reputación por pérdidas de criptomonedas que han sucedido en el pasado. Sumado a esto, si los montos que manejan fueran relativamente elevados, podrían verse más tentados de realizar un fraude. Además, la mayoría de estos servicios movilizan bajos volúmenes y, en consecuencia, poco anonimato.

Otro método que se ha desarrollado es el del coinjoin, un servicio de mezcla descentralizado, con múltiples entradas de diferentes direcciones y con firmas independientes entre sí. Sin embargo, esta técnica tampoco es tan popular y acarrea la necesidad de cierta "prolijidad" en el procedimiento para evitar inconvenientes.

Frente a estos riesgos y estas no muy eficientes propuestas para mitigarlos, los desarrolladores han buscado nuevas formas de atacar este problema que, lógicamente, al principio fue más evidente con Bitcoin. Con el correr del tiempo y los avances tecnológicos, estos riesgos fueron tomando mayor relevancia y, de ser solo un riesgo, pasaron a ser un problema real. Tal como indica el blog FixedFloat "*En los primeros años de la red Bitcoin, la criptomoneda se consideraba completamente anónima. Sin embargo, con el tiempo, los técnicos han aprendido a rastrear y desanonimizar las transacciones de Bitcoin*"[27]. En consecuencia, se tomó conciencia de que el anonimato no era absoluto y varios años después de la aparición de Bitcoin, han surgido altcoins dirigidas a ofrecer un mayor grado de anonimato y privacidad. Así lo señala también Jackeline Rivero, columnista de Criptonoticias.com, cuando escribió

[27] FixedFloat Blog, "Anonimato de las criptomonedas", 2020, (En línea) Disponible en: https://fixedfloat.com/es/blog/guides/anonymity-of-crypto (Recuperado en fecha 17/02/2021)

que "*Se ha demostrado que las compañías de análisis u otras partes interesadas cuentan con mecanismos para agrupar direcciones y vincularlas a direcciones IP y otras formas de identificación. Ante esta realidad, en el ecosistema comenzaron a surgir criptomonedas alternativas enfocadas en mantener la confidencialidad de la información de los participantes de su red*"[28]. Y las criptomonedas que mejor supieron aprovechar este problema que fue creciendo para Bitcoin fueron principalmente tres: Dash, Zcash y Monero. Las tres se encuentran dentro del selecto grupo que cuenta con un MarketCap superior a los 500 millones de dólares.

La primera, Dash, utiliza el método coinjoin, solo que, a diferencia de Bitcoin, la funcionalidad se encuentra integrada en su protocolo. Así, Dash consigue un mayor anonimato y una mayor confiabilidad que los mezcladores privados que existen para Bitcoin.

En cuanto a Zcash, esta utiliza un protocolo de conocimiento cero, mediante dos direcciones, una protegida por el protocolo de evidencia de divulgación cero y otra de código abierto como Bitcoin. Esto, si bien pierde anonimato cuando la dirección de código abierto es utilizada, guarda un mayor grado de anonimato que Bitcoin.

Por último, Monero es considerada por muchos la criptomoneda con mayor nivel de anonimato. Monero es ampliamente superior a Bitcoin en lo que a anonimato e irrastreabilidad se refiere. Mediante un protocolo CryptoNote, no permite conocer el remitente, el destinatario, ni la cantidad que se ha enviado en la transacción. Utiliza direcciones ocultas y firma de anillo o ring signature, sin dudas, la funcionalidad que vuelve a Monero tan especial. Tal como indica la página oficial de esta criptomoneda, "*Las ring signatures son adecuadas para esta aplicación porque no se puede revocar el anonimato de una firma de anillo y porque el grupo requerido para una firma de anillo se puede improvisar (no necesita de una configuración previa)*"[29].

La Blockchain: La Blockchain de las criptomonedas puede que sea la característica más importante de las mismas. Es común entre los criptoactivos, pero puede tener variaciones que vuelvan más o menos atractivas a las criptomonedas. La Blockchain de una criptomoneda puede hacerla muy diferente de otras. Por esto, es importante destacar que los especialistas suelen hacer dos clasificaciones respecto de la Blockchain que, en muchos casos, se tornan difusas y sus límites no se hallan claramente delineados.

[28] Jackeline Rivero, "¿Privadas o anónimas? Estas son las principales criptomonedas centradas en la confidencialidad", 2018, (En línea) Disponible en: https://www.criptonoticias.com/educacion/criptomonedas-confidencialidad-privacidad-anonimato (Recuperado en fecha 17/02/2021)

[29] Página Oficial de Monero, "Ring Signature", Traducido, (En línea) Disponible en: https://www.getmonero.org/resources/moneropedia/ringsignatures.html (Recuperado en fecha 17/02/2021)

La primera clasificación es entre Blockchain pública y Blockchain privada. Existen discrepancias entre quienes se mantienen atentos al mundo de las criptomonedas respecto de cuándo una Blockchain es pública o privada. Por ello, suelen tomarse distintos factores y ponderarlos para definirlo, entre los que destacan dos.

El primer factor tiene que ver con la posibilidad de unirse y participar en la red. Esto incluye la posibilidad de modificar partes de la misma, minar y validar bloques, siempre de acuerdo con las reglas del sistema.

El segundo factor responde al nivel de transparencia. Puede ser que un usuario no tenga la posibilidad de modificar aspectos de la red, pero sí tener acceso al *ledger* y poder conocer las transacciones registradas. No obstante, también puede existir un nivel de confidencialidad muy alto que solo permita el acceso a un conjunto determinado de usuarios.

Al existir tantas posibilidades en cuanto a la graduación de estos dos factores y al ser subjetiva la ponderación que cada usuario le pueda dar a cada factor, se torna complejo establecer en ciertos casos si una criptomoneda posee una Blockchain pública o privada.

La segunda clasificación es entre Blockchain centralizada y descentralizada. Nuevamente, distintos factores intervienen a la hora de definir si una Blockchain es más o menos centralizada y, en este caso, tampoco hay una postura única sobre qué patrones son los más determinantes. Sin embargo, hay dos factores que destacan.

El primer factor es la gobernanza. Depende de la fuerza de decisión que los nodos tengan sobre las partes de la red e incluso sobre el protocolo del sistema. La existencia de jerarquías entre nodos puede ir en desmedro de la descentralización y dirigir la Blockchain hacia una centralización en los nodos dominantes.

El segundo factor es la cantidad de nodos mineros que existan en la red y la posibilidad de que nuevos mineros puedan integrarse a la red. En este sentido, existe una cierta relación con las Blockchain públicas, el libre acceso de mineros torna más pública a la red y también la hace más descentralizada.

A menudo, también se incorpora una tercera rama en esta clasificación: la distribuida. Sin embargo, para los usuarios de las criptomonedas, la diferencia entre una Blockchain distribuida y descentralizada no suele ser considerada de gran significatividad.

Lo cierto es que no existe un consenso pleno de la doctrina al respecto de estas clasificaciones, e incluso a veces se tiende a pensar en “público” como sinónimo de “descentralizado” y “privado” como

sinónimo de "centralizado". Pero la falta de una postura definida no implica que los usuarios de las criptomonedas no presten atención en algún momento a las características de las Blockchain para preferir una por sobre otra.

Emisión "criptomonetaria": La política de emisión de criptomonedas varía de acuerdo al protocolo de cada una. Este aspecto impacta directamente en el precio de una criptomoneda. La mayoría de los protocolos de criptomonedas fija la forma de emisión, tanto en procedimientos a utilizar como en cantidades del circulante a emitir. Por ejemplo, para el caso de Bitcoin, se crean nuevas unidades a partir del minado y validación de cada nuevo bloque en la cadena y, además, tiene una emisión finita, tal como el columnista de Xataca.com, Alejandro Nieto, declara: "*Una de las propiedades más curiosas de Bitcoin es que el número máximo de monedas que se pueden crear está definido: 21 millones de Bitcoin*"[30]. Es decir, Bitcoin, al igual que muchas otras criptomonedas, tiene una emisión preestablecida en su Whitepaper. A este tipo de emisión se la suele denominar "programada" o "determinada". A pesar de esta emisión preestablecida, el precio de Bitcoin y de la mayoría de las criptomonedas que comparten esta característica posee una gran volatilidad, lo cual puede transformarse en algo indeseable para muchos actores del mercado. Esta alta volatilidad ha propiciado la creación de otro tipo de criptomonedas: las stablecoins. Las stablecoins reducen al mínimo la volatilidad en su cotización. Fueron creadas con ese objetivo: mantener un precio estable. Para lograrlo, tienen una política de emisión orientada a mantener una paridad constante con otras monedas, en general, la moneda elegida es el dólar estadounidense.

De esta manera, algunos agentes del mercado optan por la estabilidad de una criptomoneda como Tether (USDT) o DAI (DAI), mientras que a otros les resulta más atractiva la volatilidad que Bitcoin y otras altcoins poseen y los potenciales réditos especulativos que esto puede ofrecer.

Internet of things (IoT): Esta cualidad es distintiva de la criptomoneda IOTA (MIOTA) y ha llamado la atención especialmente importantes empresas interesadas en la Internet of Things. Ofrece no solo la posibilidad de micropagos, sino también una alternativa a la Blockchain intentando resolver problemas de escalabilidad y la necesaria presencia de mineros. Es una cualidad que ha despertado interés por su conexión con elementos de la vida cotidiana y que ha ubicado a IOTA entre una de las criptomonedas con mayor MarketCap, incluso con la disonancia que guarda respecto del resto de las criptomonedas de fuerte capitalización en el mercado.

[30] Alejandro Nieto, "El número de bitcoins es finito, no podrá haber más de 21 millones: ¿qué se espera que suceda entonces?", 2017, (En línea) Disponible en: https://www.xataka.com/criptomonedas/el-numero-de-bitcoins-es-finito-no-podra-haber-mas-de-21-millones-que-se-espera-que-suceda-entonces (Recuperado en fecha 17/02/2021)

Así como el caso de IOTA, existen muchos otros proyectos en el mercado que cuentan con criptomonedas propias. Desde 2015 han surgido numerosos proyectos que han ido captando el interés de los inversores. Algunos con más sustento que otros, pero casi todos vinculados a una criptomoneda o *token* propios. Más tarde, esas criptomonedas han salido a cotizar en el mercado y principalmente en exchanges.

La cantidad de propiedades es diversa y, en algunos casos, estas propiedades son incompatibles entre sí. Por ejemplo, una emisión controlada para sostener la cotización de una stablecoin, no puede convivir con una emisión preestablecida en un Whitepaper. También puede haber propiedades que una criptomoneda ofrezca con mayor calidad que otras, por ejemplo, el nivel de anonimato. Este menú de opciones y combinaciones de atributos permite el amplio espectro de criptomonedas actual. En consecuencia, es importante ver algunos ejemplos de criptomonedas y sus principales características que las distinguen y las hacen sobresalir entre las demás. Nuevamente, es razonable enfocar la mirada en función del criterio del nivel de MarketCap que posean y no solo en las características endógenas de cada criptomoneda.

Criptomonedas destacadas y con distintos atributos

Dirigir la atención hacia las altcoins y las oportunidades superiores que ofrecen respecto de Bitcoin, permitiría ver que analizar Bitcoin con detenimiento es preponderante para definir si es sustentable en el largo plazo. Frente a la cantidad de alternativas que rodean a Bitcoin, es prudente preguntarse si es la criptomoneda que subsistirá por sobre otros proyectos más ambiciosos, focalizados y más avanzados. Para ejemplificar sobre la cuestión de los atributos que ofrecen las criptomonedas mejor capitalizadas, se exponen cuatro casos:

1. *Monero (XMR)*. Monero es una criptomoneda enfocada principalmente en la privacidad. Tanto es así que dentro de las características que su página web oficial enumera, esta es la primera: "*Monero es la criptomoneda líder con enfoque en transacciones privadas y resistentes a la censura*"[31]. Como ya se ha mencionado, Monero utiliza un sistema totalmente distinto al de Bitcoin y otras altcoins. Sin embargo, lo relevante de poner a Monero como ejemplo es que, si lo que un usuario buscara y valorara fuera el anonimato y la irrastreabilidad de sus transacciones por sobre otras

[31] Página Oficial de Monero, "¿Qué es Monero (XMR)?", Traducido, (En línea) Disponible en: https://www.getmonero.org/es/get-started/what-is-monero (Recuperado en fecha 17/02/2021)

cualidades, es altamente probable que se incline por esta criptomoneda, perdiendo interés en las demás.

2. *Tether (USDT)*. Se trata de una stablecoin. "*Cada unidad de USDT está respaldada por un dólar estadounidense en las reservas de Tether Limited y pueden ser liberados mediante la Plataforma Tether*"[32]. Esta es una gran ventaja frente a la volatilidad. Es decir, si un usuario deseara mantener su capital seguro de la volatilidad que padecen muchas opciones del mercado, entre ellas Bitcoin, la elección que prevalecería sería esta u otra stablecoin, como DAI (DAI) o USD Coin (USDC).

3. *IOTA (MIOTA)*: IOTA es, posiblemente, la mejor representación de lo que es ofrecer un proyecto distinto. Tiene particularidades que la diferencian de Bitcoin. En su caso, ofrece posibilidades superadoras respecto de pagos con tarifa cero, un sistema distinto a la Blockchain (Tangle) y la vinculación con la Internet of Things que lo lleva a un plano de factibilidad superior a otras criptomonedas. Junto con proyectos como de criptomonedas, Ripple (XRP), Polkadot (DOT), entre otros, IOTA es una alternativa por la que un inversor podría sentirse más seducido.

4. *Bitcoin Cash (BCH)*. Similar a Bitcoin, pero con una diferencia que probablemente sea primordial en el mediano plazo: apunta a un nivel de escalabilidad mucho más elevado que el de Bitcoin. Si la cuestión de la escalabilidad de Bitcoin se convirtiera en un problema con consecuencias en su red, los usuarios podrían elegir una criptomoneda similar que no contara con esta dificultad. De todas formas, se debe considerar que BCH es menos democrática, dado que instalar un nodo de esta criptomoneda requiere mayor escala.

La mayoría de las criptomonedas posteriores a Bitcoin han tenido variantes y/o mejoras. Vistas estas interesantes y superadoras alternativas que estas criptomonedas ofrecen, es inevitable enforcarse en la criptomoneda de mayor capitalización: Bitcoin. Su hegemonía se basa principalmente en su posición de haber sido la criptomoneda pionera, la primera en ser creada. Pero existiendo altcoins con atributos superiores y proyectos tan diversos y ambiciosos, resulta interesante analizar si Bitcoin tiene lo necesario para no perder esa hegemonía o, incluso, para subsistir en el largo plazo.

[32] MarketCap.com, "Tether", Traducido, (En línea) Disponible en: https://marketcap.com/coin/USDT (Recuperado en fecha 27/02/2021)

Bitcoin

La primera criptomoneda fue Bitcoin. Fue el principio de la revolución que las criptomonedas han generado en el mercado financiero global y es prudente observarlo desde sus aspectos más elementales: las características que su creador, Satoshi Nakamoto, enunció en su Whitepaper. Estas características pueden ser interpretadas como fortalezas o, en ese momento, incluso como solo oportunidades.

En el abstract e introducción de su Whitepaper, Nakamoto enuncia diferentes fortalezas de su "Sistema de Efectivo Electrónico Usuario-a-Usuario". Entre estas fortalezas se encuentran la descentralización y la confiabilidad. Si bien no las enuncia de manera taxativa, hace referencia a ellas de otro modo. En primer lugar, refiere a las virtudes de la descentralización de los nodos que conforman la red y del valor de la Prueba de Trabajo; Nakamoto indica que "*Los mensajes son enviados bajo la base de mejor esfuerzo, y los nodos pueden irse y volver a unirse a la red como les parezca, aceptando la cadena de prueba de trabajo de lo que sucedió durante su ausencia*"[33]. En segundo lugar, está la confiabilidad que su sistema provee, sin la necesidad de un tercero confiable como ocurría hasta ese momento; el autor así lo señala cuando escribe que "*Lo que se necesita es un sistema de pagos electrónicos basado en pruebas criptográficas, en vez de confianza, permitiéndole a dos partes interesadas en realizar transacciones directamente sin la necesidad de un tercero confiable*"[34]. Vale aclarar que esta confianza propia de su sistema se basa también en la irreversibilidad de las transacciones que se añaden a la cadena de bloques. A su vez, la irreversibilidad conlleva una propiedad más: Bitcoin no es censurable.

Estas propiedades que Nakamoto establece en el abstract y en la introducción del Whitepaper de Bitcoin y que luego explica en el resto del documento, son las principales ventajas endógenas de Bitcoin. Sin embargo, también puede interpretarse que estas ventajas no son solo de Bitcoin, sino de cualquier criptomoneda con similares características que hubiese surgido con posterioridad. Esta interpretación puede hacerse por una simple razón: estas fortalezas no son de Bitcoin, sino de la Blockchain.

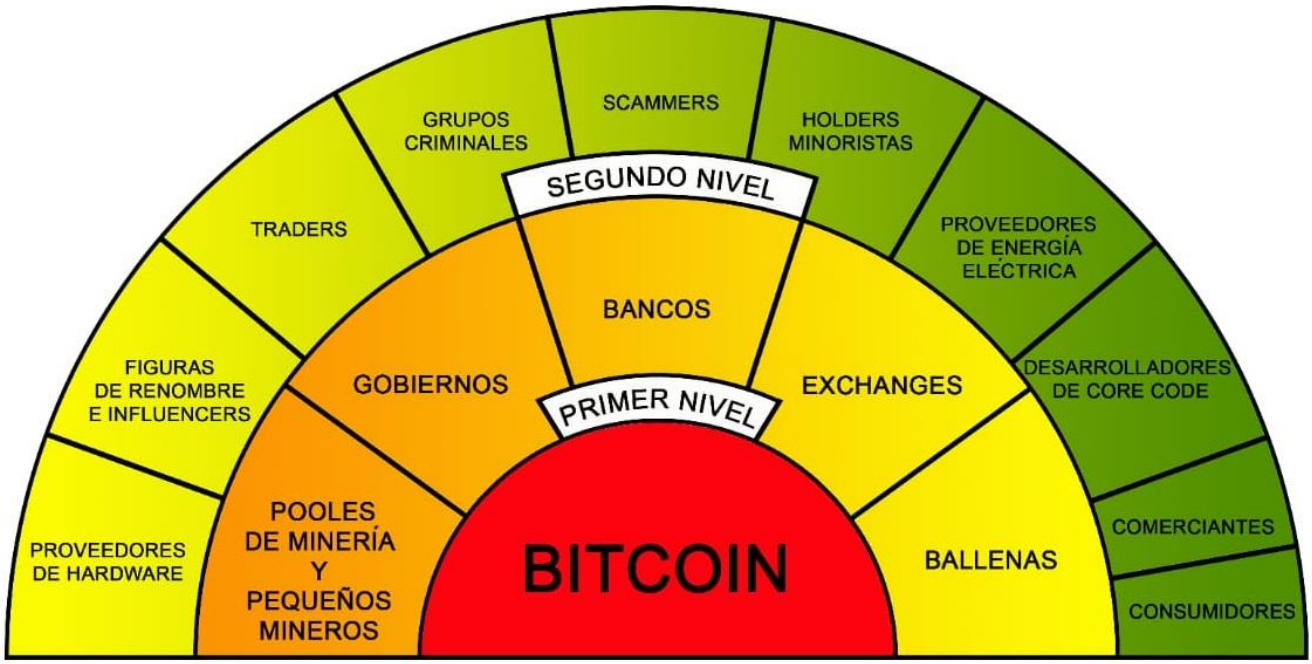
Una fortaleza fundamental que Nakamoto menciona después y a la cual le dedica un capítulo completo es el anonimato. En el capítulo 10 del Whitepaper de Bitcoin, Nakamoto profundiza sobre la idea de la privacidad en el contexto de un sistema en el que la transparencia abunda: "*El público puede ver que alguien está enviando una cantidad a otra persona, pero sin información que relacione la transacción a ninguna persona*"[35]. Sin embargo, nuevamente, al tratarse de una cualidad de la Blockchain,

[33] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Traducido, (En línea) Disponible en: https://bitcoin.org/bitcoin.pdf (Recuperado en fecha 27/02/2021)
[34] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Traducido, (En línea) Disponible en: https://bitcoin.org/bitcoin.pdf (Recuperado en fecha 27/02/2021)
[35] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Traducido, (En línea) Disponible en: https://bitcoin.org/bitcoin.pdf (Recuperado en fecha 27/02/2021)

Bitcoin se ve, al menos, en igualdad de condiciones frente a otras criptomonedas surgidas en los años subsiguientes basadas en la cadena de bloques.

A pesar de estas fortalezas que son más propias de Blockchain y del inmenso potencial que se ha descripto anteriormente, para realmente analizar si la hegemonía de Bitcoin perdurará en el tiempo es necesario enumerar las amenazas y debilidades que lo rodean y que podrían determinar su destino. Sin embargo, previo a enumerar amenazas y debilidades de Bitcoin, es provechoso describir un contexto mediante la distinción de los stakeholders que existen a su alrededor.

Muchos actores rodean a Bitcoin, pero no todos tienen el mismo nivel de importancia. Su participación y su nivel de influencia sobre Bitcoin es tan dispar como dinámico, dado que ciertos stakeholders que en un momento tuvieron roles no tan preponderantes, luego han logrado influir significativamente en el ecosistema de esta criptomoneda. Por lo tanto, se debe entender a cada stakeholder por las causas de su importancia en el sistema, pero considerando siempre que su rol puede modificarse con el tiempo. Una aproximación al mapa de stakeholders actual de Bitcoin podría ser el del siguiente cuadro:



Cuadro 2.1. Stakeholders de Bitcoin. Fuente de elaboración propia con base en "Bitcoin Stakeholders", (En línea) Disponible en: https://www.stakeholdermap.com/bitcoin-stakeholders.html (Recuperado en fecha 03/03/2021)

PRIMER NIVEL

- *Grandes pooles de minería y pequeños mineros*: Son los encargados de la creación de nuevos Bitcoin y, especialmente, de validar las transacciones y los bloques que serán añadidos a la

Blockchain. Son actores imprescindibles y permanentes, dado que, sin su existencia, la red no podría funcionar.

- *Gobiernos*: Con el tiempo han ido sumando injerencia e influencia sobre las criptomonedas en general, pero sobre Bitcoin en especial. Cada gobierno ha puesto su mirada en Bitcoin en mayor o menor medida según el caso. Su injerencia se presenta desde distintos organismos y con distintos fines:
    - *Instituciones judiciales*: Intervienen en disputas que involucran a las criptomonedas y sientan jurisprudencia que, deseada o no, van marcando un camino para diferentes situaciones.
    - *Entes recaudadores*: Las administraciones han notado que Bitcoin escapa a su alcance y les dificulta gravarlo con impuestos. Por eso y por el creciente nivel de capitalización de las criptomonedas, las administraciones recaudadoras de los gobiernos posan su mirada cada vez con mayor atención en los criptoactivos.
    - *Bancos centrales*: Una moneda descentralizada que no permite a los gobiernos controlar la cantidad de circulante (política monetaria) ni las ventajas que este control ofrece, es un problema que tiene a los bancos centrales analizando el nuevo escenario. Y muchos de ellos se encuentran con intenciones serias de lanzar su propia moneda digital al mercado (CBDC – *Central Bank Digital Currency*)
    - *Organismos legislativos*: Las legislaciones de los países han comenzado a intentar legislar las criptomonedas y son muchos los aspectos que deben tratar, no solo socioeconómicos, sino también penales, debido al financiamiento del crimen y terrorismo que las criptomonedas facilitan.
- *Bancos*: Están siempre expectantes frente a las regulaciones que los gobiernos pueden implementar, pero también mantienen la atención en las oportunidades de negocio que Bitcoin puede brindar. Muchos ofrecen servicios relacionados.
- *Exchanges*: Son grandes ganadores dentro del sistema. Facilitan el acceso a las criptomonedas para los usuarios comunes y su participación ha ido incrementando a gran velocidad.
- *Ballenas (Whales)*: Son los tenedores de gran cantidad de Bitcoin. Tienen una fuerte influencia sobre las expectativas del mercado hacia Bitcoin, que se refleja en su precio cuando estos tenedores realizan transacciones de alto volumen.

SEGUNDO NIVEL

- *Proveedores de Hardware*: Estos proveedores no solo han generado enormes ganancias con la venta de equipos, sino que, además, son imprescindibles para el minado de Bitcoin. Muchas empresas han incluso desarrollado y perfeccionado hardware específico para el trabajo de minería de Bitcoin con el objeto de incrementar el poder de minado. Esta situación ha derivado en un constante incremento de desperdicios por obsolescencia. Un caso particular es el de la empresa NVIDIA, que tuvo un crecimiento abrupto a partir de la fiebre de la minería.
- *Figuras de renombre e influencers*: Personas con peso en los mercados como Elon Musk, Warren Buffet, Jack Dorsey, entre tantos otros, han opinado en favor y en contra de las criptomonedas. Su opinión, favorable o negativa, ejerce influencia sobre las criptomonedas y su mercado. El precio y la capitalización de Bitcoin, en especial, suelen tener fluctuaciones bruscas cuando una de estas personalidades hace pública su opinión en la materia.
- *Traders*: Son agentes del mercado que operan en busca de ganancias en el corto plazo, mediante compras a precios inferiores a los que luego venderán las criptomonedas. La gran volatilidad de Bitcoin torna sumamente fructíferas las acciones de estos agentes especuladores. Sus operaciones influyen en el precio de Bitcoin, sin embargo, su injerencia no es tan determinante como el de las ballenas.
- *Grupos criminales*: Las criptomonedas han favorecido al financiamiento de grupos criminales. El anonimato que Bitcoin proporciona ha sido una ventaja para criminales y terroristas. En cierta medida, el dinero en efectivo cuenta con ese anonimato y dificultad de trazabilidad que las operaciones ilegales necesitan, pero Bitcoin tiene una ventaja accesoria: no requiere ser transportado físicamente. Por ello, este tipo de organizaciones continúan teniendo interés en Bitcoin.
- *Scammers*: Podría incluirse a los scammers dentro del grupo de criminales, pero su participación tiene una distinción. Mientras que muchas organizaciones criminales y terroristas se financian para perpetrar hechos con consecuencias muy destructivas, los scammers son estafadores que crean artilugios para conseguir dinero y que vieron en Bitcoin un canal ideal para operar sin ser identificados.
- *Holders minoristas*: Tienen una participación menor, son inversores a mediano y largo plazo. Su influencia sobre las fluctuaciones de cotización y capitalización de mercado de Bitcoin no es tan significativa.

- *Proveedores de energía eléctrica*: La energía eléctrica necesaria para la minería ha aumentado desde la creación de Bitcoin, tanto que hoy es un problema dentro del análisis de costos que repercute en el precio de la criptomoneda. Es dable destacar que de forma paulatina también se ha convertido en una cuestión medioambiental a considerar.
- *Desarrolladores del CoreCode*: Fueron fundamentales para dar vida a Bitcoin. Actualmente, y aun cuando se desconoce la identidad del verdadero creador de Bitcoin, su importancia respecto de la influencia que pudiera tener sobre la red de Bitcoin es mucho menor. Asimismo, los protocolos de Bitcoin difícilmente se modifiquen a futuro, dada la necesidad del consenso de toda la red que, en este tema, no ha tenido suficiencia.
- *Comerciantes*: Conforman uno de los grupos más numerosos del mapa de stakeholders. Actualmente, los comerciantes que aceptan criptomonedas son relativamente muy pocos, incluso con Bitcoin posicionándose como la primera opción entre todas ellas.
- *Consumidores*: Es el grupo con mayor número de agentes, la gran mayoría, potenciales. A pesar de que se ha extendido el uso entre los consumidores, ocurre algo similar que con los comerciantes: el uso de Bitcoin como medio de pago es relativamente insignificante.

Teniendo presente el mapa de los stakeholders que rodean a Bitcoin, resulta más sencillo adentrarse en el análisis de sus amenazas y debilidades. Es conveniente analizar estas amenazas y debilidades en forma organizada, dado que algunas derivan de otras y existe interconexión entre ellas. Por lo tanto, para seguir un camino lo más nítido posible, las amenazas y debilidades se pueden observar desde cinco enfoques.

Primero, debe considerarse un enfoque técnico para analizar distintos problemas inherentes a Bitcoin, como su restringida escalabilidad o su vulnerabilidad frente a ataques del 51% o de Denegación de Servicio (DoS).

En segundo lugar, conviene estudiar un enfoque desde la descentralización de Bitcoin, cualidad que comparte con la gran mayoría de altcoins. Es prudente identificar las ventajas y las desventajas de una red descentralizada y ponderar si la descentralización es tal, cuando existe una fuerte concentración del poder de minado (*pooles* de minería) y de las tenencias de la criptomoneda (ballenas).

En tercer lugar, aparecen factores externos a Bitcoin que lo amenazan. La injerencia de los gobiernos se ha vuelto un factor que aún no ha repercutido en las criptomonedas de manera contundente. En general, los gobiernos se han mantenido en alerta y observan la mejor forma de regular Bitcoin por

diferentes cuestiones: evitar crímenes, recaudar impuestos, tener una normativa clara en un tipo de activo que es nuevo y revolucionario.

En cuarto término, existe un enfoque económico y financiero que es necesario analizar. Bitcoin es el criptoactivo más popular, pero no deja de ser eso: un activo. Por lo tanto, es importante analizar si es económicamente viable su subsistencia y si lo será en calidad de dinero, para su mero atesoramiento o como inversión.

Por último, es interesante ver las consecuencias medioambientales que Bitcoin genera y que pueden acrecentarse en el mediano plazo. No suele prestarse la suficiente atención al medioambiente cuando se analizan activos financieros. Su consideración es menor a la que debería tenerse, pero es justo que en este tema se analicen los efectos de los grandes centros mineros de Bitcoin, la energía que requiere la red para funcionar y ponderar los niveles de su huella de carbono.

CAPÍTULO 3. Las dificultades técnicas de Bitcoin

La tecnología Blockchain y la criptografía han dotado a Bitcoin de fortalezas técnicas novedosas y difíciles de violentar. No obstante, existe una variedad de ataques a los que las criptomonedas se encuentran expuestos y, entre estas, Bitcoin corre con desventaja frente a muchas altcoins. En primer lugar, Bitcoin se irgue como el principal objetivo de ataques cibernéticos por su popularidad y por el desafío que representa, para ciertos grupos, hacer caer un sistema en apariencia perfecto. Y, en segundo lugar, su cotización en el mercado y el dinero que moviliza lo hacen atractivo para quienes codician obtener una recompensa mediante ataques a sus puntos débiles. Entro los interesados en que Bitcoin caiga, también puede incluirse a grupos más poderosos como gobiernos o entidades supranacionales, dada la falta de control que Bitcoin implica por su naturaleza descentralizada.

Sin importar el nombre de los interesados en vulnerar la seguridad de Bitcoin o los motivos por los cuales pudieran actuar, la posibilidad se encuentra latente. Por esto, es importante relevar los distintos tipos de ataques a los que Bitcoin está expuesto y que podrían provocar su colapso.

Ataque del 51%

Tanto en un ataque DoS como en un ataque Sybil, si una persona o un grupo asociado alcanzara a controlar el 51% de la red, las consecuencias podrían ser nocivas para todo el sistema. Esto se debería a que "*Son mayoría y como tal pueden reescribir o incluso realizar un ataque DoS sobre la red*"[36], según el sitio bit2me Academy. Es decir, tener el control del 51% de los nodos, permitiría al atacante modificar los registros de la Blockchain y quedarse con las recompensas de la minería. Este resultado sería verdaderamente catastrófico y el peor de los escenarios posibles ante un ataque a Bitcoin y su Blockchain. Sin embargo, también es cierto que Bitcoin posee la ventaja de tener la red con mayor cantidad de nodos, lo que dificulta la posibilidad de que un ataque así se concrete. Partiendo de que está situación representaría el colapso de Bitcoin y que, a su vez, es sumamente improbable, se pueden analizar otros ataques no tan nocivos, pero más probables.

Ataques de DoS (Denial of Service)

El mencionado ataque de Denegación de Servicio es definido por el sitio Binance Academy de la empresa Binance.com como "*…un método utilizado para interrumpir el acceso de los usuarios legítimos*

[36] Bit2me Academy, "¿Qué es un Ataque del 51%?", (En línea) Disponible en: https://academy.bit2me.com/que-es-un-ataque-del-51 (Recuperado en fecha 10/03/2021)

a una red de destino o recurso web. Por lo general, esto se logra mediante la sobrecarga del objetivo (a menudo un servidor web) con una enorme cantidad de tráfico, o mediante el envío de peticiones maliciosas que provocan el recurso de destino al mal funcionamiento o bloquearse por completo"[37], pero afirma, de forma acertada, que "*…el aspecto descentralizado de blockchains crea una fuerte protección contra DDoS y otros ataques cibernéticos*"[38]. Esto es así porque la red descentralizada y las fuertes características de inmutabilidad de la Blockchain permiten que, si un usuario o grupo de usuarios quedara temporalmente fuera de servicio, podría recuperar copias de la cadena de bloques cuando logren restablecer su conexión a la red.

Entonces, los distintos tipos de ataque DoS son inútiles, en principio contra una red descentralizada, en especial, si no consiguen realizar un ataque del 51%. Sin embargo, un estudio de investigadores del Cornell Tech y el Technion Israel Institute of Technology ha revelado un tipo de ataque de Denegación de Servicio mucho más eficaz contra una Blockchain que los ataques tradicionales de este tipo. El estudio se enfocó sobre la Blockchain de Bitcoin.

El denominado BDoS (Blockchain Denial of Service) se explica brevemente como un ataque que requeriría el control de tan solo el 21% de los nodos de la red de Bitcoin para apoderarse de la toma de decisiones dentro de la red. De acuerdo con el estudio, "*…un atacante con 21% del poder de minado puede exitosamente detener a todos los mineros 'racionales'*"[39]. En el estudio, los investigadores analizaron las posibles caídas en los márgenes de ganancia de los mineros al producirse un ataque semejante. Mediante distintas fórmulas estimaron que controlando el 21% del *hashrate*, se desalentaría a mineros "racionales" de seguir minando Bitcoin. Analizaron los rendimientos relativos en el equilibrio de Nash con un rango de variables y "*La simulación indica que hay un amplio rango de valores del factor de rentabilidad que permiten que un BDoS cause una desaceleración significativa en la práctica*"[40]. El mecanismo es simple: el atacante intenta demostrar una superioridad operativa respecto de otros mineros y provocar que una determinada cantidad de mineros abandonen su trabajo, incrementando la participación porcentual del atacante en la red. Los cálculos matemáticos realizados por el equipo de investigación se

[37] Binance Academy, "¿Qué es un ataque DoS?", (En línea) Disponible en: https://academy.binance.com/es/articles/what-is-a-dos-attack (Recuperado en fecha 10/03/2021)
[38] Binance Academy, "¿Qué es un ataque DoS?", (En línea) Disponible en: https://academy.binance.com/es/articles/what-is-a-dos-attack (Recuperado en fecha 10/03/2021)
[39] Michael Mirkin, Yan Ji, Jonathan Pang, Ariah Klages-Mundt, Ittay Eyal y Ari Juels, "BDoS: Blockchain Denial-of-Service", 2020, Traducido, (En línea) Disponible en: https://arxiv.org/ftp/arxiv/papers/1912/1912.07497.pdf (Recuperado en fecha 10/03/2021), p. 2.
[40] Michael Mirkin, Yan Ji, Jonathan Pang, Ariah Klages-Mundt, Ittay Eyal y Ari Juels, "BDoS: Blockchain Denial-of-Service", 2020, Traducido, (En línea) Disponible en: https://arxiv.org/ftp/arxiv/papers/1912/1912.07497.pdf (Recuperado en fecha 10/03/2021), p. 12.

orientaron a estimar el porcentaje necesario para que el comportamiento de la red en su conjunta tienda a esto, siendo 21% el resultado.

En contraposición con el tradicional ataque del 51%, este nuevo porcentaje resulta mucho más alcanzable para los atacantes y factible en la realidad. Si bien se trata de una menor cantidad de nodos, continúa siendo un número elevado, pero esto no implica que deje de ser un riesgo latente para Bitcoin.

Ataques Sybil

Un ataque Sybil es "*…un tipo de hacking que tiene lugar cuando un sistema de criptomonedas resulta vulnerado por algún ente virtual que cuenta con la capacidad de controlar más de una identidad en una misma red*"[41]. Cabe mencionar que, para el caso de Bitcoin, los nodos serían las identidades que el ataque busca controlar. En una red descentralizada como Bitcoin, un ataque Sybil sobre una cantidad distinta a la de un ataque del 51% no tendría graves implicancias en cuanto a la modificación de la cadena de bloques. Sin embargo, tal como afirma el sitio bit2me Academy "*…un ataque Sybil también puede controlar el flujo de información en la red. Así, por ejemplo, un ataque Sybil en Bitcoin puede servir para obtener información sobre las direcciones IP de los usuarios que se conectan a la red. Esto es una situación que pone en riesgo la seguridad, privacidad y anonimato de los usuarios de la red*"[42]. Por lo tanto, es poco probable que la Blockchain de Bitcoin corra peligro ante un ataque Sybil, mas los usuarios de la red corren el riesgo de perder su privacidad y su anonimato. Como se ha mencionado, la pérdida de estos elementos fundamentales para Bitcoin podría desalentar su uso.

Además del posible robo de información personal de usuarios, puede existir la posibilidad de que el atacante realice propuestas riesgosas para la red. No obstante, esta posibilidad no es tan factible, dado que una propuesta que sea evidentemente riesgosa para la red, enseguida sería rechazada y pondría de manifiesto que algo anda mal con el nodo que la propone y con los que la apoyan, dejando al descubierto el ataque.

Otro riesgo de estos ataques es la censura de opiniones. Según Alexander Ramires de la página web Criptogaceta.com "*La censura se establece a partir de que con sus múltiples identidades* (el atacante) *puede cuestionar los juicios y opiniones ajenos. Y al sentenciarlos como algo incorrecto puede lograr que*

[41] Alexander Ramires, "Aprende sobre el ataque Sybil y sus riesgos para el Bitcoin", 2020, (En línea) Disponible en: https://criptogaceta.com/aprende/aprende-sobre-el-ataque-sybil-y-sus-riesgos-para-el-bitcoin (Recuperado en fecha 10/03/2021)

[42] Bit2me Academy, "¿Qué es un Ataque Sybil?", (En línea) Disponible en: https://academy.bit2me.com/que-es-un-ataque-sybil (Recuperado en fecha 10/03/2021)

el resto de las personas los vea como algo que hay que evitar a toda costa"[43]. Es decir que, además de robar información sensible como las direcciones IP de los usuarios, el atacante también podría restringir el acceso y uso legítimo de la red a otros nodos honestos.

En 2020, Monero, el desarrollador de la criptomoneda homónima sufrió un intento de ataque Sybil. Ricardo Spagni, antiguo mantenedor líder de Monero "*…aclaró que el ataque fue novedoso, pero ineficiente y fue incapaz de afectar las transacciones sobre cadena en la red de Monero o violar sus mecanismos de privacidad*"[44]. El ataque consistió en intentar correlacionar la dirección IP de un nodo que estaba transmitiendo una transacción. Spagni también advirtió que "*…un ataque Sybil con las características descritas puede afectar a Bitcoin o cualquier otra criptomoneda, como Ethereum, Litecoin, entre otras. Además, el ataque podría ser «menos torpe», más sutiles o más sofisticados si el atacante tuviera más financiamiento*"[45]. El constante desarrollo en seguridad, privacidad y anonimato de Monero logró evitar consecuencias no deseadas para la criptomoneda. Pero la llamada de atención se corrió para otras redes más vulnerables como la de Bitcoin que, de haber recibido un ataque semejante, podrían haber sufrido fuertes daños.

Es evidente que las criptomonedas posteriores a Bitcoin han perfeccionado sus protocolos para evitar este tipo de ataques. En virtud de la característica descentralizada para la toma decisiones, Bitcoin cuenta con dificultades para actualizarse a estos fines y estos desarrollos más avanzados lo han relegado en este sentido. IOTA es otro ejemplo que, como Monero, se ha preocupado por tener avances al respecto de este tipo de amenazas. De acuerdo con Reynaldo Márquez, cronista en Crypto News Flash, la criptomoneda IOTA "*…ha desarrollado un nuevo sistema que le otorgaría una determinada reputación a cada nodo del ecosistema. El nivel de reputación sería medido por la cantidad de Mana que poseen. El mana sería un nuevo token 'sombra', no intercambiable, que se le otorgaría a cada componente después*

[43] Alexander Ramires, "Aprende sobre el ataque Sybil y sus riesgos para el Bitcoin", 2020, (En línea) Disponible en: https://criptogaceta.com/aprende/aprende-sobre-el-ataque-sybil-y-sus-riesgos-para-el-bitcoin (Recuperado en fecha 10/03/2021)
[44] Reynaldo Márquez, "Monero recibe ataque Sybil – Flufflypony advierte a usuarios de Bitcoin", 2020, (En línea) Disponible en: https://www.crypto-news-flash.com/es/monero-recibe-ataque-sybil-flufflypony-advierte-a-usuarios-de-bitcoin (Recuperado en fecha 10/03/2021)
[45] Reynaldo Márquez, "Monero recibe ataque Sybil – Flufflypony advierte a usuarios de Bitcoin", 2020, (En línea) Disponible en: https://www.crypto-news-flash.com/es/monero-recibe-ataque-sybil-flufflypony-advierte-a-usuarios-de-bitcoin (Recuperado en fecha 10/03/2021)

de realizar una tarea determinada"[46]. Sería impensable replicar este procedimiento para Bitcoin por la necesidad del consenso y por la génesis misma de su código.

Los costos de financiamiento de este tipo de ataque pueden ser muy elevados y es el principal motivo por el que se presume que un ataque Sybil es improbable. Sin embargo, el aumento del precio de Bitcoin también acrecienta las posibles recompensas de llevar adelante un ataque de este tipo. Por otro lado, el motivo económico es el más aparente, pero no puede descartarse la posibilidad de otra motivación diferente. En el pasado han ocurrido ataques cibernéticos sin otro motivo más que la malicia o la intención de demostrar la vulnerabilidad del sistema objetivo.

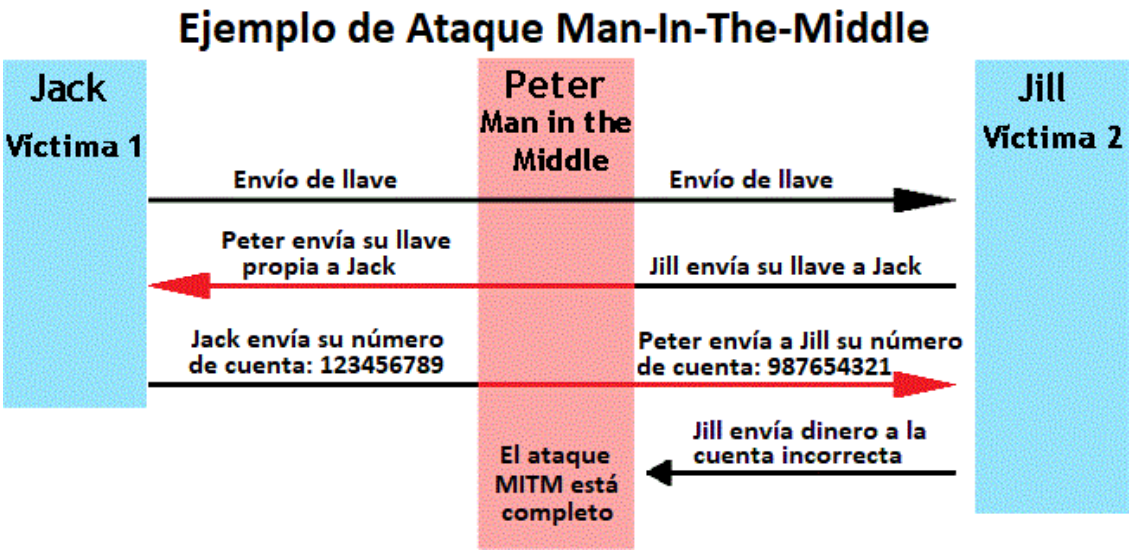
Existe también la posibilidad de que países con grandes recursos pretendan dañar a la red de Bitcoin, por ejemplo, la NSA (National Security Agency) de Estados Unidos o el Centro de Cibercrimen de la Europol de la Unión Europea. Si bien se trata de una posibilidad remota, cuentan con los recursos necesarios para llevar adelante este tipo de ataque y los motivos dependerán de la amenaza que pueda representarles Bitcoin como sistema descentralizado no manipulable a su conveniencia. No obstante, si este tipo de agencias quisiera sabotear Bitcoin y su red, podría hacerlo de una manera más práctica, en función de los recursos a su alcance: un ataque Erebus.

Ataque Erebus

Un ataque Erebus tiene una relación estrecha con el concepto de un ataque MITM (Man In The Middle Attack). En un Ataque MITM, el atacante "*…interrumpe una conversación o una transferencia de datos. Luego de ubicarse en medio de la transferencia, los atacantes aparentan ser ambos participantes. Esto permite al atacante interceptor la información y los datos de cada parte, mientras también envía enlaces maliciosos u otra información a los participantes reales de una manera tal que no pueda ser identificada hasta que es demasiado tarde*"[47]. La definición queda ejemplificada en el siguiente cuadro:

[46] Reynaldo Márquez, "IOTA desarrolla mecanismo de reputación para contrarrestar Ataques Sybil",2019, (En línea) Disponible en: https://www.crypto-news-flash.com/es/iota-desarrolla-mecanismo-de-reputacion-para-contrarrestar-ataques-sybil (Recuperado en fecha 10/03/2021)

[47] Veracode, "Man in the Middle (MITM) Attack", Traducido, (En línea) Disponible en: https://www.veracode.com/security/man-middle-attack (Recuperado en fecha 10/03/2021)

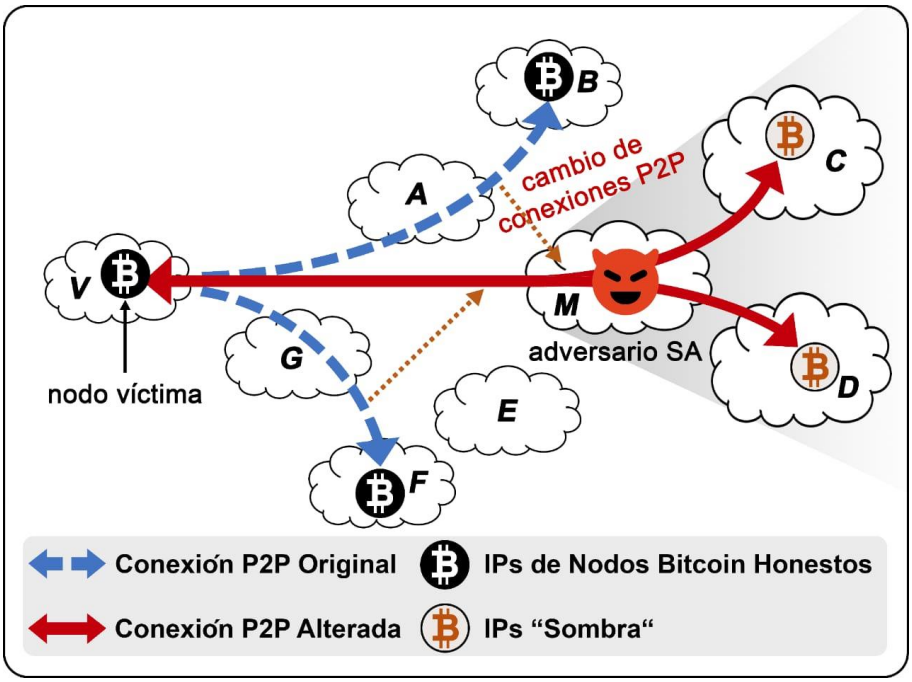


Cuadro 3.1. Ataque MITM. Fuente: Veracode.com, "Man in the Middle (MITM) Attack", Traducido, (En línea) Disponible en: https://www.veracode.com/security/man-middle-attack (Recuperado en fecha 10/03/2021)

Sin embargo, un ataque Erebus tiene una magnitud mucho mayor la de un simple ataque Man In The Middle (Hombre En El Medio). Y a esto se refiere José Maldonado de Observatorio Blockchain cuando escribe que: "*Erebus es más que un simple MITM. Es un ataque masivo de MITM, cuyo objetivo es cortar o redirigir todas las conexiones de la red. El ataque es simple y muy estilizado. Consiste en que el atacante comienza a tomar las conexiones de cada nodo para hacer que las conexiones de ese nodo atacado, terminen siendo manipuladas por el atacante. El atacante seguiría esta iteración hasta tener un grupo importante de la red bajo su dominio*"[48].

Este tipo de ataque fue descubierto por un conjunto de investigadores de la Universidad Nacional de Singapur, de la Universidad de Corea y el Instituto Superior de Ciencia y Tecnología de Japón. Fueron ellos quienes denominaron "Erebus" a este tipo de ataque. En su trabajo, realizaron una representación gráfica del ataque:

[48] José Maldonado, "Erebus, el arma de los poderosos para derribar Bitcoin y otras criptomonedas", 2020, (En línea) Disponible en: https://observatorioblockchain.com/criptomonedas/erebus-el-arma-de-los-poderosos-para-derribar-bitcoin-y-otras-criptomonedas/?utm_source=rss&utm_medium=rss&utm_campaign=erebus-el-arma-de-los-poderosos-para-derribar-bitcoin-y-otras-criptomonedas (Recuperado en fecha 12/03/2021)



Cuadro 3.2. Ataque Erebus. Fuente: Muoi Tran, Inho Choi, Gi Jun Moon, Anh V. Vu y Min Suk Kang, "A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network", Traducido, (En línea) Disponible en: https://www.comp.nus.edu.sg/~kangms/papers/erebus-attack.pdf (Recuperado en fecha 12/03/2021), p. 2

En el cuadro se ve cómo un sistema autónomo malicioso (SA) "M" indirectamente modifica todas las conexiones P2P del nodo que es víctima del ataque ("nodo "V") con otros nodos escogidos por el atacante para posicionarse justo en medio de ellos. Los investigadores aclaran que "*este Ataque no require de ninguna manipulación (por ejemplo: hijacking BGP paths) haciéndose indetectables para los sistemas de control de anomalías planos*"[49].

Basándose en el trabajo de los investigadores, Maldonado también explica que Bitcoin y su estructura Peer-to-Peer son un blanco ideal para un ataque de estas características: "*Es precisamente la IP y la estructura P2P de Bitcoin lo que habilita que Erebus sea tan peligroso para Bitcoin. Cada nodo en la red tiene una IP y conociendo los mismos se puede plantear un MITM masivo que derribe los canales de comunicación de Bitcoin, dejando a la red inoperativa. Si lo deseasen, Erebus podría ser el botón de apagado que los poderosos podrían usar para apagar Bitcoin*"[50]. En este punto, es destacable notar que

[49] Muoi Tran, Inho Choi, Gi Jun Moon, Anh V. Vu y Min Suk Kang, "A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network", Traducido, (En línea) Disponible en: https://www.comp.nus.edu.sg/~kangms/papers/erebus-attack.pdf (Recuperado en fecha 12/03/2021), p. 2.

[50] José Maldonado, "Erebus, el arma de los poderosos para derribar Bitcoin y otras criptomonedas", 2020, (En línea) Disponible en: https://observatorioblockchain.com/criptomonedas/erebus-el-arma-de-los-poderosos-para-derribar-bitcoin-y-otras-criptomonedas/?utm_source=rss&utm_medium=rss&utm_campaign=erebus-el-arma-de-los-poderosos-para-derribar-bitcoin-y-otras-criptomonedas (Recuperado en fecha 12/03/2021)

usa la palabra "poderosos" para referirse al perfil del potencial atacante. El poder no siempre implica una proporción directa con el nivel de recursos económicos. Para otro tipo de ataques a Bitcoin como el ataque del 51%, los recursos económicos necesarios serían colosales. No obstante, para un ataque Erebus bastaría con recursos asimilables a los que muchas organizaciones poseen en la actualidad y con el control sobre ciertos elementos de internet. El control de estos elementos es el tipo de poder que Maldonado menciona. Esto se debe a que "*…existen puntos que son tan vitales, que manipularlos haría que millones se queden sin servicio de Internet. (…) En este punto es claro que, Internet es un punto débil en el funcionamiento de la una red de criptomonedas. En especial, si hay alguien que pueda manipular dichas conexiones a bajo nivel, haciendo que la red de criptomonedas no funcione de forma correcta*"[51]

Este tipo de ataque no solo podría afectar a Bitcoin, sino a la mayoría de las criptomonedas basadas en el protocolo Bitcoin. Además, podría ser tremendamente efectivo en países donde haya una concentración de operadores de internet o en países propensos a la manipulación de la información en internet o la restricción de su acceso. Un ataque Erebus es novedoso, surgido de investigaciones recientes, pero puede que sea una de las amenazas a tener más en cuenta dada la falta de preparación y recursos de la red para hacer frente a una situación semejante.

Ataque Replay

Según la compañía especializada en seguridad informática Kapersky, "*Un ataque replay ocurre cuando un hacker espía una comunicación en una red segura, la intercepta, y luego de forma fraudulenta la demora o reenvía para engañar al receptor y que haga lo que el hacker quiere. Un peligro adicional de los ataques replay es que el hacker no precisa de gran pericia para decodificar un mensaje después de capturarlo en la red. El ataque puede ser exitoso simplemente con reenviar todo el paquete*"[52]. Se debe comprender que el atacante intercepta una comunicación y reproduce o repite el mensaje sin descifrarlo. La prescindencia de una decodificación es una ventaja para quien desee efectuar este tipo de ataques.

Las redes Blockchain son particularmente vulnerables a este tipo de ataques cuando se está implementando un *hard fork*. Ocurre que, cuando se realiza este proceso, "*…hay una división entre el protocolo y el libro mayor, y se crean 2 libros mayores regidos por 2 protocolos separados. Así que la*

[51] Bit2 Academy, ¿Qué es un Ataque Erebus?, (En línea) Disponible en: https://academy.bit2me.com/que-es-ataque-erebus (Recuperado en fecha 12/03/2021)
[52] Kapersky Lab, "What Is a Replay Attack?", Traducido, (En línea) Disponible en: https://www.kaspersky.com/resource-center/definitions/replay-attack (Recuperado en fecha 12/03/2021)

blockchain se divide en dos: una ejecuta la versión heredada del software y la otra ejecuta la nueva versión actualizada"[53]. El atacante con posición más ventajosa para efectuar un ataque replay durante un *hard fork*, es aquel que posee una criptomoneda antes de producirse este proceso de bifurcación. Esto se debe a que puede ocurrir que "…*una transacción procesada antes del hard fork también será válida en la otra. Como resultado, una persona que recibió una cierta cantidad de criptomonedas de otra persona en la vieja blockchain, podría cambiar a la otra, replicar la transacción y transferir de manera fraudulenta un número idéntico de unidades a su cuenta por segunda vez*"[54], De esta manera se produce una repetición de transacciones en la Blockchain que se halla "dividida en dos partes".

Otra posible consecuencia negativa de este ataque, que ciertamente es otra variante de un ataque MITM, es que "*Al caer el poder de minería de la blockchain legacy, se abre espacio para un ataque de 51%. Esto habilita la creación de nuevas transacciones que pueden ir a la nueva blockchain y dejarla fuera de servicio si se supera su potencia*"[55]. Lógicamente, si existe la posibilidad de un ataque del 51%, puede esperarse un ataque DoS de menor impacto, pero que también repercuta en la red.

Cabe mencionar que existen medidas de protección frente a estos ataques que están tanto en manos de los mineros, como de los usuarios de las criptomonedas. A pesar de que existen medidas relacionadas con un refuerzo en la trazabilidad de las transacciones para evitar su duplicación, la mejor prevención contra un ataque replay es evitar que existan transacciones durante un *hard fork*. No es necesario aclarar que un bloqueo de transacciones por un periodo de tiempo, por corto que sea, también puede ser negativo para la criptomoneda que lo lleve a cabo.

Puertas Traseras (Backdoors) en el hardware

Las puertas traseras son un instrumento común entre los hackers. Pero es importante diferenciar entre un backdoor incorporado en el hardware de un backdoor en forma de software.

Investigadores de la Universidad de Michigan describen este tipo de puerta trasera, introducido en el hardware de un equipo, como "…*un componente no autorizado y malicioso, escondido en un chip entre*

[53] Bitnovo Blog, "¿Qué es un Ataque Replay?", (En línea) Disponible en: https://blog.bitnovo.com/que-es-un-ataque-replay (Recuperado en fecha 12/03/2021)
[54] Bit2me Academy, "¿Qué es un Ataque Replay?", (En línea) Disponible en: https://academy.bit2me.com/que-es-un-ataque-replay (Recuperado en fecha 12/03/2021)
[55] Bit2me Academy, "¿Qué es un Ataque Replay?", (En línea) Disponible en: https://academy.bit2me.com/que-es-un-ataque-replay (Recuperado en fecha 12/03/2021)

miles de componentes similares"[56]. Esta situación podría permitir el robo de criptomonedas de los usuarios. Un problema adicional es que también podría darse acceso a terceros para explotar los recursos del equipo para, por ejemplo, ejecutar acciones de minado. El minado se encontraría oculto a la vista del propietario del equipo y esta explotación silenciosa de recursos aceleraría la obsolescencia de la máquina. Ambas cuestiones merecen ser consideradas con seriedad, dado que en los dos casos la motivación de los atacantes son las criptomonedas. Y las pérdidas económicas, tanto en criptomonedas como en equipamiento, pueden representar un fuerte desincentivo para el mercado e incluso para el ingreso de nuevos mineros.

Estas maniobras ilegales pueden ser obra de proveedores de hardware malintencionados. Muy probablemente, Bitcoin sería el principal objetivo de estos delincuentes. Por ser la criptomoneda más popular, la recompensa estimada sería un estímulo suficiente para llevar adelante el delito. A su vez, la cantidad de proveedores es relativamente escasa y si se descubriera la existencia de algo así, resultaría en una alta pérdida de confianza en Bitcoin.

Hackers, una permanente amenaza

Si bien muchos de los ataques que se han individualizado son efectivamente llevados a cabo por hackers o ciberdelincuentes, hay ataques que son más usuales y no tan exclusivos de las criptomonedas. Sin embargo, las criptomonedas pueden ser blanco de estos ataques y merecen su mención. A propósito de las puertas traseras, es relevante señalar que cuando aparecen en forma de software, no solo las computadoras personales pueden ser el blanco, sino también dispositivos móviles como teléfonos celulares, tablets y otros. Los hackers suelen valerse de diferentes herramientas para poder acceder a los dispositivos. Pero la principal suele ser un virus troyano que, disfrazado de un software legítimo, contenga otro malicioso que permita dar control al hacker. Con el control del equipo, el hacker puede acceder a las credenciales necesarias para robar las criptomonedas.

Además de la mayor facilidad operativa y otras ventajas, el temor a la posibilidad de perder sus criptomonedas ha llevado a gran cantidad de usuarios a operar en exchanges, que les proporcionan un servicio similar al que los bancos ofrecen sobre el dinero fiduciario, obteniendo una sensación de mayor seguridad. Tal vez esta sensación no sea más que eso: una percepción de seguridad, real o ficticia. Pero lo cierto es que las exchanges son entidades nuevas en relación con los bancos tradicionales y su confiabilidad puede ser cuestionable. Si bien es cierto que la confiabilidad de los bancos tradicionales es

[56] Juan Ranchal, "Investigadores desarrollan puerta trasera hardware, imposible de detectar", 2016, (En línea) Disponible en: https://www.muycomputer.com/2016/06/05/puerta-trasera-hardware (Recuperado en fecha 16/03/2021)

materia de opinión, existe una cantidad considerable de entidades con una trayectoria de muchos años y, en varios casos, de más de un siglo, lo que de por sí inspira una determinada confianza.

He aquí un dilema respecto de Bitcoin que, a priori, podría no tener relación con su subsistencia en el largo plazo. Si la gran mayoría de los usuarios se inclinara por conservar y operar sus criptomonedas mediante exchanges, se estaría destruyendo parte del propósito inicial de Bitcoin. Las exchanges estarían tomando el lugar del tercero confiable del que Nakamoto esperaba prescindir en su Whitepaper.

Entonces, se puede afirmar que, en parte, los hackers que pretenden robar criptomonedas han desencadenado un comportamiento entre los usuarios que resulta en una contraposición respecto del propósito original de Bitcoin. Y, aun así, las exchanges no pueden prometer la seguridad que los usuarios desearían. Han sido víctimas de diversos ataques a través del tiempo, sean centralizadas (CEX) o descentralizadas (DEX). Según el portal TradeBlock, el año en que más ataques de hackers han sufrido fue 2019, sin embargo, la mayor pérdida económica se registró en 2018, según el siguiente cuadro:

Año	Fondos robados	Ataques
2011	$ 8.800.000	2
2012	$ 865.000	4
2013	$ 3.290.000	3
2014	$ 475.574.000	9
2015	$ 7.180.000	3
2016	$ 80.870.000	4
2017	$ 6.300.000	2
2018	$ 863.500.000	6
2019	$ 279.000.000	10
2020	$ 155.000.000	4
Total	$ 1.880.379.000	47

Cuadro 3.3. Fondos robados de exchanges. Fuente: TradeBlock, “2020 Exchange attacks pick up, but remain below 2018 levels”, Traducido,(En línea) Disponible en: https://tradeblock.com/blog/2020-exchange-attacks-pick-up-but-remain-below-2018-levels (Recuperado en fecha 16/03/2021)

No puede negarse que los ataques de los hackers son contraproducentes para el avance de las criptomonedas en general. Sin importar que el ataque se dirija a equipos personales de los usuarios o a exchanges, los atentados de los hackers desincentivan tanto a un mercado que se encuentra en plena evolución, como a una enorme porción de la sociedad que aún no cuenta con una suficiente formación para encarar estas amenazas.

Es importante comprender que un ataque exitoso contra Bitcoin podría derrumbar su precio y su capitalización en el mercado. Es por ello que se debe prestar especial atención a esto, ya que, por tratarse de un activo financiero, los golpes a su cotización podrían sentar las bases de su destrucción.

Pero las amenazas de los ataques mencionados que acechan a Bitcoin no son los únicos aspectos técnicos a considerar. Existen otras dificultades que vale la pena destacar. Algunas implican amenazas menos relevantes, como la posibilidad de colisiones matemáticas y otras más relevantes como las limitaciones en la escalabilidad de Bitcoin.

Las colisiones

Las colisiones son un factor que vale la pena mencionar, pero que representan una preocupación menor para Bitcoin. Con una naturaleza matemática es incuestionable que pueden ocurrir, pero con base en la probabilidad, representan un riesgo ínfimo. No obstante, una colisión llevaría a desechar los algoritmos que Bitcoin utiliza, ya que cuando se verifica una colisión en criptografía, el algoritmo se considera obsoleto. Jorge Rivera, CSA de ThinkBig Empresas de Telefónica S.A., advierte que "*Con solo una vez que se consiga encontrar una colisión, el algoritmo o criptosistema es automáticamente catalogado como 'inseguro', 'débil', o 'vulnerable', y en consecuencia entra en desuso, cuando no directamente deshabilitado o vetado por los protocolos o aplicaciones donde se emplea. Cualquier vulnerabilidad en la seguridad de un criptosistema pone en riesgo todos los protocolos o aplicaciones que sustente; desde la privacidad en las comunicaciones, hasta la identificación de usuarios o incluso dispositivos...*"[57].

Para evitar colisiones, es fundamental el factor aleatorio en el proceso de creación de un elemento criptográfico. En concordancia con el tema de la sección anterior sobre seguridad, Rivera comenta que "*La aparente inocencia con la que eran percibidos los defectos de aleatoriedad, se tornó dramática en el verano de 2013, cuando salió a la luz una vulnerabilidad en la clase Java SecureRandom del SDK de Android que afectaba todas las versiones anteriores a la v4.2, lo que en aquella época suponía la práctica totalidad de tablets y smartphones Android (CVE–2013–7372). El impacto de esta vulnerabilidad fue terrible para los usuarios de wallets de Bitcoin para Android, estando afectados la mayoría de los existentes entonces: Bitcoin Wallet, BitcoinSpinner, Mycelium y Blockchain.info. Todos los fondos depositados en estas carteras fueron sustraídos. (...) Google reconoció el error, corrigiéndolo con*

[57] Jorge Rivera, "Colisiones, haberlas hay(las). Parte 1", 2018, (En línea) Disponible en: https://empresas.blogthinkbig.com/colisiones-haberlas-hay-ciberseguridad (Recuperado en fecha 22/03/2021)

celeridad. Pero ya era tarde, no existía posibilidad alguna de recuperar las cantidades usurpadas, ya que las transacciones quedan inmutablemente recogidas en la Blockchain"[58].

La probabilidad de colisión en las claves privadas, las claves públicas y las direcciones de Bitcoin por el uso de los algoritmos criptográficos ECDSA, SHA–256 y RIPEMD160 es diferente. Para el caso de las claves privadas, se considera que, al tener 256 bits, su seguridad es suficiente para criptosistemas de curva elíptica, siempre contemplando el factor aleatorio en su generación. En cambio, para las claves públicas y las direcciones Bitcoin, la probabilidad de que exista una *colisión hash* es relativamente mucho mayor. Esto se debe a que el número de entradas posterior a la utilización del algoritmo SHA–256 es mayor al de las salidas producidas al utilizar el RIPEMD–160. Lógicamente, si las posibles entradas son mayores que las posibles salidas, esto implica que más de una entrada se halle ligada a una misma salida. Representado en números sería:

$$2^{256} > 2^{160}$$

Esto implicaría la existencia de 2^{96} colisiones existentes. ($2^{256}/2^{160}$) que se aproxima al número $7{,}92 * 10^{28}$. El número de colisiones hash es grande, pero ínfimo en relación al número de posibilidades que se manejan. Por ello, por ser insignificante la probabilidad de colisión y, a su vez, no conocerse vulnerabilidades, se considera que los algoritmos criptográficos que utiliza Bitcoin (ECDSA curva "secp256k1", hash SHA–256 y hash RIPEMD–160) son lo suficientemente seguros, a pesar de que su protocolo implique una importante cantidad de posibles colisiones de dirección. No obstante, subestimar este factor sería inapropiado, ya que existen grupos enfocados en la búsqueda de estas colisiones y, además, la tecnología cuántica podría acercar esta insignificante probabilidad a la realidad.

La tecnología cuántica

Uno de los grupos que más repercusión tuvo en el ambiente de las criptomonedas fue el creador del llamado "Large Bitcoin Collider" (Gran Colisionador de Bitcoin). Este proyecto tenía como meta principal lograr, "*…mediante la fuerza bruta, hallar una colisión criptográfica en las llaves privadas de Bitcoin*"[59]. Como se ha analizado, la probabilidad de éxito del proyecto es mínima, pero con la acelerada

[58] Jorge Rivera, "Colisiones, haberlas hay(las). Parte 2", 2018, (En línea) Disponible en: https://empresas.blogthinkbig.com/colisiones-haberlas-hay-parte2-ciberseguridad (Recuperado en fecha 22/03/2021)
[59] Isabel Pérez, "Hackeando la blockchain: el sospechoso esfuerzo del Gran Colisionador Bitcoin", 2017, (En línea) Disponible en: https://www.criptonoticias.com/seguridad-bitcoin/hackeando-blockchain-sospechoso-esfuerzo-gran-colisionador-bitcoin (Recuperado en fecha 22/03/2021)

evolución tecnológica de los últimos años, no puede descartarse que, aunando esfuerzos de distintos sectores, pueda lograrse el objetivo propuesto: romper la criptografía de Bitcoin.

En este mismo sentido, no puede dejarse de lado la posibilidad de la computación cuántica. Para dejar en claro lo que la computación cuántica es, el renombrado investigador Ahmed Banafa la define como "*…la disciplina de estudio cuyo objeto es desarrollar tecnología informática a partir de los principios de la teoría cuántica. Según las leyes de la física cuántica, la tremenda capacidad de procesamiento de las computadoras cuánticas se deriva de su capacidad de estar en múltiples estados y realizar tareas utilizando todas las permutaciones posibles de manera simultánea*"[60]. Las características superlativas de este tipo de computadoras las hace extremadamente superiores a las computadoras tradicionales, tanto que su capacidad de cómputo es millones de veces superior. Esto también se traduce en tiempo, dado que pueden procesar cálculos complejos en escasos segundos. En este punto es donde la criptografía puede correr peligro y, particularmente, los sistemas criptográficos asimétricos como el de Bitcoin. John Biggs, columnista en CoinDesk.com, comenta sobre este tema y cita al cofundador de Ethereum, Vitalik Buterin: "*La criptografía asimétrica se basa en pares de claves, llamadas llaves privada y pública. La llave pública puede ser calculada a partir de su contraparte privada, pero no al revés. (…) Las computadoras cuánticas son más eficientes y si el cálculo se realiza a la inversa (poder calcular una llave privada a partir de una llave pública) todo el esquema se rompería*"[61]. Las computadoras cuánticas son una amenaza para la criptografía y el cofundador de Ethereum es consciente de ello. Los sistemas más débiles serán los más vulnerables y, respecto de las criptomonedas, puede que en muchos casos sea necesario un hard fork, algo que no suele ser sencillo.

Sin embargo, hasta el momento, las computadoras cuánticas con un poder de procesamiento capaz de romper la criptografía de Bitcoin son solo un sueño. No obstante, en octubre de 2019, la empresa Google publicó un artículo en el que se atribuye el desarrollo de un procesador de 54 qubits llamado "Sycamore". Google ha indicado que su "*…máquina llevó a cabo el cálculo objetivo en 200 segundos y de las mediciones en los experimentos se determinó que a la supercomputadora más rápida del mundo le tomaría 10.000 años alcanzar ese mismo resultado*"[62]. Al mes siguiente, Banafa, en atención a las todavía recientes declaraciones de la empresa Google y su equipo de investigadores, escribió que "*Las redes*

[60] Ahmed Banafa, "What is Quantum Computing?", 2014, Traducido, (En línea) Disponible en: https://www.linkedin.com/pulse/20140503185010-246665791-quantum-computing (Recuperado en fecha 22/03/2021)
[61] John Biggs, "How Should Crypto Prepare for Google's 'Quantum Supremacy'?", 2019, Traducido, (En línea) Disponible en: https://www.coindesk.com/how-should-crypto-prepare-for-googles-quantum-supremacy? (Recuperado en fecha 22/03/2021)
[62] John Martins, "Quantum Supremacy Using a Programmable Superconducting Processor", 2019, Traducido, (En línea) Disponible en: https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html (Recuperado en fecha 22/03/2021)

blockchain, incluida la arquitectura de Bitcoin, se basan en dos algoritmos: El algoritmo de firma digital de curva elíptica (ECDSA) para firmas digitales y SHA–256 como función hash. Un ordenador cuántico podría usar el algoritmo de Shor para descifrar una clave privada a partir de la pública, pero incluso según las estimaciones científicas más optimistas, incluso aun cuando se consiga en un futuro, no va a ser en los próximos 10 años"[63]. Banafa deja una advertencia en sus palabras, pero también proporciona cierto grado de calma ante los avances de la tecnología cuántica al señalar un espacio temporal seguro estimado en un mínimo de 10 años antes de que pueda pensarse en la posibilidad que plantea. Sin embargo, el desarrollo eficaz de esta tecnología tornaría obsoletas a muchas criptografías actuales, especialmente si el algoritmo de Shor[64] es implementado alguna vez en una computadora cuántica práctica.

Según John Biggs, "*El mayor peligro que plantea la computación para las redes blockchain es su capacidad para superar cualquier método de encriptación tradicional*"[65]. El desarrollo tecnológico que se acelera año tras año es una verdadera amenaza para Bitcoin y su criptografía basada en los algoritmos mencionados. Según investigadores de la Universidad de Cornell "*Para descifrar una clave de curva elíptica de 160 bits, un ordenador cuántico necesitaría alrededor de 1.000 qubits…*"[66]. Quizás los 54 qubits del procesador que llevó a cabo Google parezcan muy lejos de los 1.000 qubits que podrían ser necesarios para romper la criptografía de Bitcoin, pero muchas cosas fueron marcadas como imposibles para la humanidad en la historia reciente, hasta que se hicieron realidad.

Problemas en la Mempool

Hay dos factores relevantes que giran en torno a la Mempool, donde se almacenan temporalmente las transacciones de la red hasta ser validadas: el tiempo y el dinero. Ambos interactúan entre sí: en un contexto de congestión (demasiadas transacciones a la espera de ser validadas por los mineros) y, en consecuencia, con demoras en la validación de transacciones, el pago de una mayor tarifa (fee), aceleraría la validación de una transacción en particular. Esto se puede graficar de la siguiente manera:

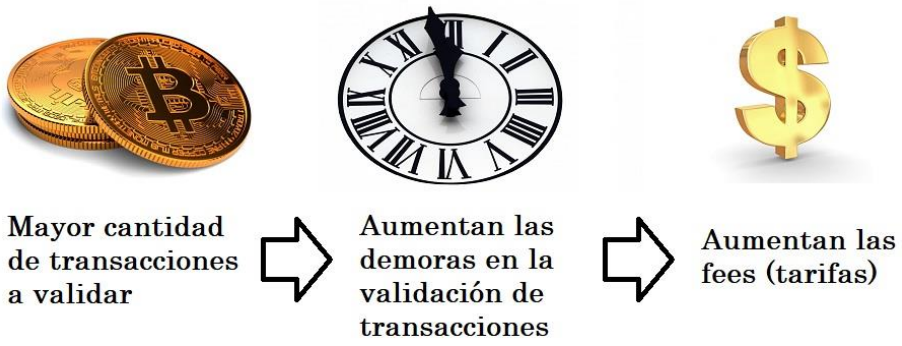
---

[63] Ahmed Banafa, "Computación cuántica y Blockchain: Mitos y realidades", 2019, (En línea) Disponible en: https://www.bbvaopenmind.com/tecnologia/mundo-digital/computacion-cuantica-y-blockchain-mitos-y-realidades (Recuperado en fecha 22/03/2021)

[64] Elisa B¨aumer, Jan-Grimo Sobez, Stefan Tessarini, "Shor's Algorithm", 2015, (En línea) Disponible en: https://qudev.phys.ethz.ch/static/content/QSIT15/Shors%20Algorithm.pdf (Recuperado en fecha 22/03/2021)

[65] John Biggs, "How Should Crypto Prepare for Google's 'Quantum Supremacy'?", 2019, Traducido, (En línea) Disponible en: https://www.coindesk.com/how-should-crypto-prepare-for-googles-quantum-supremacy? (Recuperado en fecha 22/03/2021)

[66] John Proos, Christof Zalka , "Shor's discrete logarithm quantum algorithm for elliptic curves", 2004, Traducido, (En línea) Disponible en: https://arxiv.org/abs/quant-ph/0301141 (Recuperado en fecha 22/03/2021)



Cuadro 3.4. Congestión de la Mempool. Fuente de elaboración propia.

Es importante entender que tarifas elevadas y demoras en la validación de transacciones son un indicio claro de un uso masivo de Bitcoin, pero que, al mismo tiempo, pueden ser causa de un incipiente desinterés por utilizar la criptomoneda. Es decir, un servicio de validación de transacciones lento que, además, posee una tarifa por operación más cara, va en detrimento de Bitcoin y provocaría una contracción en su uso. Este problema puede ocurrir con distintas criptomonedas, pero, para ser justos, la cuestión principal no radica en la propia Mempool, sino en los protocolos de Bitcoin y en sus limitaciones de escalabilidad.

Sin embargo, la existencia de la Mempool, desde un punto de vista técnico, sí puede llevar a una situación conflictiva como la que describe el sitio bit2me Academy: cuando "*…un usuario malicioso nos envía una transacción con un bajo fee o comisión, esta llegará a la mempool. Pero mientras este allí, es posible que dicho usuario pueda invalidarla y hacer un 'doble gasto' de esas monedas. Esto porque habrá realizado una transacción de pago a nosotros, pero, por otro lado, puede hacer una transacción de pago a un tercero con un mayor fee. Esto haría que la transacción al tercero y con un fee más alto sea procesada por la red en primer lugar, haciendo que nuestra transacción con más bajo fee se vea invalidada*"[67]. Si bien vale la pena su mención, esta es una práctica inusual, por lo que, ciertamente, es conveniente posar la mirada en la cuestión previa: la escalabilidad.

Escalabilidad

La escalabilidad de Bitcoin es una de las mayores preocupaciones en el entorno de la criptomoneda. Al mismo tiempo, la escalabilidad se puede dividir en tres componentes: el nivel de *storage* o almacenamiento, el ancho de banda requerido y las transacciones por segundo que se pueden validar.

[67] Bit2me Academy, "¿Qué es la mempool en Bitcoin?", (En línea) Disponible en: https://academy.bit2me.com/que-es-la-mempool-bitcoin (Recuperado en fecha 26/03/2021)

El primer componente es el nivel de storage. Este no es el componente que más preocupa acerca de la escalabilidad de Bitcoin, no obstante, comienza a llamar la atención, dado su crecimiento sostenido en el tiempo. El tamaño de la Blockchain de Bitcoin en el año 2016 rondaba los 60 GB y en 2021 ha logrado superar los 340 GB[68]. Es real que la capacidad de almacenamiento de las computadoras ha ido incrementándose velozmente en los últimos años, pero la velocidad en que la Blockchain de Bitcoin ha aumentado ha sido mayor. Un archivo de 60 GB no era un obstáculo difícil de sortear en 2016. En 2021, tampoco es imposible hacer frente a un archivo de 340 GB. Sin embargo, el tamaño aumenta a un ritmo sostenido y no todos los usuarios de Bitcoin, sean mineros u otro tipo de nodo, estarán en condiciones de seguir ese paso firme. En función de en qué parte del mundo resida, cada nodo existe en un contexto económico y social diferente. Y el acceso a los recursos necesarios para afrontar esta situación no es igual para todos: algunos quedarán afuera y eso es negativo para Bitcoin.

El segundo componente refiere al ancho de banda. Los nodos de recursos inferiores vuelven en este caso a ser los más perjudicados y los primeros apuntados para abandonar su posición. En este sentido, Bitcoin, por las desventajas inherentes a su génesis, se ve nuevamente menoscabado. De la misma forma, la pérdida de nodos y, por ende, de descentralización, va en desmedro de la idea original de Satoshi Nakamoto.

Cada nodo de la red de Bitcoin requiere un elevado ancho de banda para descargar continuamente los datos, lo que agrava el problema de la escalabilidad. A medida que la Blockchain crece es imperativo mover gran cantidad de datos en la red. A raíz de esto, han surgido diversas propuestas alternativas a Bitcoin. Uno de los ejemplos más resonantes es Cardano (ADA). Esta criptomoneda utiliza el método llamado RINA (Recursive InterNetwork Architecture), mediante el cual divide la red en subredes que pueden intercomunicarse entre sí de ser necesario haciendo más eficiente el uso del ancho de banda.

El componente del ancho de banda amerita una explicación con números ciertos. El sitio especializado bit2me Academy explica con claridad que "*Una transacción normal en Bitcoin suele ocupar entre 0.2kb y 1kb dentro del bloque (aunque hay algunas que ocupan más, lo normal es esto). Con estos datos tomaremos 0.5kb (que es un tamaño bastante común) como tamaño medio por transacción*"[69]. El tamaño de las transacciones es difícilmente reducible a valores inferiores a los existentes. Así las cosas, si

[68] Blockchain.com, "Tamaño de Blockchain (MB)", https://www.blockchain.com/charts/blocks-size (Recuperado en fecha 26/03/2021)
[69] Bit2me Academy, "¿Qué es la escalabilidad de Bitcoin?", (En línea) Disponible en: https://academy.bit2me.com/que-es-escalabilidad-de-bitcoin (Recuperado en fecha 26/03/2021)

se tomaran como meta, las casi 2.400 transacciones[70] que VISA, la mayor empresa de medios de pago del mundo, valida por segundo, la velocidad de las transacciones de Bitcoin debería alcanzar el nivel de 1.228.800 bytes por segundo (2.400 * 0,5 Kb –ó 512 bytes–). Esto equivale a 1,2 Mbps, según la siguiente operación:

2.400 TPS * 512 bytes = 1.228.800 bytes/s, que equivale a:
1.228.800 bytes/s / 1000 = 1.228,8 kilobytes/s, equivalente a:
1228,8 Kbps / 1024 = **1,2 Mbps**

Esta velocidad no es alcanzable en gran cantidad de lugares del planeta. Por ello, el componente del ancho de banda sigue siendo un problema a la hora de intentar escalar Bitcoin.

Tanto el storage como el ancho de banda, representan limitaciones que alejan a ciertos nodos de menores recursos. Esto podría generar una concentración en la minería en menor cantidad de nodos, creando un problema adicional para Bitcoin.

El último componente tal vez sea el más importante. La cantidad de transacciones que pueden ser validadas por segundo en la Blockchain de Bitcoin está lejos de las validaciones que otros medios de pago electrónico pueden ejecutar en ese mismo lapso de tiempo. El siguiente cuadro presenta una comparativa de la cantidad de transacciones por segundo (TPS) que cada medio de pago puede validar actualmente:

Medios de Pago	Transacciones por segundo (TPS)
VISA	2.400*
Ripple	1.500
MasterCard	1.000
PayPal	190
Bitcoin Cash	60
Ethereum	20**
Bitcoin	7

*Aunque se estima que podría soportar hasta 55 000 TPS.

**Su creador cree que en unos años podría alcanzar a VISA, pero su crecimiento no es tan veloz como el de Ripple, por ejemplo.

Cuadro 3.5. Comparativa de medios de pago. Fuente de elaboración propia con base en “El Bitcoin contra otros métodos de pago, ¿es una alternativa real?”, (En línea) Disponible en: https://www.elespanol.com/omicrono/tecnologia/20180207/bitcoin-metodos-pago-alternativa-real/283223239_0.html (Recuperado en fecha 30/03/2021)

[70] Elías Rodríguez García, “El Bitcoin contra otros métodos de pago, ¿es una alternativa real?”, 2018, (En línea) Disponible en: https://www.elespanol.com/omicrono/tecnologia/20180207/bitcoin-metodos-pago-alternativa-real/283223239_0.html (Recuperado en fecha 30/03/2021)

Del análisis del cuadro, surge que Bitcoin puede alcanzar, en un cálculo optimista, unas 7 TPS de acuerdo con su protocolo. Sin embargo, en un panorama más realista, se debería considerar que una transacción suele ocupar, como se ha visto, 0,5 kilobytes y un bloque tiene un tamaño de 1.024 kilobytes, por lo que en cada bloque caben aproximadamente 2.048 transacciones. Es importante resaltar que los factores de tiempo (10 minutos por bloque) y de tamaño de bloque (1024 kilobytes) están preestablecidos en el protocolo de Bitcoin, por lo que son inalterables mientras el protocolo no sea modificado. Entonces, si en un bloque caben aproximadamente 2.048 transacciones y se genera un bloque cada 10 minutos (600 segundos), la cuenta es sencilla:

$$2.048 \text{ Tx} / 600 \text{ seg} \approx 3{,}41 \text{ TPS}$$

Es decir, en un contexto más realista, Bitcoin valida aproximadamente 3,41 TPS, un número aún más lejano a los de VISA, MasterCard o, incluso, otras criptomonedas como Ripple o Ethereum.

Estas comparativas son relevantes en las finanzas. El Grupo Velas, que ha investigado en profundidad el problema de la escalabilidad, sostiene que "*…el sistema de pago Visa es ampliamente considerado como el punto de referencia que una criptomoneda basada en blockchain debe superar para ser capaz de alcanzar una escala verdaderamente masiva y una adopción global*"[71]. En otras palabras, si Bitcoin pretende ser masivo, tendrá que, al menos, equipararse a este punto de referencia, aunque, por lo expuesto, eso no sucederá.

Es dable destacar en este apartado el caso de Bitcoin Cash. Este surgió como una posible solución a estos problemas que Bitcoin atraviesa. La propuesta refería a mantener las características de Bitcoin, pero con un minado de bloques de datos más grandes: 8 MB en un comienzo y, posteriormente, 32 MB. Si bien se mantiene vigente, no ha logrado aún acercarse a la popularidad de Bitcoin, pero también es cierto que Bitcoin aún no ha atravesado su peor momento para saber lo que pasará con una altcoin tan similar a este como Bitcoin Cash.

Otro elemento a tener en cuenta respecto de la escalabilidad de las transacciones es el concepto de Proof of Stake (PoS), en contraposición con el Proof of Work (PoW) que utiliza Bitcoin. La Prueba de Trabajo o Proof of Work involucra a todos los mineros en una carrera por conseguir el siguiente bloque

[71] Grupo Velas, "¿Puede la blockchain competir con tecnologías como la de VISA en cuanto a TPS?", 2020, (En línea) Disponible en: https://medium.com/velasinspanish/puede-la-blockchain-competir-con-tecnolog%C3%ADas-como-la-de-visa-en-cuanto-a-tps-6a2f1698e884 (Recuperado en fecha 30/03/2021)

de la Blockchain con un nivel de dificultad que varía según el ritmo de minado para ajustarse a la regla de un bloque cada 10 minutos. Esta práctica que se halla descripta en el Whitepaper de Bitcoin consume grandes cantidades de energía y es más lenta que la Prueba de Participación o Proof of Stake que fue creada con posterioridad. "*Los nodos que minan en un protocolo PoS son seleccionados previamente de forma aleatoria (...) bajo el criterio de la tenencia de criptomonedas (...). Es decir, que los nodos que poseen mayor cantidad de criptomonedas tienen mayor posibilidad de ser seleccionados como nodos validadores*"[72]. Así como Proof of Work, Proof of Stake tiene sus ventajas y desventajas. Mientras que la Prueba de Trabajo es susceptible, por ejemplo, al ataque del 51% con concentraciones de mineros que unen sus fuerzas para dominar la red, la Prueba de Participación es susceptible a que existan usuarios concentrando grandes cantidades de criptomonedas y sean los únicos beneficiarios de las tarifas que se ofrecen. Sin embargo, este riesgo se mitiga introduciendo factores de aleatoriedad para la selección de nodos y, en lo que respecta a la escalabilidad, lo cierto es que la Prueba de Participación es más veloz y consume mucha menos energía eléctrica (un costo a considerar). Y por ello, estas ventajas de la Proof of Stake podrían representar otra amenaza para Bitcoin, dado que sobran ejemplos de criptomonedas que la emplean, tales como: Dash (DASH), Qtum (QTUM), Cosmos (ATOM) o Tezos (XTZ)[73]. Una vez más, cabe resaltar que cada criptomoneda que se alza sobre una debilidad de Bitcoin, se convierte en una amenaza adicional para este.

Otro aspecto a destacar es que, soluciones como Lighting Network para micropagos, la reducción del tiempo de minado o la creación de Sidechains (Blockchains alternativas) pueden parecer interesantes frente al grave problema de escalabilidad que Bitcoin padece. Sin embargo, muchas propuestas distintas para ser dirimidas entre tantos participantes y esperar un consenso para hacerlas realidad, llevan a repensar la idea de la descentralización y sus ventajas, pero más aún, sus desventajas.

Bitcoin se encuentra sitiado por dificultades técnicas y, como se ha analizado, es el principal objetivo de ataques por su popularidad y la capitalización que posee en el mercado. Pero todo este panorama que sufre Bitcoin es aprovechado por desarrolladores de nuevas criptomonedas que han tomado nota de las vulnerabilidades de Bitcoin y que fortalecen las propiedades de sus propios proyectos, lo que origina una fuerte competencia para Bitcoin a largo plazo. El protocolo de Bitcoin dificulta la posibilidad

[72] José Maldonado, ¿Qué es la Proof of Stake (PoS)?, 2020, (En línea) Disponible en: https://es.cointelegraph.com/explained/what-is-the-proof-of-stake-pos (Recuperado en fecha 30/03/2021)
[73] José Maldonado, ¿Qué es la Proof of Stake (PoS)?, 2020, (En línea) Disponible en: https://es.cointelegraph.com/explained/what-is-the-proof-of-stake-pos (Recuperado en fecha 30/03/2021)

de fortalecerse frente a estas amenazas. Su descentralización y normas del consenso pueden ser una fortaleza, pero también una debilidad a la hora de tomar decisiones fundamentales para evitar encontrarse en desventaja ante nuevos peligros.

CAPÍTULO 4. La descentralización; Un arma de doble filo

La descentralización de Bitcoin es inherente a su protocolo. No contemplar la descentralización en Bitcoin, implicaría estar hablando de una criptomoneda totalmente diferente: ya no sería Bitcoin, sino una nueva criptodivisa. Por ello, es importante analizar su formato descentralizado, especialmente, desde tres puntos de vista:

- Sus ventajas
- Sus desventajas
- Los riesgos que atentan en su contra

Asimismo, es importante remarcar que la descentralización puede ser vista desde distintos flancos. Pero lo que debe quedar claro es que para que exista una descentralización real, no debería existir un administrador único o un grupo reducido capaz de ejercer influencia significativa sobre las decisiones de la red. La descentralización ha formado parte de los estandartes de Bitcoin desde su nacimiento.

Las ventajas

Blockchain brinda ventajas claras y concretas a las criptomonedas. La descentralización permite alcanzar tres objetivos relevantes.

El primer objetivo es la transparencia en la red. Cualquier usuario puede acceder a la información que yace en la red. Es decir, cualquier usuario puede ver las transacciones que se han llevado a cabo y verificar por sí mismo el origen y destino de cada operación.

El segundo objetivo radica en la importancia de que no puede haber un punto central de fallo. La descentralización en múltiples nodos que llevan el registro de las transacciones, habilita a que, si hubiera un fallo en alguno de esos nodos, los demás impedirían que dicho fallo se traslade al resto de la red.

Por último, la descentralización posibilita la prescindencia de un tercero confiable velando por el sostenimiento de la red. Esta es, quizás, la ventaja más importante de la descentralización, dado que incluso Satoshi Nakamoto hizo especial énfasis en este aspecto en su Whitepaper de Bitcoin. Nakamoto expresa allí la necesidad de "…*un sistema de pagos electrónicos basado en pruebas criptográficas en vez de confianza, permitiéndole a dos partes interesadas realizar transacciones directamente sin la necesidad de un tercero confiable*"[74]. Vale decir que, comúnmente, se entiende por tercero confiable a una autoridad

[74] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Traducido, (En línea) Disponible en: https://bitcoin.org/bitcoin.pdf (Recuperado en fecha 15/04/2021)

central capaz de brindar la confianza necesaria para garantizar que las transacciones que los usuarios realicen estarán respaldadas. En pocas palabras, se entiende que un tercero confiable es una autoridad central. Nakamoto indica que, a partir de la criptografía y las pruebas de trabajo, se evita la necesidad de tal centralidad. Evitar esa centralidad es fundamental para evadir los riesgos inherentes que conlleva su existencia. Tales riesgos son diversos, pero especialmente destacan el fraude y robo, la posibilidad de un fallo central, la toma de decisiones unilateral de las reglas del sistema y la pérdida de anonimato frente a esta autoridad.

La mayoría de las criptomonedas gozan de estas ventajas, no solo Bitcoin. Y, de hecho, poseen más ventajas, que hacen que Bitcoin pueda quedar relegada frente a ellas en el largo plazo. Bitcoin fue la primera criptomoneda, lo que le dio la ventaja de ser la más popular, la pionera. Esto le ayudó, además, a ser la preferida del mercado hasta hoy. Sin embargo, las criptomonedas que le siguieron tuvieron otras ventajas, por ejemplo, la de poder optimizar sus protocolos en función de los problemas que veían que iban surgiendo para Bitcoin, sin abandonar las virtudes de la descentralización.

Las desventajas

La descentralización aumenta al ritmo que aumenta la cantidad de nodos en la red. La continua adición de nodos a la red es un factor positivo para la descentralización. Esto refuerza sus ventajas, pero también saca a la luz sus desventajas.

Las desventajas de una red descentralizada bien podrían ser evaluadas desde una simetría con las ventajas que aporta una centralización.

Una red centralizada podría entenderse desde una mirada organizacional como un sistema en donde existen jerarquías y, especialmente, una unidad de mando. En este caso, la unidad de mando podría no ser propiedad de un solo agente, sino también de un grupo reducido capaz de tomar las decisiones que tendrán consecuencias para el resto del sistema.

Así como la descentralización de una red tiene ventajas, una centralidad también. La unidad de mando suele ser mucho más efectiva en ciertos aspectos fundamentales. Una red centralizada se nutre de ventajas como:

- *Coordinación eficaz y trabajo en equipo*: Siguiendo directivas claras del rango superior. La formación de equipos de trabajo con un objetivo preciso favorece al cumplimiento de los objetivos.

- *Decisiones rápidas e inmediatas*: Dada la unidad de mando, no existe la necesidad de consensos que, muchas veces jamás ocurrirán, en especial en casos de complejidad donde pueden coexistir más de dos opciones.
- *Reducción de esfuerzos duplicados*: Una única voz que emite órdenes claras y una coordinación sin fallas impiden que los miembros de la red repitan tareas. Tal es el caso de la Prueba de Trabajo de Bitcoin, en la que los nodos mineros, en simultáneo, gastan recursos económicos y energéticos con el fin de encontrar un hash candidato para la Blockchain. Solo uno de ellos consigue añadir su bloque a la Blockchain en cada periodo de 10 minutos, mientras que el esfuerzo y recursos del resto de los nodos se pierde para siempre y se transforman en costos hundidos.

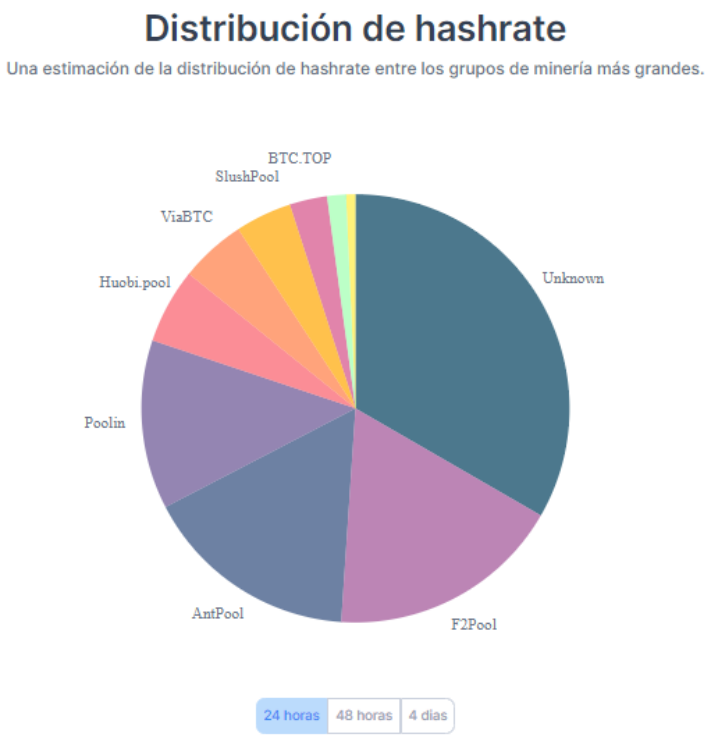
Aquí, entonces, vale la pena rememorar el caso de una criptomoneda como Cardano (ADA). En su caso, sigue existiendo una descentralización, pero la separación de la red en subredes permite optimizar el uso de recursos, reduciendo el gasto. Este es un ejemplo claro de las ventajas que han tenido las criptomonedas posteriores a Bitcoin. Cardano tuvo la posibilidad de adecuar su protocolo para capitalizar este aprendizaje. Por ello, sin abandonar las ventajas de la descentralización, Cardano, que es solo un caso entre muchos otros, es sumamente más eficiente que Bitcoin en la explotación de recursos, lo que, económicamente, se traduce en mayores márgenes de ganancia. Como se ha mencionado, cualquier altcoin con características superiores a Bitcoin, representa una amenaza real para este y su perdurabilidad.

Los riesgos

Sin perjuicio de la válida y extendida discusión sobre la conveniencia de una mayor centralización o descentralización, es evidente que la mayoría de los proyectos de criptomonedas se ha inclinado por aproximarse a una descentralización y alejarse de autoridades centrales. Sin embargo, hay una discusión posterior: una vez definida una posición tendiente a la descentralización, es imperativo evaluar si la misma puede perdurar frente a diferentes amenazas.

Una intención centralizadora puede provenir no solo de autoridades gubernamentales, sino también de otros stakeholders: grandes pooles de minería, exchanges, ballenas. Estos stakeholders, como se ha analizado, tienen gran incidencia en los acontecimientos que rodean a Bitcoin. Asimismo, no solo los stakeholders pueden representar una amenaza contra la descentralización, sino también el propio protocolo de Bitcoin. No obstante, cada amenaza a la descentralización es relevante analizarla de forma debida.

Pooles de minería: De acuerdo con el sitio Blockchain.com, un pool o grupo de minería es "*...un grupo de mineros que comparten su poder de cómputo en una red y son recompensados en función de la cantidad de energía que cada uno aporta en lugar de si el grupo encuentra un bloque o no*"[75]. A modo de ejemplo, se tomará el día 30 de abril de 2021 para observar y cuantificar la contribución de bloques de los pooles mineros, en comparación con el resto de mineros más pequeños:



Resumen de bloques minados

Minero / Piscina	Bloques minados
Unknown	47
F2Pool	25
AntPool	23
Poolin	18
Huobi.pool	8
ViaBTC	7
SlushPool	6
BTC.TOP	4
SBI Crypto	2
EMCD Pool	1

Cuadro 4.1. Distribución del hashrate. Fuente: Blockchain.com "Distribución de hashrate",
(En línea) Disponible en: https://www.blockchain.com/charts/pools-timeseries (Recuperado en fecha 30/04/2021)

Del análisis del gráfico y la tabla extraídos del sitio Blockchain.com, se puede advertir el nivel de incidencia de cada pool de minería y la concentración que refleja cada uno y, también, en conjunto. Poniendo atención a los cinco pooles que más bloques añadieron a la Blockchain en las 24 horas del día tomado como ejemplo, se pueden sacar los siguientes porcentajes de bloques minados:

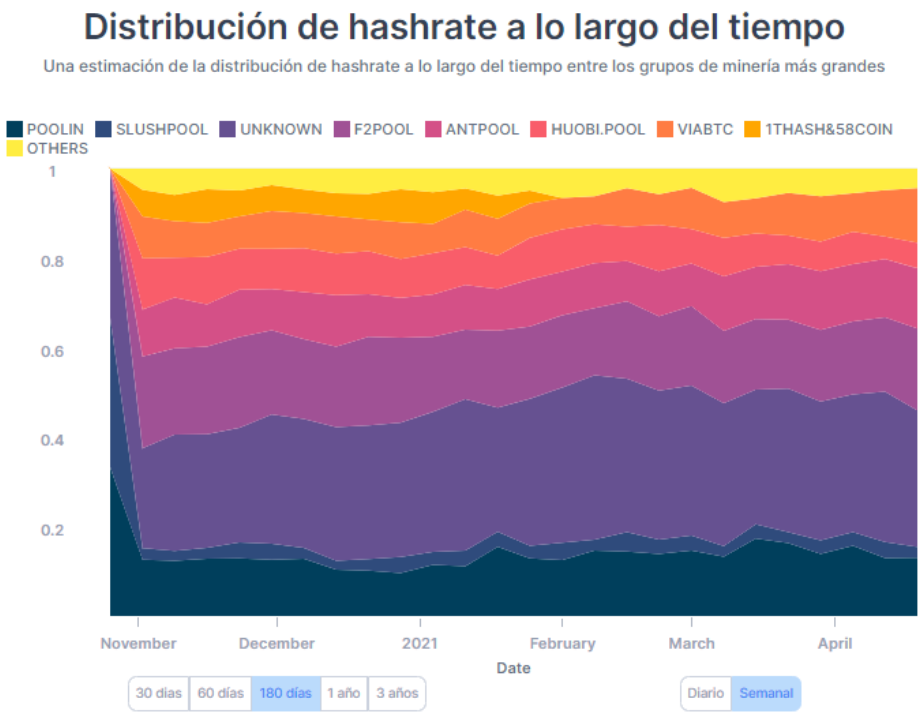
- Los 5 grupos que más minaron: 57,44%
- Los 4 grupos que más minaron: 52,48%
- Los 3 grupos que más minaron: 46,8%
- Los 2 grupos que más minaron: 34,04%

[75] Blockchain.com, "Distribución de hashrate", (En línea) Disponible en: https://www.blockchain.com/charts/pools (Recuperado en fecha 30/04/2021)

Para los interesados en la descentralización de Bitcoin, estos porcentajes son alarmantes. Se puede apreciar a simple vista que, en un día elegido de manera azarosa, cinco pooles de minería alcanzan un 57,44% de la distribución de los bloques minados en esas 24 horas. Siendo objetivos, no es difícil pensar que una cantidad tan reducida de pooles de minería podrían alcanzar un acuerdo para coordinar el control de la red de Bitcoin. Las consecuencias de algo así podrían ser catastróficas. Al observar los porcentajes con detenimiento, se puede apreciar que, incluso con solo tomar los cuatro pooles con mayor participación en la distribución del *hashrate*, es suficiente para conseguir más del 50%.

Si bien los restantes porcentajes no alcanzan la mitad necesaria para el control de la red, también representan un peligro considerable como ya se ha visto en el capítulo anterior (Ataque BDoS). Además de esto, se debe tener en cuenta un posible comportamiento gregario de otros nodos particulares. Nodos individuales pueden ver que un conjunto de nodos actúa de una determinada manera y siguen sus pasos, desconociendo que ese conjunto es manipulado por un mismo grupo o pool de minería con intereses propios.

Pero ver únicamente un ejemplo de un día sería sesgar la mirada y es necesario tener un horizonte más holgado del tema tratado. En el siguiente gráfico se puede tener una visión más extendida en el tiempo del protagonismo de estos pooles en la Blockchain de Bitcoin:



Cuadro 4.2. Distribución del hashrate a lo largo del tiempo. Fuente: Blockchain.com "Distribución de hashrate a lo largo del tiempo" (noviembre 2020 a abril 2021), (En línea) Disponible en: https://www.blockchain.com/charts/pools-timeseries (Recuperado en fecha 02/05/2021)

Del gráfico surge la innegable hegemonía en el tiempo de una escasa cantidad de grupos mineros. El gráfico toma mayor importancia si se tiene en cuenta que el período de tiempo de abscisa coincide con una de las mayores alzas del precio y capitalización de mercado de Bitcoin.

La concentración minera en los grandes pooles de minería trae consigo dos dificultades relevantes. Por un lado, al centralizar el poder de minería, los pooles son los que disponen de la mayor parte de las recompensas de nuevos Bitcoin que se crean en cada bloque y de las tarifas (fees). Esto tiene como consecuencia, la concentración de Bitcoin o, en otras palabras, el origen de nuevas ballenas o el fortalecimiento de las que ya existen.

Por otro lado, existe la ya mencionada posibilidad de que estos grandes pooles puedan dominar muchos nodos en la red, lo que les permite tener un control más amplio de las decisiones del sistema, las que, a su vez, podrían tomar para su propio beneficio. Es decir, a partir de este escenario, se podría dar una centralización de la toma de decisiones.

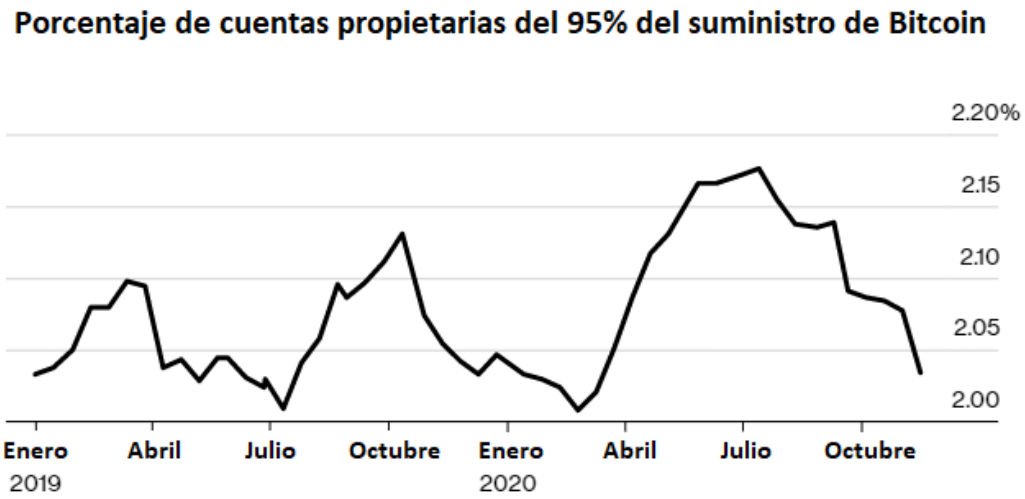
A su vez, la centralización que generan los pooles de minería puede aumentar con el tiempo. La existencia de mayor cantidad de nodos en la red se traduce en una mayor competencia. Más participantes compitiendo por los fees y, sobre todo, por la recompensa de nuevos Bitcoin, resultan en una disminución gradual de la ganancia marginal si el precio de Bitcoin no aumenta en paralelo. Una quietud o contracción en el precio de Bitcoin en un escenario como este, supondría una desaparición paulatina de pequeños mineros y una expansión del poder de los pooles de minería. Como agravante, la reducción de recompensas que ocurre en cada *halving*, sin dudas impulsa aún más esta posibilidad.

En función de la distribución de hashrate vista, es interesante pensar en una comparación de un escenario como este con un ataque del 51%. La desaparición de pequeños mineros y la subsistencia de contados pooles de minería, podría darles a estos últimos un control real de las decisiones de la red. Es importante destacar que no se trataría de un ataque en sí, sino de una manera "legítima" de hacerse del dominio de la red. No obstante, las consecuencias podrían ser similares y sumamente dañinas para Bitcoin.

Por otra parte, los pooles de minería representan un punto débil desde otra mirada: un ataque directo a estos pooles de minería podría tener efectos negativos para Bitcoin. La alta concentración de equipamiento en un sector geográfico lo hace vulnerable a dificultades tales como regulaciones gubernamentales o aumento repentino de costos de energía eléctrica. Estas causales harían caer abruptamente el margen de ganancias de los pooles. Así, los pooles de minería podrían verse obligados a mudarse o, de no ser esa una opción viable, simplemente a desaparecer y, junto con ellos, una gran cantidad de nodos que debilitaría la red.

Ballenas: El término "ballenas" (whales) refiere "*...a los mayores inversores de monedas digitales. El término se utiliza como una metáfora para describir a un individuo u organización que posee grandes cantidades de una criptomoneda particular*"[76]. Las significativas tenencias de criptomonedas les brindan un fuerte poder económico a las ballenas. Tal poder se traduce en que una sola transacción puede movilizar el precio de la criptomoneda sustancialmente. Esto hace muy volátil el precio de la criptomoneda y tenedores más pequeños son susceptibles de verse perjudicados en pocos segundos.

La compañía Bloomberg, basándose en datos de la empresa Flipside Crypto, realizó un informe a fines de 2020 en el que advertía que "*Cerca del 2% de cuentas de propietarios anónimos que pueden ser seguidas en la Blockchain de Bitcoin controla el 95% del activo digital...*"[77]. En su informe, la compañía presenta el siguiente gráfico con las variaciones en los porcentajes de cantidad de cuentas poseedoras del 95% de los Bitcoin existentes en cada momento entre enero de 2019 y finales de 2020:



Cuadro 4.3. Propietarios del 95% del suministro de Bitcoin. Fuente: Bloomberg, basado en información de Flipside Crypto, "Bitcoin Whales' Ownership Concentration Is Rising During Rally", Traducido, (En línea) Disponible en: https://www.bloomberg.com/news/articles/2020-11-18/bitcoin-whales-ownership-concentration-is-rising-during-rally (Recuperado en fecha 10/05/2021)

Ciertamente, cada una de las cuentas (wallets) no pertenece necesariamente a una sola persona. Esto entonces abre dos posibilidades. La primera refiere a que ese 2% de cuentas pertenezca a pocas

[76] Hannah Pérez, "¿Qué o quiénes son las "ballenas" de criptomonedas?", 2020, (En línea) Disponible en: https://www.diariobitcoin.com/mercados/bitcoin-mercados/que-o-quienes-son-las-ballenas-de-criptomonedas (Recuperado en fecha 10/05/2021)
[77] Olga Kharif, "Bitcoin Whales' Ownership Concentration Is Rising During Rally", 2020, Traducido, (En línea) Disponible en: https://www.bloomberg.com/news/articles/2020-11-18/bitcoin-whales-ownership-concentration-is-rising-during-rally (Recuperado en fecha 10/05/2021)

personas que, sin dudas, se las puede denominar ballenas. La segunda posibilidad es que algunas de esas cuentas pertenezcan a exchanges que almacenen allí los Bitcoin de una gran cantidad de usuarios. Como sea, ambas posibilidades son una alerta para la anhelada descentralización que Bitcoin promete. En el primer caso, las ballenas serían una realidad y su poder en el mercado, un problema. Mientras que, en el segundo caso, la centralización se da al existir pocas cuentas con muchos Bitcoin en posesión de unas pocas exchanges que podrían tener intereses maliciosos.

La distribución de tenencias de Bitcoin es dinámica, la concentración descripta puede cambiar de un momento a otro. Sin embargo, el informe de Bloomberg advierte una tendencia de las tenencias de Bitcoin a centralizarse aún más. Marianella Vanci, columnista de Criptonoticias.com, relata en un artículo que a principios de 2021 "*…la cantidad de grandes tenedores de BTC siguió aumentando mientras los minoristas se desprendían de sus posiciones. También los mineros bitcoin cada vez venden menos sus monedas y han estado reteniendo sus fondos…*"[78].

En relación a los efectos contraproducentes que pueden ocasionar las ballenas, a principios de 2021, José Jiménez del sitio especializado Finanzas.com, reveló en un artículo que "*…la tercera parte del mercado está en manos de muy pocos inversores, con lo que las ventas de estas 'ballenas' (como se les conoce en el sector) ante una mala noticia inesperada podría generar un efecto arrastre de consecuencias imprevisibles*"[79]. Como se ha visto, no son pocos los expertos que alertan sobre esta situación que menoscaba la descentralización de Bitcoin, que parece tendiente a profundizarse y que, además, puede traerle consecuencias muy negativas: bajas estrepitosas en su cotización y una crisis de confianza que podrían ser muy nocivos para su futuro.

Exchanges: La mera existencia de las exchanges puede interpretarse como la destrucción del propósito inicial de Bitcoin. Atraen usuarios, concentran criptodivisas y tienen un control implícito sobre los activos de sus clientes. Para entender el concepto de "exchange", el sitio bit2me Academy utiliza la siguiente

[78] Marianella Vanci, "Ballenas acumularon 90.000 bitcoins durante casi todo el mes de abril", 2021, (En línea) Disponible en: https://www.criptonoticias.com/mercados/ballenas-acumularon-90000-bitcoins-durante-casi-todo-mes-abril (Recuperado en fecha 10/05/2021)

[79] José Jiménez, "Los peligros del bitcoin. Solo 2.225 inversores controlan casi el 30% del mercado", 2021, (En línea) Disponible en: https://www.finanzas.com/divisas/los-peligros-del-bitcoin-solo-2-225-inversores-controlan-casi-el-30-del-mercado_20114254_102.html (Recuperado en fecha 10/05/2021)

definición: "*El nombre de exchange de criptomonedas o intercambio de criptomonedas, hace mención a un espacio generalmente virtual, en el que se realiza acciones de compra-venta de criptomonedas*"[80].

Se han perdido muchos Bitcoin desde su creación. Por imprudencia al almacenar o intercambiarlos o por robos de ciberdelincuentes, los tenedores de criptomonedas han encontrado en las exchanges un tercero confiable que les ayude contra estas situaciones indeseadas. De la misma forma, hallaron en ellas mayor practicidad para hacer transacciones en la red. Son, como se mencionó en el capítulo anterior, un tercero que brinda confianza y que podría asimilarse a un banco tradicional. Por esto, las exchanges son un impedimento en el propósito de Satoshi Nakamoto de desligarse de terceros confiables en el sistema financiero. Son un obstáculo que nació de la propia creación de Bitcoin y las criptomonedas que le siguieron. Paradójicamente, no hubieran existido sin Bitcoin y se han transformado en un enemigo de los ideales de este.

Sin embargo, vale decir que la confianza depositada en las exchanges ha sido defraudada en varias oportunidades. Desde uno de los casos más emblemáticos ocurridos en 2014 como fue el de Mt. Gox, hasta otros más recientes, como los de Hotbit o Thodex, no han sido pocas las ocasiones en que una exchange se vio envuelta en pérdidas de criptomonedas. Aun así, la tendencia indicaría que las exchanges brindan una practicidad y una confianza superior a la que la red y cada usuario de forma individual pueden ofrecer, dado que su popularidad y clientela aumenta día tras día.

No es la descentralización de Bitcoin la única faceta que se pone en peligro debido a las exchanges. También se pierde otro estandarte de Bitcoin: el anonimato. Las exchanges suelen tener una política de KYC – Know Your Client (Conozca a Su Cliente). La política de Know Your Client se basa en "*...la práctica que realizan las compañías para verificar la identidad de sus clientes cumpliendo con las exigencias legales y las normativas y regulaciones vigentes*"[81]. Una identificación exhaustiva de sus clientes termina definitivamente con la búsqueda de privacidad que Nakamoto planteaba en su Whitepaper. Para poder operar o, simplemente, almacenar las criptomonedas en una exchange, los usuarios deben someterse a una identificación que a menudo involucra fotografías de rostro, datos personales y, en muchos casos, fotografías de documentos de identidad y constancias de domicilio. El resultado es evidente: el fin del anonimato.

[80] Bit2me Academy, "¿Qué es un exchange de criptomonedas?", (En línea) Disponible en: https://academy.bit2me.com/que-es-exchange-criptomonedas (Recuperado en fecha 10/05/2021)
[81] ElectronicIdentification, "Qué es KYC (Know Your Customer) y su actualidad en 2021", 2021, (En línea) Disponible en: https://www.electronicid.eu/es/blog/post/que-es-kyc-know-customer/es (Recuperado en fecha 10/05/2021)

Pero para no perder de vista el quid de la cuestión, es importante concluir que, la pérdida de anonimato y el deterioro de la descentralización que provocan las exchanges, están vinculadas entre sí. La pérdida de anonimato es la consecuencia de una centralización mayor. La información recopilada en un servidor central termina siendo un blanco fácil para regulaciones y, indefectiblemente, para la pérdida de privacidad de los usuarios de las criptomonedas.

Un rígido protocolo: Hay un cuarto elemento que reduce la descentralización de Bitcoin y que no es exógeno como los pooles de minería, las ballenas o las exchanges. Se trata del propio protocolo de Bitcoin. Dadas las normas del consenso, su protocolo es prácticamente inalterable. La descentralización hace que el consenso sea algo impensado, fuera de lo que a la validación de nuevos bloques refiere. El consenso se da con frecuencia a la hora de validar bloques nuevos en la Blockchain de Bitcoin. Sin embargo, cuando se trata de tomar decisiones estructurales, la descentralización hace que el consenso sea una posibilidad muy remota.

Las reglas del consenso no han sido una imposición caprichosa de Nakamoto. La rigidez que implican es fundamental para proteger la red. Desde la perspectiva de los atacantes es un escollo difícil de superar. A su vez, torna casi inalterables algunas cuestiones como su política monetaria (emisión de Bitcoin), pautada desde su creación misma. Para este caso, modificar algo tan esencial como la cantidad de Bitcoin a emitir podría ser un peligro para sí mismo. Cambiar las reglas de juego podría traer incertidumbre en el mercado.

Aun así, en varias ocasiones se ha planteado la necesidad de realizar cambios en algunos aspectos del protocolo de Bitcoin. En virtud de lo expuesto, es importante que el protocolo posea la rigidez que tiene. No obstante, tal rigidez puede volverse en contra cuando se detecta un problema como la ya mencionada baja escalabilidad que Bitcoin ofrece. La escalabilidad es un problema a resolver y necesita del consenso de los nodos.

Otro potencial problema del protocolo es que no hay un límite de nodos. Por el contrario, se cree que el incremento de nodos favorece a la descentralización y ayuda a combatir el problema de los grandes pooles. Esto puede ser cierto, siempre que no sean los pooles instalados los que añadan esos nuevos nodos a la red y fortalezcan su posición dominante. Y es en este supuesto en el que un cambio en el protocolo podría evitar el escenario antes descripto, con mayor competencia, menor ganancia marginal y mayor concentración de pocos mineros capaces de subsistir.

Por lo dicho, se puede percibir que la rigidez del protocolo de Bitcoin tiene sus ventajas y sus desventajas. Pero, para bien o para mal, su protocolo es así: rígido. Y esto lo fortalece contra posibles amenazas, pero también lo deja incapaz de adaptarse a nuevos desafíos.

El valor de la descentralización

La descentralización tiene un valor intrínseco inmenso, pero para algunos temas puede ser más provechosa que para otros. La descentralización puede ser explotada por la tecnología Blockchain en muchas industrias y sectores de la sociedad, como se ha ejemplificado en el Capítulo 2. La Blockchain permite pensar en grande respecto de estructuras descentralizadas. Pero para Bitcoin, la descentralización puede representar tanto una fortaleza como una debilidad, según la situación que tenga por delante. Su protocolo le impide tener una reacción adecuada frente a situaciones adversas, pero los proyectos de criptomonedas que le sucedieron han tenido la oportunidad de explotar la experiencia de Bitcoin a su favor y se han convertido en competidores dignos de considerar.

Ahora bien, enfocando la atención en Bitcoin y considerando los distintos impedimentos que se han analizado, resulta difícil responder a preguntas como si perdurará la descentralización de Bitcoin, si los stakeholders de Bitcoin con un dominio tácito desean una real descentralización o, si los usuarios están dispuestos a resignar la descentralización para dejar el cuidado de sus criptomonedas en "terceros confiables". Respecto a la última cuestión, es dable agregar que las exchanges son, a la vez, una forma eficaz de llegar a la universalización, aunque vayan contra la idea descentralizadora que proponía Nakamoto.

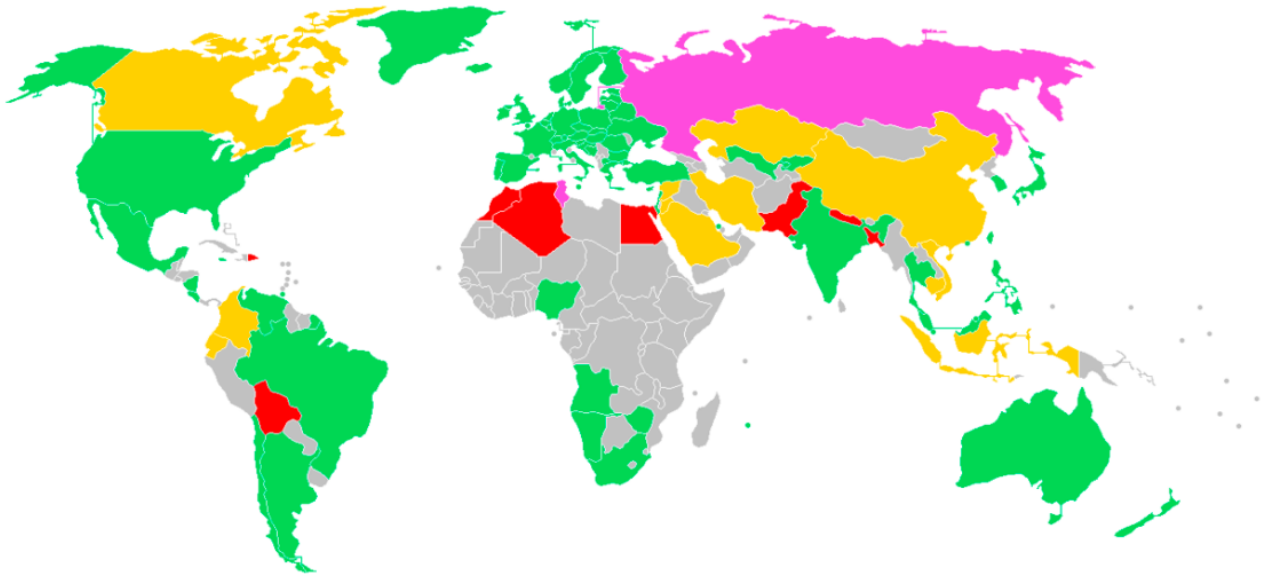
Las bondades de la descentralización pueden ser aprovechadas por las nuevas criptomonedas que surjan y que aprendan de la experiencia de Bitcoin. Asimismo, pueden incorporar nuevas medidas en sus protocolos para beneficiarse de las ventajas que tradicionalmente han ofrecido los sistemas centralizados. Conjugando las ventajas de ambos sistemas, las nuevas criptomonedas se transformarían en verdaderos candidatos a suceder a Bitcoin. Como ya se ha señalado, toda altcoin que surja con características superiores a Bitcoin, podría desplazarlo en el mercado, hacer descender su cotización y lentamente llevarlo por un camino tendiente a la desaparición.

CAPÍTULO 5. Amenazas regulatorias de Bitcoin. Enfoque legal y tributario

Bitcoin, como la primera criptomoneda y la más popular, se ha convertido en el centro de atención de los gobiernos de los países más importantes y de organismos multilaterales. Bitcoin ha recibido distinto tratamiento según cada gobierno, por lo que, dependiendo del país, puede estar legalmente categorizado en una de estas cuatro posibilidades:

- Legal: Su uso es permitido y se encuentra regulado.
- Restringido: Su uso tiene restricciones regulatorias.
- Alegal: No existe regulación, pero tampoco se halla prohibido su uso.
- Ilegal o prohibido: Su uso no está permitido.

Es de gran relevancia entender la dinámica de las regulaciones. Es difícil tener un panorama completo y actualizado de la situación legal de Bitcoin. Las regulaciones cambian a diario en distintos lugares del planeta. Es por ello que una plataforma como Wikipedia, que puede no ser considerada confiable para algunos expertos, puede, por sus características colaborativas, ser una buena herramienta para tener una noción lo más actualizada posible del cuadro de situación legal de Bitcoin. Así se puede apreciar en el siguiente gráfico:



Cuadro 5.1. Mapa de la legalidad de Bitcoin. Fuente: Wikipedia, "Legality of bitcoin by country or territory", 2021, Traducido, (En línea) Disponible en: https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory (Recuperado en fecha 12/05/2021)

Es dable aclarar que, observando la fuente citada, los países marcados con un Bitcoin "legal" incluyen tanto a aquellos en donde es legal como alegal.

Ver tantos países en donde Bitcoin no es ilegal podría interpretarse como una buena señal para la criptomoneda. Sin embargo, hay que tener en cuenta que, desde la legalidad, los gobiernos pueden aplicar regulaciones e, incluso, recaudar tributos gravando de su uso.

Además, es importante remarcar que los países han tenido dificultades para legislar sobre Bitcoin dada su naturaleza inmaterial y desarraigada. Aun así, los gobiernos han puesto en marcha distintos mecanismos para regularlos, generalmente con la participación conjunta de sus Bancos Centrales, legisladores y organismos recaudadores. En consecuencia, las normativas resultantes son variadas y con particularidades según el país. Para comprender mejor el abanico de posibilidades normativas que se han originado en distintas partes del mundo, es conveniente ver la situación en cuatro puntos neurálgicos del globo: China, Estados Unidos, Rusia y la Unión Europea:

China: El pujante país asiático es un protagonista clave en la minería mundial. No obstante, la situación legal de Bitcoin en ese país es particular. En China, el intercambio de criptomonedas a través de exchanges se encuentra prohibido, pero su tenencia está permitida debido a fallos recientes de la justicia. "*En septiembre de 2017, las autoridades nacionales prohibieron el funcionamiento de los exchanges locales. Como resultado de esta restricción, la gente en China puede tener criptomonedas, pero legalmente no puede cambiarlas por dinero fiduciario a través de plataformas comerciales*"[82]. Pero la normativa tiene un vacío legal cuando se trata de intercambios persona a persona (P2P – Peer to Peer). Por lo tanto, la situación legal de Bitcoin en China contiene un alto grado de incertidumbre y las libertades parecen ser menos que las prohibiciones para el uso de Bitcoin.

Estados Unidos: Bitcoin es legal en Estados Unidos. A partir de esta premisa de legalidad, distintos actores del gobierno estadounidense han intentado acorralar a Bitcoin. En un contexto aparente de libertad para poseer e intercambiar criptomonedas, entes como el Departamento de Justicia (DOJ – Department of Justice) o la Comisión de Bolsa y Valores (SEC – Securities and Exchange Commission), entre otros, han ido en la búsqueda de regular las operaciones mediante Bitcoin. Por ejemplo, a mediados de 2020, el Departamento de Justicia de Estados Unidos intentó decomisar más de 300 direcciones Bitcoin por asociarlas con Corea del Norte. "*Según la institución, los hackers usaron comercios OTC o extrabursátiles*

[82] Roy Álvarez, "China reconoce la legalidad de bitcoin", 2019, (En línea) Disponible en: https://www.cripto247.com/comunidad-cripto/china-reconoce-la-legalidad-de-bitcoin-183431 (Recuperado en fecha 12/05/2021)

en China y otros mecanismos para lavar los fondos, pasando mayoritariamente a BTC y la stablecoin Tether. El DOJ también alegó que ha estado siguiendo de cerca el desenvolvimiento de estos casos, en busca de 'proteger la seguridad nacional estadounidense'"[83]. En definitiva, el país norteamericano ha dado una figura de legalidad a Bitcoin, pero, por razones de seguridad nacional, antilavado y de prevención de evasión fiscal, ha ido implementado regulaciones y tiene una gran cantidad de jurisprudencia sentando precedentes para Bitcoin y su no tan libre uso. En nombre de "proteger la seguridad nacional" podría haber consecuencias muy negativas que representan un riesgo para tenedores que puedan ser relacionados con este tipo de eventos.

Rusia: Este país es otro caso muy particular. Rusia ha legalizado la tenencia e intercambio de criptomonedas, pero con un elevado nivel de regulación. Helen Partz, columnista de Cointelegraph.com, señala que en la legislación que Rusia implementa a partir de 2021, "…*el Banco de Rusia, será autorizado oficialmente para supervisar la actividad que implica la emisión de monedas digitales dentro del país. Además, (…) el banco podría imponer requisitos adicionales a los emisores de criptomonedas, así como a los exchanges de criptomonedas. El banco central de Rusia también se encargará de proporcionar un marco sobre qué tipos de monedas digitales pueden ser compradas por los inversores calificados y no calificados*"[84]. Por lo que la legalidad de Bitcoin en Rusia viene acompañada de un sinnúmero de regulaciones y restricciones para quienes deseen hacer uso de este. La normativa en Rusia es tan estricta que "*El conflicto constante entre las empresas de criptomonedas y el Banco Central de Rusia causó un retraso en el proceso. El Banco Central no es aficionado a la criptografía*"[85]. El propósito de Bitcoin de la descentralización y el anonimato suenan a una utopía entre tantos controles de las autoridades rusas.

Unión Europea: Los países que conforman la Unión Europea también aparecen en su gran mayoría como promotores de la legalidad de Bitcoin. No obstante, Carlos Fernández, cronista del diario El País señala que "*Bitcoin nació como una moneda electrónica usada entre particulares, sin ninguna autoridad detrás que la respaldase. Pero se ha acabado convirtiendo en un medio de inversión de alto riesgo y, lo que es peor, en herramienta de ciberdelincuentes. Ello ha hecho que la Unión Europea esté impulsando un*

[83] Juan Ibarra, "Estados Unidos pretende decomisar 300 direcciones de bitcoin vinculadas a Corea del Norte", 2020, (En línea) Disponible en: https://www.criptonoticias.com/judicial/estados-unidos-decomisar-300-direcciones-bitcoin-corea-norte (Recuperado en fecha 12/05/2021)
[84] Helen Partz, "Rusia finalmente aprueba el mayor proyecto de ley cripto del país", 2020, (En línea) Disponible en: https://es.cointelegraph.com/news/russian-lawmakers-finally-pass-countrys-major-crypto-bill (Recuperado en fecha 12/05/2021)
[85] Rahul N., "La primera ley de criptomonedas de Rusia se implementará en 2021", 2020, (En línea) Disponible en: https://es.beincrypto.com/primera-ley-criptomonedas-rusia-implementara-en-2021 (Recuperado en fecha 12/05/2021)

amplio conjunto de medidas legislativas para regular estas monedas digitales"[86]. Así como Estados Unidos arguye motivos de seguridad nacional, la Unión Europea se inclina a justificar las regulaciones a Bitcoin por ser de gran ayuda para la ciberdelincuencia y por la supuesta intención de querer proteger a los inversores de la alta volatilidad que posee esta criptomoneda. Estas justificaciones podrán parecer loables, sin embargo, no son las únicas. En diciembre de 2020, durante una reunión del G7 (Grupo de las 7 Naciones más desarrolladas), el ministro de Finanzas de Alemania, Olaf Scholz, dijo que "*Debemos hacer todo lo posible para asegurarnos de que el monopolio monetario permanezca en mano de los estados*"[87]. Seguramente exista una real intención de prevenir catástrofes económicas y delitos, pero también es cierto que los gobiernos no están dispuestos a renunciar al monopolio de la emisión monetaria. Y esto pone a Bitcoin en una posición de rivalidad contra los gobiernos más poderosos del mundo.

Los gobiernos acorralan a Bitcoin. Las consecuencias de las regulaciones suelen ser perjudiciales para el activo que pretende ser regulado. Una avalancha de controles sobre Bitcoin haría caer su precio, aumentaría el costo de utilizarlo, entraría lentamente en desuso y comenzaría a alejar inversores. Un éxodo de inversiones es una de las cosas más indeseadas en una economía nacional. No obstante, si no pueden regular Bitcoin y gravarlo impositivamente, los gobiernos lo verán como un problema, dado que una porción de riqueza se desplazaría hacia este, desde otros activos que sí pueden regular y gravar.

Algunos países, sin más, han prohibido el uso de Bitcoin e incluso hacen caer leyes de índole penal sobre quienes lo utilicen. Otros lo permiten, pero con restricciones de uso que varían según la jurisdicción. En cambio, la mayoría de los países desarrollados lo ha legalizado, pero con fuertes controles. Esos controles generalmente enfocan hacia dos direcciones: criminales y tributarios.

Enfoque tributario

Los objetivos de regular Bitcoin varían según la autoridad de aplicación. Algunos países lo hacen para prevenir la comisión de delitos. Otros Estados lo regulan para resguardar el monopolio de la emisión monetaria. La mayoría lo hace por ambos motivos. Pero las regulaciones habilitan a los países a perseguir un tercer objetivo derivado: incrementar la recaudación tributaria. Un mayor control sobre las criptomonedas, permitiría gravarlos impositivamente con mayor alcance.

[86] Carlos B. Fernández, "Europa quiere regular las criptomonedas para hacer su uso más seguro", 2021, (En línea) Disponible en: https://cincodias.elpais.com/cincodias/2021/01/21/legal/1611218981_865970.html (Recuperado en fecha 19/05/2021)
[87] Andrea Shalal y Christian Kraemer, "G7 finance officials back need to regulate digital currencies: Treasury", 2020, (En línea) Disponible en: https://www.reuters.com/article/idUSKBN28H1Y6 (Recuperado en fecha 19/05/2021)

Si las regulaciones pueden derivar en un desincentivo para Bitcoin, la aplicación de impuestos sin dudas lo hará. Un impuesto que recaiga sobre Bitcoin representa una pérdida evidente de capital o de margen de ganancia, según se trate de un impuesto patrimonial o un impuesto a la renta. Las pérdidas ahuyentarían a inversores y esto fomentaría una caída en la cotización de Bitcoin.

No hace falta aclarar que los impuestos no son exclusivos de las criptomonedas, dado que existe gran cantidad de activos que ha tenido impuestos desde hace cientos de años. Sin embargo, las criptomonedas son activos que no son bien vistos por los gobiernos, ya que es difícil controlarlos y legislar sobre ellos. Esta dificultad pueden verla como un ataque a su soberanía nacional. Por otro lado, su carácter fungible, difícil de rastrear e inmaterial, lo hace mucho más favorable para el financiamiento de las actividades ilegales que los mismos gobiernos pretenden reducir. Por ello, es probable que las leyes tributarias que se les apliquen sean más gravosas que las generales.

La reciente aparición de las criptomonedas ha encontrado a los países sin la suficiente preparación para tomar las medidas adecuadas para ejercer su dominio. Sin embargo, las regulaciones aumentan a diario. Si se entiende que, para poder gravar las criptomonedas, se las debe legislar y regular previamente, entonces se puede concluir que los impuestos sobre ellas aún son escasos debido a que el proceso regulatorio recién comienza. Un ejemplo de esto es la postura de Oficina de Contralor de la Moneda de Estados Unidos (OCC – Office of the Comptroller of the Currency) que en 2020 aprobó que "…*los bancos federales custodien criptomonedas*"[88]. Esto implica más poder de control, aunque aún no existan tributos específicos sobre estas.

Por lo dicho, es lógico pensar que los impuestos irán acrecentándose en los años venideros. No obstante, algunos países, en especial los más desarrollados, han empezado a tomar intervención en este asunto y se distinguen tres casos claros. El primer caso es el de países que ya han creados nuevos impuestos sobre las criptomonedas. El segundo caso es el de los gobiernos que utilizan normas preexistentes considerando a las criptomonedas dentro del hecho imponible de las mismas. Y el tercer caso es el de países, incluso, la Unión Europea que ya han puesto en marcha la creación de proyectos de ley apuntados específicamente a las criptomonedas.

Un ejemplo de país que ha creado impuestos particulares para las criptomonedas es el de Corea del Sur. El país asiático ha comenzado a aplicar mediante un nuevo código fiscal "*…una tasa impositiva del*

[88] Kollen Post, "Reguladores de Estados Unidos aprueban que los bancos federales custodien criptomonedas", 2020, (En línea) Disponible en: https://es.cointelegraph.com/news/us-banking-regulator-green-lights-crypto-custody-at-federally-chartered-banks (Recuperado en fecha 19/05/2021)

20% para los ingresos generados por el trading de criptomonedas"[89]. En este caso el enfoque principal apunta al trading, por lo que se puede considerar que, en principio, Corea del Sur aplicaría tributos sobre la renta, lo que no implica que pueda también crear leyes impositivas que graven el patrimonio (tenencia de criptomonedas).

Un ejemplo de país que ha estado aplicando leyes preexistentes a las criptomonedas es Estados Unidos. "*El IRS considera las criptomonedas como propiedad sujeta al pago de impuestos al menos desde 2014. Sin embargo, tal como el resto del gobierno estadounidense, ha estado prestando cada vez más atención al tema*"[90]. Y esto quedó completamente reafirmado por el Memorándum Nro. 202035011 de la Oficina del Abogado General del IRS – US Internal Revenue Service (Servicio de Impuestos Internos de Estados Unidos) que concluye que "*...el dinero virtual convertible es gravable como un ingreso ordinario*"[91], es decir que, se encuentra gravado, como el resto de los ingresos, por la normativa existente.

Finalmente, la Unión Europea en su conjunto intentará dar un marco regulatorio integral a las criptomonedas. El proyecto que se ha dado a conocer indica que "*Para 2024, la UE debería crear un marco integral que permita la adopción de la tecnología de libros mayores distribuidos (DLT) y criptoactivos en el sector financiero. (...) Debería también abordar los riesgos asociados con este tipo de tecnologías*"[92]. Luego, cada país miembro contará con una base regulatoria común para aplicar los impuestos que crea pertinentes. Sin embargo, esta fecha parece distante y algunos países como España se han adelantado. España ha comenzado a introducir regulaciones sobre los contribuyentes para "*...un mayor control de criptomonedas con la obligación de informar sobre su tenencia, tanto en territorio español como en el extranjero. Los tenedores de criptomonedas no solo tendrán que comunicar sobre el dinero digital que poseen sino también su adquisición, transmisión o pago con dicha moneda*"[93]. Lo verdaderamente destacable de este caso es que resulta indistinto si un usuario de criptomonedas reside o no en el territorio español. Por ello, se puede inferir que la complejidad para ubicar geográficamente un criptoactivo no será un impedimento en el futuro para los gobiernos a la hora de recaudar. Esto así, podría

[89] Marie Huillet, "Corea del Sur aprueba un impuesto del 20% sobre las criptomonedas", 2020, (En línea) Disponible en: https://es.cointelegraph.com/news/south-korea-finalizes-cryptocurrency-income-tax-of-20 (Recuperado en fecha 23/05/2021)

[90] Juan Ibarra, "Estados Unidos cobrará impuestos hasta a tus pequeñas fracciones de bitcoin", 2020, (En línea) Disponible en: https://www.criptonoticias.com/finanzas/estados-unidos-cobrara-impuestos-pequenas-fracciones-bitcoin (Recuperado en fecha 23/05/2021)

[91] Office of Chief Counsel de la IRS, "Memorándum Nro. 202035011", 2020, Traducido, (En línea) Disponible en: https://www.irs.gov/pub/irs-wd/202035011.pdf (Recuperado en fecha 23/05/2021)

[92] Huw Jones, "EU to introduce crypto-assets regime by 2024, EU documents say", 2020, Traducido, (En línea) Disponible en: https://www.reuters.com/article/us-eu-cryptoassets-idUSKBN2692CP (Recuperado en fecha 23/05/2021)

[93] Rodrigo Ponce de León, "El Gobierno aprueba el anteproyecto de ley que prohíbe las amnistías fiscales", 2020, (En línea) Disponible en: https://www.eldiario.es/economia/gobierno-aprueba-anteproyecto-ley-prohibe-amnistias-fiscales_1_6287827.html (Recuperado en fecha 23/05/2021)

generar escenarios de doble o múltiple imposición que, de poder materializarse, terminaría por destruir cualquier valor sobre este tipo de activos.

Es visible que la presión tributaria es incipiente, pero que la intención de los gobiernos por hacerla crecer es un hecho. Es importante resaltar que, para que esto ocurra, será fundamental una figura que ya ha sido mencionada: las exchanges y, junto con ellas, su política de Know Your Client (KYC).

Las exchanges se convierten en un blanco fácil para las regulaciones gubernamentales. Se trata de compañías que deben cumplir con requisitos y normativas. Son mucho más fáciles de fiscalizar que una multitud de nodos dispersos por todo el mundo con un alto grado de privacidad. Pero una buena porción del público acude a ellos, como se ha visto, por su practicidad y la sensación de mayor seguridad que brindan.

Ha habido muchos ejemplos de lo afirmado en el párrafo anterior, pero, tal vez, el caso más emblemático haya sido el de la exchange Coinbase en 2016. El Departamento de Justicia de Estados Unidos, bajo el caso 16–1404 del 30 de noviembre de 2016[94], falló a favor del IRS y en contra de la exchange Coinbase para que esta última entregara "*…información concerniente a los ciudadanos estadounidenses registrados en su plataforma que serían contribuyentes al Estado*"[95]. Este caso fue un hito para el ambiente de las criptomonedas, dado el notorio triunfo de un Estado regulador sobre los usuarios, que deja a las claras lo planteado: la pérdida total de anonimato. Y este caso no implica que solo en Estados Unidos se haya podido avanzar sobre las exchanges y la información que tienen de sus clientes. Sin ir más lejos, cuando se ejemplificó sobre los gobiernos más importantes que impulsaban regulaciones a las criptomonedas, se vio que Rusia y China apuntaban directamente contra estas compañías.

Analizando con mayor profundidad, las exchanges son más fiscalizables por sus características, pero, a la vez, lo que las convierte en un objetivo de los gobiernos son sus políticas KYC. Para evitar redundar sobre lo visto en el capítulo precedente acerca de que la política de KYC, conviene únicamente enfocarse en los tres fines que esta política busca:

- Identificar y autenticar clientes
- Evaluar el riesgo de dichos clientes

[94] U.S. Department of Justice, "Court Authorizes Service of John Doe Summons Seeking the Identities of U.S. Taxpayers Who Have Used Virtual Currency", 2016, (En línea) Disponible en: https://www.justice.gov/opa/pr/court-authorizes-service-john-doe-summons-seeking-identities-us-taxpayers-who-have-used (Recuperado en fecha 23/05/2021)

[95] Jaime Sandoval, "Coinbase pierde batalla legal en Estados Unidos y entregará base de datos de usuarios", 2016, (En línea) Disponible en: https://www.criptonoticias.com/regulacion/coinbase-legal-estados-unidos-datos-usuarios (Recuperado en fecha 23/05/2021)

- Evaluar las transacciones de esos clientes

Estos fines son una clara muestra del control de terceros sobre las operaciones de los usuarios y, al mismo tiempo, la completa destrucción del anonimato que se hubiera planteado en el Whitepaper de Bitcoin. Hay que enfatizar que los clientes son conscientes de que si los gobiernos los fiscalizan por sus operaciones con criptomonedas es debido a estas políticas de las exchanges. Durante los últimos años el IRS ha estado enviado cartas a usuarios de criptomonedas. De acuerdo con un artículo de Shehan Chandrasekera, publicado por el prestigioso sitio Forbes: "*...se desconoce cuántos contribuyentes recibieron estas cartas en 2020 o cómo el IRS consiguió la información sobre esos contribuyentes. Es lógico pensar que los datos pudieron haber llegado al IRS provenientes de alguna exchange de criptomonedas con base en Estados Unidos que recolecta la información de sus usuarios como parte del procedimiento de Know Your Client (KYC)*"[96].

Un año antes de la resolución del caso de Coinbase a favor del IRS, en 2015, había aparecido la BitLicense en el Estado de Nueva York. Consistente en una licencia obligatoria para operar con criptomonedas y la inscripción en un registro oficial, esta decisión del Departamento de Servicios Financieros de Nueva York (DFS – Department of Financial Services) ha traído consecuencias desde su puesta en marcha. No solo ha proporcionado mucha información al Estado para poder regular el mercado de criptomonedas, sino que, al principio, provocó la caída de muchas compañías y un fuerte desaliento a Bitcoin. El New York Business Journal lo describió en su momento como "*El Gran Éxodo de Bitcoin*"[97], un ejemplo más de las consecuencias negativas que el exceso de regulaciones podría tener sobre Bitcoin.

En un enfoque tributario, es acertado analizar cada aspecto en particular, pero hace falta tener una mirada global del asunto. Las exchanges son de preferencia para una enorme cantidad de usuarios y proliferan. Los gobiernos fomentan la utilización de las políticas de KYC para prevenir crímenes, pero, en el proceso, les dan la posibilidad de disponer de los datos y la información de las transacciones de los clientes de las exchanges. Esta información les permite ir en busca de estos clientes con fines

[96] Shehan Chandrasekera, "Crypto Users Are Receiving IRS Tax Warning Letters, Again", 2020, Traducido, (En línea) Disponible en: https://www.forbes.com/sites/shehanchandrasekera/2020/08/25/crypto-tax-warning-letters-2020/?sh=2e5ac6ee17f7 (Recuperado en fecha 23/05/2021)

[97] Michael del Castillo, "The 'Great Bitcoin Exodus' has totally changed New York's bitcoin ecosystem", Traducido (En línea) Disponible en: https://www.bizjournals.com/newyork/news/2015/08/12/the-great-bitcoin-exodus-has-totally-changed-new.html (Recuperado en fecha 23/05/2021)

recaudatorios. Se hace real entonces una presión tributaria sobre estos activos que acaba desalentando su utilización.

Enfoque criminal

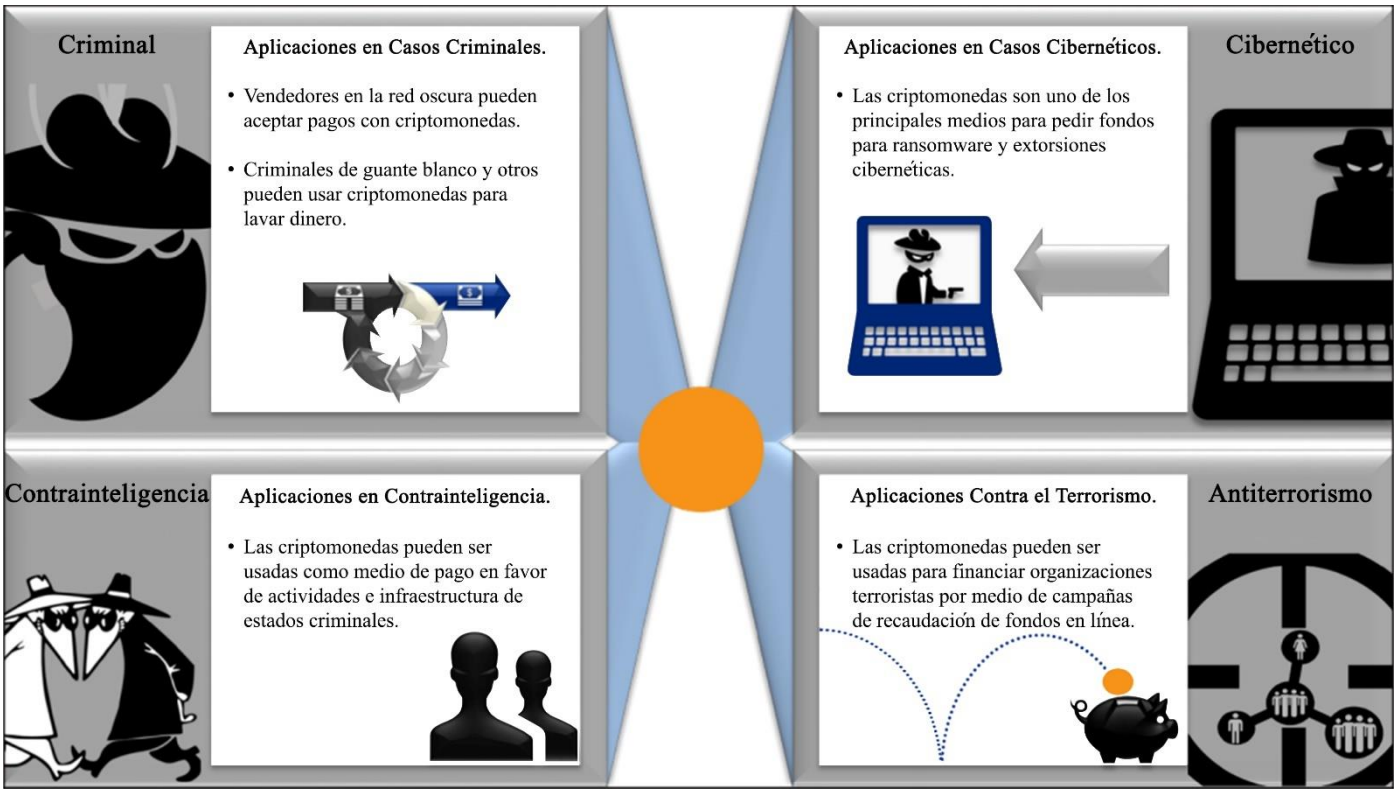
Podría plantearse que la prevención de crímenes es una excusa con fines recaudatorios, pero la relación de Bitcoin con el delito y el terrorismo también es una realidad y una fuerte crítica de los gobiernos hacia la criptomoneda.

En honor a la verdad, el delito ha existido desde siempre y es cierto también que otros activos como el dinero en efectivo o metales preciosos, con características fungibles y de dificultosa trazabilidad son funcionales a la criminalidad. Considerando solo esto, no habría motivos para apuntar contra las criptomonedas de forma tan rigurosa. Sin embargo, las criptomonedas cuentan con dos factores más que benefician a terroristas y demás delincuentes: la inmediatez en el pago y la inmaterialidad que hace imposible su geolocalización. Estas son ventajas que el dinero en efectivo u objetos suntuosos no poseen.

Las criptomonedas en general poseen estas características tan atractivas para el delito. No obstante, los grupos criminales parecen haber adoptado una en particular: Bitcoin.

En 2020, el Departamento de Justicia de Estados Unidos elaboró un marco legal sobre el uso de criptomonedas en el mundo criminal. Si bien el informe menciona a las que denomina AECs – Anonymity Enhanced Cryptocurrencies (Criptomonedas de Anonimato Mejorado), como Monero, Zcash o Dash, con mayor anonimato y más ventajoso para los delincuentes, apunta principalmente a Bitcoin. Este reporte relata que "*…los criminales se apoyan cada vez más en las características de las criptomonedas para mejorar y encubrir esquemas ilegales. En general, los ilícitos con criptomonedas encuadran en tres categorías. (…) (1) participar en transacciones asociadas con la comisión de delitos, como la compraventa de drogas y armas en la red oscura, rentar servidores para cometer crímenes cibernéticos, o solicitar financiamiento para actividades terroristas; (2) participar en maniobras de lavado de dinero o evasión impositiva de actividades legítimas; o (3) perpetrar crímenes directamente implicando al mercado de criptomonedas en sí, como robar criptomonedas de exchanges a través del hackeo o uso de promesas de criptomonedas para estafar a inversores ingenuos*"[98]. Sin perjuicio de estas tres categorías que define, luego señala que focaliza sus investigaciones en cuatro elementos, según el siguiente cuadro:

[98] U.S. Department of Justice, "Cryptocurrency – Enforcement Framework", 2020, Traducido, (En línea) Disponible en: https://www.justice.gov/archives/ag/page/file/1326061/download (Recuperado en fecha 26/05/2021), pp. 5 y 6



Cuadro 5.2. Objetivos de investigación del DOJ. Fuente: U.S. Department of Justice, "Cryptocurrency – Enforcement Framework", 2020, Traducido, (En línea) Disponible en: https://www.justice.gov/archives/ag/page/file/1326061/download (Recuperado en fecha 26/05/2021), p. 6.

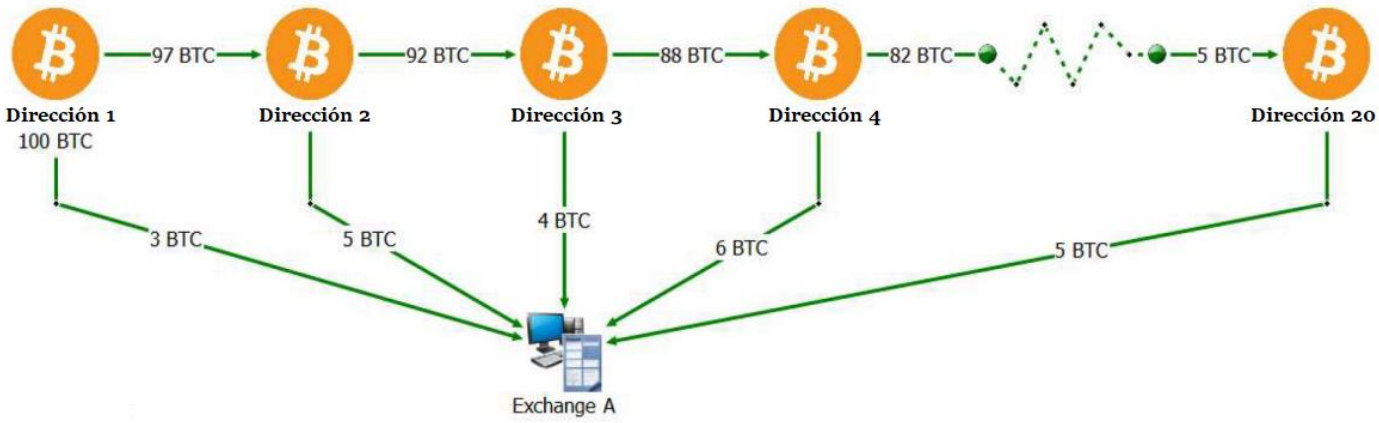
La variedad de delitos con criptomonedas es amplia. Pero, de lo expuesto por el Departamento de Justicia de Estados Unidos, vale la pena concentrase en entender y ejemplificar cuatro problemas graves que involucran directamente a Bitcoin:

- Lavado de dinero
- Estafas en línea (Scams)
- Ransomware
- Financiamiento de actividades delictivas y terroristas
- Mercado negro en línea

Lavado de dinero: El anonimato y la difícil trazabilidad de Bitcoin, lo convierten en un instrumento ideal para el lavado de dinero. La principal arma contra el lavado de dinero que han implementado los gobiernos son las medidas de AML (Anti Money Laundering), incrustadas en las políticas de KYC que tienen las exchanges. Pero que es ineficaz cuando las exchanges no participan en las transacciones.

Es importante recordar lo mencionado sobre los servicios de mezcla. Estos pueden traer problemas a quienes actúen de forma honesta por sus costos o el riesgo de pérdida de criptomonedas, pero son funcionales a usuarios deshonestos, a delincuentes.

El reporte del Departamento de Justicia estadounidense también menciona una metodología similar al servicio de mezcla a la que denomina "Peel Chain". Ha relacionado esta maniobra con Corea del Norte frente a casos de fraude con algunas exchanges. Consiste en una cadena de direcciones que fraccionan un importe elevado de Bitcoin para asegurarse de que, dada la inmensa cantidad de direcciones, se haga imposible detectar indicios que permitan sospechar del destinatario final, propietario de una cuenta dentro del "sistema legal" en una exchange. El reporte presenta el siguiente gráfico:

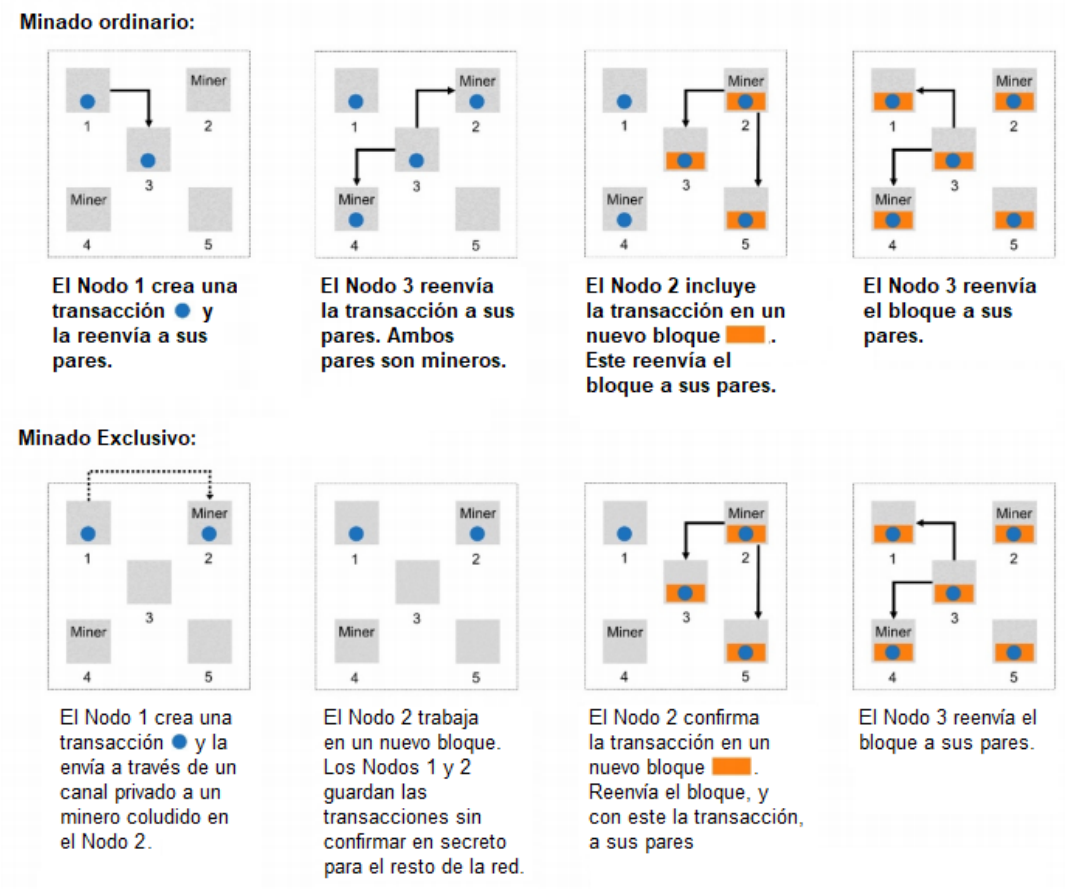


Cuadro 5.3. Servicio Peel-Chain. Fuente: U.S. Department of Justice, "Cryptocurrency – Enforcement Framework", 2020, Traducido, (En línea) Disponible en: https://www.justice.gov/archives/ag/page/file/1326061/download (Recuperado en fecha 26/05/2021), p. 28.

Es remarcable que los reportes oficiales cuantifican las operaciones sospechosas en Bitcoin. Lo que demuestra que Bitcoin es el principal objetivo a regular.

Otro mecanismo de lavado de dinero que se utiliza es el de la minería exclusiva. "*La minería exclusiva, que es un tipo de colusión entre un iniciador de transacciones y un solo minero o grupo, utiliza canales privados para confirmar transacciones en lugar de transmitirlas en una blockchain pública*"[99]. Este mecanismo permite a los delincuentes blanquear su dinero con apoyo de mineros, aprovechando las ventajas propias de la red. El siguiente gráfico muestra las diferencias entre la minería regular y la minería exclusiva:

[99] Felipe Erazo, "Expertos dicen que la "minería exclusiva" podría tener implicaciones negativas para la industria Blockchain", 2020, (En línea) Disponible en: https://es.cointelegraph.com/news/exclusive-mining-could-have-negative-implications-for-the-blockchain-industry-say-experts (Recuperado en fecha 26/05/2021)



Cuadro 5.4. Minería exclusiva. Fuente: Elias Strehle y Lennart Ante, "Exclusive Mining of Blockchain Transactions", 2020, Traducido, (En línea) Disponible en: https://www.blockchainresearchlab.org/wp-content/uploads/2020/05/Exclusive_Mining_of_Blockchain_Transactions_BRL_Working_Paper_No_13.pdf (Recuperado en fecha 26/05/2021)

La minería exclusiva tiene correlación con los peligros planteados acerca de la descentralización. Los pooles de minería que concentran poder de hash y una participación superior vuelven a representar en esta figura un problema contra la descentralización que Bitcoin intenta promover.

El lavado de dinero a través de las criptomonedas se ha incrementado en el último tiempo y lo han notado las autoridades de todas partes del mundo. Como un ejemplo mayúsculo, se puede estudiar el caso de los cárteles mexicanos. Diego Oré, columnista de Reuters, escribió que "*Las criptomonedas están emergiendo como un frente de batalla en la lucha de Latinoamérica contra los cárteles que se disputan el control de un vasto mercado de sexo, drogas, armas y personas (...). Usar Bitcoin para lavar dinero es una práctica que aumenta particularmente entre los cárteles de drogas como el Cártel de Jalisco la Nueva Generación (CJNG) y el Cártel de Sinaloa del capturado líder Joaquín 'El Chapo' Guzmán, según las*

autoridades de México y Estados Unidos"[100]. Una vez más Bitcoin está en el centro del problema para las autoridades.

Se debe señalar un aspecto fundamental que explica por qué Bitcoin es la criptomoneda predilecta para lavar dinero y no otras con mayor anonimato como las AECs. La causa principal de la elección de Bitcoin es que, junto con Ethereum, es la que cuenta con mayores facilidades para convertir en moneda fiat o fiduciaria.

Scammers: Los scammers o estafadores existen en internet desde antes de la aparición de Bitcoin. Han ido mejorando la calidad de sus engaños con el tiempo. Existen distintos tipos de estafas que circulan por la red. Entre estos destacan estafas con acciones benéficas, ofertas de empleo, oportunidades millonarias y estafas bancarias. Suelen tener un diseño de phishing que induzca a la víctima a caer en el scam. Pero lo llamativo es que, desde la invención de Bitcoin, este se ha transformado en una herramienta ideal para estas prácticas. Por ser irrastreable, anónimo, inmaterial y de acreditación inmediata sin importar la ubicación, Bitcoin es aquí, nuevamente, un catalizador del delito. Una prueba fehaciente de esto es el scam a gran escala producido a mediados de 2020, en un caso trascendente, cuando las cuentas de Twitter de personalidades importantes como Bill Gates, Jeff Bezos y Barack Obama fueron hackeadas para entablar una estafa con Bitcoin[101]. Bitcoin ha facilitado estas prácticas, pero también ha dado la oportunidad de perfeccionarlas y crear nuevas posibilidades.

Ransomware: Según lo define la compañía especializada en seguridad informática Panda Security, un ransomware "*…es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados*"[102]. Abundan casos de ransomware en la actualidad, como el de las negociaciones que la UCSF (Universidad de San Francisco de California) sostuvo con un delincuente que les había secuestrado información valiosa mediante encriptación. "*Expertos en ciberseguridad dicen que este tipo de negociaciones están sucediendo en todo el mundo –a veces por importes mayores– (…) 116,4 bitcoins fueron transferidos a billeteras electrónicas de Netwalker*

[100] Diego Oré, "Latin American crime cartels turn to cryptocurrencies for money laundering", 2020, Traducido, (En línea) Disponible en: https://www.reuters.com/article/idUSKBN28I1KD (Recuperado en fecha 26/05/2021)
[101] Amanda Mars, "Pirateadas las cuentas de Twitter de Obama, Biden, Bezos y Gates en una aparente estafa con bitcoins", 2020, (En línea) Disponible en: https://elpais.com/tecnologia/2020-07-15/piratean-las-cuentas-de-twitter-de-obama-biden-bezos-y-gates-en-una-aparente-estafa.html (Recuperado en fecha 26/05/2021)
[102] Panda Security S.R.L., "¿Qué es un Ransomware?", 2013, (En línea) Disponible en: https://www.pandasecurity.com/es/mediacenter/malware/que-es-un-ransomware (Recuperado en fecha 29/05/2021)

y el software de desencriptado se envió a la UCSF. (...) La USFC le contó a la BBC: 'La información que fue encriptada es importante para algunos de los trabajos académicos que perseguimos como una universidad qué sirve al bien público. Por lo que tomamos la difícil decisión de pagar una porción de al rescate, aproximadamente $1,14 millones, a los individuos detrás del ataque a cambio de una herramienta para desbloquear la información encriptada y recuperar la información que habían secuestrado"[103]. Otro caso más reciente que involucró a la Dirección General de Migraciones de Argentina que, en 2020, sufrió el secuestro de su base de datos con información sensible sobre ciudadanos y extranjeros. En el caso, "*...los secuestradores demandaban inicialmente 2 millones de dólares de rescate. Pasados siete días, el rescate aumentó a 4 millones de dólares, o aproximadamente 355 bitcoin*"[104], pero en esta ocasión, todo concluyó con la difusión al público de información confidencial tras la negatoria de la Dirección a pagar el rescate. Es remarcable en estos casos que el pago era requerido en Bitcoin. No obstante, esto no es una coincidencia. César Otero, cronista del Diario AS de España, en coincidencia con lo que se ha planteado, explica que "*Dada la celeridad y anonimato de una criptodivisa, el cibercriminal suele pedir un rescate en estas monedas. De hecho, hasta el 98% de los pagos por Ransomware son en criptomonedas, y el Bitcoin es de los métodos de pago más demandados y usados*"[105].

Bitcoin, fuente de financiamiento de actividades ilegales: Uno de los principales cuestionamientos a Bitcoin es su relación con el financiamiento de actividades terroristas y otros delitos de gran magnitud. Dentro de los casos que se han desarrollado, este es el primero que podría involucrar consecuencias directamente relacionadas con la vida de personas inocentes. Se vincula a Bitcoin con actividades tales como terrorismo, trata de personas y prostitución infantil. Al igual que en los casos que se han visto, Bitcoin es utilizado por organizaciones criminales para desarrollar sus actividades. Sin embargo, en algunos casos, Bitcoin no solo es una opción para estos grupos, sino que es la única. Según relata The New York Times, "*Los gobiernos de Occidente y algunos otros han catalogado a Hamás, el grupo miliciano de Palestina, como una organización terrorista y la han dejado fuera del sistema financiero tradicional. Sin embargo, (...) su brazo militar ha desarrollado una campaña cada vez más sofisticada para recaudar dinero por medio de Bitcoin. En la versión más reciente del sitio web que montó su ejército,*

[103] Joe Tidy, "How hackers extorted $1.14m from University of California, San Francisco", 2020, Traducido, (En línea) Disponible en: https://www.bbc.com/news/technology-53214783 (Recuperado en fecha 29/05/2021)
[104] Lawrence Abrams, "Netwalker ransomware hits Argentinian government, demands $4 million", 2020, Traducido, (En línea) Disponible en: https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-argentinian-government-demands-4-million (Recuperado en fecha 29/05/2021)
[105] César Otero, "Delitos y estafas, la otra cara de las Criptomonedas", 2019, (En línea) Disponible en: https://as.com/meristation/2019/08/09/betech/1565360759_387892.html (Recuperado en fecha 30/05/2021)

conocido como Brigadas Al Qassam, todos los visitantes reciben una dirección única de Bitcoin a donde pueden enviar la moneda digital, un método que hace que las donaciones sean casi imposibles de rastrear para las agencias de seguridad"[106]. Los métodos son similares a los delitos previamente mencionados, pero las consecuencias en esta clase de acciones son inmensamente más negativas. Existe, a su vez, una estrecha conexión entre estas actividades y la *darknet*, donde, entre otras cosas, se desenvuelve un mercado negro.

Mercado negro: Cuando explotó el auge de internet, el mercado negro se trasladó a la red. Si bien se halla desplegado por todo el mundo, "*La empresa forense blockchain, Chainalysis, ha descubierto que los mercados de la darknet ejercen una presencia desproporcionada en el criptosector de Europa oriental*"[107]. Las criptomonedas han tomado un rol preponderante en este ambiente delictivo, donde se comercia desde drogas hasta armas. De hecho, el mercado negro en línea fue uno de los primeros lugares donde Bitcoin comenzó a tener importancia. En el famoso caso del sitio Silkroad, Bitcoin y el mercado negro comenzaron una relación de simbiosis que aún prospera. "*El sitio era un mercado negro en línea de la Deep Web, operada por el servicio Tor que permite que los usuarios naveguen anónimamente y libres del monitoreo de sus actividades. Las cuentas de vendedores en su lanzamiento eran limitadas, pero ante el éxito del sitio, salieron a la venta por medio de un sistema de subasta. El método de pago en estas plataformas es la moneda virtual Bitcoin*"[108]. Este caso es uno más de los tantos que tienen en vilo a las autoridades. Los productos ilegales circulan y Bitcoin facilita el sistema de pagos. Esto pone a esta criptomoneda, una vez más, en la mira de quienes desean regularlo.

Una respuesta de los gobiernos: las CBDC

Ha quedado claro que la respuesta de los gobiernos es intentar regular Bitcoin. No obstante, sus planes podrían ir más allá. Dada la complicada tarea de regular un activo con características tan elusivas al control, los gobiernos se han planteado la creación de una moneda digital propia, creada por sus propios bancos centrales: las CBDC (Central Bank Digital Currency). Una moneda digital de este tipo sería mucho

[106] Nathaniel Popper, "Los terroristas ahora se financian con Bitcoin", 2019, (En línea) Disponible en: https://www.nytimes.com/es/2019/08/21/espanol/negocios/bitcoin-terrorismo.html (Recuperado en fecha 30/05/2021)
[107] Samuel Haig, "El sexto servicio de criptomonedas más grande de Europa del Este es un mercado en la darknet", 2020, (En línea) Disponible en: https://es.cointelegraph.com/news/eastern-europes-sixth-largest-crypto-service-is-a-darknet-market (Recuperado en fecha 30/05/2021)
[108] Milenio.com, "Qué es Silk Road y porqué su fundador irá a la cárcel", 2015, (En línea) Disponible en: https://www.milenio.com/estilo/que-es-silk-road-y-porque-su-fundador-ira-a-la-carcel (Recuperado en fecha 30/05/2021)

más fácil de controlar. Las altcoins son una amenaza para Bitcoin por las razones expuestas anteriormente, por sus características mejoradas, pero las CBDC son una amenaza distinta, especial.

Muchos países están planeando implementar en el mediano plazo sus propias CBDC. Algunos de los ejemplos más destacados son el de Brasil[109], China[110], Estados Unidos, Japón e, incluso, la Unión Europea[111]. Sin embargo, el BIS (Bank for International Settlements) concluye, en un estudio que realizó, que han notado que "…*los proyectos de CBDC difieren en extremo entre los países, tanto en sus motivaciones como en su diseño económico y técnico. Muchos bancos centrales están buscando modelos en los que una CBDC es directamente solicitada en el banco central y no por intermediarios privados*"[112].

Por otro lado, Marie Huillet, cronista en Cointelegraph, señala que, según el estudio del BIS, "*…2020 es el año en que el impulso de las monedas digitales de los bancos centrales (CBDC) realmente ha despegado*"[113]. El grado de aceptación parece ir en aumento y ello hace pensar que, indefectiblemente, siempre la población termina por depositar su confianza en el Estado. Depositar la confianza en el respaldo que los gobiernos ofrecen es contrario a lo que la idea original de Bitcoin proponía. Por lo que esta será una batalla más para Bitcoin que definirán los usuarios en función de la elección que hagan.

Matías Bari, cofundador de SatoshiTango dijo que "*En el comercio global, a nadie lo obligan a usar dólares. Particulares y empresas recurren al billete verde por la confianza que genera*"[114] y aquí las CBDC corren con ventaja frente a otras criptomonedas, dado el respaldo de países enteros detrás. Aunque las CBDC vayan en contra la esencia de Bitcoin, puede que la necesidad de un tercero confiable respaldando las operaciones sea más fuerte que las propuestas de Nakamoto.

Resulta inexorable pensar que las CBDC cuentan con una grave falencia respecto de Bitcoin: el anonimato. No obstante, en otro informe del BIS, los autores Bech y Garratt indican que "*La tecnología*

---

[109] Colin Adams, "El Banco Central de Brasil podría lanzar su propia CBDC para el año 2022", 2020, (En línea) Disponible en: https://es.beincrypto.com/banco-central-brasil-podria-lanzar-propia-cbdc-para-2022 (Recuperado en fecha 03/06/2021)

[110] Federico McDougall, "China y EE.UU. avanzan en su "propio Bitcoin": el motivo detrás de la carrera cripto y qué pasa en Argentina", 2021, (En línea) Disponible en: https://www.iproup.com/finanzas/20941-criptomonedas-que-paises-avanzan-con-su-propia-divisa-digital (Recuperado en fecha 03/06/2021)

[111] Javier Pastor, "Europa, Japón y EE.UU. se unen para la creación de una moneda digital con la que adelantarse a la de China y a la Libra de Facebook", 2020, (En línea) Disponible en: https://www.xataka.com/empresas-y-economia/europa-japon-ee-uu-se-unen-para-creacion-moneda-digital-que-adelantarse-a-china-a-libra-facebook (Recuperado en fecha 03/06/2021)

[112] Raphael Auer, Giulio Cornelli and Jon Frost, "BIS Working Papers. No. 880 - Rise of the central bank digital currencies: drivers, approaches and technologies", 2020, (En línea) Disponible en: https://www.bis.org/publ/work880.pdf (Recuperado en fecha 03/06/2021)

[113] Marie Huillet, "El interés público en las monedas digitales de los bancos centrales supera a Bitcoin en 2020", 2020, (En línea) Disponible en: https://es.cointelegraph.com/news/public-interest-in-central-bank-digital-currencies-surpasses-bitcoin-in-2020 (Recuperado en fecha 03/06/2021)

[114] Alejandro D'Agostino, "La cuenta regresiva ya empezó: qué países avanzan con su moneda digital y por qué proponen el ePeso argentino", 2020, (En línea) Disponible en: https://www.iproup.com/economia-digital/18191-criptomonedas-que-paises-impulsan-su-propia-divisa-digital (Recuperado en fecha 03/06/2021)

en la que se basarían las CBCC podría permitir a los bancos centrales ofrecer una alternativa de dinero digital con características de anonimato similares a las del efectivo. En su papel de emisor, el banco central tendría que decidir si exige o no la información del consumidor (la identidad real de quien utiliza una dirección pública). Esto determinaría el grado de anonimato ante terceros que proporcionarían las CBCC minoristas. Aunque puede parecer extraño que un banco central emita una criptomoneda que permite transacciones anónimas, eso es exactamente lo que hace con el dinero físico, es decir, el efectivo"[115]. Si esta característica fuera realmente aplicada, el atractivo de las CBDC podría incrementarse. La gente encontraría en las CBDC una de las cualidades más preciadas de Bitcoin y de la mayoría de las criptomonedas. Algo como esto, podría aumentar en gran medida el grado de aceptación de las CBDC en la sociedad y, en definitiva, la aceptación del público es la que permitirá prevalecer a una u otra criptomoneda. En este sentido, el economista Nouriel Roubini, profesor de Economía en la Universidad de Nueva York, "*…nota que las CBDC superarán a las criptomonedas con un uso más extendido incluso en el sector privado*"[116].

Los proyectos de CBDC son distintos y no solo no hay regulaciones aún, sino que son tan solo una idea en el horizonte. No obstante, aunque no sea en el corto plazo, representan un peligro más para Bitcoin.

[115] Morten Bech y Rodney Garratt, "Criptomonedas de bancos centrales", 2017, (En línea) Disponible en: https://www.bis.org/publ/qtrpdf/r_qt1709f_es.pdf (Recuperado en fecha 03/06/2021), p. 8.
[116] Samuel Town, "American economist: Bitcoin won't be digital gold and CBDCs will kill cryptos", 2021, Traducido, (En línea) Disponible en: https://finbold.com/american-economist-bitcoin-wont-be-digital-gold-and-cbdcs-will-kill-cryptos (Recuperado en fecha 03/06/2021)

CAPÍTULO 6. Análisis económico sobre la sustentabilidad de Bitcoin

La sustentabilidad de Bitcoin a largo plazo debe analizarse también desde un punto de vista económico. Puede que su esencia sea novedosa respecto de otros activos del mercado, pero está sometido a las mismas reglas que el resto.

A su vez, es conveniente analizar a Bitcoin desde tres enfoques diferentes: un análisis funcional, un análisis de su precio-valor y un análisis de sus amenazas.

Habrá conceptos que estarán presentes en más de un tipo de análisis, causando diferentes efectos. Algunos conceptos desencadenan distintos problemas o impedimentos para Bitcoin, según el lugar desde el que se lo pretenda analizar.

Es importante atender a la situación en que quedará Bitcoin al final de cada análisis.

Análisis funcional

La primera línea del Whitepaper de Bitcoin comienza hablando de "*Una versión puramente electrónica de efectivo…*"[117]. En este sentido, Bitcoin ha sido considerado desde su nacimiento como una moneda. El dinero, como tal, cuenta con tres funciones principales según autores como Wells, Krugman y Mankiw[118]. Estas tres funciones son:

- Unidad de medida
- Medio de cambio
- Reserva de valor

Dadas estas tres funciones que toda moneda debería tener para ser considerada como tal, es necesario dilucidar si Bitcoin cumple con ellas.

Reserva de valor: Cuando se habla de que una moneda cuenta con la función de preservar valor, se dice que tiene la capacidad de transferir el poder adquisitivo presente hacia el futuro. Es decir, que la conservación de esa moneda en el tiempo, permitirá comprar la misma cantidad de bienes o servicios en el futuro. No obstante, el dinero es una reserva de valor imperfecta, debido a la inflación en la economía. Un incremento generalizado y sostenido de los precios impide que el dinero sea una perfecta reserva de

[117] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Traducido, (En línea) Disponible en: https://bitcoin.org/bitcoin.pdf (Recuperado en fecha 07/06/2021)
[118] N. Gregory Mankiw, "Macroeconomía", Barcelona, España, Antonio Bosch Editor S.A., 2014, 8va. Ed., p. 148.

valor. Sin embargo, el dinero es utilizado globalmente y aquel que logra tener la mayor estabilidad en el tiempo, alcanza un nivel más alto de reserva de valor. Por otro lado, aquella moneda que es inestable y pierde valor incesantemente solo es sostenida por los gobiernos soberanos que la emiten.

Si Bitcoin nació con el objeto de ser dinero (o efectivo, como dice su Whitepaper), debería cumplir con la función de preservar su valor en el tiempo. Es evidente que Bitcoin no cumple con esto, dado que tiene un alto nivel de volatilidad en su cotización.

Bitcoin ha tenido subas y caídas en su valor que superan el 40% en cuestión de horas. La frecuencia de estos altibajos ha convertido a Bitcoin en un activo altamente especulativo. Incluso un organismo como la SEC ha dicho que "*...Bitcoin es 'Altamente especulativo' y con 'potencial para fraudes'*"[119]. Este componente especulativo, producto de la fuerte volatilidad en su cotización, lo ha descartado definitivamente como dinero, puesto que esa desmedida inestabilidad de su precio jamás le permitiría considerarlo una reserva de valor.

Unidad de medida: Los bienes y servicios pueden ser medidos en unidades monetarias. El dinero se usa como unidad de medida por su capacidad de ser fraccionado y su rol como patrón para medir los precios de los bienes y servicios. También se podría medir el precio de un bien en función de la cantidad de unidades de otro, de acuerdo con los precios relativos de la economía. Sin embargo, para estas mediciones se usa al dinero como patrón, por su capacidad de fraccionamiento.

Dicho esto, Bitcoin no podría considerarse como unidad de medida. Una vez más, su alta volatilidad no le permite ejercer esta función. Para poder llevar a cabo este rol, sería necesario que tuviera una cierta estabilidad en el tiempo y ser una unidad de referencia para determinar el precio de otros bienes.

Asimismo, la realidad muestra que, en la mente de los consumidores, inversores y especuladores, está arraigado el pensamiento de medir el precio de los bienes en moneda fiduciaria. Una irrefutable evidencia de esto, que descarta de pleno las esperanzas de Bitcoin de convertirse en unidad de medida, es que el precio del propio Bitcoin es medido en todo el mundo en moneda fiduciaria o fiat. Hablar de Bitcoin conlleva inexorablemente a expresar su precio en dólares, euros u otra moneda fiat.

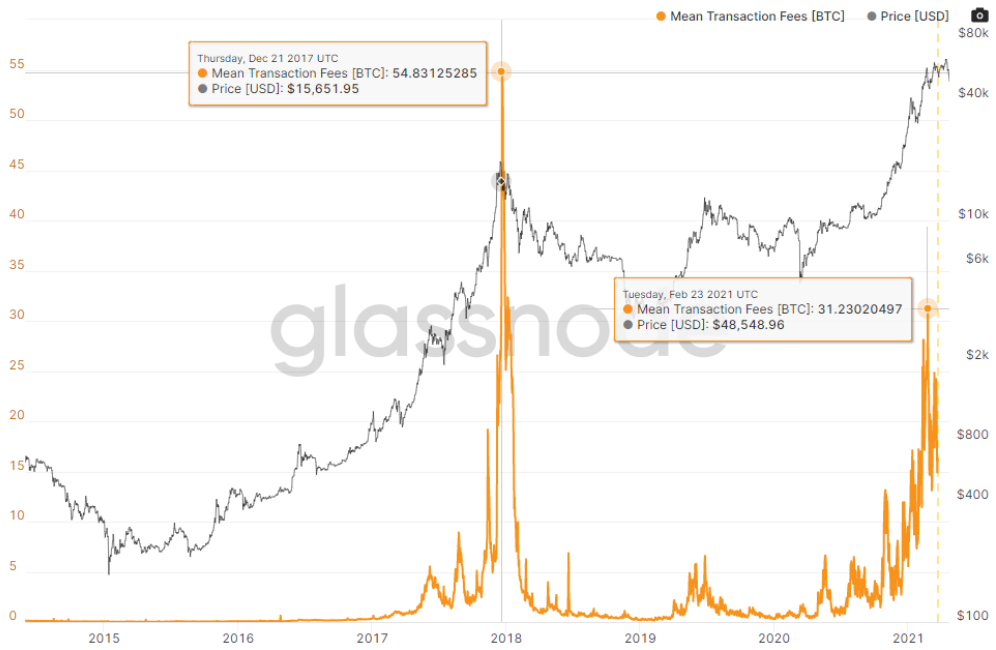
Medio de cambio: Ha habido intentos de convertir a Bitcoin en un medio de cambio de mayor aceptación en el mercado. La empresa Tesla anunció a fines de marzo de 2021 la posibilidad de comprar sus

[119] David Dierking, "SEC Calls Bitcoin 'Highly Speculative" With 'Potential For Fraud'', 2021, (En línea) Disponible en: https://www.thestreet.com/etffocus/market-intelligence/sec-calls-bitcoin-highly-speculative-potential-for-fraud (Recuperado en fecha 07/06/2021)

automóviles mediante Bitcoin[120]; lo mismo ocurrió con el sitio Mercado Libre[121]. Sin embargo, Tesla desestimó esta posibilidad unas cuantas semanas después[122]. A pesar de estos intentos, lo cierto es que Bitcoin cuenta con más de un argumento en contra para convertirse en un medio de cambio.

En primer lugar, cuenta con un problema de escalabilidad que se ha analizado previamente. Para ser un medio universal para ejecutar transacciones necesita contar con la capacidad de validar una cantidad mucho más elevada de transacciones por segundo. Las demoras en la validación de transacciones juegan en contra a la hora de considerar a Bitcoin como un medio de cambio aceptable.

En segundo lugar, las demoras en la validación provocan un nuevo problema: el aumento de las comisiones (fees). Tal como se ha mencionado, la congestión de la Mempool con abundancia de transacciones por validar, origina aumentos en las fees. Este tipo de congestiones ya ha ocurrido en la historia de Bitcoin, tal como surge del siguiente gráfico, donde se observan picos de 31 dólares (en 2017) y 54 dólares (en 2021) de comisión por transacción:



Cuadro 6.1. Tarifas de Bitcoin. Fuente: Glassnode Studio, "Bitcoin: Mean Transaction Fees", (En línea) Disponible en: https://studio.glassnode.com/metrics?a=BTC&m=fees.VolumeMean&c=USD (Recuperado en fecha 07/06/2021)

[120] Diego Gutiérrez, "Tesla ya acepta Bitcoin como forma de pago y puede ser una jugada maestra a largo plazo", 2021, (En línea) Disponible en: https://www.hibridosyelectricos.com/articulo/actualidad/tesla-acepta-bitcoin-como-pago-puede-ser-jugada-maestra/20210324144237043639.html (Recuperado en fecha 07/06/2021)

[121] Fernando Meaños, "Mercado Libre aceptará precios en Bitcoins: para vender qué productos estará disponible la opción cripto", 2021, (En línea) Disponible en: https://www.infobae.com/economia/2021/04/28/mercado-libre-aceptara-precios-en-bitcoins-para-vender-que-productos-estara-disponible-la-opcion-cripto (Recuperado en fecha 07/06/2021)

[122] Borja Díaz, "Tesla dice no al Bitcoin: La criptomoneda ya no será aceptada como método de pago", 2021, (En línea) Disponible en: https://www.caranddriver.com/es/coches/planeta-motor/a36416967/tesla-rechaza-bitcoin (Recuperado en fecha 07/06/2021)

El gráfico da fe de que en los momentos en que el uso de Bitcoin aumenta, las comisiones suben de forma desproporcionada. Un aumento en las comisiones no solo desincentiva el uso de Bitcoin para realizar transacciones, sino que, en casos de importes menores, las comisiones podrían comenzar a superar el valor de la transacción en sí misma. Por ejemplo, si se desea hacer una transacción de 15 dólares y el fee que se debe pagar es de 25 dólares, la situación seguramente concluiría con el desistimiento de la operación. En definitiva, los mayores costos por comisiones tornarían inviable realizar transacciones menores y, tal como se evidencia en la gráfica, no es un escenario improbable.

Por último, se podría decir que Bitcoin no cuenta con la capacidad de ser funcional como medio de pago de operaciones de bajos importes, mas sí de transacciones de proporciones mayores. Esa clase de operaciones suele darse en bienes registrables como inmuebles o automotores. No obstante, hay que decir que las operaciones que involucran bienes registrables requieren validar la licitud del origen de los fondos con lo que se adquirirán. Los notarios públicos pueden negarse a avalarlas debido al anonimato e irrastreabilidad de Bitcoin. Es difícil determinar con un adecuado grado de certidumbre que los fondos en Bitcoin no provienen de actividades criminales. Aun si los notarios estuvieran dispuestos a avalar dichas transacciones, las agencias antilavado pondrían trabas y podrían iniciar investigaciones al respecto. Esto desalienta aún más la utilización de Bitcoin y lo invalida, incluso, para este tipo de transacciones.

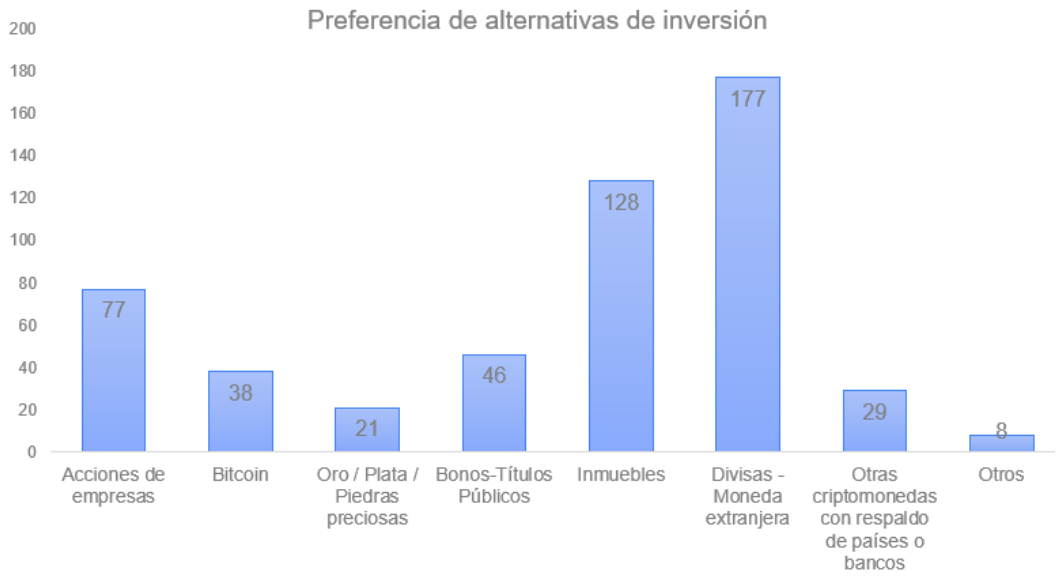
En consecuencia, es difícil pensar que Bitcoin logrará una función transaccional a largo plazo con tantos argumentos en contra, más aún cuando existen billeteras digitales de dinero fiduciario que son un sustituto con características similares, menos dificultades y de aceptación vigente en los mercados.

Instrumento financiero: Si Bitcoin no puede ser considerado como dinero, sí podría ser considerado como un instrumento financiero en el mercado de capitales y merece ser brevemente analizado como tal. Para analizar esta opción, se tomó como caso de estudio a Argentina, dado que es uno de los países con mayor adopción de criptomonedas según un estudio de principios de 2020[123].

A mediados de ese año, se realizó una encuesta sobre un total de 220 residentes de Argentina de diferentes edades, niveles de ingresos y niveles de estudios. La encuesta determinó que solo el 28% sabía lo que era Blockchain, el 59% no sabía y 13% creía tener una idea aproximada de lo que era. En cambio, al indagar si conocían lo que era Bitcoin, el 70% respondió afirmativamente, el 17% dijo tener una idea aproximada y tan solo el 13% respondió que desconocía lo que era Bitcoin. Así, se puede decir que, según la muestra, Bitcoin es mucho más conocido que la revolucionaria tecnología que le dio origen.

[123] Ezio Rojas, "Top 10 países en adopción de criptomonedas: Argentina y Colombia en el top 5", 2020, (En línea) Disponible en: https://es.beincrypto.com/top-10-paises-adopcion-criptomonedas-argentina-colombia-top-5 (Recuperado en fecha 09/06/2021)

Finalmente, en la encuesta se ofrecieron varias alternativas de inversión para que los encuestados eligieran hasta un máximo de tres opciones de dónde invertir sus ahorros, según el atractivo que vieran en ellas. Los resultados fueron los siguientes:



Cuadro 6.2. Preferencia de alternativas de inversión. Fuente: Elaboración propia, mediante GoogleForms

De la observación del gráfico surge que inversiones más tradicionales como la adquisición de divisas, inmuebles y acciones de empresas superan ampliamente a Bitcoin como una alternativa de inversión. Se puede entender que el público prefiere activos con mayor nivel de tangibilidad para invertir sus ahorros. Por otro lado, es interesante observar que otras criptomonedas con respaldo de países o bancos tuvieron un grado de elección muy cercano a Bitcoin. Esto puede representar la importancia que el público en general le da a la existencia de una figura real detrás de un activo.

En consecuencia, se puede concluir que en general existe una aversión a invertir en Bitcoin. Esto puede explicarse por su alto componente especulativo, a raíz de su alta volatilidad. En estas condiciones, Bitcoin podría ser un interesante activo financiero para especular a corto plazo, pero inviable para invertir ahorros a largo plazo.

Análisis precio-valor

Es sabido que precio y valor poseen definiciones distintas. La Real Academia Española define al precio como el "*Valor pecuniario en que se estima algo*"[124]. Se entiende entonces que el precio es la forma

[124] Real Academia Española, "Precio", (En línea) Disponible en: https://dle.rae.es/precio (Recuperado en fecha 12/06/2021)

en que el valor se expresa en dinero. Por otra parte, existe el valor intrínseco, precio teórico o valor fundamental, que "*…es el valor que se obtiene teniendo en cuenta todos los componentes que rodean a un activo, incluyendo elementos tangibles e intangibles*"[125].

Se considera que el respaldo de instituciones o gobiernos es el que justifica el valor de las monedas fiduciarias. Para otros activos, como las acciones de empresas, puede verse un capital, una marca o patentes, fundamentando su valor. Sin embargo, el principal fundamento del valor de Bitcoin es su tecnología basada en la Blockchain. Pero esta tecnología no es propiedad de Bitcoin; otras criptomonedas competidoras, que también cuentan con ella, se hallan en posición de ofrecer mejores ventajas y desplazar a Bitcoin del mercado.

El Premio Nobel de Economía Paul Krugman es muy crítico del verdadero valor de Bitcoin y ha ironizado con que "*Su valor se basa en la percepción de que es una forma tecnológicamente sofisticada de protegerse del inevitable colapso del dinero fiduciario, que se avecina uno de estos días, o tal vez uno de estos siglos*"[126].

Entonces, Bitcoin puede que no tenga un valor intrínseco significativo, tal como plantean economistas de la talla de Krugman. Pero es importante estudiar el comportamiento de su precio a través del tiempo y los riesgos relacionados con este.

Existen diversos escenarios posibles relacionados con el precio de Bitcoin que pueden representar su caída. Estos escenarios se pueden analizar en función de cuatro variables:

- R = Recompensa de un nuevo bloque
- f = Tarifas o comisiones (fees)
- C = Costos (equipamientos, energía)
- PB = Precio de Bitcoin

Para que minar Bitcoin sea sustentable, debe ser rentable en el tiempo. Utilizando las variables expuestas, la fórmula para determinar si minar Bitcoin es rentable, sería:

$$R \times PB + f \times PB - C > 0$$

[125] Andrés Sevilla Arias, "Valor intrínseco", (En línea) Disponible en: https://economipedia.com/definiciones/valor-intrinseco.html (Recuperado en fecha 12/06/2021)

[126] Carla Mozée, "Paul Krugman throws in the towel on calling the demise of bitcoin: 'Think of it as a cult that can survive indefinitely'", 2021, Traducido, (En línea) Disponible en: https://www.businessinsider.in/cryptocurrency/news/paul-krugman-throws-in-the-towel-on-calling-the-demise-of-bitcoin-think-of-it-as-a-cult-that-can-survive-indefinitely/articleshow/82784951.cms (Recuperado en fecha 12/06/2021)

Si la suma de las recompensas (R) y las tarifas (f) menos los costos (C) es mayor a cero, entonces minar Bitcoin es rentable. No obstante, de cada variable surgen observaciones a realizar.

En cuanto a las recompensas, hay que tener en cuenta que son exactas, que se distribuyen cada 10 minutos (tiempo en adición de cada nuevo bloque a la Blockchain) y que cada cuatro años se reducen a la mitad debido al *halving*.

Tanto las recompensas como las tarifas guardan estrecha relación con el precio de Bitcoin (PB). A diferencia de los costos que, generalmente, se pagan en dinero fiduciario, las recompensas y las tarifas se adquieren en Bitcoin. Para determinar la ganancia por medio de la fórmula, se debe homogeneizar la unidad de medida, multiplicando los Bitcoin adquiridos mediante recompensa y tarifas por el precio de la criptomoneda.

Respecto de las tarifas, es crucial tener presente que, si sufrieran un aumento desmedido, esto conllevaría consecuencias negativas para Bitcoin. Como se ha visto, tarifas elevadas significarían un desincentivo generalizado en el uso de Bitcoin.

Los costos se componen principalmente del equipamiento y la energía necesaria para el minado. Es dable considerar que los costos pueden variar en el tiempo, pero seguramente siempre serán mayores a cero.

En función de lo expuesto, es de interés suponer escenarios de acuerdo con el comportamiento que cada variable puede asumir:

Escenario 1 – Incremento de nodos: En el apartado sobre los pooles de minería del Capítulo 4, se ha comentado la posibilidad de que, en un escenario en el que Bitcoin goza de un florecimiento y expansión, comenzaría a verse un ingreso de más nodos a la red intentando captar las recompensas que un nuevo bloque candidato otorga. Como allí se ha descripto, una creciente cantidad de nodos mineros implicaría más competencia y, luego, una pérdida gradual de ganancia marginal, a menos que los costos bajen o el precio de Bitcoin o las tarifas aumenten. Considerando la problemática de aumentar las tarifas, que la disminución de costos tiene un límite y, que las recompensas son constantes cada 10 minutos, el sostenimiento del sistema dependería exclusivamente de que el precio de Bitcoin en el mercado aumente. Si el precio se mantuviera estable o incluso bajara, esto haría desaparecer, en primer término, a los mineros más pequeños, concentrando el poder de hashrate en los mineros con mayor solvencia. Hay que recordar que los nodos que no pertenecen a los grandes pooles de minería son los que fortalecen la

descentralización. Su desaparición representaría un incremento en la centralización de la red, se perdería la confianza en la criptomoneda y acabaría por derrumbarse definitivamente.

Escenario 2 – Aumento de costos: Los costos podrían subir por muchos motivos. Podría haber un aumento de tarifas de la energía eléctrica, especialmente en países como China, donde se encuentra la mayor parte de la minería de Bitcoin. Otra posibilidad es que aumenten los precios de los insumos necesarios para la minería. Sin importar el motivo que aconteciera, se debe observar que, si el peso de los costos aumentara, sería imprescindible que las tarifas o el precio de Bitcoin aumenten para que la minería continúe siendo rentable. No es necesario volver a mencionar las limitaciones económicas que recaen sobre las tarifas o las limitaciones de protocolo inherentes a las recompensas. Dicho esto, cabe destacar que el costo promedio de minar un Bitcoin tiene un peso en la ecuación que no puede pasarse por alto. En 2020, "*…la empresa de inteligencia BitOoda estima que el precio promedio de minar un bitcoin (1 BTC) es de USD 5000…*"[127]. Teniendo en cuenta que el precio de Bitcoin ha permanecido durante mucho tiempo por debajo de los 10.000 dólares luego de su máximo local a fines de 2017, este costo puede considerarse alto. Aún peor fue la situación que se dio por momentos en 2019, cuando el costo de minar un Bitcoin superó al precio de la criptomoneda. De acuerdo con un "*…informe del JP Morgan, el precio del Bitcoin a principios de 2019 se mueve en torno a los 3.600 dólares por token, mientras que el coste unitario de minado supera los 4.060 dólares de media en todo el planeta, con pequeñas variaciones dependiendo del país*"[128]. Luego de esto, la red de Bitcoin continuó vigente solo porque las recompensas de minado aún eran altas. En resumen, el costo de Bitcoin no es barato y hay evidencia empírica de que puede superar su precio. Si volviera a producirse este escenario en el largo plazo, cuando las recompensas disminuyan de acuerdo con lo que su protocolo estipula, Bitcoin dejaría de ser rentable y sucumbiría.

Escenario 3 – Nuevos gastos: Es probable que se incorpore en el futuro una nueva variable a la fórmula. En un futuro no muy lejano, se tendrán que ponderar gastos. Estos gastos serán burocráticos, impositivos o de otro tipo, originados en las regulaciones que los distintos países e incluso organismos supranacionales tienen en agenda. Esta variable existe actualmente, pero su incidencia viene en aumento. Lejos de ayudar,

[127] José Colmenares, "Minar hoy 1 Bitcoin tiene un costo de USD 5000 en promedio", 2020, (En línea) Disponible en: https://www.criptonoticias.com/mineria/minar-1-bitcoin-costo-usd-5000-promedio (Recuperado en fecha 12/06/2021)
[128] Eduardo Álvarez, "El coste de minar un Bitcoin ya supera al precio de venta", 2019, (En línea) Disponible en: https://computerhoy.com/noticias/tecnologia/coste-minar-bitcoin-ya-supera-previo-venta-368787 (Recuperado en fecha 12/06/2021)

representarían otra disminución en las ganancias. Al incluir esta variable, la ecuación podría representarse de la siguiente manera:

$$R \times PB + f \times PB - C - G > 0$$

La inclusión de nuevos gastos (G) podría significar un peso demasiado grande para que los primeros dos términos puedan sopórtalo. En un escenario en que los gastos ahogaran a las dos fuentes de ingresos (R y f), sería inevitable el colapso de la red de Bitcoin.

Escenario 4 – La tragedia de los comunes: José Rodríguez, columnista del sitio IHODL, explica que "*La Tragedia de los Comunes hace referencia a un momento futuro en el que habrá menos mineros de bitcoin disponibles debido a la poca o ninguna recompensa de la minería. Las únicas comisiones que se obtendrán provendrán de las comisiones de transacción, que también disminuirán con el tiempo a medida que los usuarios opten por pagar comisiones más bajas por sus transacciones*"[129]. En este escenario, se pretende describir cómo el halving que se establece en el protocolo de Bitcoin, acabará por tornar insignificante la recompensa del minado: la disminución de la variable R. Por ello, a raíz de esta tendencia, la ecuación quedará reducida a que las tarifas tendrán que afrontar todo el peso de los costos, a menos que se optimice el minado o se produzca un constante aumento del precio de Bitcoin.

Es importante aclarar que, fuera de un enfoque puramente económico, existe una alta probabilidad de que se produzca un ataque del 51% en un escenario como este, dada la reducción de mineros que se plantea.

Escenario 5 – Impopularidad: Las expectativas y la reputación de un activo, suelen impulsar o sepultar el precio de este. La vinculación generalizada de Bitcoin con actividades criminales y con perjuicios severos a la ecología, o la aparición de regulaciones, pueden ocasionar una caída abrupta del precio de Bitcoin. El precio de Bitcoin es un factor determinante en la ecuación expuesta, dado que influye directamente en las magnitudes de las variables que aportan ingresos. El derrumbe de enero de 2018 fue prueba de la factibilidad de este escenario. Las principales razones que se le atribuyen a tal caída en el precio de Bitcoin fueron las sospechas de fraude, comercio sospechoso y temor a mayores regulaciones. Otro ejemplo fue

[129] José Rodríguez, "Proof-of-stake: cómo funciona", 2018, (En línea) Disponible en: https://es.ihodl.com/tutorials/2018-07-06/proof-stake-como-funciona (Recuperado en fecha 14/06/2021)

el ocurrido en mayo de 2021, cuando se puso en el centro de la escena la contaminación que producía el minado de Bitcoin y que redujo a la mitad su precio e hizo caer fuerte su capitalización de mercado.

Análisis de amenazas

Fahad Kamal, jefe de inversiones del banco Société Générale, ha dicho que "*…las amenazas regulatorias, su alta utilización de la energía y la competencia de otras criptodivisas podrían significar que el Bitcoin pierda su relevancia en la próxima década*"[130]. En su pronóstico, Kamal menciona tres grandes amenazas para Bitcoin. Menciona la amenaza de las regulaciones, tal como se ha estudiado en capítulos previos, pero, además del alto gasto de recursos energéticos, menciona la fuerte competencia de otras criptomonedas como una amenaza significativa.

Desde un punto de vista económico, Bitcoin se ve amenazado principalmente por tres elementos: la competencia, la volatilidad y las stablecoins (monedas estables).

En primer lugar, la competencia refiere a aquellas altcoins que se hallan en condiciones de desplazar a Bitcoin por contar con cualidades superiores o distintivas. Son una amenaza real, dado que los nuevos proyectos han podido observar las experiencias de Bitcoin y han visto sus puntos débiles para encontrar la manera de solucionarlos.

En segundo lugar, la volatilidad del precio de Bitcoin es un hecho. Esto se puede comprobar con facilidad con tan solo observar el comportamiento del precio de Bitcoin través del tiempo. Vale enfocarse en esta amenaza para saber adónde puede posicionar a Bitcoin.

Por último, las stablecoins son un caso especial, dado que son una combinación de las dos primeras. Las monedas estables son, al mismo tiempo, una competencia para Bitcoin y resuelven aparentemente el problema de la volatilidad.

Los tres merecen ser estudiados de manera individual.

Competencia: Se suele decir que "*Cualquier criptomoneda que no sea el Bitcoin puede ser una altcoin…*"[131], sin embargo, para un mejor análisis, es conveniente segregar a las CBDC y las stablecoins del amplio conjunto de altcoins. Es importante separar estas dos especies del resto de las altcoins por sus

[130] Diario Infobae, "El pronóstico apocalíptico sobre el Bitcoin de un gurú de las finanzas: puede 'desaparecer' frente a sus competidores en pocos años más", 2021, (En línea) Disponible en: https://www.infobae.com/economia/2021/04/29/el-pronostico-apocaliptico-sobre-el-bitcoin-de-un-guru-de-las-finanzas-puede-desaparecer-frente-a-sus-competidores-en-pocos-anos-mas (Recuperado en fecha 14/06/2021)

[131] Davies, "¿Qué son las altcoins y qué tienen que ver con el Bitcoin?", (En línea) Disponible en: https://www.daviescoin.io/es/blog/que-son-las-altcoins-y-que-tienen-que-ver-con-el-bitcoin (Recuperado en fecha 14/06/2021)

características únicas.

Para el caso de las CBDC, estas contarían con un respaldo gubernamental que ninguna otra altcoin tiene. La amenaza de las CBDC ha sido analizada desde un punto de vista regulatorio en el capítulo precedente. No obstante, desde un enfoque netamente económico, debe decirse que las CBDC, por ser emitidas por los gobiernos, tienen una importancia que no puede ser obviada. El Premio Nobel de Economía, Eric Maskin, en conversación con la cadena de noticias CNN explica que "*Si el Bitcoin se hiciera realmente popular, de modo que la gente comenzara a usar Bitcoin en lugar de dinero normal, dólares, pesos, euros, etc. Entonces sería mucho más difícil para los gobiernos tener una política monetaria. Y la política monetaria es un arma muy importante contra la recesión. Por ello, si el gobierno quiere combatir una recesión, lo que puede hacer es expandir la oferta monetaria para darle a los empresarios más liquidez, para expandir el empleo, expandir la producción y devolver la economía a la normalidad*"[132]. Las CBDC no interferirían con estas facultades de los países para hacer frente a épocas de crisis y ahí es donde radica su importancia económica.

Tal vez, la amenaza más importante para Bitcoin se halla entre las criptomonedas que son similares, pero mejoradas en sus cualidades, Es por ello que vale la pena volver a hacer mención de esto, dado que la competencia forma parte fundamental de un estudio de carácter económico. Dejando de lado las CBDC y las stablecoins, existen numerosos proyectos de criptomonedas que superan a Bitcoin en muchos y diversos aspectos. A principios de 2021, existían miles de criptomonedas con diferentes características. Sin embargo, es de destacar la presencia de la criptomoneda Ethereum (ETH). Citando una vez más a Fahad Kamal, ha dicho que "*En comparación con bitcoin, ethereum es más escalable, ofrece más usos y soluciones, como contratos inteligentes que ya se utilizan en muchos sectores, y está respaldado con tecnología blockchain superior. Ethereum ya está años por delante de bitcoin en todo menos en precio y fama*"[133]. Ethereum ha incrementado su popularidad y capitalización de mercado posicionándose en el segundo lugar entre las criptomonedas y se ha acercado con velocidad a Bitcoin. Por otro lado, cuenta con dos ventajas: su estrecha vinculación con los smartcontracts, cuya adopción va en aumento, y el probable paso a Proof of Stake, que implicaría una baja significativa de sus fees, dado que no es toda la red la que

[132] Eric Maskin, Entrevista televisiva del Canal CNN, 2021, Traducido, (En línea) Disponible en: https://cnnespanol.cnn.com/video/riesgos-bitcoin-gobiernos-premio-nobel-economia-eric-maskin-oppenheimer-presenta-cnn (Recuperado en fecha 14/06/2021)

[133] Sitio Forbes, "Ethereum apunta a un precio de US$5.000, ¿qué pasa con Bitcoin y Dogecoin?",2021, (En línea) Disponible en: https://forbes.co/2021/05/03/actualidad/ethereum-apunta-a-un-precio-de-us5-000-que-pasa-con-bitcoin-y-dogecoin (Recuperado en fecha 14/06/2021)

tiene la posibilidad de validar el próximo bloque de la cadena como en Proof of Work, sino un grupo seleccionado de acuerdo con el protocolo. Probablemente, Ethereum sea el competidor que representa la mayor amenaza para Bitcoin.

Otras altcoins tienen otras ventajas competitivas como: transacciones gratuitas, sin abonar fees; confirmación de transacciones más veloz; ser más amigables con el medio ambiente; mayor grado de anonimato; o un nivel de protección elevado contra la volatilidad de cotización.

Nano (NANO) es una criptomoneda a tener en cuenta respecto de las primeras dos ventajas mencionadas. De acuerdo con Rubén Colomer, que escribe en el sitio Lemmin Work, "*Nano es una criptodivisa con cero comisiones, que se basa en el voto representativo abierto para el consenso y la seguridad. Para ser claros, las tasas cero no se deben a un subsidio temporal – las tasas cero están incorporadas en el protocolo. Además de tener las tasas más bajas, Nano también gana en el tiempo que se tarda en confirmar una transacción, que es de 0,14 segundos*"[134]. Esta criptomoneda ofrece validaciones casi instantáneas y ausencia de comisiones en las transacciones. Estas cualidades hacen de Nano una amenaza para Bitcoin a considerar. No solo porque Bitcoin posee fees, sino porque, según lo visto previamente, es probable que sus tarifas sigan subiendo a medida que las recompensas sean reducidas mediante el halving. Asimismo, Bitcoin no puede competir con el tiempo de validación de Nano, ya que, tal como se ha analizado, su protocolo tiene serios problemas de escalabilidad.

Otra criptomoneda sin tarifas o comisiones es IOTA (MIOTA). Cuenta con la misma ventaja competitiva que Nano, sin embargo, su tiempo de validación de transacciones es mucho mayor, ya que "*tiene una tasa de confirmación del 79% en 10 minutos…*"[135]. No obstante, IOTA se caracteriza también por ser mucho más amigable con el medio ambiente que otras. Con su sistema Tangle, "*…dos miembros de la red pueden ejecutar una micro-transacción mediante uno o muchos canales de micropagos alternativos, y así pueden paralelizar la ejecución de transacciónes en varias cadenas de bloques distintas (…) Tan solo informarán al ecosistema del resultado final de todas las micro-transacciones, lo cual trae una gran eficiencia, tanto en costes de energía como en capacidad de procesamiento*"[136]. Este sistema

[134] Rubén Colomer, "¿Qué criptomonedas tienen menos comisiones por transacción?", 2021, (En línea) Disponible en: https://www.lemmingatwork.com/inversiones/criptomonedas/que-criptomonedas-tienen-menos-comisiones (Recuperado en fecha 14/06/2021)

[135] Rubén Colomer, "¿Qué criptomonedas tienen menos comisiones por transacción?", 2021, (En línea) Disponible en: https://www.lemmingatwork.com/inversiones/criptomonedas/que-criptomonedas-tienen-menos-comisiones (Recuperado en fecha 14/06/2021)

[136] DerBlaueMond, "Éstas son las criptoalternativas al desastre energético (y medioambiental) de Bitcoin", 2018, (En línea) Disponible en: https://www.elblogsalmon.com/economia/estas-son-las-criptoalternativas-al-desastre-energetico-y-medioambiental-de-bitcoin (Recuperado en fecha 14/06/2021)

permite la validación de transacciones sin la necesidad de que toda una red de nodos deba buscar intensivamente el siguiente bloque de la cadena, como ocurre con Bitcoin.

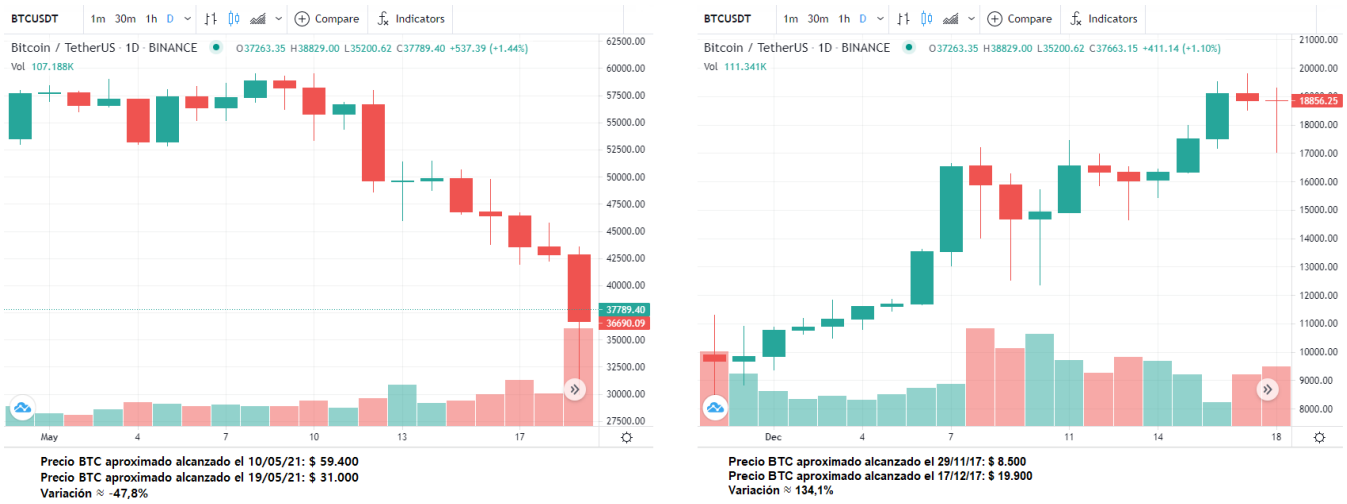
Si se priorizara la privacidad de los usuarios, Bitcoin se halla en inferioridad con las criptomonedas que se han mencionado y cuyos protocolos se han desarrollados en el Capítulo 2: Monero, Dash y Zcash.

En cuanto a la volatilidad, una de las principales debilidades de Bitcoin, las stablecoins conservan una ventaja competitiva que difícilmente sea igualada: su estabilidad de cotización. Representan una amenaza interesante como competidoras.

Finalmente, cabe destacar que nuevos proyectos surgen mes a mes y que pueden superar incluso a estas criptomonedas competidoras que ya han superado a Bitcoin en casi todos los aspectos.

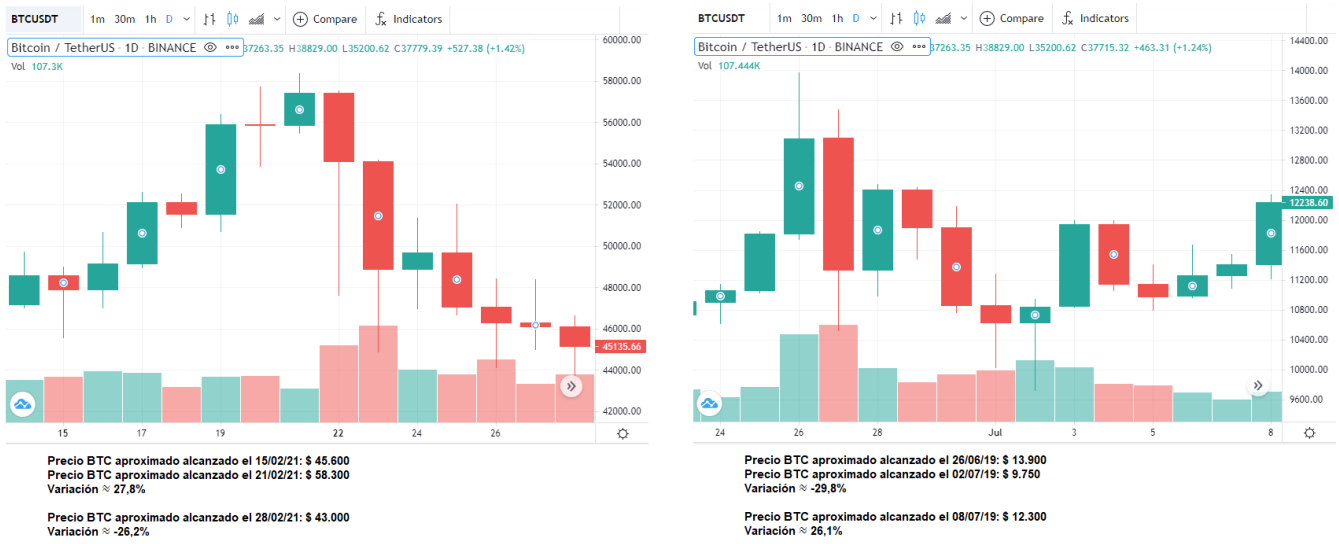
Volatilidad: Se ha observado que el nivel de protección contra la volatilidad es una ventaja competitiva que otras criptomonedas tienen frente a Bitcoin. Sin embargo, la volatilidad no es solo una desventaja de Bitcoin en comparación con otras criptomonedas, sino que, incluso ante la ausencia de competencia, la volatilidad podría significar el fin de Bitcoin en el mercado. Una volatilidad desmesurada y constante en el tiempo ahuyentaría a todo tipo de inversores, incluso a aquellos con menor aversión al riesgo.

La evolución del precio de Bitcoin es extremadamente volátil. Posee, además, una volatilidad sostenida en el tiempo y pocas veces vista. En reiteradas ocasiones, ha sufrido variaciones intensas en periodos de tiempo que, en muchos casos, no superan los 15 días. Estas variaciones han alcanzado porcentuales de hasta 134% al alza en menos de 20 días y del 47% a la baja en tan solo 9 días, es decir, duplicación de precio y reducción a la mitad de su cotización, respectivamente. Estos dos ejemplos se pueden observar en los siguientes gráficos del precio de Bitcoin, con las fechas y variaciones aproximadas al pie:



Cuadro 6.3. Volatilidad de Bitcoin. Fuente: CoinMarketCap, (En línea) Disponible en: https://coinmarketcap.com/es/currencies/bitcoin (Recuperado en fecha 14/06/2021)

Por otro lado, las bajas y alzas coexisten en periodos igual de cortos. Por ejemplo, en el periodo de tiempo existente entre las fechas 15/02/2021 y 28/02/2021, se da un máximo local de $ 59.300. Desde la primera fecha en que el precio de Bitcoin era de $ 45.600 subió en tan solo 6 días (el día 21/02/2021) al precio de $ 59.300 (un alza del 27,8%) para bajar 7 días después hasta los $ 43.000 (una caída del 26,2%). El mismo escenario se da a la inversa con un mínimo local de $ 9.750 entre las fechas 26/06/2019 y 08/07/2019. El precio de fecha 26/06/2019 era de $ 13.900, alcanzando el mínimo local el día 02/07/2019 de $ 9.750 (una baja del 29,8%), para volver a subir hasta los $ 12.300 el 08/07/2019 (un alza de 26,1%). Este ejemplo quedaría graficado de la siguiente forma:



Cuadro 6.4. Volatilidad de Bitcoin con mínimos y máximos locales. Fuente: CoinMarketCap, (En línea) Disponible en: https://coinmarketcap.com/es/currencies/bitcoin (Recuperado en fecha 14/06/2021)

En los gráficos se ve plasmado que la volatilidad de Bitcoin es un hecho. Pero es importante entender cuáles son las probables causas de semejante nivel de volatilidad. Entre estas causas probables, destacan dos.

Por un lado, una posible causa tiene un origen psicológico que se denomina FOMO – Fear Of Missing Out. Según el Diccionario de Cambridge, el FOMO es "*un sentimiento de preocupación por perderse eventos excitantes que otra gente aprovechará, especialmente cosas que se ven en las redes sociales*"[137]. Este sentimiento representa un miedo al arrepentimiento de no haber aprovechado una oportunidad, de haberla dejado pasar. Con relación a los efectos económicos de este sentimiento, el mismo ocasiona una falta de racionalidad en las decisiones, las que se toman de forma impulsiva y sin medir riesgos. Es común que se hable de este fenómeno cuando se trata de Bitcoin. Debido a la falta de fundamentos de su valor intrínseco, cuando Bitcoin sufre alzas abruptas en su cotización, suele atribuírsele estos aumentos al FOMO. Una fuerte suba en el nivel demandado, hace subir el precio en función del juego de oferta y demanda, pero sin una motivación real que lo justifique.

Los resultados de un comportamiento FOMO pueden ser tres: no vender a tiempo el activo, tolerar pérdidas por más tiempo del razonable, comprar sin analizar la conveniencia con base en argumentos reales. En los tres casos, la demanda se ve fortalecida y hacen subir el precio de Bitcoin. Sin embargo, estas alzas abruptas y sin fundamentos sustentables, acabarán por tener una caída también abrupta. Por ello, tanto en las altas como en las bajas, se puede encontrar en el FOMO una posible causa de la volatilidad de Bitcoin.

La otra causa, mucho más real y concreta, de la volatilidad a la que el precio de Bitcoin se expone son las ballenas. Ya se ha analizado sobre las nocivas consecuencias que pueden tener las ballenas para Bitcoin y su idea de descentralización. Pero también tienen influencia en las fluctuaciones de precio. Existe una relación más directa y precisa entre las ballenas y la volatilidad que sufre el precio de Bitcoin. Por ello, se puede afirmar que cuando una ballena compra o vende Bitcoin, el precio de la criptomoneda se mueve bruscamente. La explicación radica, una vez más, en el crecimiento repentino de la oferta –si venden– o de la demanda –si compran–, haciendo bajar o subir el precio en el momento en que operan.

Podría argumentarse que las denominadas ballenas pueden existir en otros instrumentos financieros y no únicamente con Bitcoin. Sin embargo, también puede contraargumentarse que en la mayoría del resto los de instrumentos financieros está presente la SEC y otros organismo de control para

[137] Cambridge Dictionary, "FOMO", Traducido, (En línea) Disponible en: https://dictionary.cambridge.org/es/diccionario/ingles/fomo (Recuperado en fecha 15/06/2021)

evitar esta clase de abusos por parte de grandes tenedores, por ejemplo, para el caso de acciones de empresas.

Por otra parte, una comparación entre Bitcoin y las acciones de empresas u otros activos similares, que también sufren, en algunos casos, de volatilidad de precios, solo es válida si se descarta la idea de que es una moneda y se lo considera definitivamente como un instrumento financiero, con una función únicamente de resguardo de valor o especulación. Dicho esto, es importante citar al Premio Nobel, Roubini, cuando dice que *"…la volatilidad de precio elimina la posibilidad de las monedas digitales de convertirse en una perfecta reserva de valor*"[138]. En consecuencia, si cabía alguna posibilidad de concebir a Bitcoin como una moneda, esta clase de comparaciones elimina por completo esa posibilidad. Y, a su vez, su volatilidad de precio la inhabilita para ser una reserva de valor, cualidad que sí poseen otros activos. Por lo que se podría concluir que solo tiene utilidad como un activo altamente especulativo.

Stablecoins: Es conveniente tratar a las monedas estables como una amenaza particular. Las stablecoins reúnen dos formas de peligro para Bitcoin. No son solo parte de las criptomonedas competidoras, sino que, además, representan la única categoría de criptomoneda que se ha dispuesto a resolver el problema de la volatilidad que afecta, en especial, a Bitcoin.

Un informe publicado por el Banco Central Europeo, expresa que, "*Para mantener un precio estable frente a la moneda, o monedas, de referencia, algunas stablecoins se comprometen a mantener fondos y/u otros activos ("colaterales") como respaldo de las tenencias de stablecoins. Alternativamente, las stablecoins se basan en un mecanismo que intenta igualar la oferta y la demanda para mantener la paridad entre la stablecoin y la moneda de referencia, o monedas, y para guiar las expectativas de los usuarios sobre su valor futuro*"[139]. Así, el informe explica cómo actúan las criptomonedas estables para estabilizar su cotización en el mercado y evitar altibajos bruscos e incertidumbre de precio. En virtud de este documento, la entidad europea "*califica a las criptomonedas ancladas o stablecoins como dinero electrónico. Bitcoin y otras criptomonedas se clasifican como instrumentos financieros*"[140]. Con esto, una

[138] Samuel Town, "American economist: Bitcoin won't be digital gold and CBDCs will kill cryptos", 2021, Traducido, (En línea) Disponible en: https://finbold.com/american-economist-bitcoin-wont-be-digital-gold-and-cbdcs-will-kill-cryptos (Recuperado en fecha 15/06/2021)

[139] Banco Central Europeo, "Stablecoins, implicancias para la política monetaria, estabilidad financiera, infraestructura de mercado y pagos y supervisión bancaria en la eurozona", 2020, Traducido, (En línea) Disponible en: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op247~fe3df92991.en.pdf?b85631de8b2fdfa5395c2a4c87de05e1 (Recuperado en fecha 15/06/2021)

[140] Glenda González, "Comisión Europea: stablecoins son dinero electrónico, bitcoin instrumento financiero", 2020, (En línea) Disponible en: https://www.criptonoticias.com/regulacion/comision-europea-stablecoins-dinero-electronico-bitcoin-instrumento-financiero (Recuperado en fecha 15/06/2021)

autoridad protagonista en el futuro de las criptomonedas, reafirma la idea de que las monedas estables pertenecen al grupo de las principales competidoras de Bitcoin. De la misma manera, también afianza la noción de que Bitcoin es solo un instrumento financiero que, como se ha mencionado, tiene un fin meramente especulativo a raíz de su fuerte volatilidad.

CAPÍTULO 7. Bitcoin, la ecología y los recursos naturales

Inexorablemente, se debe contemplar el impacto de la minería de Bitcoin en el medioambiente. Lo realmente importante aquí es determinar si el elevado consumo de energía y la huella de carbono producida por Bitcoin es válida respecto de lo que ofrece, es decir, si existe una razonabilidad entre los efectos ecológicos negativos y los beneficios de minar Bitcoin.

Determinar el impacto de las emisiones de carbono de la red de Bitcoin es complicado. No solo debe conocerse la energía que necesita la red, sino también el origen de esa energía, Sin embargo, existen estudios que, ponderando factores como la localización de los mineros o el costo de la energía que consumen, han podido arribar a ciertas estimaciones.

Para ambos análisis, debe establecerse la función de Bitcoin en el mercado. Si se lo considera un medio de pago, entonces sería de utilidad comparar el consumo energético de Bitcoin y el sistema de pagos de VISA. Por otro lado, si se lo considera como un resguardo de valor y basándose en que muchos lo han llamado "*oro digital*"[141], se lo podría comparar con el oro mismo. No obstante, desde un punto de vista ecológico, parece mucho más conveniente profundizar en la primera comparación, dado que comparar Bitcoin con el oro, carece de sentido cuando se plantea que la minería de oro puede detenerse cuando el impacto ecológico sea significativo, mas detener el minado de Bitcoin representaría su propio fin.

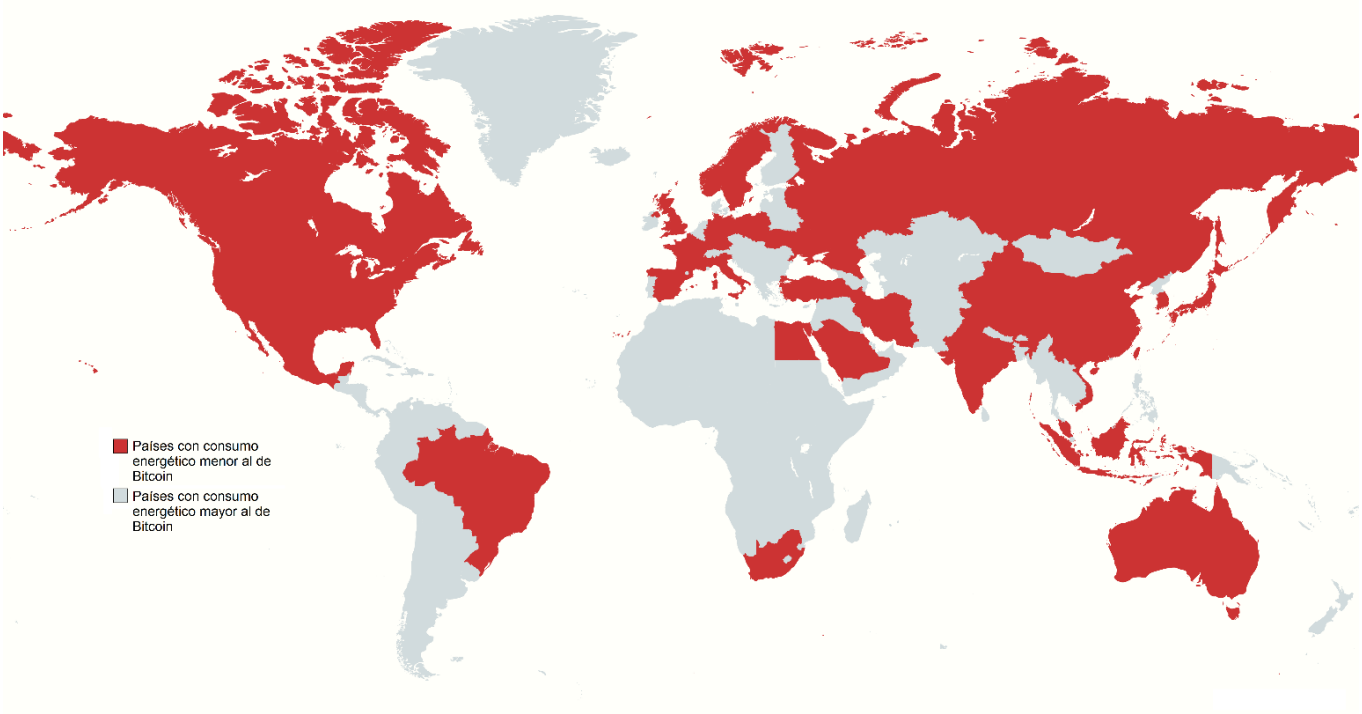
El consumo energético de Bitcoin y su producción de emisión de carbono son los dos factores a considerar para entender su conexión con el medioambiente y el papel que este puede interpretar para que la sociedad acabe por desechar Bitcoin. Sumado a esto, están proliferando altcoins más ecológicas que podrían acelerar un proceso de desuso de Bitcoin.

Consumo energético

Para ponderar el consumo de energía de Bitcoin es necesario compararlo con otros parámetros. El parámetro más común que se utiliza para tomar perspectiva del consumo energético de Bitcoin es el consumo de países enteros. Las estimaciones de consumo de energía de Bitcoin varían según el índice que se pretenda considerar. Sin embargo, uno de los índices más respetados es el de los investigadores que "*…trabajan con el Índice de Consumo Eléctrico del Bitcoin de Cambridge (CBECI, por sus siglas en*

[141] Reuters Staff, "Bitcoin emergence as 'digital gold' could lift price to $146,000, says JPM", 2021, Traducido, (En línea) Disponible en: https://www.reuters.com/article/us-crypto-currencies-jpm-idUSKBN29A1IF (Recuperado en fecha 17/06/2021)

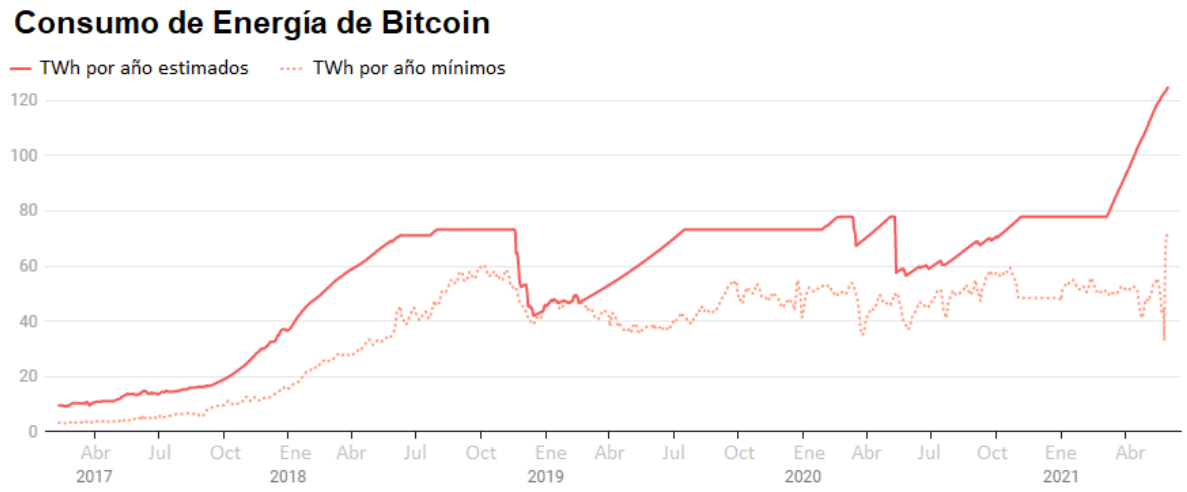
inglés), el cual provee estimaciones en tiempo real sobre cuánta electricidad consume la generación de la divisa"[142]. En función de dicho índice, se puede observar en el siguiente mapa que Bitcoin consume más energía que casi todos los países no desarrollados e incluso más que algunos países desarrollados como Suiza, Nueva Zelanda, Singapur o Dinamarca:



Cuadro 7.1. Mapa de consumo energético. Fuente: Elaboración propia con base en BBC News Mundo, "Qué tanto contamina el bitcoin, la moneda que consume más electricidad que Finlandia, Suiza o Argentina", 2021, (En línea) Disponible en: https://www.bbc.com/mundo/noticias-56049826 (Recuperado en fecha 17/06/2021)

De acuerdo con este índice, si Bitcoin fuera considerado un país, sería uno de los primeros 30 que más energía consume en 2021. Esto da cuenta de la significatividad de su consumo energético en el mundo. Y esa significatividad parecería ir en aumento. En los últimos años, Bitcoin ha marcado una tendencia al alza respecto de su consumo de energía. Un estudio del sitio Digiconomist.net permite ver este incremento en el consumo de teravatios-hora, el cual se ha multiplicado por más de 12 veces en el primer cuatrimestre del año 2021, en relación con los valores que contemplaba en el año 2017 en esa misma época del año. Estos datos y el comportamiento de esta variable se pueden apreciar en el siguiente gráfico:

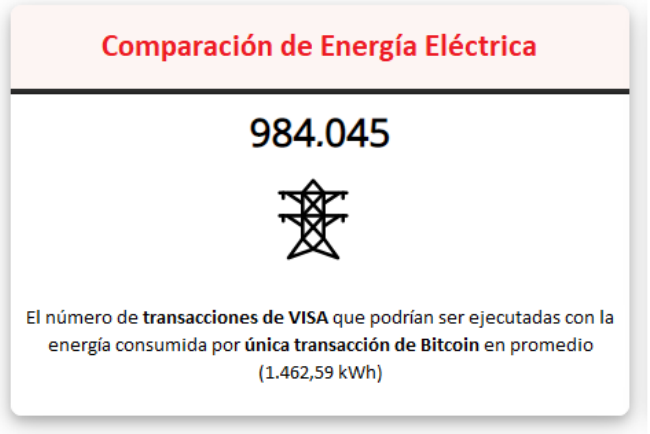
[142] BBC News Mundo, "Qué tanto contamina el bitcoin, la moneda que consume más electricidad que Finlandia, Suiza o Argentina", 2021, (En línea) Disponible en: https://www.bbc.com/mundo/noticias-56049826 (Recuperado en fecha 17/06/2021)



Cuadro 7.2. Consumo energético de Bitcoin. Fuente: Digiconomist, "Bitcoin Energy Consumption Index", 2021, Traducido, (En línea) Disponible en: https://digiconomist.net/bitcoin-energy-consumption (Recuperado en fecha 17/06/2021)

El estudio considera las dificultades de mediciones que se han mencionado, por lo que añade la estimación mínima de teravatios-hora consumidos por Bitcoin. Se puede apreciar que incluso las estimaciones mínimas conservan altos niveles de consumo. Esto es alarmante, dado que "*Con estos niveles de consumo, la minería de bitcoins se situará en el puesto 12 del ranking mundial de países por demanda energética*"[143].

Retomando el concepto de que Bitcoin puede ser comparable como medio de pagos con el sistema VISA, el sitio Digiconomist ha calculado también la cantidad de transacciones que se podrían ejecutar con la energía que una sola transacción de Bitcoin consume:



Cuadro 7.3. Comparativa de energía consumida Bitcoin-VISA. Fuente: Digiconomist, "Bitcoin Energy Consumption Index", 2021, Traducido, (En línea) Disponible en: https://digiconomist.net/bitcoin-energy-consumption (Recuperado en fecha 17/06/2021)

[143] David Bollero, "Para 2024, la minería bitcoin será el duodécimo 'país' por consumo de energía", 2021, (En línea) Disponible en: https://blogs.publico.es/kaostica/2021/04/09/bitcoin-medioambiente (Recuperado en fecha 17/06/2021)

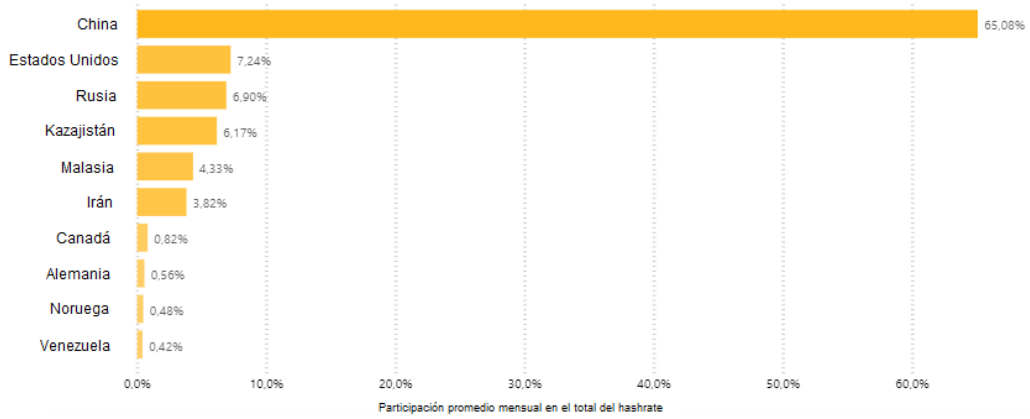
El cálculo resulta en que una transacción de Bitcoin consume casi tanta energía como un millón de transacciones del expandido sistema de pagos de VISA. Es fácil contemplar el ineficiente uso de energía de Bitcoin si se pretendiera adoptarlo como medio de pago generalizado.

Defensores de Bitcoin sostienen que "*…si se suman todos los recursos eléctricos que demanda el sector bancario, el consumo de las entidades financieras es mucho mayor*"[144]. Sin embargo, ese argumento es fútil. No consideran que el sistema establecido actualmente proporciona gran cantidad de empleos, brinda una mayor cantidad de servicios, permite realizar una cantidad de transacciones sumamente superior y que, principalmente, su utilización se encuentra expandida a nivel mundial. En función de los datos recabados por Digiconomist que se han mencionado, Bitcoin es incapaz de expandirse como lo ha hecho el sistema bancario actual sin destruir el medioambiente.

Por otra parte, vale decir que si se deseara comparar la contaminación que producen Bitcoin y el dinero físico, habría que entender la forma en que lo hacen. El dinero físico produce contaminación cuando se produce, mientras que Bitcoin lo hace cuando se realizan transacciones. Por lo que es sencillo notar que mientras que uno contamina cuando se crea, el otro lo hace infinitas veces, cada vez que se utiliza. Por otro lado, el dinero físico es solo una forma del dinero fiduciario. Si existiera una amenaza relevante respecto de la contaminación que genera el dinero físico, las transacciones podrían pasar a ser netamente electrónicas y, como se ha evidenciado, en ese punto Bitcoin no es rival para los centros de procesamiento de sistemas como el de VISA.

Es oportuno percatarse de la localización geográfica del poder de minado (o *hashrate*). Como se ha visto, China es el país en donde se agrupa la mayor cantidad de mineros de Bitcoin. La localización de los mineros que incorporan un nuevo bloque a la cadena puede variar en función de cuál sea el minero que logre encontrar el bloque candidato. Sin embargo, si la mayor cantidad de nodos se encuentra en una región específica, es más probable que los mineros que logren añadir los nuevos bloques pertenezcan a esa región. Es por ello que China ocupa el primer lugar en participación promedio mensual del *hashrate* total. Esto se visibiliza en el siguiente gráfico realizado por la Universidad de Cambridge:

[144] Melisa Reinhold, "Criptos: ¿puede el consumo de energía poner en jaque al bitcoin?", 2021, (En línea) Disponible en: https://www.lanacion.com.ar/economia/negocios/criptos-puede-el-consumo-de-energia-poner-en-jaque-al-bitcoin-nid19042021 (Recuperado en fecha 17/06/2021)



Cuadro 7.4. Participación promedio mensual en el hashrate por país. University of Cambrdige - Judge Business Scholl, "Cambridge Bitcoin Electricity Consumption Index", 2020, Traducido, (En línea) Disponible en: https://cbeci.org/mining_map (Recuperado en fecha 17/06/2021)

El caso de China: La minería en China merece un estudio diferenciado. Como se percibe en el gráfico anterior, la minería en China representa más de la mitad de la minería mundial de Bitcoin, según el índice de la Universidad de Cambridge. No es casualidad que China sea el lugar preferido de los mineros para instalar sus operaciones. "*Debido a la proximidad a los fabricantes de hardware especializado y al acceso a electricidad barata, la mayor parte del proceso de minería se ha llevado a cabo en China…*"[145] y, por ello, estudiar la participación de China en el proceso de minado de la red de Bitcoin permitiría llegar a conclusiones representativas respecto del verdadero impacto de Bitcoin en la ecología. A partir de analizar únicamente su situación, se estima que "*En China, (…) el proceso creará tantas emisiones de carbono en un año como Italia o Arabia Saudí en 2024, además hay situaciones como los cortes de energía localizados…*"[146]. Se prevé que el impacto de la minería de Bitcoin en China afectará la provisión de energía de sus habitantes en menos de cinco años si no se toman medidas drásticas al respecto.

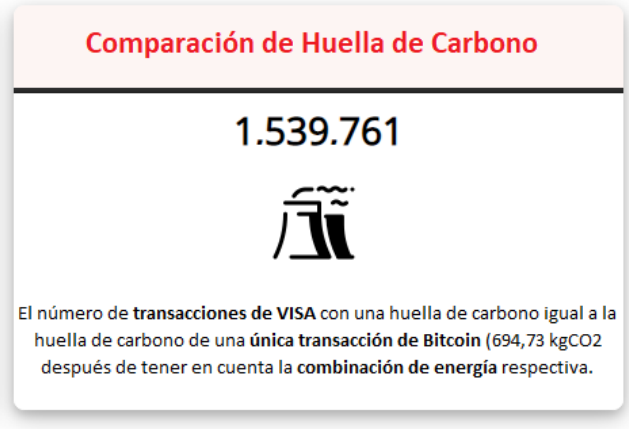
Emisiones de carbono, la contaminación de Bitcoin

Siguiendo con el caso de China y de acuerdo con un estudio de la prestigiosa revista Nature, "*…sin intervención política, se estima que el consumo anual de energía de la blockchain de Bitcoin en China alcance un pico en 2024 de 296.59 Twh y genere 130.50 millones de toneladas métricas de emisión de*

[145] Diario Infobae, "El 75% de la minería de Bitcoin se realiza en China y podría convertirse en un problema para el medio ambiente", 2021, (En línea) Disponible en: https://www.infobae.com/america/tecno/2021/04/09/el-75-de-la-mineria-de-bitcoin-se-realiza-en-china-y-podria-convertirse-en-un-problema-para-el-medio-ambiente (Recuperado en fecha 17/06/2021)

[146] David Walsh, "¿Qué es la criptomoneda "verde" Chia y hasta qué punto es ecológica?", 2021, (En línea) Disponible en: https://es.euronews.com/2021/05/13/que-es-la-criptomoneda-verde-chia-y-hasta-que-punto-es-ecologica (Recuperado en fecha 17/06/2021)

carbono"[147]. Las emisiones futuras estimadas de la minería de Bitcoin son preocupantes, pero también lo son las actuales. Para poner en perspectiva las emisiones de carbono actuales de la red de Bitcoin, basta con remitirse nuevamente al estudio de Digiconomist:



Cuadro 7.5. Comparativa de huella de carbono Bitcoin-VISA. Fuente: Digiconomist, "Bitcoin Energy Consumption Index", 2021, Traducido, (En línea) Disponible en: https://digiconomist.net/bitcoin-energy-consumption (Recuperado en fecha 17/06/2021)

Según el estudio, una sola transacción de Bitcoin deja la misma huella de carbono que más de un millón y medio de transacciones del sistema de pagos de VISA. Es evidente que Bitcoin, como medio de pago, es inmensamente ineficiente desde un punto de vista ecológico. No solo derrocha gran cantidad de energía, sino que produce una huella de carbono desproporcionada respecto de los beneficios que trae, ya que los mismos son mínimos en comparación con sistemas ya establecidos en el mercado.

La revista Nature también hace mención de las emisiones de dióxido de carbono de Bitcoin, afirma que "*...el uso proyectado de Bitcoin, si sigue la tasa de adopción de otras tecnologías ampliamente adoptadas, podría por sí solo producir suficientes emisiones de CO2 para impulsar el calentamiento por encima de 2°C en menos de tres décadas*"[148]. Este valor es muy elevado si se tiene en cuenta que desde el año 1950 la temperatura en la atmósfera ha aumentado a razón de aproximadamente 0,1°C por decenio[149]. Y lo realmente preocupante es que Bitcoin podría generar esto por sí solo.

[147] Shangrong Jiang, Yuze Li, Quanying Lu, Yongmiao Hong, Dabo Guan, Yu Xiong y Shouyang Wang, "Policy assessments for the carbon emission flows and sustainability of Bitcoin blockchain operation in China", 2021, Traducido, (En línea) Disponible en: https://www.nature.com/articles/s41467-021-22256-3.pdf (Recuperado en fecha 17/06/2021)
[148] Camilo Mora, Randi L. Rollins, Katie Taladay, Michael B. Kantar, Mason K. Chock, Mio Shimada & Erik C. Franklin, "Bitcoin emissions alone could push global warming above 2°C", 2018, (En línea) Disponible en: https://www.nature.com/articles/s41558-018-0321-8?hmsr=joyk.com&utm_source=joyk.com&utm_medium=referral (Recuperado en fecha 17/06/2021)
[149] GreenFacts, "Cambio Climático Evaluación 2001", (En línea) Disponible en: https://www.greenfacts.org/es/cambio-climatico-ie3/l-3/cambio-climatico-1.htm#0p0 (Recuperado en fecha 17/06/2021)

El hardware: Se debe tener en cuenta el papel del hardware dentro de la minería de Bitcoin. Es, sin dudas, otro factor más de la creciente incidencia de Bitcoin en el medioambiente. Según Aubrey Hansen, columnista del sitio Cointelegraph, "*Los fabricantes de chips mineros, con los más prolíficos asentados en China, trabajan incansablemente para desarrollar procesadores cada vez más potentes. Con cada nueva iteración, estos chips de alta capacidad requieren cada vez más energía para funcionar. Las nuevas máquinas mineras hacen que las viejas sean obsoletas, lo que resulta en un creciente flujo de desechos de electrónicos, la mayoría de los cuales no se reciclan*"[150]. La rentabilidad de Bitcoin de los últimos años ha dado nacimiento a nuevo hardware, especializado y particularmente preparado para la minería. Jorge García del diario El País señala que "*La resolución de algoritmos complejos, llamada prueba de trabajo, es el peaje obligatorio que deben pasar los mineros para obtener su beneficio. La dificultad para los mineros es que, según se resuelven los acertijos matemáticos, se complican cada vez más para obtener la misma cuantía de bitcoins. Para que la mina no baje su rendimiento, se estresan al máximo las supercomputadoras*"[151], lo que implica un mayor consumo energético.

El incremento de desechos de hardware y el mayor consumo eléctrico son el resultado de una mayor competencia por la obtención de los nuevos Bitcoin producto del minado. Dicha competencia se repite con las altcoins, aunque de maneras distintas. El enorme desperdicio y la incipiente contaminación de Bitcoin son también la consecuencia de que su protocolo se base en el algoritmo de consenso de Proof of Work (Prueba de Trabajo) para el minado. Muchas altcoins han percibido este defecto en Bitcoin y cuentan con protocolos alejados de la Proof of Work, adoptando nuevas y mejorados algoritmos de consenso.

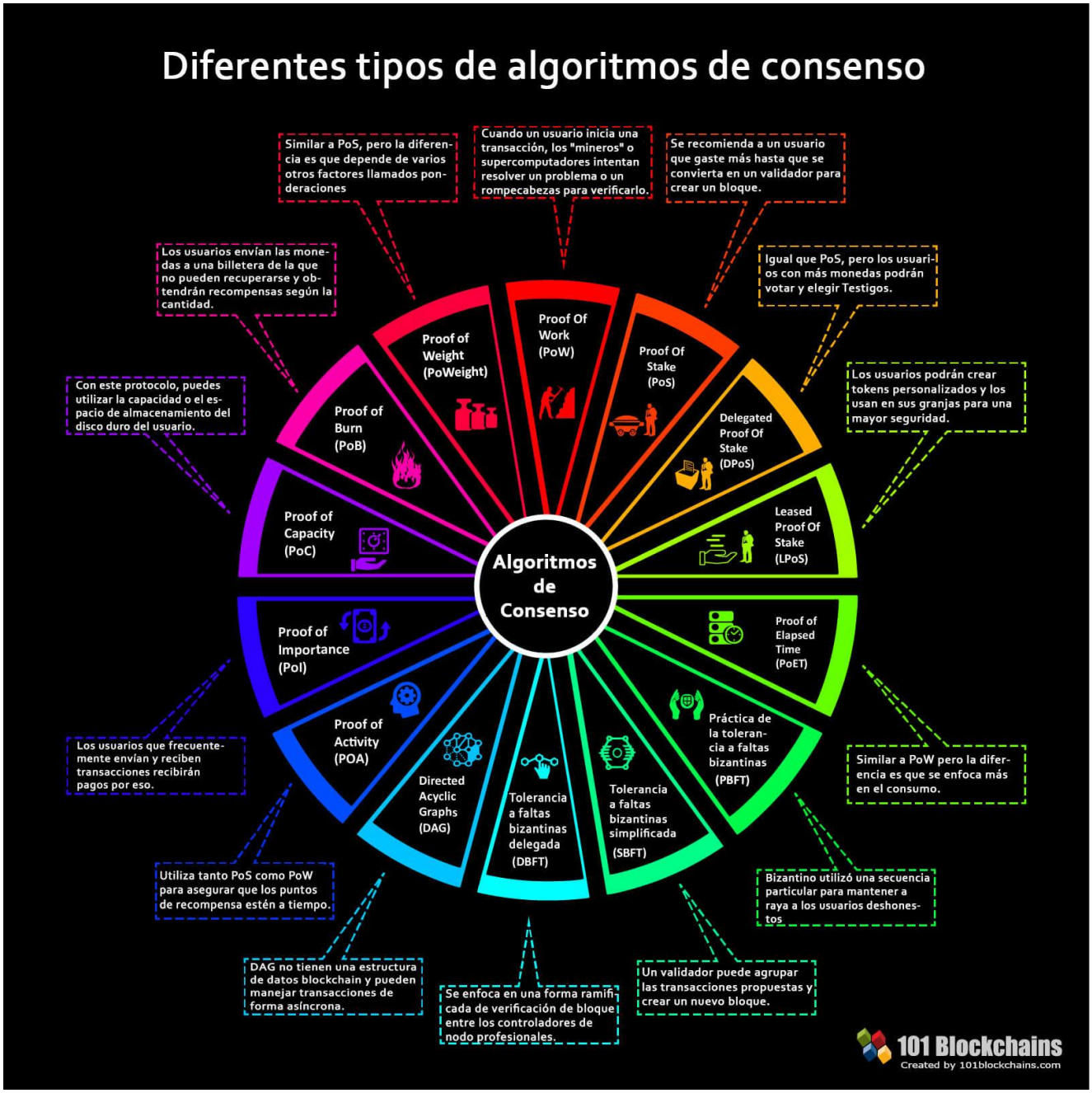
Alternativas

La Prueba de Trabajo que utiliza Bitcoin es la causa principal del impacto medioambiental negativo de esta criptomoneda. Por medio de la fuerza bruta, miles de nodos intentan arribar a un resultado criptográfico que cumpla con los requisitos para añadir un nuevo bloque a la Blockchain de Bitcoin. Los miles de equipos consumen energía simultáneamente. Mientras que solo uno conseguirá hallar el hash que permitirá agregar un nuevo bloque; el resto de ellos solo desperdicia recursos.

[150] Aubrey Hansen, "¿Qué energía es la que impulsa la industria cripto-minera de China? ¿Es sostenible?", 2019, (En línea) Disponible en: https://es.cointelegraph.com/news/what-powers-chinas-crypto-mining-industry-and-is-it-sustainable (Recuperado en fecha 18/06/2021)

[151] Jorge G. García, "La minería de bitcoin: un riesgo para el medio ambiente", 2018, (En línea) Disponible en: https://elpais.com/retina/2018/08/09/tendencias/1533814810_389211.html (Recuperado en fecha 18/06/2021)

Existen otros algoritmos de consenso, pero que, por su baja popularidad, no merecen un análisis profundo. Cabe sí mencionarlos a fin de conocer el abanico de posibilidades en este sentido. El sitio 101Blockchain.com explica una gama de algoritmos diferentes mediante el siguiente cuadro:



Cuadro 7.6. Algoritmos de consenso. Fuente: Nelson Rodríguez, "Algoritmos De Consenso: La Raíz De La Tecnología Blockchain", 2018, (En línea) Disponible en: https://101blockchains.com/es/algoritmos-de-consenso-blockchain (Recuperado en fecha 18/06/2021)

Dentro de este grupo de algoritmos, muchos han sufrido ligeras variaciones y mejoras. Varios de ellos podrían representar una potencial competencia para Bitcoin en el futuro y otros ya lo son. Dentro de

esta gama de alternativas, Proof of Stake (PoS) es la opción que mayor popularidad ha adquirido. Esta opción busca reemplazar definitivamente a Proof of Work (PoW), dejando atrás a los protocolos basados en este algoritmo. Es oportuno mencionar ejemplos de criptomonedas que han surgido, más sustentables con el medioambiente. Estos ejemplos, a excepción de IOTA (MIOTA) que utiliza el algoritmo de consenso DAG – Directed Acyclic Graph (Gráfico Acíclico Dirigido), se manejan mediante las Proof of Stake, con ligeras modificaciones orientadas a optimizar sus procesos:

- Polkadot (DOT) usa NPoS – Nominated Proof of Stake (una variante de PoS con nodos nominadores)
- Cardano (ADA) usa Ouroboros (una variante de PoS)
- Tezos (XTZ) usa LPoS – Liquid Proof of Stake (otra variante de PoS)
- IOTA (IOTA) usa DAG – Directed Acyclic Graph

Los beneficios de Proof of Stake son tan superiores a Proof of Work que Ethereum, la principal competencia de Bitcoin, ha tomado nota de esto. Martínez Mosquera del diario El Economista informa que "...*Ethereum está en proceso de transición de la tecnología Proof of Work a la tecnología Proof of Stake, lo cual reduciría sensiblemente su consumo por transacción. Es un esfuerzo enorme de coordinación ya que en este mundo no hay una fuerza centralizada que lleve la batuta (...) Esa es la razón, en parte, por la que no es esperable que Bitcoin lo siga a Ethereum en aquel cambio tecnológico. De hecho, los bitcoiners se enorgullecen del formato Proof of Work y suelen decir que es la única forma segura de mantener la descentralización*"[152]. Como se comentó al analizar la escalabilidad de Bitcoin, nuevamente se observa que es improbable que Bitcoin cambie su algoritmo de Proof of Work por el de Proof of Stake o cualquier otro más eficiente debido a las características de su protocolo. No obstante, además de las dificultades técnicas para llevar a cabo esta transformación, se percibe que los principales defensores de Bitcoin no se hallan dispuestos al cambio, lo que torna aún más improbable esta posibilidad. Por todo esto, también en cuanto a sustentabilidad, Ethereum se posiciona como el principal candidato a desplazar a Bitcoin.

[152] Gonzalo Martínez Mosquera, "'Ganó Greta': ¿comienzo del fin para el Bitcoin?", 2021, (En línea) Disponible en: https://eleconomista.com.ar/2021-05-comienzo-del-fin-para-el-bitcoin (Recuperado en fecha 19/06/2021)

CAPÍTULO 8. Conclusiones

En el presente trabajo, se ha podido comprender y tomar magnitud del alto potencial que posee la tecnología Blockchain y se ha observado que es una realidad en numerosos rubros, con resultados positivos. Esta tecnología ha resuelto el problema de la confianza ante la ausencia de un tercero confiable mediante la utilización de registros inalterables.

Las criptomonedas fueron el experimento perfecto de Blockchain. La criptomoneda pionera fue Bitcoin y sus características atrajeron la atención de muchos participantes del mercado por sus cualidades, particularmente su nivel de privacidad, la dificultad de seguimiento de transacciones y su red descentralizada. No obstante, Bitcoin se enfrenta a diversos desafíos y en su horizonte se vislumbran retos nuevos aún más complejos.

Se han relevado diversas debilidades técnicas en Bitcoin y su protocolo. Algunas debilidades son comunes a otras criptomonedas y otras exclusivas de Bitcoin por sus características. Se ha visto que Bitcoin es pasible de robos y de una diversa cantidad de ataques, con mayor y menor probabilidad de ocurrencia, que podrían significar su derrumbe. Si sucediera un ataque exitoso de grandes dimensiones contra su red, se esparciría la desconfianza, caería su cotización y su capitalización de mercado. El desencanto entre sectores especulativos, sería el comienzo de un final anunciado.

Además, se ha evidenciado que Bitcoin posee graves problemas de escalabilidad que lo incapacitan para ser una versión puramente electrónica de efectivo, como su creador pretendía. Su limitada escalabilidad es una barrera que le impedirá proliferar en el mercado. A este problema se le suma la incipiente aparición de computadoras cuánticas, amenazando con dejar obsoleto su algoritmo.

Se ha estudiado la compleja discusión entre centralización o descentralización. En ella, se ha visto que Bitcoin carece de las ventajas que un sistema centralizado puede ofrecer, pero que, al mismo tiempo, la alta concentración minera en pooles de minería, la presencia de exchanges y la existencia de ballenas invalidan su intento de representar una verdadera red descentralizada. A su vez, estos elementos privan a Bitcoin de las ventajas que una red verdaderamente descentralizada brindaría.

Se ha tomado consciencia del rol que Bitcoin tiene en la sociedad. Se advirtió que su esencia inmaterial, su carácter anónimo, su facultad para no ser rastreable, su capacidad para acreditar con suficiente inmediatez las transacciones sin importar la ubicación geográfica de las partes y la facilidad de convertirse a dinero fiduciario, lo convierten en una herramienta ideal para financiar y cometer delitos y

actos terroristas. Bitcoin cuenta con las características perfectas para que el crimen lo aproveche para sus fines. Evidenciado esto, los gobiernos han tomado cartas en el asunto y no permitirán que Bitcoin se expanda si ello implicase que el delito prospere.

Por otro lado, más pronto que tarde, pasará a ser blanco de los entes recaudadores, lo que reducirá su atractivo económico. Además, su cualidad para no poder ser localizado con exactitud puede generar problemas de múltiple imposición que le llevarían a tributar impuestos en más de un país, ahuyentando aún más a los inversores.

Se ha concluido que Bitcoin no cumple con las características de una moneda. Ha quedado claro su problema de escalabilidad frustra cualquier intento de transformarse en un medio de pago extendido. También ha quedado en evidencia que su elevada volatilidad le impide ser una reserva de valor o una adecuada unidad de medida en la economía. Esta misma volatilidad lo limita a ser una inversión meramente especulativa, de corto plazo y altamente riesgosa. No ha sido posible determinar un valor intrínseco suficiente que pueda demostrar que no es más que un activo especulativo sin fundamentos.

Se ha determinado que es altamente probable que Bitcoin desaparezca por su incapacidad en el largo plazo para ser rentable sin incrementar las tarifas que se pagan por sus transacciones. Se ha visto que este inexorable incremento en las tarifas tornará inviable el uso de Bitcoin.

Por si esto fuera poco, existe un abundante número de criptomonedas que han superado a Bitcoin en todos sus aspectos y que acabarán por desplazarlo del mercado en el largo plazo.

Por último, Bitcoin implica un inmenso consumo de energía y produce una huella de carbono tal, que no se condice con los beneficios que ofrece, especialmente existiendo nuevas opciones de criptomonedas en el mercado que procesan más transacciones por segundo, con menor tiempo de validación y que son ecológicamente más eficientes.

La caída de Bitcoin en el largo plazo es ineludible. Esto no implica que el resto de las criptomonedas sufran el mismo destino. Existen proyectos que han sabido corregir los defectos de Bitcoin y otros que han ido en caminos diferentes apuntando a tener funcionalidades prácticas interesantes. Por otra parte, día tras día surgen nuevos proyectos, mejorados y más ambiciosos, más eficientes y más sustentables para el medioambiente. Por ello, el fin de Bitcoin no sería el fin de las criptomonedas, sino el cierre de un capítulo que dará paso a uno nuevo.

Glosario

Blockchain: Registro estructurado en forma de bloques que se vinculan con los anteriores de forma cronológica, propiciando inmutabilidad de la información contenida.

Bitcoin: Es una criptomoneda que con un protocolo de código abierto y red entre iguales.

MarketCap: Capitalización de mercado. En el caso de las criptomonedas, es el resultado de multiplicar la cantidad de criptomonedas en circulación por el precio de cotización.

GAFI: Grupo de Acción Financiera Internacional.

CBDC: Central Bank Digital Currency.

Problema de los Generales Bizantinos: Metáfora sobre el problema que se da entre un conjunto de agentes con un objetivo común que solo se consigue si existe confianza entre todos.

KSI: Tecnología Blockchain diseñada en Estonia usada en sistemas alrededor del mundo.

Ledger: Libro mayor donde se deja constancia de las transacciones.

Whitpaper: Documento guía que explica a los usuarios un tema determinado. Para el caso de las criptomonedas, indica los detalles del proyecto.

Token: Se utiliza de diferentes formas según el contexto. Suele usarse como sinónimo de criptomoneda.
Stakeholders: Son las partes interesadas alrededor de un determinado elemento.

Ley de Moore: Expresa que aproximadamente cada 2 años se duplica el número de transistores en un microprocesador.

Hashrate: Poder de minado.

Hijacking: Proceso mediante el cual se intenta secuestrar un elemento específico del entorno de Internet, empleando rutas que no están autorizadas.

Hard fork: Son actualizaciones importantes de un protocolo.

Halving: Proceso automatizado mediante el cual se reduce a la mitad la recompensa de minado con una frecuencia determinada.

Darknet: Cuenta con diferentes acepciones. En esta red se navega con alto grado de anonimato y suele escapar a cualquier tipo de regulación institucional