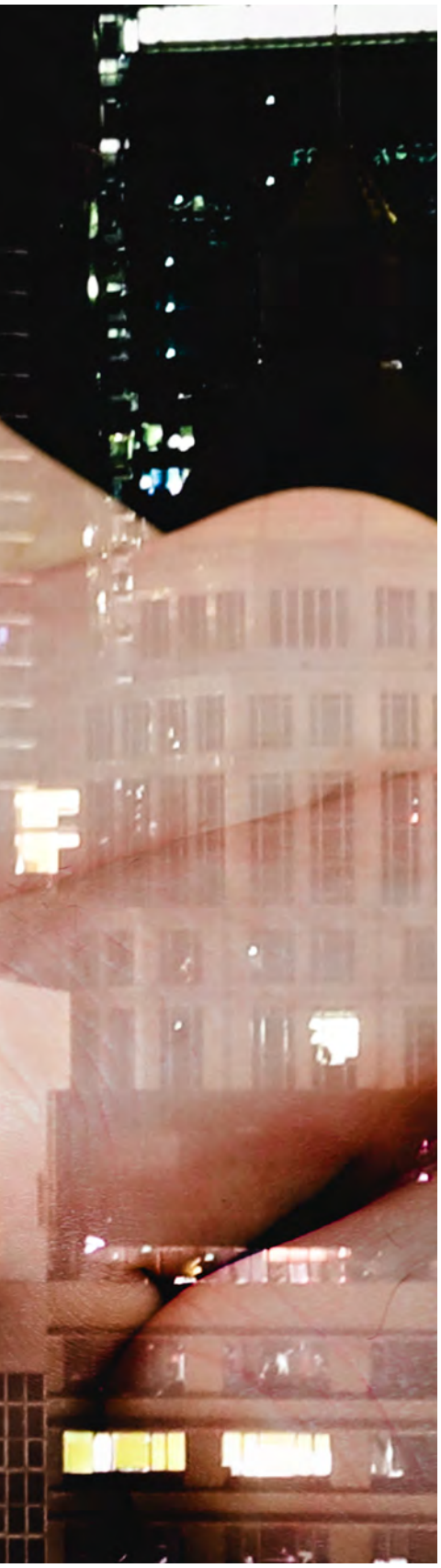
ISSN 2215-5910
Ensayo



BITCOIN YA EXISTE. UNA EVOLUCIÓN EN LA NATURALEZA DEL DINERO

Nancy Quirós Aguilar
y Eugenio Corea Zúñiga

RESUMEN

Bitcoin es dinero en efectivo de forma digital que cuenta con las propiedades de dinero duro y está emergiendo del mercado. Es un activo real digital, por lo tanto, no está basado en deuda y, parte de su innovación, es que representa la escasez digital. Bitcoin se compone de la unidad de valor llamada "bitcoin" y de la red peer-to-peer (nodos, mineros y *blockchain*). La Prueba de Trabajo es el componente que permite que la red llegue a un consenso sin la presencia de intermediarios y que las transacciones en su *blockchain* sean inmutables, ya que enlaza a Bitcoin con el mundo tangible. Bitcoin es la tecnología en sí, por lo tanto, es único e irrepetible y cada proyecto que intente replicar sus propiedades se convierte en un intento fracasado. Además, Bitcoin redefine el concepto de propiedad privada, lo cual tiene consecuencias profundas. Sin embargo, en estas fases tempranas de adopción, la humanidad todavía no ha logrado asimilar los alcances de esta innovación. Este ensayo tiene como objetivo aclarar los mitos más comunes con respecto a Bitcoin, mostrar su lugar en el mundo y que sirva como una guía de referencias para el lector principiante.

Palabras clave: bitcoin, minería, *blockchain*, tecnología, innovación, adopción

ABSTRACT

Bitcoin is digital cash, hard money and it's emerging from the market. Bitcoin is also a real digital asset thus it's not credit based and part of its innovation is that it represents digital scarcity. Bitcoin is made up of its unit of value called bitcoin and its peer-to-peer network (nodes, miners and blockchain). Proof of Work is what allows the network to reach consensus without the need of intermediaries and transaction immutability on the blockchain. It also links Bitcoin to the tangible world. Bitcoin is a unique technology so every project that tries to replicate its properties becomes a failure. Furthermore, Bitcoin redefines the concept of private property which has profound implications. However, in these early stages of adoption, humanity hasn't yet understood the extent of this innovation. The objective of this essay is to clarify the most common misconceptions regarding Bitcoin, to show its place in the world and to serve as a reference for the novice Bitcoiner.

Keywords: bitcoin, mining, blockchain, technology, innovation, adoption

Nancy Quirós Aguilar es PhD en Física, MSc en Digital Currencies: Estudió Bachillerato en Física en la Universidad de Costa Rica (UCR). Obtuvo su doctorado en Física Atómica en la Universidad de Nevada en Reno (UNR). En el 2021 finalizó una maestría en Digital Currencies de la Universidad de Nicosia en Chipre (UNIC).

Eugenio Corea Zúñiga es Ingeniero especialista en revisión de diseños electrónicos y entusiasta de la tecnología. Desde el 2016 se interesó en Bitcoin y se ha dedicado a su estudio de forma autodidacta por 6 años.

BITCOIN YA EXISTE. UNA EVOLUCIÓN EN LA NATURALEZA DEL DINERO

Bitcoin es el primer ejemplo de una nueva forma de vida. Vive y respira en Internet. Vive porque puede pagarle a la gente para que lo mantenga con vida (…) No se puede cambiar. No se puede discutir con él. No se puede manipular. No se puede corromper. No se puede detener. Si una guerra nuclear destruyera la mitad de nuestro planeta, seguiría vivo, incorruptible (Merkle, 2021, p. 14).

Actualmente, la palabra Bitcoin está permeando, cada vez más, los intereses de la sociedad, no es sorpresa encontrarla en cualquier tipo de conversaciones referentes a distintas áreas de conocimiento, sin importar si estas son casuales o profesionales. Y es que, Bitcoin, parece ya haber adquirido en el pensamiento un sentido de valor, pero esto no solo puede ser positivo, puesto que como su escalado a la cima del interés general ha sido efervescente, ha dado pie a que concepciones precipitadas logren aprovecharse para relacionarlo con otros temas como ganancia, dinero fácil, *trading*[2], inversión y hasta fraudes, como si su esencia fuera la misma o parte de lo mismo. Para aquellos que lo ven desde una posición neutral, logran entrever en ella un potencial de cambio que puede, incluso, compararse con la llegada del Internet. Pero comprender qué es Bitcoin con profundidad tiene cierta complejidad, ya que realmente toca distintas áreas del conocimiento como criptografía, ciencia computacional, economía, filosofía y derecho, solo por mencionar algunas. Por esto, es fácil encontrar a figuras reconocidas, con conocimiento de Bitcoin, valiéndose de pintorescas analogías para intentar describirlo, un ejemplo de esto es Strolight (2021), quien se refiere a Bitcoin como una tecnología alienígena (párr. 2), solo para hacer ver que no se parece a nada en nuestro planeta.

Por esta razón es que existe una gran brecha entre lo que es Bitcoin y lo que una persona que desconoce del tema concibe, esto sin contar el hecho de que se ha desviado la verdadera importancia que trae consigo; su facilidad de resolver, de manera óptima, el problema de la transferencia de valor económico a través del espacio y el tiempo. El dinero, en su forma de oro, solucionó este problema durante miles de años, no obstante, el concepto del dinero se ha deformado, y al no tener conocimiento de esto, no se puede reconocer la innovación que significa Bitcoin. El problema de esto es que, sin una forma de mantener valor a través del tiempo, nos volvemos a enfrentar con las recientes crisis inflacionarias que experimentan muchos países a lo largo del mundo (OECD, 2022, pp. 1-6).

A razón de que Bitcoin se vuelve cada vez más conocido, se ha visto la necesidad de mostrar en este artículo, la historia, la naturaleza, el funcionamiento y de esclarecer los mitos que se le han asociado; además, de acompañar al lector en un paso a paso para el debido conocimiento de lo que realmente consiste de una forma simple, a partir de lo que se puede encontrar a la hora de profundizar en el tema utilizando distintos espacios como podcasts, artículos, libros, entre otros; de forma que pueda servir como una guía de referencias para quien inicia su aprendizaje.

Por lo que en este ensayo se puede encontrar un conjunto de ideas de distintos pensadores contemporáneos quienes se han tomado la tarea de adentrarse en el tema y exponerlo, además, de las opiniones propias de los autores, con el fin de que sean cuestionadas para así contribuir a cambiar el enfoque que existe hacia el precio de bitcoin y redireccionar la atención a su verdadero impacto. No está de más resaltar que el presente ensayo no se debe tomar como una serie de consejos financieros y que los puntos de vista expresados representan solamente la posición de los autores y no la de sus afiliaciones.

NACIMIENTO DE BITCOIN

Con la aparición del Internet, un grupo de criptógrafos activistas de los años noventa, autodenominado *cypherpunks*, reconocieron la importancia de la privacidad en línea, puesto que temían que el Internet podría ser una herramienta de vigilancia. Hughes (1993), en el "Manifiesto Cypherpunk", expresa: Nosotros los cypherpunks, nos dedicamos a construir sistemas anónimos. Defendemos nuestra privacidad con criptografía, con sistemas de envío anónimo de e-mail, con firmas electrónicas y con dinero electrónico (párr. 7).

Como un baluarte de los ideales cypherpunks, se encuentra Phil Zimmerman, quien en 1991 desarrolló el sistema de mensajería *Pretty Good Privacy*. Ante esto y más sistemas de encriptación, se da el inicio de las

[2] Actividad de comprar y vender instrumentos financieros líquidos y volátiles con el objetivo de generar ganancias.

Crypto Wars, que surgen a partir de la oposición del gobierno estadounidense por ser considerado un tipo de arma. Sin embargo, el código fuente de Pretty Good Privacy se publicó en un libro por medio del *MIT Press*, lo que le permitió obtener una protección bajo la Primera Enmienda[3] a la Constitución de Estados Unidos (Gladstein, 2022, pp. 36-63). Este acontecimiento beneficiaría tiempo después a Bitcoin, debido a que este también se trata de un código.

Para el año 2008, un documento titulado "Bitcoin: Un Sistema Peer-to-Peer de Dinero en Efectivo Electrónico", fue publicado en una lista de correos especializada en criptografía del dominio *metzdowd.com* en la que participaban los cypherpunks. Firmando con el nombre desconocido de Satoshi Nakamoto, el autor del artículo con la descripción técnica de Bitcoin anunció: He estado trabajando en un nuevo sistema de efectivo electrónico que es totalmente peer-to-peer[4], sin un tercero de confianza (Nakamoto, 2008).

Por primera vez en la historia de la humanidad fue posible "transaccionar" información, como si de un bien físico se tratase, sin intermediarios y sin que se conservase una copia válida o equivalente del mismo. Así como un mismo objeto físico no puede ocupar dos lugares en el espacio simultáneamente; así también, un mismo bitcoin (o fracciones de él), no puede ocupar dos direcciones en el ciberespacio. De esta manera, después de una colaboración constante entre entusiastas y Nakamoto para implementar el sistema en código, la red Bitcoin fue lanzada el 3 de enero del año 2009.

Un dato que no se puede omitir, es que Nakamoto desaparece a finales del 2010 sin dejar rastros de su identidad. Por lo que Bitcoin, sin un líder, se convierte en un sistema verdaderamente descentralizado.

Propuestas pre-Bitcoin

Mucha gente descarta automáticamente la moneda electrónica como una causa perdida debido a todas las empresas que fracasaron desde la década de 1990. Espero que sea obvio que fue solo la naturaleza de control central de esos sistemas lo que los condenó. Creo que esta es la primera vez que intentamos con un sistema descentralizado, no basado en la confianza (Nakamoto, 2009).

Bitcoin nace como resultado de intentos infructuosos por parte de los cypherpunks por crear dinero electrónico:

- 1989: *e-chash*, las firmas ciegas [*blind signatures*] han regresado y ahora son parte de *Fedimint* (Chaum, 1983), que será descrito en secciones posteriores.
- 1997: *Hashcash* (Back, 2002), sistema antispam del cual Nakamoto extrajo ideas para la Prueba de Trabajo.
- 1998: *b-money*, dinero electrónico en efectivo distribuido que incorpora las ideas de Back (Dai, 1998). Nakamoto referenció este sistema en su publicación de Bitcoin.
- 1998: *bitgold* (Szabo, 2005), que sería el sistema precursor de Bitcoin.
- 2004: *Reusable Proof of Work* (Finney, 2004), quien fue un colaborador entusiasta de Bitcoin en sus inicios.

De acá es donde viene el poder revolucionario de Bitcoin y su carácter único e irrepetible, pues Nakamoto combinó varias tecnologías existentes, con algunas innovaciones propias, como se ilustra en la figura 1.

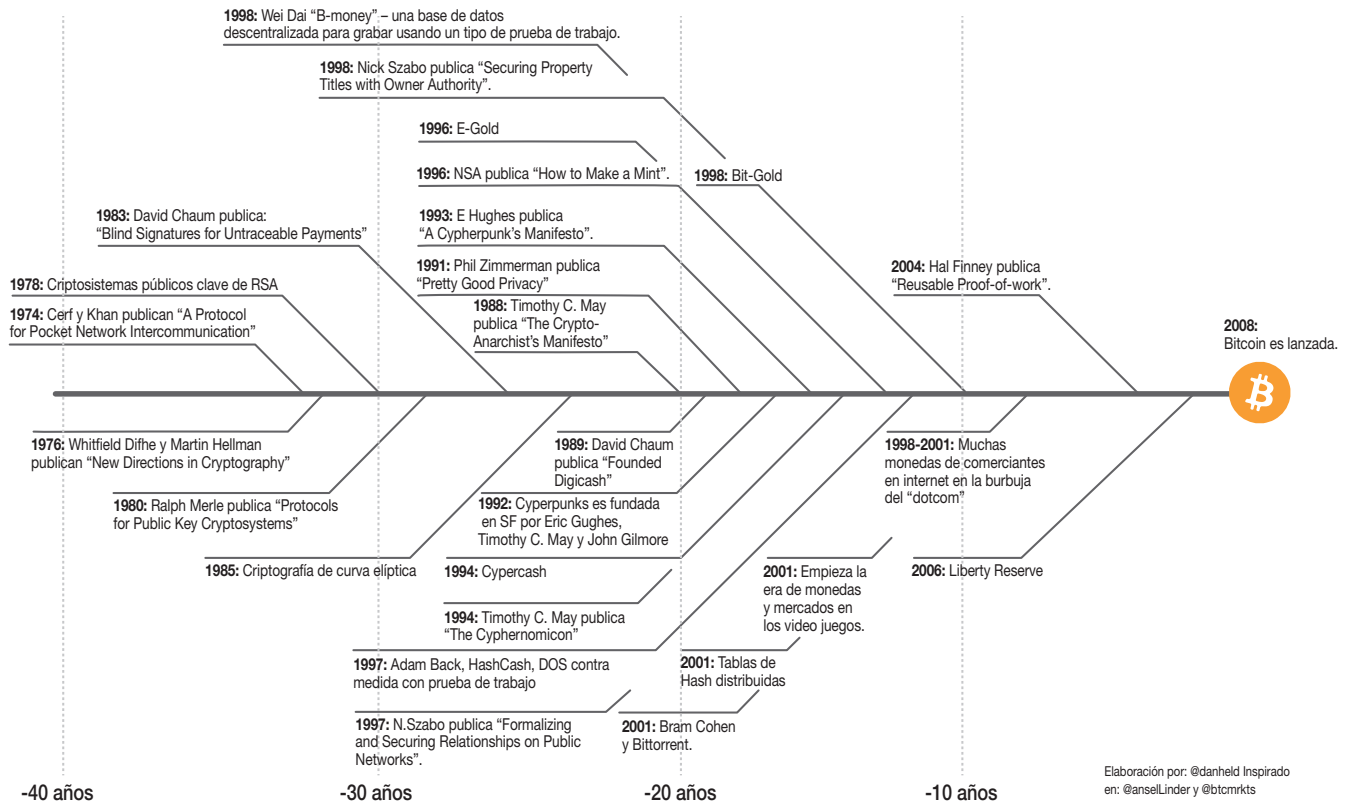
Bitcoin no es "la primera de muchas"

Se puede tener la concepción de que Bitcoin podría ser fácilmente imitada, más por la gran ola de nuevas "apariciones" de otras criptomonedas, entendiendo por criptomoneda "una unidad de valor creada utilizando *Blockchain Technology* o *blockchain*"[5], pero esto no puede estar más lejos de la realidad; Bitcoin no es la primera de muchas otras, Bitcoin es la culminación de muchos intentos previos realizados por los cypherpunks con el fin de crear dinero en efectivo digital, por lo que se podría decir que las propuestas parecidas a Bitcoin emergieron antes de su llegada.

Las propiedades monetarias de Bitcoin, tales como la cantidad total de unidades de valor y su frecuencia de emisión, no se pueden alterar; porque están basadas en las reglas del consenso expuestas en la Prueba

[3] Enmienda a la Constitución Estadounidense que garantiza la libertad de religión, expresión, prensa, reunión y petición al gobierno.
[4] Uno a uno.
[5] Los autores de este ensayo no están de acuerdo con este enfoque de criptomonedas. Más adelante se explicarán las razones.

FIGURA 1: DESARROLLOS CRIPTOGRÁFICOS PRE-BITCOIN



Bitcoin es una tecnología que se basa en investigaciones en criptografía que datan de la década de los 80.
Fuente: Tomado de "Planting Bitcoin-Soil (3/4)", por D. Held, 2019 (www.danheld.com).

de Trabajo que, a su vez, está anclada en la realidad física. Bitcoin presenta una dualidad al estar presente en el mundo digital y tangible. Nakamoto (2010) lo explicaba cuando decía que la naturaleza de Bitcoin es tal que, una vez que la versión 0,1 fue liberada, su diseño fundamental fue escrito en piedra por el resto de su vida.

Para dar una mejor idea, se podría decir que Bitcoin es como el oro, porque, así como no podemos modificar las propiedades químicas de este elemento, de forma similar, no podemos alterar las propiedades monetarias de Bitcoin. Si bien Bitcoin, a lo largo de su existencia, ha experimentado cambios en su software, estos no han alterado sus fundamentos sino su funcionalidad, como firmas y conexión entre nodos, en beneficio y aceptación por parte de sus usuarios; además, si alguno decidiera no optar por los cambios, lo puede hacer, en contraste con otras redes donde las modificaciones son de carácter impositivo. Por estas razones, Bitcoin es la señal, el resto es ruido.

PROBLEMA QUE BITCOIN RESUELVE

En una entrevista en 1999, Friedman, Premio Nobel de Economía 1976, dijo: Creo que el Internet va a ser una de las principales fuerzas para reducir el papel del gobierno. Lo único que falta pero que pronto se desarrollará es un dinero en efectivo electrónico confiable, un método mediante el cual en Internet se pueden transferir fondos de A a B sin que se conozcan (AC Squared, 2013, 3m18s).

La llegada del Internet revolucionó la forma en que transferimos información, pero es hasta la llegada de Bitcoin que la transferencia de valor en el mundo digital se convierte en una realidad; como consecuencia, Bitcoin es un avance tecnológico de proporciones inimaginables y tan relevante como el Internet mismo.

Nakamoto logra resolver de forma práctica el problema de ciencia computacional de los Generales Bizantinos[6] que, en términos de dinero, se conoce como el problema del doble gasto[7]. El fundamento de la dificultad para este problema de coordinación radica en la confianza. En palabras de Nakamoto (2008): El problema, por supuesto, es que el beneficiario no puede verificar que uno de los propietarios no gastó dos veces la moneda. Una solución común es introducir una autoridad central de confianza, o casa de moneda, que verifique cada transacción en busca de doble gasto. El problema con esta solución es que el destino de todo el sistema monetario depende de la empresa que dirige la casa de la moneda, y cada transacción tiene que pasar por ellos, al igual que un banco (sección Transactions, párr. 2).

Dinero

El dinero es el bien que le permite a los humanos la especialización y, con esto, el desarrollo de las civilizaciones, puesto que también resuelve el problema de la coincidencia mutua de deseos[8]. Lewis (2020) lo explica de la siguiente forma: La civilización tal cual la conocemos no podría existir sin dinero (sección Money as a necessity, párr 1). Todos pueden contribuir con sus propias habilidades en función de sus propios intereses y preferencias personales: recibir dinero a cambio del valor entregado hoy y luego usar ese mismo dinero para adquirir el valor especializado creado por otros en el futuro (sección Money as a necessity, párr 3). Se puede ver al dinero a partir de sus funciones, como depósito de valor, cuando permite la transmisión de valor a través del tiempo y, como medio de pago y unidad de cuenta, cuando la transmisión es a través del espacio. Cuando el dinero cumple con la función de depósito de valor, las personas realizan esta transmisión de valor, usualmente, consigo mismas: una persona deposita en un bien el fruto de su tiempo y energía con la expectativa de utilizarlo a futuro. Cuando el dinero funciona como un medio de pago y unidad de cuenta, la transferencia de valor se puede dar entre personas que no confían entre sí.

Para que un bien sea dinero debe cumplir con características específicas como escasez, durabilidad, divisibilidad, fungibilidad, ampliamente aceptado y fácil de transportar. Además, debe poseer las funciones antes dichas: depósito de valor, medio de pago y unidad de cuenta. Si un dinero cumple con esto, se le llama "buen dinero". Por esto, a lo largo del tiempo, los humanos en distintas partes del mundo, han llegado a la conclusión de que el mejor tipo de dinero ha sido el oro; Ammous (2018) explica las razones de la siguiente forma: El claro ganador en esta carrera a lo largo de la historia humana ha sido el oro, que mantiene su función monetaria debido a dos características físicas únicas que lo diferencian de otras mercancías: primero, el oro es tan estable químicamente que es prácticamente imposible de destruir; y segundo, el oro es imposible de sintetizar a partir de otros materiales (a pesar de lo que los alquimistas afirman) y solo se puede extraer de su mineral sin refinar, que es extremadamente raro en nuestro planeta (p. 21). Además, como lo expresa Lewis (2020): El dinero es una solución a un problema intersubjetivo, los sistemas monetarios tienden a converger en un solo medio. O más bien, los sistemas económicos surgen naturalmente de un solo medio debido a la función del dinero (párr. 3).

Para entender esto, es crucial entender el concepto de "dinero duro", *hard money* en inglés, aunque podría traducirse mejor como "dinero difícil", ya que se define como el dinero cuya oferta monetaria es difícil de incrementar. La propiedad de escasez es vital para encontrar formas de dinero duro como el oro. Otra característica importante del oro es la de "bien al portador", cuando se realiza un pago con oro, la transacción es final y desaparece la obligación; en otras palabras, no hay deuda. A esto, Morgan, en su testimonio ante el Congreso en el año 1912, asertivamente expresó: el oro es dinero, todo lo demás es crédito (como se citó en Investment Office, 2022, párr. 5).

Sin embargo, el uso del oro como dinero no solo mostró desventajas en sus propiedades de transportabilidad y divisibilidad, sino que la circulación del oro en monedas acortó los alcances de la política

[6] Problema de coordinación en sistemas distribuidos que ilustra los retos a la hora de transmitir información sin la intervención de un ente central y en la presencia de entes maliciosos. Se dice que Bitcoin soluciona este problema de forma práctica porque utiliza incentivos económicos.

[7] Un doble gasto supone un fraude ya que equivale a gastar el mismo dinero dos o más veces. En el mundo digital los intercambios digitales representan copias de la información y el reto es que ocurran solo una vez. La solución de este problema (antes de la llegada de Bitcoin) involucra registros centralizados que aseguren una transferencia única.

[8] Para que exista un intercambio entre partes, ambas deben querer lo que el otro ofrece.

monetaria de los bancos centrales. De esta forma nació la representación del oro en forma de papel, a modo de promesas redimibles en oro. Cuando el oro se encontró en las reservas de los bancos centrales, existió para ellos la oportunidad de inflar la cantidad de billetes en circulación.

Hoy en día, el efectivo es la forma de dinero que posee el comportamiento de finalidad de las transacciones, el problema es que está basado en deuda (dinero fiat[9]). En un tema relacionado, una situación alarmante es el desinterés de la población ante las iniciativas que manifiestan sus líderes por crear sociedades sin efectivo, como lo es Suecia, Noruega, China, Canadá y España (Quirós, 2022, párr. 4-8), puesto que el dinero en efectivo es el último vestigio de privacidad y de pagos, sin intermediarios, que queda en el sistema financiero tradicional.

Actualmente, la mayor parte del dinero se encuentra de forma digital. Es posible realizar intercambios de valor digital a través de intermediarios que basan en promesas (crédito) y relaciones de confianza los registros de las transacciones entre sus usuarios. Pero hay que tener en cuenta dos puntos: los créditos tienen una relación directa con la identidad del usuario y el dinero se ha transformado en información de quién le debe qué a quién, o sea, deuda.

De la familiarización social de las transacciones de dinero a través de intermediarios de confianza y el recuerdo del oro como dinero, es de dónde surge la idea de "respaldo". Esta noción se encuentra tan arraigada en la sociedad actual que, a pesar de que el respaldo del dinero con oro es inexistente y es la confianza con intermediarios lo que brinda ese sostén, todavía un porcentaje de la población cree que el dinero que utiliza cotidianamente está basado en oro, por ejemplo, en Estados Unidos un tercio de los habitantes tiene esta opinión (Genesis Mining, 2022, –sección What is the US dollar backed by).

De forma más concisa, para tener una idea más profunda sobre qué es el dinero, el economista Juan Ramón Rallo, en una entrevista, lo explica:

> *Antes que nada, habría que distinguir entre el dinero y moneda o medio de cambio. Moneda es todo medio de cambio indirecto, todo instrumento para articular cambios indirectos. Dentro de la moneda, es decir, dentro de los medios de intercambio, podemos tener dinero o deuda. El dinero es un medio de intercambio basado en un activo real. La deuda es un medio de intercambio basado en un activo financiero. Por otro lado, un activo financiero es aquel que tiene como contraparte un pasivo financiero, no puede haber un activo financiero, que es un derecho de cobro, sin que haya una contraparte en forma de pasivo financiero, es decir, una obligación de pago. Un activo real no son derechos de cobro, porque no tienen obligaciones de pago asociadas, son un bien que podemos utilizar por ser un bien como medio de intercambio. En cambio, en la deuda, los medios de intercambios que se utilizan como deuda, son medios de intercambio que utilizamos porque nos otorgan un derecho de cobro de calidad contra una tercera persona que tiene capacidad de pago. Entonces, el dinero sería un medio de cambio indirecto basado en un activo real. (Lunaticoin, 2020, 12m58s)*

Bitcoin

Bitcoin es dinero en efectivo de forma digital, esto significa que sus transacciones no requieren de un bien tangible para realizar intercambios de valor uno a uno, finales e inmediatos, y elimina la necesidad de intermediarios para transferir valor. Estos intercambios cuentan también con la propiedad de inmutabilidad, debido a la forma en que opera la Prueba de Trabajo. Por esto es que Yakes (2021), al profundizar sobre la inmutabilidad de Bitcoin, incluso la llega a describir como la séptima propiedad, y explica por qué a raíz de esto Bitcoin pasa a ser una forma de dinero superior al oro: [Bitcoin] es la única forma de dinero que mantiene la séptima propiedad monetaria de inmutabilidad. Bitcoin es un sistema peer-to-peer de dinero en efectivo. Sus características tecnológicas fueron diseñadas para crear propiedades monetarias superiores para el mundo digital. A través del tiempo, su red ha crecido lo suficiente, que actualmente, su activo monetario es el más escaso, el más durable, el más portable, el más divisible y el más descentralizado del mundo (p. 279).

[9] Dinero fiat o fiat: dinero decretado por los gobiernos y bancos centrales de cada país. Su respaldo está dado por las autoridades políticas y monetarias de los distintos países.

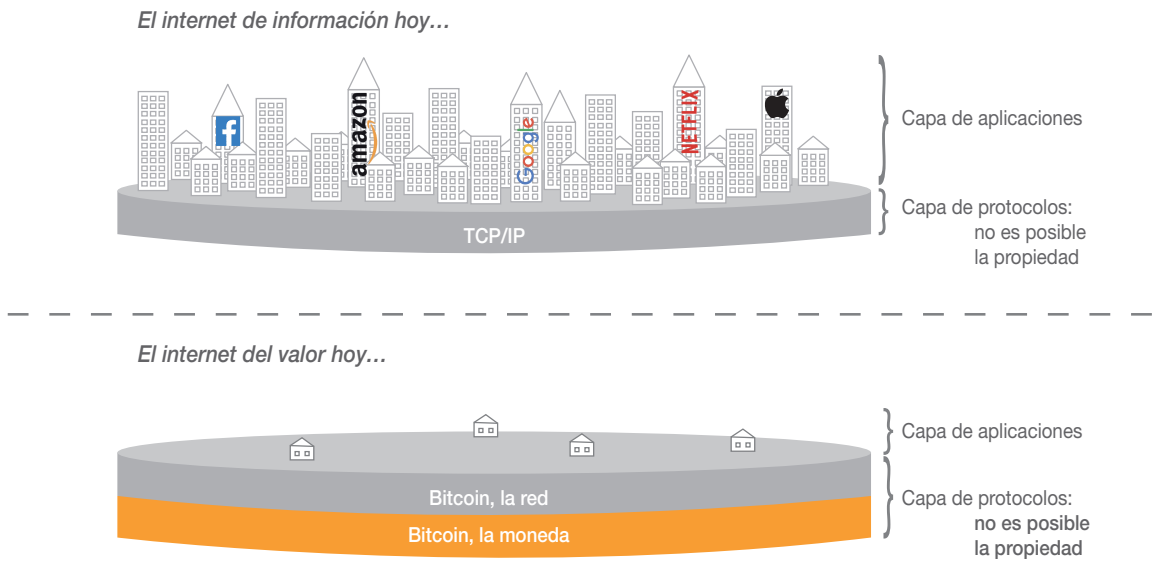
Con la llegada de Bitcoin la noción de respaldo y confianza se redefinen, ahora existe la posibilidad de transaccionar con un activo real digital en posesión completa del portador, en otras palabras, sin riesgos de contraparte; ya que al no existir ninguna promesa u obligación qué honrar, no está basado en deuda. Es por esta razón, por su escasez y el trabajo que se realiza para crear nuevas unidades ("minería"), que a Bitcoin se le conoce como "oro digital"; y es que gracias a esto y a su política fija de emisión monetaria, lo hace ideal como depósito de valor[10]. Nunca habíamos tenido un activo real digital que, además, contara con las características de dinero en efectivo y dinero duro simultáneamente. Aquí radica la utilidad de Bitcoin y su trascendencia tecnológica, no por nada es común escuchar entre los Bitcoiners[11] la frase "Bitcoin es el Internet del dinero"[12] y no, "el dinero del Internet". Por lo que es interesante tener en cuenta una comparación del rol de Bitcoin con el Internet, como se puede ver en la Figura 2.

Otro aspecto donde Bitcoin ha mostrado una gran utilidad es en la reducción de los costos de transacción, por ejemplo, se ha realizado un movimiento[13] de aproximadamente $2.011.009.210 con solamente $0,78 dólares de tarifa de transacción. Aunque Bitcoin no ha completado su proceso de monetización[14], y por esto todavía no es un medio de pago generalmente aceptado, lo será entre cada vez más usuarios se unan a la red. Por lo que, bajo la opinión de algunos, Bitcoin es dinero porque cuenta con las propiedades de dinero y cuando esta realidad se comprenda de forma generalizada, Bitcoin cumplirá con las funciones de dinero.

FUNCIONAMIENTO DE BITCOIN

¿Qué tienen en común las antigüedades, el tiempo y el oro? Son costosos, ya sea por su costo original o por la improbabilidad de su historia, y este costo es difícil de falsificar Hay algunos problemas relacionados

FIGURA 2: COMPARACIÓN ENTRE INTERNET Y BITCOIN



Con Bitcoin se puede transferir valor a través de Internet. Las aplicaciones sobre el protocolo de Bitcoin apenas están empezando a ser construidas.

Fuente: Tomado de Twitter, por Croesus [@Croesus_BTC], 2021. (https://twitter.com/croesus_btc/status/1367165017280237569).

[10] Solamente existirán 21 millones de bitcoin (unidad de valor). Bitcoin es un buen depósito de valor porque si un usuario tiene hoy 1 bitcoin, sin adquirir más y tampoco gastar el que tiene, en 20 años, tendrá 1 bitcoin y su parte del total de unidades permanecerá constante el tiempo: 1/21 millones. No hay inflación entendiendo por inflación un aumento en la cantidad total de unidades.

[11] Individuos entusiastas por Bitcoin y han tomado sobre sí la tarea de comunicar los pilares de esta tecnología.

[12] Antonopoulos ha publicado tres volúmenes bajo el título *The Internet of Money* una colección de sus charlas, que se recomienda al lector principiante

[13] El lector puede buscar la transacción:
e09d4bb6c6b30a10b8168ab1f55dcb9b7fd571270f14beea2dcb5fb8dcac967a
en el explorador de Bitcoin https://mempool.space

[14] Supuesto basado en que el dinero evoluciona en 4 etapas: recaudable, depósito de valor, medio de intercambio y unidad de cuenta.

con la implementación de un costo infalsificable en una computadora. Si tales problemas se pueden superar, podemos alcanzar 'bit gold'. Esta sería la primera moneda en línea basada en una confianza altamente distribuida y un costo infalsificable en lugar de la confianza en una sola entidad y los controles contables tradicionales (Szabo, 2008, párr. 1-4).

Elementos de Bitcoin

La red es robusta en su simplicidad no estructurada (Nakamoto, 2008, Sección Conclusion, párr. 1).

Bitcoin la red y bitcoin la unidad de valor

Bitcoin (con mayúscula) es un sistema que se compone de la red y su unidad de valor también llamada "bitcoin", para esto ver la Figura 2. La red de Bitcoin es del tipo peer-to-peer y sus nodos[15] pueden clasificarse de acuerdo con sus funciones. Los nodos más comunes son aquellos que reciben, verifican y transmiten información (transacciones de bitcoin) a los demás nodos; también almacenan el libro de registro de transacciones llamado "*blockchain*". Con el objetivo de cumplir estas labores, los nodos "corren" el *software* de Bitcoin comúnmente conocido como *Bitcoin Core*[16]. En la red de Bitcoin también existen nodos especiales llamados "mineros"[17] que, además, se encargan de agrupar las transacciones más recientes con el fin de que sean agregadas al *blockchain*. La unidad de valor bitcoin (con minúscula), es el activo digital que se mercadea en términos fiat, oro, bienes y servicios, entre otros.

El blockchain *de Bitcoin*

El *blockchain* fue propuesto por Haber y Stronetta (1991) quienes trabajaron en una forma que fuera capaz de "*time stamp*" documentos digitales con las siguientes propiedades: marcar la hora de los datos en sí, sin depender de las características del medio en el que aparecen los datos, de modo que sea imposible cambiar un solo bit del documento sin que el cambio sea evidente. En segundo lugar, debería ser imposible sellar un documento con una hora y datos diferentes a los reales (sección Introduction párr. 4). Como solución proponen el uso de funciones *hash*[18] unidireccionales aplicadas a los documentos para ligarlos entre sí (sección Summary párr. 2), Nakamoto implementa, con ciertas variaciones, esta idea en Bitcoin.

El *blockchain* de Bitcoin es el libro que registra todas las transacciones ocurridas en la red, es un elemento fundamental, pero no es la tecnología en sí, como muchos erróneamente han creído en los últimos años. El *blockchain* es una estructura de datos que agrupa información en lo que se ha denominado "bloques". Los bloques se conforman por transacciones agrupadas en otra estructura de datos llamada "*Merkle tree*" y el encabezado que contiene la información del bloque presente y el identificador del bloque previo. El enlace por medio de funciones hash con el bloque anterior es lo que le da la característica de "cadena" y por lo tanto el nombre de *blockchain*. Todos los nodos de Bitcoin mantienen una copia del *blockchain* y su actualización, o sea, el bloque nuevo, y este es propuesto por los nodos del tipo mineros.

La red de Bitcoin es una red abierta y pública, por lo que es resistente a la censura, ya que todo el que quiera puede participar corriendo un nodo y validar de forma independiente las transacciones. Sin embargo, esto posee un riesgo para el sistema, debido a que pueden existir nodos maliciosos que intenten propagar transacciones que supongan un doble gasto. Nakamoto, de forma ingeniosa, propuso una forma en la que los nodos sin necesidad de confiar entre sí, sean incentivados a mantener la red segura y estén expuestos a pérdidas económicas si la atacan.

Por otro lado, es común escuchar expresiones como "Bitcoin es la primera aplicación sobre *Blockchain Technology*". No obstante, Bitcoin es la tecnología en sí, entendiendo por tecnología una herramienta que nos permite realizar "algo" que no se podía hacer antes. Bitcoin es dinero duro, y como dinero, resuelve el problema de la transferencia de valor a través del espacio

[15] Participante de la red que es tanto cliente como servidor.

[16] Puede ser descargado aquí: https://bitcoin.org/en/bitcoin-core/

[17] Los mineros están conformados por *mining pool*s y utilizan miles de *ASICs (Application Specific Integrated Circuit)* con el fin de reszolver el reto matemático. Con el fin de comprender el papel de los mineros y los demás participantes que lo conforman, se recomienda el podcast de Lunaticoin *¿Qué actores componen la industria minera de Bitcoin?* (https://www.youtube.com/watch?v=3dHYDjORIn4).

[18] Función criptográfica de una dirección (no se puede revertir) que convierte los elementos de entrada (datos) en una salida de tamaño fijo, determinístico y funciona como identificador. En Bitcoin se utiliza el SHA-256 *(Secure Hash Algorithm).*

y el tiempo, incluso, de una forma más eficiente que el oro porque, como se explicó antes, el oro es posible de confiscar y está sujeto al control.

Otro error se encuentra en el uso de la palabra "criptoactivo" o "criptomoneda" para referirse a bitcoin, queriendo indicar que es un activo digital que utiliza un *blockchain* en el que se registran los intercambios de su unidad de valor. Como bien lo explicó el economista Juan Ramón Rallo, las técnicas subyacentes de un activo no indican su naturaleza:

> *Lo que caracteriza un activo no es la tecnología o el soporte, sería como hablar de papiro-activo para meter en el mismo saco el franco suizo, el peso argentino o un certificado de una acción de* Apple. *La tecnología puede ser muy importante, la criptografía puede ser clave, pero no define la naturaleza de un activo. (Mundo Crypto, 2022, 0m55s)*

La Prueba de Trabajo

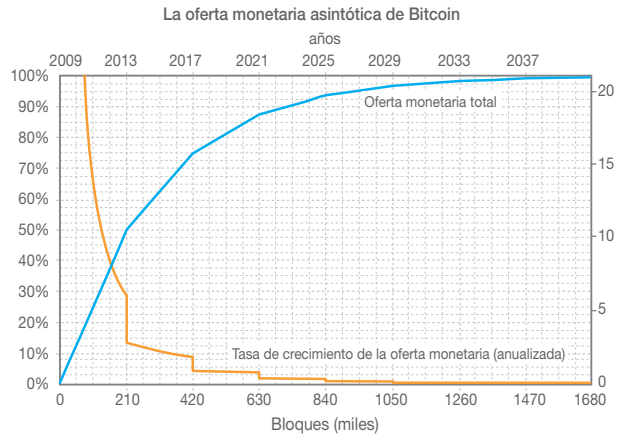
Según Vitalik Buterin, la Prueba de Trabajo está basada en las leyes de la física, de forma que tienes que trabajar con el mundo tal como es (Walker, 2022, 0m59s). La Prueba de Trabajo o "PoW", por sus siglas en inglés de *Proof of Work*, fue la solución práctica propuesta por Nakamoto, para evitar el doble gasto. De esta forma es como la red llega a un consenso acerca de lo que ha ocurrido y su orden.

Los mineros al agrupar las transacciones con el fin de crear un nuevo bloque deben, por prueba y error, resolver un reto matemático tal que la identidad, o sea, el identificador o huella digital del bloque, cumpla con condiciones preestablecidas por el protocolo. Cuando un minero resuelve el reto, el protocolo le otorga cierta cantidad de bitcoin nuevas (actualmente 6,25 bitcoin) como recompensa o incentivo por el trabajo realizado; por lo tanto, los mineros compiten entre sí, comprometiendo sus propios recursos en la forma de equipo computacional y electricidad, con el propósito de ganar bitcoin.

Si los mineros incluyen transacciones inválidas en el bloque propuesto, los nodos no aceptarán tal bloque como válido y no será incluido en su *blockchain*. De esta manera, está en el mejor interés de los mineros actuar de forma honesta, porque de lo contrario, su gasto en equipo y electricidad no se verá retribuido. Por otro lado, estos nuevos bloques, creados por los mineros, se generan en promedio cada 10 minutos, este intervalo debe permanecer constante, así que la dificultad de creación de bloques es el parámetro que varía. Esta es la forma en la que bitcoin, un bien digital, se enlaza con el mundo físico, material o tangible.

La política de emisión monetaria de Bitcoin ha sido preestablecida en 21 millones, a partir del bloque génesis 50 bitcoin fueron creados por bloque y otorgados como incentivo a los mineros por un periodo de 210.000 bloques, aproximadamente 4 años. En este punto ocurrió un recorte a la mitad (*halving*) en la recompensa por bloque, que pasó de ser 50 bitcoin a 25 bitcoin. Los mineros al cabo de este primer recorte ganaron 25 bitcoin por bloque hasta el siguiente recorte, otros 210.000 bloques, y así sucesivamente hasta que la cantidad de bitcoin total emitida llegue a lo preestablecido de forma asintótica, suceso que ocurrirá en el año 2140[19]. En la Figura 3 se ilustra la política de emisión monetaria de Bitcoin.

FIGURA 3: POLÍTICA DE EMISIÓN MONETARIA DE BITCOIN



La línea azul muestra un crecimiento exponencial en la red durante los primeros 210000 bloques, y una disminución de su pendiente al cabo del primer y sucesivos recortes. La línea roja muestra la razón anualizada del crecimiento de la oferta de bitcoin (inflación).

Fuente: Tomado de "The Bitcoin Central Bank's Monetary Policy" por Rochard (2013), (https://nakamotoinstitute.org/mempool/the-bitcoin-central-banks-perfect-monetary-policy/).

[19] A partir del momento en que la emisión de nuevo bitcoin haya terminado, el incentivo de minería será la suma de las tarifas por transacción aportadas por los usuarios de la red.

Uno de los mitos más comunes relacionados con la minería es el de decir que el propósito de la minería es crear bitcoin. No obstante, el objetivo de la minería es proveer de seguridad a la red de Bitcoin. Por lo tanto, la energía invertida con este propósito no se está desperdiciando. La forma en la que la Prueba de Trabajo resuelve el problema del doble gasto se discute en el Anexo A, donde se explica el Ciclo de Vida de una Transacción.

El Ajuste de Dificultad

En lugar de que la oferta cambie para mantener el mismo valor, la oferta está predeterminada y el valor cambia (Nakamoto, 2009). Debido a variaciones en el hash power[20] la frecuencia de creación de bloques puede aumentar o disminuir: si el hash power aumenta, el tiempo promedio de minado de los bloques será menor a 10 minutos y, si el hash power disminuye, este tiempo de minado promedio será mayor a 10 minutos. Nakamoto propone otra idea llamada "El Ajuste de Dificultad". De acuerdo con esto, cada 2016 bloques, aproximadamente 2 semanas, los nodos ajustan la dificultad del reto matemático con el fin de que la frecuencia se mantenga en el promedio establecido. Este proceso se ilustra en la Figura 4.

Este ajuste convierte a Bitcoin en el primer y único sistema que fusiona la emisión de nuevas unidades de valor a un intervalo de tiempo predeterminado, es este el ingrediente "secreto" de Nakamoto. En este sistema, bitcoin representa un bien en el que su aumento de precio no dispara la oferta, ya que su emisión total no puede ser cambiada. En contraste, en el caso de materias primas, si su precio aumenta, hay mayor incentivo por crearlas, lo que provocaría que su oferta aumente y, por consiguiente, resultaría en una caída en su precio.

En el caso de Bitcoin, un aumento de precio de bitcoin incentivará a más mineros unirse a la red y participar con el fin de crear bitcoin nuevos, pero el aumento de mineros en la red no provoca una creación más rápida de bitcoin, porque su emisión está anclada al tiempo, sino que provocaría un aumento en el hash power y, por lo tanto, mayor seguridad de la red. Esta forma novedosa de alinear incentivos basada en Teoría de Juegos en conjunto con la Prueba de Trabajo es lo que hace de Bitcoin una tecnología sin precedentes ni sucesores.

FIGURA 4: AJUSTE DE DIFICULTAD

Si más mineros se integran a la red, el tiempo promedio para crear un bloque disminuye y, en el siguiente ajuste, el software incrementará la dificultad del reto al cabo de 2016 bloques y viceversa.

Fuente: Tomado de "Mi Primer Bitcoin Libro de Trabajo" por Mi Primer Bitcoin, 2022. (https://github.com/MiPrimerBitcoin/Diplomado_v3.0).

Time chain

La Prueba de Trabajo en un entorno peer-to-peer funciona porque no requiere de confianza y esto se da porque está desconectada de todos los elementos externos –como la lectura de relojes (o periódicos, por ejemplo). Se basa solamente en una cosa: los cálculos requieren de trabajo, y en nuestro universo, el trabajo requiere de energía y tiempo (Der Gigi, 2021, Proof of Time, párr. 4).

Es necesario subrayar que Nakamoto en su artículo no hizo mención a la palabra *blockchain*, sino que utilizó el término "*time chain*" para referirse al registro de transacciones. La coordinación por medio de la Prueba de Trabajo, provee la forma en que los nodos sean capaces de llegar a un acuerdo acerca del orden cronológico de las transacciones y los bloques en su libro de registros.

En el ciberespacio no existe el tiempo de la forma en que lo percibimos, por lo que, si se organizan las transacciones y bloques con respecto a un sistema

[20] Sumatoria de la cantidad de operaciones por segundo (cálculo de hashes/s) de la red.

de referencia temporal, se estaría insertando un elemento de coordinación central en la red. Desde un punto de vista relativista, no existe una forma absoluta de medir el tiempo, la simultaneidad de eventos separados especialmente depende del observador y su marco de referencia; por esto, lo que se mide es el intervalo entre ellos.

La Prueba de Trabajo es la forma en la que Nakamoto ideó, basado en investigaciones que lo preceden, con el fin que la red llegue a un consenso del orden cronológico de los eventos, o sea, un consenso en la sucesión temporal de las transacciones y los bloques, sin la necesidad de confiar en el reloj de un tercero. Por esta razón, es más apropiado referirse al *blockchain* de Bitcoin como un "time chain", cuya medida interna de tiempo son los bloques, ya que, por sí mismos, tienen una frecuencia de creación (Der Gigi, 2021). En consecuencia, imaginando un escenario poco probable en que los usuarios de la red de Bitcoin intentaran cambiar su protocolo de consenso de Prueba de Trabajo a algún otro mecanismo, se correría el riesgo de agregar un elemento externo para lograr la coordinación temporal. Esta es una de las razones por las que los Bitcoiners se encuentran renuentes a considerar esta opción a pesar de las críticas del consumo energético de la red.

Propiedades de Bitcoin

En los siguientes párrafos se muestra de forma breve las propiedades más significativas de Bitcoin que son irrepetibles en otros sistemas.

Descentralización

No confíe, verifique (mantra Bitcoin). La descentralización es una distribución completa y funcional del sistema entre actores independientes coordinados a través de incentivos varios, estos pueden ser de naturaleza económica, política, social y ética. Bitcoin cumple con esta propiedad tanto para la emisión de su unidad de valor como para su transferencia a nivel de protocolo. También se puede argumentar que estas características ya han sido impregnadas en la mente de los usuarios y cualquier cambio será repudiado.

Un ejemplo histórico de un registro descentralizado de información es "La Biblia". A pesar de que han existido diferentes traducciones y versiones a lo largo de los años; la historia, los principios y los fundamentos son inmutables porque han sido transmitidos por generaciones. Imagine el caso de una variante escrita en que Jesús no resucitó, los cristianos rechazarían tal interpretación como la base de su fe y el libro donde estuviera escrita esta versión de los hechos no sería "La Biblia". Las propiedades monetarias de Bitcoin no solo se encuentran como parte del protocolo en los nodos, sino que ya pertenecen a la tradición oral y escrita entre los Bitcoiners que, en conjunto con la Prueba de Trabajo, ocasiona que sean imposibles de cambiar.

Inmutabilidad

Según Antonopoulos (2017), *blockchain* asegura que no se pueda cambiar algo sin que nadie se dé cuenta. En el campo de la ciberseguridad lo llamamos "*tamper-evident*", lo que significa es que, si existe un cambio, este es evidente. No puedes manipular sin evidencia de su manipulación. Pero hay un estándar más alto en seguridad, que llamamos "*tamper-proof*" o, a prueba de manipulaciones, o sea, algo que no se puede manipular. No solo será visible si se manipula, sino que no se puede cambiar, es inmutable.

Y la característica que le da a Bitcoin su capacidad *tamper-proof* no es *blockchain*, es la Prueba de Trabajo, ya que es lo que hace que Bitcoin sea fundamentalmente inmutable. Este concepto es muy importante de entender, porque muchas personas están lanzando palabras como *blockchain* y afirmando que estas cosas son inmutables, aunque no tengan una Prueba de Trabajo o cualquier tipo de algoritmo de consenso que les otorgue inmutabilidad. En el mejor de los casos, las *blockchain* pueden ofrecer evidencia de manipulación; lo que significa que alguien se dará cuenta, pero no son inmutables. Esta distinción va a ser históricamente importante (5m39s).

Dentro de los errores más recurrentes se encuentra la afirmación: "lo que se registra en un *blockchain* es inmutable". Esta creencia se debe a que los bloques se entrelazan consecutivamente por medio de huellas digitales o identificadores obtenidos al aplicar funciones criptográficas de una dirección a la información que se agrupa en ellos. Muchos aseguran que, si el *blockchain* está distribuido por diferentes nodos, esto provocará que lo que esté escrito en él no se pueda cambiar, pero en realidad si se cambia la información de algún bloque en algún nodo, nos daríamos cuenta, y cambiar esta información sólo es posible porque no hay un costo energético asociado. En un escenario donde no hay un coste

energético se necesita la confianza en "nodos principales" o "nodos coordinadores", para que algún otro nodo sepa distinguir cuál es el *blockchain* correcto.

La propiedad de inmutabilidad es una característica exclusiva de Bitcoin que se manifiesta en su *blockchain* como consecuencia de la Prueba de Trabajo. Si un ente malicioso desea cambiar el pasado, es decir, manipular una transacción que ha sido incluida en el *blockchain* de Bitcoin, dicho actor debe invertir tiempo y energía para resolver el reto matemático, por lo que los nodos sólo incluirán en su registro aquellos bloques que cumplan con las condiciones establecidas por la Prueba de Trabajo. Esto quiere decir que se requiere de un costo energético para cambiar las transacciones del *blockchain* de Bitcoin, esto porque los nodos escogen el *blockchain* que presenta la mayor cantidad de trabajo, por lo que no hay necesidad de "nodos coordinadores"; en otras palabras, si un nodo presenta un *blockchain* "nuevo", deberá enseñar el trabajo o coste energético que conlleva su creación, y si este no es mayor al del *blockchain* que posee cada nodo, no será aceptado. De esta forma cada nodo puede distinguir cuál es la cadena principal.

La siguiente explicación es certera en la relevancia de la Prueba de Trabajo para que las propiedades de inmutabilidad y escasez emerjan del sistema: La información que se genera a través de la Prueba de Trabajo sólo puede existir porque sucedieron ciertas "cosas" en el mundo real. Ciertos eventos que son tan improbables, tan increíblemente improbables, que realmente tuvieron que ocurrir a pesar de que cada evento individual fue un evento digital (Der Gigi, 2022, Sección Digital Reality, párr. 10).

Escasez

Debido a la importancia de esta propiedad, a lo largo de este documento la escasez de bitcoin se ha discutido en varias ocasiones. No obstante, es interesante meditar en las palabras del emprendedor y tecnólogo Booth (2022), cuando dijo: El dinero abundante crea escasez en todo lo demás. La escasez en el dinero crea abundancia en todo lo demás (Energy (as a part of security), párr.1).

Inconfiscabilidad

> *La revolución es de tal magnitud que nos permite acumular riqueza sin que nadie más en el mundo pueda quitárnosla, para bien o para mal. Es un contrato de propiedad sin necesitar a los Estados, permite tener el control exclusivo de un bien sin necesidad de leyes ni intermediarios. (D. María, 2022, Capítulo 6, párr. 4)*

El usuario tiene acceso a las bitcoin que posee por medio de un par de llaves criptográficas. Si el usuario sigue buenas prácticas de seguridad y privacidad de su llave privada, nadie sabrá que es dueño de bitcoin. Esto es totalmente innovador porque no existe un bien tangible que no esté sujeto a la confiscación, sin mencionar el hecho de que los bienes digitales pueden ser copiados, pero esto cambia con la aparición de Bitcoin.

Muchos Bitcoiners manifiestan que Bitcoin representa la separación del dinero y el estado. Y aún más allá, están quienes expresan que Bitcoin redefine el concepto de propiedad privada, ya que bitcoin es lo único que el individuo realmente puede poseer. En otras palabras, Bitcoin tiene el potencial de brindar derechos de propiedad privada a toda la humanidad.

A partir de la definición de propiedad, según Rousseau, es un derecho natural que requiere de la presencia de los Estados para su defensa; por el otro lado, de acuerdo con la visión de Stirner, propiedad es aquello que está bajo el dominio del individuo y bitcoin es el único bien que cae bajo esta última interpretación (Begleri, 2022, párr. 6). Como consecuencia, el contrato social se redefine con bitcoin como núcleo y diferentes modelos pueden surgir luego de una etapa de transición del sistema fiat a un sistema con Bitcoin como estándar sin la presencia de los Estados.

Neutralidad

El sistema Bitcoin permite a cualquier actor transaccionar en la red en igualdad de condiciones, independientemente de su etnia, credo, calificación crediticia o postura política, en contraste con el sistema actual. El protocolo de Bitcoin no distingue entre usuarios ni transacciones. Una transacción válida es incensurable e imparable para cualquier poder de tipo tecnológico o político, en Bitcoin no existen transacciones ilegales.

Independiente de terceros

A lo largo de este documento se ha explicado por qué Bitcoin no necesita de la presencia de intermediarios.

LIGHTNING NETWORK (LN)

Bitcoin comenzó con un diseño inteligente desde el principio. Creó una red de liquidación y oro digital subyacente, con un confiable grado de descentralización, auditabilidad, escasez e inmutabilidad que ninguna otra red rivaliza actualmente. Además, sobre estas bases se está desarrollando Lightning como red de pago y ha alcanzado una masa crítica de liquidez y usabilidad (Alden, 2022, párr. 5).

Problema de escalabilidad

Como parte de las críticas que experimenta Bitcoin es que si bien es cierto es utilizado como oro digital y depósito de valor, no es idóneo como medio de pago, ya que el usuario debe esperar a que su transacción sea incluida en el *blockchain* de Bitcoin y este es un proceso que ocurre en promedio cada 10 minutos. A esta dificultad se conoce como el "problema de escalabilidad", en términos coloquiales, se ilustra con la frase "no puedo comprar un café con bitcoin".

La escalabilidad se refiere al bajo número de transacciones por segundo (tps) que Bitcoin es capaz de procesar (alrededor de decenas de tps mientras que redes como Visa o Mastercard pueden procesar hasta miles de tps). La velocidad de la red Bitcoin en términos de tps existe supeditada a su descentralización, el costo de ancho de banda y equipo computacional necesario para sincronizar los nodos, debido a que estos deben ser económicamente accesibles para la mayor cantidad de personas y al mismo tiempo generar consenso sobre todas las transacciones a nivel global.

Una forma que parece obvia para incrementar la cantidad de tps es aumentar el tamaño del bloque y/o su frecuencia de minado, puesto que bloques más grandes y frecuentes pueden incluir más tps. Han existido múltiples iniciativas para promover cambios y crear nuevas versiones de Bitcoin basadas en la priorización de tps en detrimento de la descentralización. Destaca dentro de estos movimientos un evento conocido como el *Blockcksize Wars* que tuvo lugar en el 2017 en el cual personalidades adineradas con el apoyo de un importante porcentaje de mineros (los cuales se verían económicamente beneficiados con este cambio) intentaron convencer al resto de la red en aumentar el tamaño de los bloques.

El resultado que han tenido estas iniciativas ha sido un aplastante rechazo por parte de la gran mayoría de los nodos y del mercado. El precio en dólares, capitalización de mercado, volumen de transferencias y capacidad computacional minera de estas redes son comparables a cualquier proyecto aleatorio sin propuesta de valor, tales como monedas-*memes* de perritos, y ocupan un lugar junto a los miles de proyectos fallidos en el llamado "ecosistema cripto". Estas bifurcaciones fracasadas mostraron la verdadera naturaleza descentralizada de Bitcoin. De manera práctica, todo lo que un conjunto de actores poderosos puede hacer es cambiar el código y sus parámetros, pero tal cadena será vista por los nodos y valorada por el mercado como otra imitación más.

Así que en lugar de comprometer la inmutabilidad y descentralización buscando una red que sea capaz de procesar un número elevado de transacciones, el enfoque de los desarrolladores de Bitcoin es escalar por capas. Las "capas" son protocolos donde el intercambio de bitcoin ocurre sin necesidad directa de utilizar el *blockchain* para cada una de las transacciones. Este método de escalabilidad ha tenido una acogida favorable por los nodos de Bitcoin y el mercado.

Con respecto a este suceso del 2017, es interesante el análisis de Bier (2021) y las lecciones que los Bitcoiners deben aprender para el futuro: Sin embargo, no hay garantía de que esta característica de dinero controlada por el usuario persista para siempre. Las Blocksize Wars solo le dieron tiempo a Bitcoin, varios años más. Es posible que esta guerra solo sea un simulacro para los desafíos que se avecinan, cuando los principales beneficiarios de los sistemas monetarios controlados centralmente finalmente se den cuenta del potencial del dinero impulsado por el usuario y es posible que no les guste. Estas futuras batallas podrán ser sobre la resistencia a la censura, en lugar de la escalabilidad y el tamaño del bloque. Esta vez, es probable que el establecimiento financiero y político inicie el conflicto (p. 214).

Solución al problema de escalabilidad: Lightning Network (LN)

En el año 2015, los investigadores Joseph Poon y Thaddeus Dryja, proponen a Lightning Network (LN) como la solución al problema de escalabilidad de Bitcoin y expresan: para que Bitcoin tenga éxito, se requiere la confianza de que, si llegara a ser extremadamente popular, sus ventajas actuales derivadas de la descentralización sigan existiendo (Poon y Dryja,

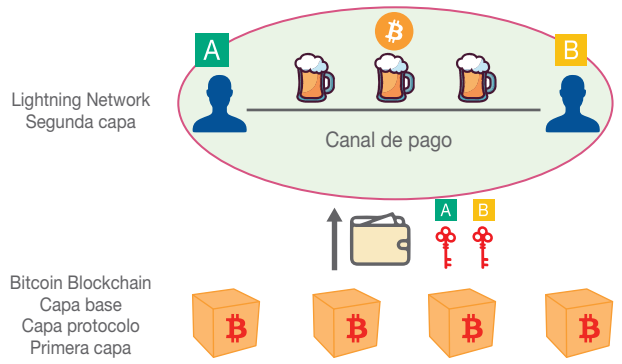
2016, p. 3). LN es un protocolo de interacción peer-to-peer con la cadena principal de forma segura y se le conoce como "segunda capa". Por medio de esta red es posible crear "canales de pago" o conexiones entre los nodos de LN. Los canales de pago son relaciones transaccionales entre dos partes con condiciones de vínculo establecidas por medio de direcciones multifirma[21]. LN, al igual que Bitcoin, es una forma de usar bitcoin, es una red abierta que opera en todo el mundo 24/7. En el protocolo base, los intercambios de bitcoin se conocen como transacciones y son del tipo "*on-chain*", lo que significa que se registran en el *blockchain* de Bitcoin, mientras que en LN los intercambios de bitcoin se llaman pagos y son del tipo "*off-chain*", no están registrados en el *blockchain* de Bitcoin.

Estos pagos de bitcoin entre los canales de pago, tienen un costo mucho menor que una transacción y mantienen las propiedades de inmutabilidad y finalidad de la capa base. Además, LN provee de mayor privacidad al usuario. Las transacciones de apertura y cierre de canales sí son registradas en el *blockchain*. Una característica importante de la red es que no todos los nodos deben tener canales[22] abiertos entre sí, ya que el protocolo de LN es capaz de enrutar pagos por medio de otros canales entre nodos en la red que tengan suficiente liquidez de satoshis[23]. LN puede llegar a ser capaz de procesar millones de tps, solucionando así el problema de escalabilidad.

Para comprender el funcionamiento de LN a muy alto nivel, usualmente, se utiliza el ejemplo de unos amigos que van a un bar y abren una cuenta a nombre de alguno, dejando como respaldo una tarjeta de crédito, al final de la noche, todo lo que ha sido consumido por ellos se consolida en una sola transacción, como se muestra en la Figura 5, con la diferencia que los pagos en LN no representan deudas.

La transacción de apertura y cierre del canal de pago entre peers se registra en el *blockchain* de Bitcoin. Los pagos de bitcoin que ocurren en los canales son inmediatos, seguros y finales. En la ilustración se muestra un canal de pago abierto entre un comercio y su cliente. LN permitirá a bitcoin ser utilizado como medio de pago, una de las funciones del dinero.

FIGURA 5: LIGHTNING NETWORK



Haciendo paralelismos del sistema financiero tradicional con el sistema Bitcoin, encontramos un desarrollo por capas[24]. Lewis (2019) explica que: El dinero y la tecnología de pagos son problemas distintos. La razón fundamental es que hay dos lados en cada transferencia de valor; un lado casi siempre involucrando dinero y el otro como el cumplimiento de bienes y servicios. Las capas de pagos ayudan a proporcionar un puente (sección Bitcoin vs. The Federal Reserve, párr. 2).

En Bitcoin, la primera capa es una red de finalidad con su propia política monetaria de emisión de su unidad de valor, bitcoin. Bitcoin es análogo a los bancos centrales que tienen a cargo la propia política de emisión monetaria de la moneda de curso legal de un país. Las transferencias interbancarias por medio de los bancos centrales son finales y los montos que se transfieren son altos, ya que representan la sumatoria de miles de transacciones ocurridas entre los bancos comerciales por medio de las redes de pago.

La segunda capa, LN, es una red de pagos de bitcoin, pero los montos tienden a ser mucho menores que en la capa base, pues representan el uso de bitcoin como medio de pago. Cuando los canales de pago se cierran, la transacción de cierre en el *blockchain* de Bitcoin puede representar miles de pagos ocurridos en la capa

[21] Las direcciones multifirma (multisign) requieren de más de una firma para utilizar los fondos de bitcoin asociados con esa dirección. Este tipo de direcciones son útiles para custodiar bitcoin por más de un usuario.

[22] Un canal de pago es una relación financiera entre nodos, asignando fondos desde una dirección de multifirma a través de un protocolo criptográfico estrictamente definido. (Pickhardt *et al.*, 2022, sección What is a Payment Channel párr. 2)

[23] En LN es común referirse a los pagos en unidades de satoshis. 1 bitcoin = 100 millones de satoshis.

[24] Para una mejor comprensión del desarrollo por capas del dinero se le recomienda la lectura del libro "*Layered Money*" por Nik Bathia.

FIGURA 6: VISUALIZACIÓN DE LIGHTNING NETWORK ALREDEDOR DEL MUNDO. NODOS Y CANALES DE LN ALREDEDOR DEL MUNDO

Fuente: Tomado de Acinq (https://explorer.acinq.co/).

superior. LN es análoga a Visa, Master Card, Paypal, Venmo, SINPE[25] y las compañías de remesas. Las redes de pagos tradicionales no emiten dinero ni lo "mueven", ya que son redes de comunicación; la información que se transmite son las promesas de pago entre sus usuarios. LN se diferencia de las redes de pagos tradicionales en que sus pagos no representan deudas o créditos, todos los pagos están garantizados por bitcoin subyacente, así que los pagos en LN también son finales.

LN es una red global, ver Figura 6, la cual tiene sus propios efectos de red que se alimentan, también, de los efectos de red de la capa base de Bitcoin y del Internet. LN está creciendo exponencialmente, debido a sus avances y crecimiento, es que los países de El Salvador y la República Central Africana, deciden convertir a bitcoin en moneda de curso legal. También cabe resaltar que la compañía Twitter adopta LN para su integración de propinas.

MÁS DESARROLLOS SOBRE BITCOIN

Además de LN, existen una serie de protocolos y desarrollos interesantes que interactúan con la capa principal del *blockchain* de Bitcoin, entre ellas se destacan Fedemints, Taro y Liquid.

Fedimints

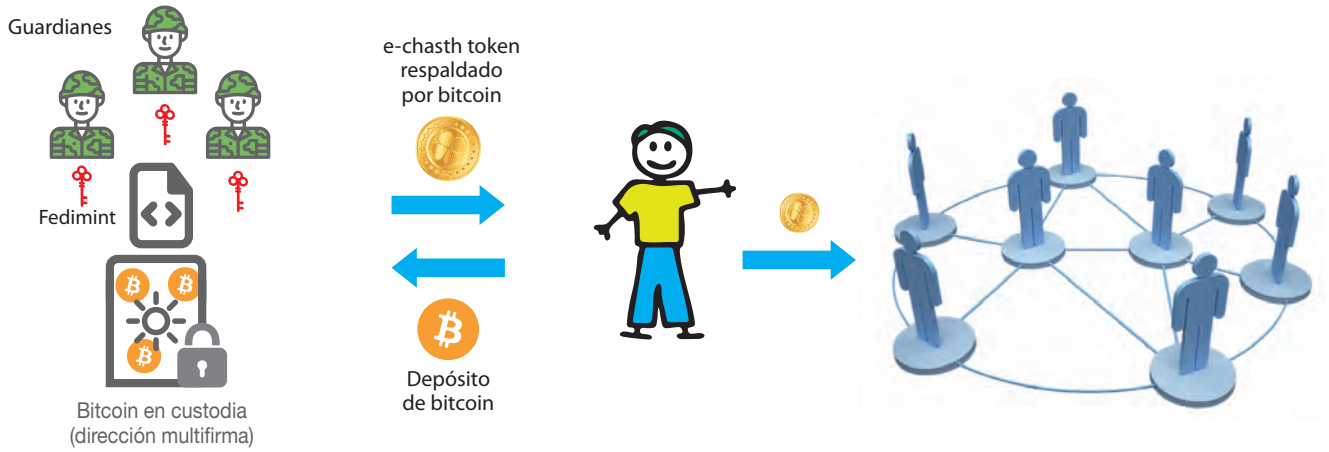
Las *Federated Chaumian Mints* o *Fedimints* tienen la capacidad de habilitar transacciones respaldadas en bitcoin, sin incurrir en los costos de transacción de la cadena principal, y son una alternativa dirigida a personas que no desean realizar su auto custodia, o sea, la manipulación de las llaves criptográficas.

Las Fedemints[26] son un protocolo de custodia comunitaria de bitcoin donde un conjunto de "Guardianes", quienes pueden ser desde una familia hasta personas de reputación en la comunidad, custodian las llaves

[25] Sistema Nacional de Pagos Electrónicos (SINPE) es una plataforma tecnológica desarrollada y administrada por el Banco Central de Costa Rica.

[26] El podcast de Lunaticoin *Creación y Evolución del ecash: Chaumian Mints, Fedimint y Cashu* https://www.youtube.com/watch?v=_XmQSpAhFN4 es un recurso valioso para principiantes.

FIGURA 7: COMPONENTES DE UNA FEDERACIÓN



Los guardianes de una federación se encargan de la custodia de las llaves criptográficas que controlan los bitcoins que, a su vez, respaldan el token e-cash aceptado por la comunidad.

Fuente propia.

de los fondos y, solamente, si una mayoría de ellos está de acuerdo, se puede tener acceso a los mismos. Este modelo de custodia federada permite que, por cada cantidad de bitcoin depositada en el fondo, el usuario reciba uno o varios *tokens* digitales o *e-cash* tokens con valor equivalente a lo depositado redimibles al portador, como si de efectivo digital se tratara. La técnica criptográfica de las firmas ciegas de Chauman[27] es empleada en este sistema, así que el ente emisor no conoce la identidad y el monto adjudicado a cada usuario, preservando su privacidad.

De la misma forma en que los bancos anteriormente emitían certificados en papel redimibles en oro, estos tokens digitales pueden intercambiarse dentro de la comunidad como si de bitcoin se tratase, sin necesidad de interactuar continuamente con el *blockchain*, evitando así costos de transacción y trazabilidad. Los usuarios pueden realizar actividades comerciales y pagos respaldados en bitcoin, sin costo y de forma privada. La Figura 7 muestra los principales componentes de una federación.

Dentro de las principales diferencias con una empresa de intercambio convencional, se encuentran la distribución de la custodia, una mejor auditabilidad de los fondos ubicados en la dirección multifirma, mayor privacidad, ínfimos o nulos costos de transacción y un aumento significativo en la capacidad de tps al no encontrarse limitado por la velocidad del *blockchain*.

Los Fedimints son uno de los desarrollos más interesantes y novedosos de este espacio, Gladstein (2022) lo explica de la siguiente forma: Los Fedimints son una idea provocativa porque violan la primera regla de Bitcoin: *Not your keys, not your coins*. Este mantra lo repiten todos los usuarios serios de Bitcoin, que saben que no deben almacenar sus BTC en intercambios de terceros. Cuando se usa correctamente, Bitcoin debería permitir que las personas sean sus propios bancos. Como muestran las protestas de este verano en Henan, China, incluso en regímenes dictatoriales, las personas se preocupan profundamente por sus ahorros y están dispuestas a arriesgar sus vidas para proteger sus ganancias. La capacidad de ser su propio banco es una revolución. Fedimint opta por una tercera vía, entre la custodia propia y la custodia de terceros. Nwosu lo llama custodia de "segunda parte": confiar en amigos, familiares o líderes comunitarios (Sección From Bicycle to Jumbo Jet, párr. 2-3).

Taro

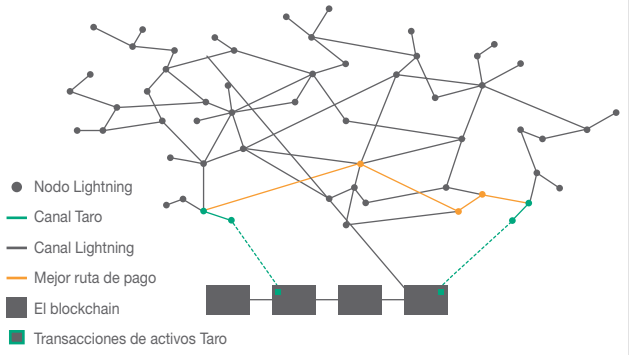
Este protocolo de código abierto desarrollado por la empresa Lightning Labs[28], permite emitir y transaccionar activos digitales diferentes a bitcoin de forma privada, utilizando la cadena principal de Bitcoin o LN como vía para transacciones. Taro combina ciertas funcionalidades incluidas en la última actualización

[27] Firma digital criptográfica que se emplea para firmar información oculta.

[28] Sitio web: https://lightning.engineering/.

de Bitcoin (Taproot) y los canales de Lightning como rieles de transporte para transaccionar activos digitales diferentes a bitcoin, por ejemplo, monedas estables como dólares digitales, NTFs (non fungible tokens), derivados de acciones de la bolsa de valores, etc. En la Figura 8 se ilustra una transacción con dinero sintético a través de Taro.

FIGURA 8: TARO. REPRESENTACIÓN DE UNA TRANSACCIÓN DE ACTIVOS DIGITALES, EN ESTE CASO DINERO FIAT SINTÉTICO, UTILIZANDO EL PROTOCOLO TARO A TRAVÉS DE LIGHTNING NETWORK



Fuente: Tomado de "What Is Taro in Bitcoin", por River Financial (https://river.com/learn/what-is-taro-in-bitcoin/).

Liquid

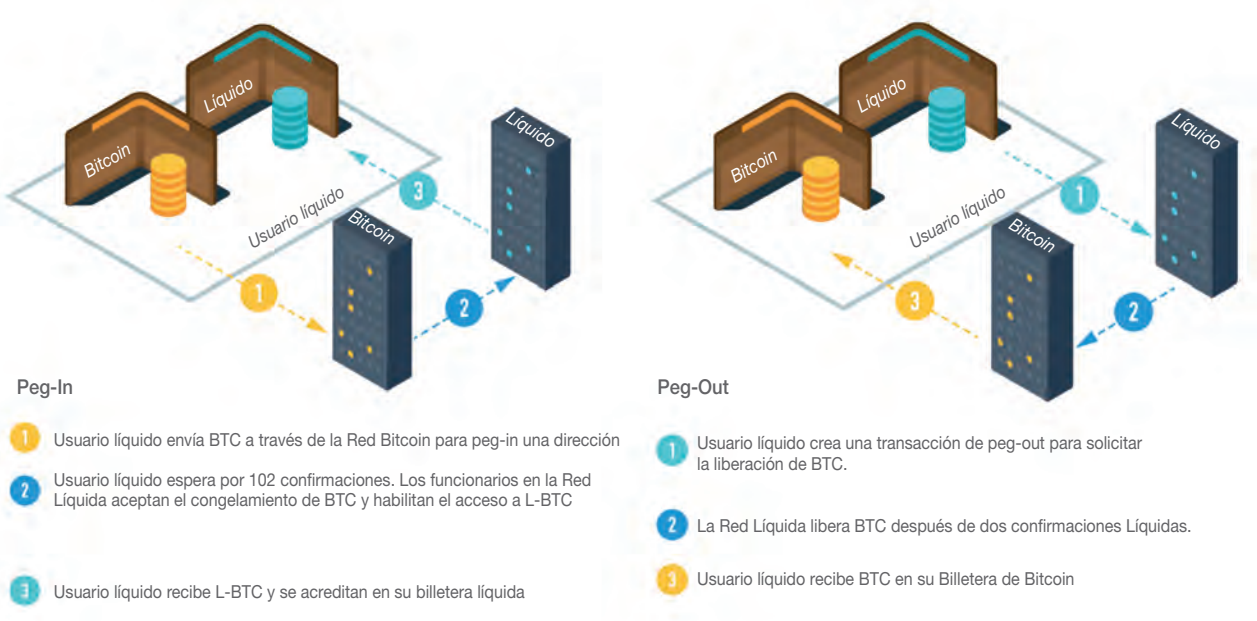
La red Liquid es una cadena lateral de Bitcoin desarrollada por la empresa Blockstream[29], la cual utiliza custodia federada que posibilita la emisión de toda clase de activos digitales incluyendo un token intercambiable por bitcoin (L-Bitcoin). De forma similar a los Fedimints, el usuario puede enviar sus bitcoins a una dirección donde se bloquean, y esto le permite realizar un intercambio por L-Bitcoin con transacciones confidenciales, rápidas y baratas. Este protocolo también posibilita la emisión de activos digitales diferentes a bitcoin, tales como monedas estables. En la Figura 9 se muestra en un alto nivel el funcionamiento de Liquid.

CRÍTICAS HACIA BITCOIN

Volatilidad

La presidenta del Banco Central Europeo, Christine Lagarde, se ha referido en reiteradas ocasiones a Bitcoin y lo ha descrito como un activo altamente especulativo (Keller, 2022, párr. 1). Tal opinión ha sido reproducida por el presidente de la Reserva Federal de Estados

FIGURA 9: LIQUID. DIAGRAMA QUE DESCRIBE EL USO DE LA RED LIQUID PARA UN USUARIO DE BITCOIN



Fuente: Tomado de "Technical Overview", por Blockstream, 2022, *Blockstream* (https://docs.blockstream.com/liquid/technical_overview.html).

[29] Sitio web: https://blockstream.com/

Unidos quien expresó que: Bitcoin y otras monedas digitales no están respaldadas por nada, y la criptomoneda más grande del mundo es más como un activo especulativo (Jafar, 2021, párr. 1). Estas afirmaciones parecen ser correctas debido a que bitcoin experimenta un alto grado de volatilidad cuando se mide en términos fiat, y la práctica de trading con bitcoin ha aumentado en popularidad, precisamente, por estos cambios abruptos de precio. Sin embargo, lo que Bitcoin realmente es, no es reflejado por el interés de algunos en obtener ganancias fiat a corto plazo.

Cabe destacar que, desde el lanzamiento de la red hasta que bitcoin tuvo cierto valor monetario en fiat (más de un año después[30]), no existían incentivos económicos para modificar sus parámetros. Es claro que las decisiones sobre el diseño de Bitcoin fueron tomadas con el objetivo de priorizar la robustez y la antifragilidad de la red, y con el fin de que fuera capaz de resistir incluso un embate gubernamental. Mientras la red crecía y se fortalecía, Nakamoto intentó al máximo postergar la atención hacia Bitcoin y mostró su preocupación cuando *WikiLeaks* le dio cierta visibilidad, contrario a los actuales proyectos *blockchain*, que su intención es atraer a la mayor cantidad posible de usuarios desde un inicio. Nakamoto expresó: WikiLeaks ha pateado el avispero y el enjambre se dirige hacia nosotros (Nakamoto, 2010).

Debido a que Bitcoin no es completamente comprendido por muchos y todavía se encuentra en sus fases iniciales de adopción[31], aquellos que especulan pueden emocionarse mucho cuando inversionistas importantes, compañías, figuras reconocidas, instituciones o gobiernos muestran su interés en Bitcoin. O bien, decepcionarse cuando estos participantes muestran desaprobación y, como consecuencia, el precio de bitcoin cae.

Alden (2022) explica que, como consecuencia del proceso de adopción, al ser la oferta de bitcoin inelástica, los cambios en la demanda se van a ver reflejados en volatilidad: Un activo no puede monetizarse sin volatilidad. Por definición, un activo no puede pasar de valer cero a tener una capitalización de mercado de un millón de dólares, a mil millones de dólares, o un billón de dólares, a varios billones de dólares, sin volatilidad al alza. Ese movimiento alcista del precio, debido a la adopción de los usuarios es la volatilidad. Siendo ese el caso, cualquier volatilidad al alza de esta magnitud atraerá a los especuladores, el apalancamiento y los aumentos repentinos de la demanda, y estos especuladores eventualmente se verán atrapados y obligados a vender por una u otra razón, lo que resultará en periodos de fuerte volatilidad a la baja (The Volatile Process of Monetization, párr. 1-2).

De esta forma, la volatilidad no es una característica desfavorable, tomando en cuenta el momento histórico en que se encuentra Bitcoin, respecto a la volatilidad Erik Vorhees expresa que un activo no puede tener el mejor desempeño y no ser volátil. Imagine un "activo de mejor rendimiento" teórico que fuera relativamente estable. Tal joya se compraría con avidez y la estabilidad se convertiría en volatilidad. La volatilidad es una característica esencial del alto rendimiento (Voorhees, 2021).

Por ejemplo, el crecimiento de Amazon y Google ha sido también sujeto a la volatilidad. No hay que olvidar que bitcoin, al ser intercambiable, tiene un precio de mercado, pero bitcoin no es una acción sino la unidad de valor de la red.

Consumo energético

El dinero sin energía es crédito (Saylor, 2022). La naturaleza de la generación eléctrica hace que localmente exista una gran cantidad de fuentes de energía sobrante no transportable a largas distancias ni almacenable. En general, los generadores eléctricos funcionan con cierta sobrecapacidad para la demanda pico y planeando de antemano un incremento en la necesidad futura. Al no poder transportarse más de unos cuantos cientos de kilómetros sin pérdidas significativas, el exceso o escasez de electricidad se manifiesta como

[30] El 22 de mayo del 2010 Laszlo Hanyecz compró dos pizzas a cambio de 10.000 bitcoin, fue la primera vez que bitcoin se utilizó en una transacción comercial. Cada 22 de mayo se celebra el Bitcoin Pizza Day.

[31] La duda que surge al analizar la volatilidad y que ha empezado a ser objeto de estudio en círculos académicos es si bitcoin es inherentemente volátil: si la respuesta es afirmativa, lo sería aún en las fases tardías de su proceso de adopción y por lo tanto no podría ser dinero, utilizando la definición de dinero como "un medio de pago generalmente aceptado". Las siguientes referencias son sugeridas para aquel que desee explorar más estas ideas: Why is bitcoin inherently volatile? por fernandom (https://gist.github.com/fernandonm/81cb21bdce0910055de32b98ee4119e1), ¿Es Bitcoin irremediablemente volátil? por Manuel Polavieja (https://juandemariana.org/ijm-actualidad/analisis-diario/es-bitcoin-irremediablemente-volatil/), Reflexiones sobre la regla monetaria de bitcoin y su viabilidad por Gael Sánches Smith (https://laeradebitcoin.substack.com/p/reflexiones-sobre-la-regla-monetaria) y el podcast de Lunaticoin ¿Será bitcoin dinero? (https://www.youtube.com/watch?v=UqjE7If2uwM)

un fenómeno local. La portabilidad de los mineros de Bitcoin lo hace ser un carroñero energético de estos puntos alrededor del planeta con exceso de producción. En este sentido Bitcoin no consume de la forma tradicional la energía eléctrica, es decir, no compite localmente por un recurso limitado frente a otros usos, sino que tiene su propio nicho de consumo, actuando de esta manera como un comprador de último recurso sin competencia, disminuyendo así el riesgo financiero de las inversiones para la producción energética.

También es importante recordar que lo que protege a Bitcoin no es la electricidad en sí sino su costo. La minería de Bitcoin es una barrera protectora, porque hace que sea costoso intentar "mentir" momentáneamente a la red y, al mismo tiempo, premia utilizar el poder computacional para incrementar su seguridad. Además, es gracias a la Prueba de Trabajo que las transacciones en el *blockchain* de Bitcoin son inmutables. Es importante resaltar que la electricidad que utilizan los mineros no está relacionada con un costo de procesamiento de transacciones, así que la métrica de "energía por transacción", utilizada en muchos artículos para desacreditar la minería de Bitcoin, es incorrecta y está basada en una interpretación equivocada del funcionamiento de la Prueba de Trabajo.

El enfoque acerca del consumo energético tiene un trasfondo más filosófico relacionado a si Bitcoin presenta algún beneficio en el mundo y, por consiguiente, si "merece" consumir energía. No es el consumo de energía lo que debería concentrar la atención de activistas ambientales[32], sino su fuente y utilidad de la red. También están quienes proponen que Bitcoin debe migrar hacia otro protocolo de consenso, pero sin la Prueba de Trabajo se convertiría en otro sistema, Bitcoin dejaría de ser dinero duro, no sería un activo real digital y perdería sus propiedades de descentralización e inmutabilidad.

La crisis de cambio climático que enfrenta la humanidad es el núcleo del argumento contra el consumo energético de Bitcoin, pero es importante cuestionarnos si es Bitcoin verdaderamente un contribuyente a este desastre, y además, cómo puede un individuo responder a la urgencia de esta crisis, si los pilares del sistema económico actual están sostenidos en el Keynesianismo, que motiva el gasto para estimular la economía, la cultura del consumo y la obsolescencia programada. Por el contrario, un cambio hacia un Patrón Bitcoin, tiene el potencial de inclinar al individuo hacia la austeridad y el ahorro.

Actividades ilegales

Noam Chomsky, en una entrevista en el 2014, expresó que la tecnología es básicamente neutral. Es como un martillo, al martillo no le importa si lo usas para construir una casa o para torturar, o si lo usas para aplastarle el cráneo de alguien. El martillo puede hacer cualquiera de las dos cosas, de la misma forma que la tecnología moderna (Learning Reimagined, 2014, 1m38s).

La tecnología es una herramienta que nos permite realizar algo que no podíamos hacer antes de su llegada. El Internet y Bitcoin son tecnologías, por lo tanto, son amorales. Aquellos que utilizan la tecnología son quienes agregan intencionalidad. Estas herramientas han sido, son y serán utilizadas para fines nobles o perversos.

RETO DE BITCOIN: PRIVACIDAD

En el 2021, el conocido *whistleblower* Edward Snowden, manifiesta lo siguiente: Bitcoin realmente está fallando de manera integral desde el punto de vista de la privacidad (Daily Hodl, 2021, 13m15s). La privacidad es un derecho humano. El artículo 12 de la Declaración Universal de Derechos Humanos expresa que: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (United Nations, 1948).

Uno de los mensajes más importantes con respecto a la privacidad se encuentra en "El Manifiesto Cypherpunk", a continuación, un extracto de (Hughes, 1993): La privacidad es necesaria para una sociedad abierta en la era electrónica. La privacidad no es secretismo. Un asunto privado es algo que uno no quiere

[32] Otro enfoque interesante es el de la sostenibilidad y los criterios Environmental, Social and Governance (ESG). Hoy en día, las compañías persiguen estos ideales y es común escuchar quienes desacreditan a Bitcoin cuando lo miran bajo estos estándares. Hofacker (2022) realizó un análisis de Bitcoin bajo los factores ESG, a pesar de que Bitcoin no es una compañía. Entre las conclusiones más interesantes se encuentra: La independencia que tiene Bitcoin significa que puede utilizar fuentes de energía que no se aprovechan en su totalidad, como el exceso de energía hidroeléctrica, eólica, solar e inclusive gas natural que en otras circunstancias se hubiesen desperdiciado (sección Factores ESG, párr. 6).

que todo el mundo sepa, pero un asunto secreto es algo que uno no quiere que nadie sepa. La privacidad es el poder de revelarse selectivamente al mundo.

Si dos personas están haciendo cualquier tipo de transacción, entonces tienen un recuerdo de su interacción. Cada uno de ellos puede hablar de su propio recuerdo sobre el tema, pero ¿cómo podría prevenirse esto? Quizás se podrían presentar leyes en contra, pero la libertad de expresión es aún más fundamental para una sociedad abierta que la privacidad; nuestra intención no es restringir la libertad de expresión. Si muchas personas hablan juntas en un mismo foro, cada una puede hablar con las demás y aumentar el conocimiento global acerca de esas personas. Las posibilidades de las comunicaciones electrónicas hacen posibles grupos así, y no van a desaparecer sólo porque nosotros queramos.

Dado que deseamos privacidad, tenemos que asegurar a cada persona que intervenga en una transacción que sólo conozca lo que es estrictamente necesario para esa transacción. Dado que se puede transmitir cualquier información, debemos asegurarnos de revelar lo mínimo posible. En la mayoría de los casos, la identidad personal no es relevante. Cuando compro una revista en una tienda y pago en efectivo, quien recibe el dinero no tiene necesidad de saber quién soy. Cuando le pido a mi proveedor de correo electrónico que envíe y reciba mensajes, mi proveedor no necesita saber con quién hablo, lo que estoy diciendo o lo que otros me están diciendo; mi proveedor solo necesita saber cómo hacer llegar el mensaje y cuánto le debo. Cuando mi identidad es revelada debido al mecanismo subyacente de la transacción, no tengo privacidad. En este caso, no es posible revelarme selectivamente porque siempre debo revelarme.

Por lo tanto, la privacidad en una sociedad abierta requiere sistemas de transacciones anónimas. Hasta ahora, el dinero en efectivo ha sido el mecanismo principal para asegurar la privacidad. Un sistema de transacciones anónimo no es un sistema de transacciones secretas. Un sistema anónimo permite a las personas revelar su identidad solo cuando lo deseen; esta es la esencia de la privacidad (párr. 1-4).

En los párrafos anteriores se describe con claridad la relevancia de la privacidad. Desde el punto de vista de transacciones económicas, gozar de privacidad es imprescindible debido a que en ellas se encuentra información de los datos personales del individuo, sin embargo, el individuo ha dejado de lado su privacidad a cambio de conveniencia; bien lo dice Snowden: Cuando alguien dice que no le interesa su privacidad porque no tiene nada que esconder, es como que diga que no le interesa su libertad de expresión porque no tiene nada que decir (Rusbridger *et al*., 2015, 0m00s).

No se puede asumir que la privacidad será otorgada, por la privacidad se debe luchar. Cabe resaltar las enfáticas palabras de la filósofa Véliz (2021):

> *En el mundo suceden cosas terribles como atentados terroristas o epidemias y seguirán sucediendo. Pensar que podemos evitar que ocurran si renunciamos a nuestra libertad y a nuestra privacidad es como creer en los cuentos de hadas. Esa confusión de los deseos con la realidad solo puede llevarnos a sumar el autoritarismo a la lista de catástrofes a la que nos tenemos que enfrentar. Irónicamente, el autoritarismo sí es un desastre que podemos evitar, para ello tenemos que defender nuestros derechos civiles y eso significa proteger nuestros datos personales. (p. 34)*

Tan claro tenían los cypherpunks el concepto e importancia de la privacidad y, sobre todo, de la privacidad en línea, que tomaron sobre sí la responsabilidad de crear el mundo que deseaban ver. Como herramienta para convertir sus ideales en una realidad, se valieron de código computacional y criptografía. El siguiente es un otro fragmento de (Hughes, 1993): Tenemos que defender nuestra privacidad si es que queremos tenerla. Tenemos que unirnos y crear sistemas que permitan las transacciones anónimas. La gente ha estado defendiendo su privacidad durante siglos mediante susurros, oscuridad, sobres, puertas cerradas, apretones de manos en clave y mensajeros. Las tecnologías del pasado no permitían una encriptación "fuerte", pero las actuales sí.

Los cypherpunks escriben código. Sabemos que alguien tiene que escribir software para defender la privacidad, y como no podemos obtenerla a menos que todos la tengamos, nosotros vamos a escribir el código. Publicamos nuestro código para que nuestros compañeros cypherpunks puedan practicar y jugar con él. Nuestro código es gratuito para todos, en todo el mundo. No nos importa mucho si no apruebas el software que escribimos. Sabemos que el software no se puede

destruir y que un sistema muy disperso no se puede cerrar (párr. 7,9).

Los cypherpunks conocían la necesidad de un dinero descentralizado que, como parte de su estructura, favoreciera la privacidad. El reconocido Hal Finney, uno de los grandes visionarios y mentes más brillantes en Bitcoin, quien incluso se sospecha que puede ser Satoshi Nakamoto, se refirió, en 1992, acerca del trabajo de David Chaum: Me parecía tan obvio. Aquí nos enfrentamos a los problemas de pérdida de privacidad, informatización progresiva, bases de datos masivas, más centralización, y Chaum ofrece una dirección completamente diferente, una que pone el poder en manos de individuos en lugar de gobiernos y corporaciones. La computadora puede usarse como una herramienta para liberar y proteger a las personas, en lugar de controlarlas. A diferencia del mundo actual, donde las personas están más o menos a merced de las agencias de crédito, las grandes corporaciones y los gobiernos, el enfoque de Chaum equilibra el poder entre los individuos y las organizaciones. Ambos tipos de grupos están protegidos contra el fraude y el maltrato por parte del otro.

Naturalmente, en la sociedad actual, con el poder asignado de manera tan desproporcionada, tales ideas son una amenaza para las grandes organizaciones. Equilibrar el poder significaría una pérdida neta de poder para ellos. Por lo tanto, ninguna institución va a acoger y defender las ideas de Chaum. Tendrá que ser por medio del activismo, en el que las personas primero aprendan cuánto poder pueden tener y luego lo demanden (Finney, 1992, párr. 5-6).

Bitcoin es público con el fin de que cada nodo sea auto soberano y no dependa de ninguna entidad. Cada nodo puede verificar las transacciones, su trazabilidad y conocer, con exactitud, la cantidad de bitcoin que han sido minadas, sin embargo, este diseño tiene como desventaja que compromete la privacidad.

Con el fin de reflexionar acerca del reto que enfrenta Bitcoin con respecto a la privacidad, es importante analizar una de las propiedades del dinero conocida como la fungibilidad. La fungibilidad es la capacidad que tiene un bien, activo o dinero de ser intercambiado por otro del mismo tipo. Por ejemplo, una moneda de un centavo no es diferente a otra moneda de un centavo y si alguna de ellas es utilizada como medio de intercambio por un bien, servicio o pago de una deuda, aquel quien la reciba debe aceptarla sin preferencia por otra. De la misma forma, si ambas monedas se encuentran en un monedero, no se puede hacer distinción entre ellas de acuerdo con su procedencia, ya que son intercambiables o fungibles. A nivel de protocolo y de red, las transacciones de Bitcoin son tratadas todas de la misma forma, no existe preferencia ni censura hacia ninguna transacción, son fungibles.

A pesar que popularmente se considera a Bitcoin como un mecanismo para realizar transacciones de forma anónima, lo cierto del caso es que por medio de técnicas sofisticadas de análisis, es posible rastrear la procedencia de las transacciones en el *blockchain*, ligarlas con billeteras digitales, incluso con la identidad física del dueño y conocer las actividades para las que fueron utilizadas (Fleder, Kester y Pillai, 2015); dotar de completa privacidad e irrastreabilidad a las transacciones de Bitcoin puede suponer la pérdida del conocimiento de la cantidad total de bitcoin creadas en un momento determinado. Por este motivo, si los bitcoins se pueden ligar con direcciones específicas y su procedencia, no son del todo intercambiables o fungibles.

Es posible para un ente gubernamental, obligar a los comercios a no aceptar pagos en bitcoin provenientes de direcciones que no aprueben, ya sea por actividades ilícitas o por otros motivos de censura. De esta forma, muchos comerciantes podrían negarse a aceptar bitcoin que previamente hayan sido usadas en actividades que parezcan tener dudosa procedencia, aunque la persona que realice el pago no esté directamente relacionada con ellas.

A pesar de que el sistema Bitcoin no representa, al día de hoy, el cumplimiento del sueño cypherpunk por los retos de privacidad que enfrenta, tal dificultad se puede ver como una oportunidad para el individuo de hacerse cargo de sí mismo, de su propio dinero, en aprender y seguir las mejores prácticas de seguridad y privacidad relacionadas con en el uso de su bitcoin y datos personales, ya que sí es posible emplear técnicas que incrementen su privacidad si el individuo se lo propone.

PARA QUIÉN ES BITCOIN

Bitcoin brinda a cualquiera (sin importar su nacionalidad, estatus, riqueza, género, raza o creencias) acceso a la mejor tecnología de ahorros del planeta, también provee de dinero programable que no se puede detener, no se puede devaluar, censurar, que se opone

a la vigilancia y confiscación. Los disidentes, manifestantes en democracias, líderes de oposición y periodistas independientes alrededor del mundo lo han empezado a entender, desde Minsk a Lagos, en Los Ángeles y hasta Buenos Aires. (Gladstein, 2022, p. 88)

El proceso de monetización por el que atraviesa Bitcoin ocasiona que su unidad de valor sea volátil en términos fiat y es por esta razón que se convierte en blanco ideal para los *traders*. Sin embargo, este uso no demuestra el potencial de Bitcoin. Aquel que comprende el problema que Bitcoin resuelve y cuáles activos se están desmonetizando ante la presencia de Bitcoin, se alejan de las actividades cortoplacistas y dejan el trading a aquellos actores experimentados que están dispuestos a arriesgarse.

Bitcoin es para aquel individuo que ha logrado expandir su horizonte temporal. Es común escuchar entre los Bitcoiners referirse a la "baja preferencia temporal", aquella que retrasa la gratificación momentánea en favor de la retribución futura, ya que por fin existe un dinero duro que incentiva el ahorro y reduce el consumismo. La civilización humana se ha construido por aquellos visionarios que tuvieron una baja preferencia temporal. Bitcoin le devuelve al individuo de cualquier parte del mundo la capacidad de construir su futuro al ser una tecnología resistente a la censura y a la desvalorización de sus unidades por terceros. Bitcoin no es una tecnología enfocada en el bien colectivo, sino en el individuo y, específicamente, aquel que decide volverse soberano; tal como lo describen Davidson y Ress-Mogg (1999) en su libro acerca de las consecuencias de la transición a la era de la información, cuando expresan: La tecnología de la era de la información hace posible la creación de activos que están fuera del alcance de muchas formas de coerción. Esta nueva asimetría entre protección y extorsión se basa en una verdad fundamental de las matemáticas (p. 112).

Más allá del cambio de preferencia temporal de los Bitcoiners y aquellos que, desde su perspectiva, niegan sus beneficios porque viven en lugares del mundo donde cuentan con servicios financieros funcionales; Bitcoin y LN ya son totalmente útiles para aquellos que viven bajo inflación descontrolada, para los desbancarizados y quienes encuentran sus cuentas bancarias congeladas por motivos de censura como reporteros, oposición política y otros. En palabras de Gladstein (2022): Solamente el 13% de la población de nuestro planeta ha nacido utilizando el dólar, euro, el yen japonés, la libra británica, el dólar australiano, el dólar canadiense o el franco suizo. El restante 87% ha nacido bajo autocracias o divisas mucho menos confiables. Para diciembre del 2021, 4,3 mil millones de personas viven bajo autoritarismo y 1,6 mil millones de personas se encuentran bajo inflación de dos o tres dígitos.

Los críticos en la burbuja del dólar no logran ver el panorama completo: cualquiera que tenga acceso a Internet ya puede participar de la red Bitcoin, un nuevo sistema de dinero con reglas iguales para todos los participantes, que no censura ni discrimina, que puede ser usado por individuos que no necesitan mostrar una identificación, custodiado por ciudadanos, de forma que es difícil de confiscar e imposible de devaluar (p. 17).

PROCESO DE ADOPCIÓN DE BITCOIN

El famoso inventor y futurista, Buckminster Fuller, nos deja como un legado sus sabias palabras: Nunca podrás cambiar algo peleando contra la realidad existente. Para cambiar algo debes crear un nuevo modelo que convierta el modelo existente en obsoleto (McElroy, 2013, párr. 3).

Los humanos tenemos la tendencia de imaginar el futuro como una extensión del presente y les puede ser difícil creer que algo desconocido pueda suplantar aquello con lo que tenemos familiaridad. Por ejemplo, Krugman (1998), Premio Nobel de Economía en el 2008, no contempló un mundo donde el Internet pudiera cambiar la forma en que nos relacionamos y comunicamos entre sí: El crecimiento de Internet disminuirá drásticamente conforme se haga aparente su falla en la Ley Metcalfe, que establece que la cantidad de conexiones potenciales en una red es proporcional al cuadrado de la cantidad de participantes: ¡la mayoría de las personas no tienen nada que decir entre sí! Alrededor del 2005, quedará claro que el impacto del Internet en la economía no habrá sido mayor que las máquinas de fax (Sección Future Thought, párr. 4).

Por el contrario, existe otro tipo visionarios que logran ver más allá del ruido, entre ellos nuevamente Fuller, quien en 1967 visualizó la llegada de lo que sería un tipo de dinero o riqueza basada en energía: Me referiré a algo que será uno de los descubrimientos para el 2000, un sistema de contabilidad científico de lo que significa riqueza. La riqueza no es el oro que los viejos

piratas solían tener, la riqueza es energía (Roemmele, 2020, 0m00s).

De forma similar, Henry Ford pronosticó lo siguiente: Bajo el sistema de moneda energética, el estándar sería una cierta cantidad de energía ejercida durante una hora que equivaldría a un dólar. Es simplemente un caso para pensar y calcular en términos diferentes de lo que nos ha establecido el grupo bancario internacional, al que nos hemos acostumbrado tanto, que pensamos que no hay otro estándar deseable (Bourgi, 2021, Sección Bitcoin as an energy currency, párr. 2).

La predicción de Buckminster Fuller y Henry Ford podrían haberse personificado en Bitcoin. Pero también, están aquellos que no solamente ven en Bitcoin el potencial para asentar las bases de un nuevo sistema monetario mundial, sino también, como es el caso de Jason Lowery, que menciona: Lo que la Prueba de Trabajo de Bitcoin, realmente representa, es un sistema de ciberseguridad, en que las personas están aprendiendo a defenderse a sí mismas, aprendiendo a defender el acceso a aquella propiedad que ellos libremente valoran se le llama "moneda" y las personas actúan como si fuera una moneda pero esto es solamente uno de los tantos usos El hecho de que llamemos a este gran sistema masivo físico de defensa que las personas están usando para asegurar su propiedad, "moneda", no implica, automáticamente, que el Departamento de Tesorería o la Reserva Federal Estadounidense, sea quien debe pronunciarse con respecto a los méritos de esta tecnología y, mucho menos, los banqueros (Pysh, 2022, 2h05m00s).

Si Bitcoin es intrínsecamente dinero, si funciona como dinero, si es solamente un depósito de valor a largo plazo sin ser medio de pago, si es un sistema de ciberseguridad que se puede usar como dinero, o, si bien, es algo mucho más profundo que posee todas las características anteriores, lo sabremos en los próximos años. Esta falta de certeza acerca de la naturaleza de Bitcoin se debe a que nos encontramos en las fases tempranas del proceso de adopción.

Una de las exposiciones más claras acerca de las etapas iniciales del proceso de adopción de nuevas tecnologías es presentada por Antonopoulos (2020), que al hablar sobre la "inversión de infraestructura", se refiere a cómo las cosas cambian cuando la infraestructura que es nueva se sobrepone sobre infraestructura que es vieja y cómo esto genera conflicto (sección Bitcoin is new, 0m18s). Durante el proceso inicial de inversión infraestructural se puede llegar a tener la percepción equivocada que la nueva tecnología no funciona tan eficientemente como la anterior.

Como un ejemplo histórico de este suceso, Antonopoulos menciona el uso de módems con el objetivo de transmitir paquetes de información a través de Internet por medio de líneas telefónicas que contaban con un ancho de banda optimizado para cierta función (transmisión de la voz humana a largas distancias). Las compañías telefónicas mostraron oposición al uso de sus redes con este fin. Al día de hoy, todas las llamadas telefónicas son hechas a través del Internet. Aquí tenemos la inversión de infraestructura (sección Demodulator, 13m12s).

Actualmente estamos enfrentando otro proceso de inversión infraestructural con Bitcoin - LN y el sistema financiero tradicional. La mayoría de las personas necesita la colaboración de los bancos y el sistema de pagos para utilizar los ahorros de sus cuentas o tarjetas de crédito con el fin de comprar bitcoin en una casa de intercambio, esto es lo que se conoce como el proceso de *on-ramp*[33]. Los usuarios que desean utilizar la tecnología disruptiva, Bitcoin, se están apoyando en las pasarelas de pago tradicionales para obtener acceso a la unidad de valor del nuevo sistema, pero el sistema financiero tradicional no les está haciendo esta labor sencilla.

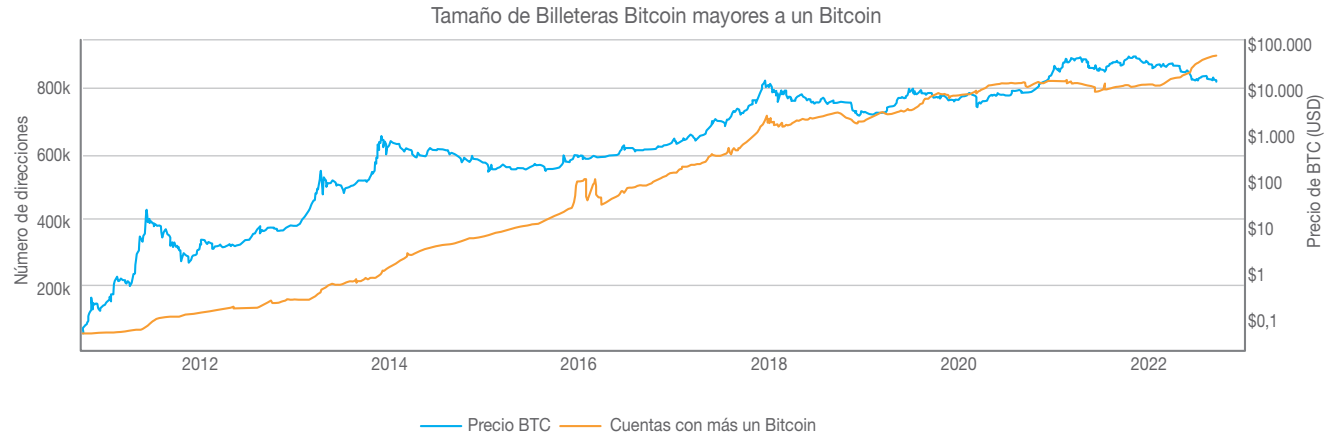
Es importante mencionar la característica dual de las innovaciones tecnológicas: destrucción-creación, D. María lo explica así:

> *Internet, la globalización, la informática y las telecomunicaciones –en el ciberespacio– han permitido el desarrollo de Bitcoin; y como es inherente a la innovación tecnológica la destrucción de aquello a lo que sustituyen, estas innovaciones deben tener un carácter destructivo proporcional a su magnitud. (D. María, 2022, p. 23)*

Bitcoin redefine el concepto del dinero, propiedad privada y vuelve innecesarias las intervenciones de política monetaria de los bancos centrales. Bitcoin y LN derriban los pilares del sistema de pagos tradicional,

[33] Proceso de entrada a Bitcoin: conversión de fiat a bitcoin. Usualmente se utilizan casas de intercambio y el usuario debe proveer su información debido a las políticas de KYC (Know Your Customer).

FIGURA 10: BILLETERAS ASOCIADAS CON MÁS DE 1 BITCOIN



Fuente: Tomado de lookintobitcoin (https://www.lookintobitcoin.com/charts/wallets-greater-than-1-btc/).

así que se puede esperar la llegada de una destrucción-creación de proporciones inimaginables, pero este cataclismo no se dará sin resistencia del sistema que está siendo obsoleto. Como parte de la oposición que Bitcoin ya experimenta se pueden citar las propuestas de *Central Bank Digital Currencies*, regulaciones hostiles y los ataques a la minería como una industria que se desalinea con los estándares ESG.

Cuando bitcoin sea de uso generalizado, no habrá necesidad de realizar un *off-ramp*[34], no existirá el precio en términos fiat y se podrá esperar que todo el sistema financiero mundial esté apoyado por un estándar de Bitcoin. Como resultado, se habrá completado otro proceso de inversión de infraestructura.

La adopción de tecnologías disruptivas emergentes a lo largo del tiempo por nuevos usuarios, tiende a pasar por etapas que se caracterizan por el tipo de interesados en su uso: innovadores, adoptadores tempranos, mayoría inicial, mayoría tardía y los rezagados. Estas fases se logran visualizar con mayor claridad por medio de las curvas S. Inicialmente, la adopción parece ser lenta hasta que ocurre un punto de inflexión en el cual el crecimiento ocurre de manera exponencial, pero en donde surge la interrogante es en que si tal momento crucial se va a dar, cuándo y cuánto durará. En el caso de Bitcoin, si logra penetrar masivamente en el mercado y es adoptado por la mayoría, se dice que se habrá alcanzado la "hiperbitcoinización".

Por el momento, Bitcoin se encuentra en la fase de adoptadores tempranos y cuenta con aproximadamente más de 100 millones de usuarios alrededor del mundo. Interesantemente, a pesar de que al momento de escritura de este ensayo Bitcoin se encuentra en un mercado bajista (en términos fiat), la cantidad de direcciones con un monto mayor a 1 bitcoin ha estado en aumento, como se puede ver en la Figura 10. Este dato nos indica que bitcoin está siendo continuamente acumulado por usuarios minoristas.

Anteriormente fue descrito cómo el proceso de adopción va de la mano con la volatilidad en el precio de bitcoin. El bitcoin que está en las casas de intercambio[35] en manos de los *traders,* es lo que está determinando su precio, sin embargo, la cantidad de bitcoin "cambiando de manos" representa menos del 10% del bitcoin que ha sido minado hasta el día de hoy. Conforme la adopción de bitcoin va aumentando, la cantidad de bitcoin en las casas de intercambio disminuye porque más usuarios lo "mueven"[36] a billeteras en frío. Por lo tanto, podría darse un evento de "*upply shock*"[37] e, incluso, si consideramos el caso hipotético en que todo el bitcoin esté fuera de las casas de intercambio, el precio deja de existir.

[34] Proceso de salida de Bitcoin: conversión de bitcoin a fiat.

[35] bitcoin en las casas de intercambio significa que tales entidades tienen acceso a las llaves criptográficas asociadas a ese bitcoin.

[36] "Mover" bitcoin significa cambiar de dueño, es decir, el control de las llaves criptográficas por parte de un nuevo ente.

[37] Situación en que la demanda ampliamente excede la oferta.

Un aspecto trascendental e innovador de Bitcoin es que se encuentra en un equilibrio Nash. En Teoría de Juegos este tipo de equilibrio es aquel en el cual los jugadores han definido su estrategia y no tienen incentivos para cambiarla dado lo que decidan los otros jugadores. Los mineros son aquellos quienes actuando en su propio beneficio mantienen la red segura, puesto que tienen un incentivo económico para hacerlo, los mineros se benefician más por mantener la red segura que en atacarla, al recibir pagos en bitcoin, estarían actuando en contra de sí mismos y sus ingresos si reducen la confianza en el sistema, ya que han invertido recursos en forma de electricidad y equipo computacional que no podrían recuperar. Satoshi incorporó estos incentivos en la red y manifestó: Los incentivos pueden motivar a los nodos a mantenerse honestos deberían encontrar más rentable jugar de acuerdo con las reglas que erosionar el sistema y la validez de su propia riqueza (Satoshi, 2008, Sección Incentive, párr. 3).

PREDICCIONES

Si ves un relámpago a lo lejos, puedes pronosticar con un alto grado de confianza que se avecina un trueno. Pronosticar las consecuencias de las transiciones megapolíticas implica plazos mucho más largos y conexiones menos seguras, pero es un tipo de ejercicio similar (Davidson y Ress-Mogg, 1999, p. 33).

Predicción 1

Todo aquel bien que sin tener características dinerarias se ha utilizado como depósito de valor (bienes inmuebles, arte y los bonos de deuda soberana), se verán en riesgo de perder este estatus en un mundo en el cual bitcoin haya alcanzado más penetración (D. María, 2022, p. 54).

Estos bienes verán su precio caer y se utilizarán para lo que fueron creados, una casa se comprará para vivir y no como una inversión a largo plazo.

Predicción 2

Mientras se manifiesta un mayor entendimiento de Bitcoin y su naturaleza, veremos el cumplimento de la Ley de Gresham[38] y entraremos en una fase de mucha más acumulación.

Predicción 3

Bitcoin se convierte en el estándar monetario global porque cuenta con las siguientes características:

- La red es neutral, segura, abierta, pública y mundial. El dinero de reserva nunca había contado con la propiedad de neutralidad. Bitcoin no es dinero politizado. El oro funcionó por años como patrón, pero fue susceptible a la confiscación y control, que son rasgos que van en contra de la misma naturaleza de Bitcoin.
- No existe una entidad a cargo.
- Es un protocolo. Bitcoin también es un software que se basa en una serie de reglas que todos los participantes acuerdan seguir.
- La minería de Bitcoin es una industria global.

Predicción 4

Entraremos en un periodo de transición. Los autores de este ensayo presagian un cambio trascendental[39] que ha iniciado con la Era de la Información, y que, con llegada de Bitcoin, se catalizará y acentuará, ya que esta innovación toca fibras muy profundas del individuo como lo es el dinero, porque captura su tiempo y energía; además, la propiedad privada, ya que por primera en la historia existe un bien que no puede ser confiscado. El estado ya no tendrá injerencia sobre él.

Bitcoin ya existe. Bitcoin es una idea que inevitablemente se continuará esparciendo. Bitcoin ya está siendo adoptado y utilizado por millones de personas alrededor del mundo, solo hace falta que la mayoría interiorice el significado de su aparición. Este cambio traerá consigo un periodo de transición con grandes retos, que será cuestionado y resistido por los entes de poder centralizado. Está en el mejor interés de cada individuo comprender la naturaleza disruptiva de Bitcoin mientras continúe en su fase inicial, darle la bienvenida a una nueva etapa en la historia de la humanidad y transmitir este conocimiento a su descendencia.

[38] El dinero "malo" expulsa del mercado el "bueno": existe una tendencia a acumular el dinero bueno y usar como medio de pago el malo.

[39] Con el fin de comprender un periodo de transición que se podría avecinar, se le recomienda al lector la lectura de los siguientes libros: *El Individuo Soberano* por James Dale Davidson y Lord William Rees-mogg, *The Fourth Turning* por Neil Howe y William Strauss, y *The Price of Tomorrow* por Jeff Booth.

CONCLUSIONES

El reconocido economista Hayek indica cuál es la única forma en la que podemos volver a tener un buen dinero, en sus palabras le llama "la desnacionalización del dinero": No creo que volvamos a tener un buen dinero hasta que no se lo quitamos de las manos al gobierno, y como no podemos quitárselo violentamente, todo lo que podemos hacer es mediante alguna manera astuta e indirecta introducir algo que no puedan detener (Anglo Libertarian, 2020, 0m48s).

Satoshi Nakamoto finalmente resuelve, de forma práctica, el problema de ciencia computacional de los Generales Bizantinos, utilizando desarrollos criptográficos que preceden por muchos años a Bitcoin. Existe la creencia de que Nakamoto dejó una receta, no obstante, lo que hizo fue crear la escasez digital, así que las copias de Bitcoin no tienen sentido, por lo que solo puede existir un Bitcoin.

En sus primeros años de vida, Bitcoin alcanza popularidad entre nichos conformados por entusiastas con inclinaciones tecnológicas y computacionales, estos mismos propusieron sistemas que pretendían mejorar las propiedades monetarias de Bitcoin y sus reglas de consenso, a partir de un carácter subjetivo. Los actores individuales pueden decidir bifurcarse de Bitcoin y crear su propia red, pero Bitcoin no sufre de bifurcaciones y, cualquier cambio en sus propiedades fundamentales, da como resultado una entidad nueva inferior que no es Bitcoin.

De esta forma, los proyectos que surgen a partir de Bitcoin nacen a su sombra, con un valor económico de mercado escogido por sus creadores, se mantienen centralizados, incluso con necesidad de mercadeo, representantes, lobbyists y, sobre todo, aparecen en un mundo donde Bitcoin ya existe y no se puede reinventar. Aunque el código pueda ser reproducido y modificado, es imposible replicar los efectos de red y la descentralización obtenida por medio de la Prueba de Trabajo. Como ha sido explicado, la descentralización no depende solamente de cuántos softwares existan distribuidos en diferentes computadoras alrededor del mundo, sino también en la imposibilidad de realizar cambios en él que alteren las reglas de consenso y sean aceptados por los participantes de la red. En otras palabras, estos proyectos no conservan propiedades fundamentales, ya que son susceptibles a decisiones de terceros.

Además, cuando el dinero emerge del mercado con propiedades de dinero duro, provoca que la humanidad decida converger en uno, así como ocurrió con el oro, y este fenómeno lo estamos volviendo a experimentar con Bitcoin. La “magia” de Bitcoin radica en que sus usuarios voluntariamente deciden integrarse a la red y cada nuevo integrante, la fortalece.

Bitcoin redefine el concepto de propiedad privada al ser el primer activo de naturaleza inconfiscable. Esto tiene fuertes implicaciones para la reestructuración social bajo un estándar de Bitcoin. Sin embargo, el proceso de transición puede estar lleno de incertidumbre e ilusión, puesto que durante la etapa de inversión de infraestructura presenciaremos la dualidad entre destrucción y creación. Estamos viviendo un momento histórico porque Bitcoin ya existe. Bitcoin también es una idea y como tal, su tendencia es la propagación. En palabras de Lopp (2022), Bitcoin es una nueva forma de vida: la electricidad es su comida, el Internet es su sistema circulatorio, los mineros son su corazón, los bloques son los latidos, los nodos son las células blancas y los participantes humanos son las neuronas.

REFERENCIAS BIBLIOGRÁFICAS

AC Squared (2022). *Milton Friedman Predicts Bitcoin in 1999* [Video]. https://www.youtube.com/watch?v=leqjwiQidlk

Alden, L. (2022). A Look at the Lightning Network. https://www.lynalden.com/ lightning-network/

Ammous, S. (2018). *The Bitcoin Standard: The Decentralized Alternative to Cen- tral Banking*. Wiley

Anglo Libertarian (2020). *Friedrich Hayek predicting cryptocurrency* [Video]. https://www.youtube.com/watch?v=1tHO3cylCRM.

Antonopoulos, A. M. (2020). *Bitcoin and the coming infrastructure inversion: Remastering series.* [Video]. https://www.youtube.com/watch?v=KXIaILHl7Rg.

Back, A. (2022). *Hash Cash: A Denial of Service Counter-Measure.* http://www.hashcash.org

Begleri (2022). *Systems falln't.* https://bitcoinbarcelona.xyz/Systems-falln-t-bceb9be6dc3e47849d9deeb985b22674.

Bier, J. (2021). *The Blocksize War: The Battle Over Who Controls Bitcoin's Protocol Rules*. Jonathan Bier.

Bourgi, S. (2021). *100 years ago, henry ford proposed 'energy currency' to repla-ce gold*. https://cointelegraph.com/news/100-years-ago-henry-ford-proposed-energy-currency-to-replace-gold.

Chaum, D. (1983). Blind Signatures for Untraceable Payments. *Advances in Cryptology Proceedings of Crypto 82*, pages 199-203.

Dai, W. (2022). B Money. http://www.weidai.com/bmoney.txt.

Davidson, J. D. and Rees-Mogg, L. W. (1999). *The Sovereign Individual: Maste- ring the Transition to the Information Age*. American Media.

Der Gigi (2021). *Bitcoin is Time*. https://dergigi.com/2021/01/14/bitcoin-is- time/

Der Gigi (2022). *Bitcoin is Digital Scarcity*. https://dergigi.com/2022/10/02/bitcoin-is-digital-scarcity/.

Finney, H. (1992). *Hal Finney Essays: Why Remailers I.* http://fennetic.net/irc/finney.org/~hal/why_rem1.html.

Finney, H. (2004). *RPOW: Reusable Proofs of Work*. https://nakamotoinstitute.org/finney/rpow/index.html.

Fleder, M.; Kester, M.S. y Pillai, S. (2015). *Bitcoin Transaction Graph Analy- sis. arXiv.*

Genesis Mining (2019). *Perceptions of Money and Banking in the US 2019 a study*. https://www.genesis-mining.com/moneyandbanking.

Gladstein, A. (2022). *Check Your Financial Privilege: Inside the Global Bitcoin Revolution*. BTC Media, LLC

Gladstein, A. (2022). *Can Fedimints Help Bitcoin Scale to the World?* https://bitcoinmagazine.com/culture/will-fedimints-bring-bitcoin-to-the-world.

Haber, S. y Stornetta, S.W. (1991). How to Time Stamp a Digital Document. *Journal of Cryptology,* pp. 99-111.

Held, D. (2019). *Planting bitcoin - soil (3/4).* https://www.danheld.com/blog/2019/1/6/planting-bitcoinsoil-34

Hofacker, R. (2022). ¿Qué tan ESG es Bitcoin? Juzgando la red, política monetaria e impacto ambiental de Bitcoin desde una perspectiva de ESG. *LOGOS*, pp. 68-83.

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

Jafar, B. (2021). *Bitcoin Is a Speculative Asset, Says Fed Chair.* https://www.financemagnates.com/cryptocurrency/news/bitcoin-is-a-speculative-asset-says-fed-chair/.

Keller, L. (2022). *Cryptocurrency is worthless: ECB Christine Lagar- de*. https://www.yahoo.com/video/cryptocurrency-worthless-ecb-christine-lagarde-004747430.html.

Krugman, P. (1998). *Why most economists' predictions are wrong.* http://web.archive.org/web/19980610100009/www.redherring.com/mag/issue55/economics.html

Lewis, P. (2019). *Bitcoin is Not Too Slow | Gradually, Then Suddenly.* https://nakamotoinstitute.org/mempool/bitcoin-is-not-too-slow/.

Lewis, P. (2020). *Bitcoin Obsoletes All Other Money).* https://nakamotoinstitute.org/mempool/bitcoin-obsoletes-all-other-money/.

Lopp, J. (2022). *Bitcoin is a new form of life*. https://twitter.com/lopp/status/1569574891027943424.

Lunaticoin (2022a). *Podcast: Historia del dinero y Bitcoin con Juan Ramón Rallo* [Video]. https://www.youtube.com/watch?v=K3JobVJU1uI.

Maria, A. D. (2022). *La Filosofía de Bitcoin*. Libros.com

McElroy, D. (2013). *We can't defeat existing system; we must build better one instead*. https://davidmcelroy.org/?p=18991.

Mi Primer Bitcoin (2022). *Mi Primer Bitcoin - Libro de Trabajo*. https://github.com/MiPrimerBitcoin/Diplomado_v3.0.

Nakamoto, S. (2008a). *Bitcoin P2P e-cash paper*. https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

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

Nakamoto, S. (2009). *Bitcoin open source implementation of p2p currency* [Publicación en un foro online]. Mensaje publicado en: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9493.

Nakamoto, S. (2010a). *Re: PC World Article on Bitcoin* [Publicación en un foro online]. Mensaje publicado en: https://bitcointalk.org/index.php?topic=2216.msg29280#msg29280.

Merkle, R.C. (2021). *Daos, Democracy and Governance*. http://merkle.com/papers/DAOdemocracyDraft.pdf

OECD (2022). *Consumer Prices, OECD - Updated: 6 September 2022*. https://www.oecd.org/newsroom/consumer-prices-oecd-updated-6-september-2022.htm

Poon, J. y Dryja, T. (2016). *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. https://lightning.network/docs.

Rochard, P. (2013). *The Bitcoin Central Bank's Perfect Monetary Policy*. https://nakamotoinstitute.org/mempool/the-bitcoin-central-banks-perfect-monetary-policy

Roemmele, B. (2020). *Buckminsterfuller on money based on energy*. https://twitter.com/BrianRoemmele/status/133960499856964403.2

Pysh, P. (2022). *Podcast: Proof of Stake (PoS) Versus Proof of Work (PoW) with Jason Lowery* [Video]. https://www.youtube.com/watch?v=ikPnr23h7qg.

Quirós, J. (2022). *Estos países se podrían convertir en los primeros en eliminar el efectivo*. https://es-us.finanzas.yahoo.com/noticias/paises-eliminar-efectivo-123440194.html.

Rusbridger, A.; MacAskill, E. y Gibson, J. (2015). *Edward Snowden: a right to privacy is the same as freedom of speech*. [Video]. https://www.theguardian.com/us-news/video/2015/may/22/edward-snowden-rights-to-privacy-video.

Saylor, M. (2022). *Money without energy is Credit*. https://twitter.com/saylor/status/1576670456488218624.

Strolight, T. (2021). *Why People Wonder if Bitcoin is Alien Techno- logy*. https://tomerstrolight.medium.com/why-people-wonder-if-bitcoin-is-alien-technologyf9fda5b018b

Szabo, N. (2005). *Bit Gold*. https://nakamotoinstitute.org/bitgold/

Szabo, N. (2008). *Antiques, time, gold, and bit gold*. http://unenumerated.blogspot.com/2005/10/antiques-time-gold-and-bit-gold.html.

United Nations (1948). *Universal Declaration of Human Rights*. https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Voorhees, E. (2021). Asset Volatility. https://twitter.com/ErikVoorhees/status/1397582067647590403.

Véliz, C. (2021). *Privacidad es Poder*. DEBATE.

Yakes, E. (2021). *The 7th Property: Bitcoin and the Monetary Revolution*. Black Poodle Publishing

ANEXO A: CICLO DE VIDA DE UNA TRANSACCIÓN

Ahora que se han expuesto los componentes más relevantes del sistema de Bitcoin, es más fácil de comprender el ciclo de vida de una transacción que será resumido desde un alto nivel: imagine que Alicia desea enviar 1.000 satoshis a Bob. Un bitcoin está subdividido en unidades más pequeñas llamadas satoshis o sats, en honor a Satoshi Nakamoto, 1 bitcoin = 100 millones de satoshis.

Como primer paso, Bob debe proveer a Alicia su dirección de Bitcoin. Las direcciones de bitcoin representan las condiciones para gastar los bitcoin (o satoshis), y como parte de esas condiciones, la más importante es quién puede gastarlas, o sea, quién es el nuevo dueño. También pueden existir condiciones de cuándo pueden ser gastadas las unidades de valor. Luego, la billetera digital[40] de Alicia creará la transacción utilizando la dirección de Bob y la firmará por medio de las llaves criptográficas de la billetera de Alicia. Una transacción está compuesta por entradas *(inputs)* y salidas *(outputs)*, esto quiere decir que hay dinero que entra por parte de quien envía y sale dirigido hacia quien recibe. Como fue explicado anteriormente, bitcoin es dinero en efectivo digital, es un bien al portador, así que podemos imaginar (para fines de comprensión solamente) que el bitcoin que entra y sale son monedas, tal como si fueran monedas de oro.

La creación de la transacción se basa en el concepto de UTXOs *(Unspent Transaction Output)*, que en palabras simples, representa bitcoins que han sido recibidas anteriormente en otra transacción y que no han sido gastadas, o sea, son las salidas no gastadas de transacciones previas. Imaginemos a estas UTXOs como las monedas de oro mencionadas en el párrafo anterior. Continuando con el ejemplo de la transacción de Alicia hacia Bob, imaginemos que la billetera de Alicia encuentra dos UTXOs: una de 900 satoshis y otra de 500 satoshis. O sea, de acuerdo a nuestra analogía, una moneda con denominación de 900 satoshis y otra con denominación de 500 satoshis. Bob espera recibir una moneda con denominación de 1.000 satoshis, por lo tanto, ambas monedas serán consumidas en la transacción: la billetera de Alicia creará una transacción con las monedas de 900 y 500 satoshis como entradas y en la salida habrán otras dos monedas nuevas; una de 1.000 satoshis (para Bob), otra de 350 satoshis como cambio para Alicia y la diferencia de 50 satoshis será el pago para los mineros. Todas las UTXOs en el *blockchain* de Bitcoin están enlazadas entre sí y esto es lo que permite ver su trazabilidad. El *blockchain* de Bitcoin es público y todos los nodos son capaces de encontrar el historial de los UTXOs.

El concepto de UTXOs es vital porque ilustra que Bitcoin no se basa en un sistema de saldos o balances, como el sistema tradicional, aquí radica una gran diferencia porque tendemos a pensar en cuentas con saldos (por ejemplos las cuentas bancarias), pero en el mundo Bitcoin esto es erróneo y lo ideal es traer a la mente la analogía con monedas tangibles, es solo que estas monedas en Bitcoin no existen. Esto es difícil de captar inicialmente, es por esto que a lo largo de este documento se ha hecho hincapié en la noción de Bitcoin como dinero en efectivo de forma digital. Aunque es recomendable relacionar los UTXOs con monedas para fines educativos, no es así cómo funciona Bitcoin realmente. Este es el momento ideal para aclarar dos mitos:

- Las bitcoin no se mueven de billetera a billetera.
- Las bitcoin tampoco se encuentran en las billeteras de los usuarios. Si quisiéramos pensar que las bitcoin residen en un lugar, sería en la red, aunque técnicamente no tienen representación física o digital, por esto no se pueden copiar.

[40] *Software* que calcula y almacena las llaves criptográficas del usuario y se utiliza para firmar las transacciones.

Podemos utilizar otra analogía para que el lector visualice lo que ocurre en una transacción. Imagine que cuando Alicia transfiere 1000 satoshis a Bob, ella está creando una caja transparente, pues toda la red la puede ver y verificar el monto que está adentro, con un candado creado con la dirección de Bitcoin de Bob, de esta forma, solamente Bob puede abrir este candado por medio de su llave privada. Si en un futuro, Bob quiere gastar estas 1.000 satoshis, tendrá que abrir el candado y, con esta acción, Bob le demuestra a la red que él es dueño de estas 1.000 satoshis.

Regresando al ejemplo de Bob y Alicia, una vez creada la transacción, la billetera digital de Alicia se comunicará con el nodo más cercano y compartirá la transacción (información, datos). El nodo la verificará, guardará transitoriamente en el *mempool*[41] y la transmitirá a los otros nodos con los que esté conectado. Dichos nodos, a su vez, verificarán la transacción y la guardarán en su propio mempool. Este proceso continúa hasta que la transacción se haya propagado por la red.

Los mineros tomarán transacciones de su mempool para agruparlas en bloques, entre estas transacciones estará la de Alicia a Bob, e iniciará el proceso de la competencia por proponer el siguiente bloque de la red conocido como el bloque candidato. El primero en resolver el reto matemático, compartirá el bloque, los nodos lo verificarán y lo agregarán a su *blockchain* de ser válido. De esta forma, la transacción de Alicia a Bob es agregada al *blockchain* de Bitcoin (en cada nodo). Seguidamente, vuelve a iniciar otra competencia con nuevas transacciones tomadas del mempool que conformarán el bloque consecutivo, un bloque que se construirá sobre el bloque que contiene la transacción de Alicia.

Cuando la transacción de Alicia hacia Bob se agrega a un bloque del *blockchain*, se dice que tiene una confirmación, si otro bloque se construye sobre el bloque que tiene dicha transacción, entonces tiene dos confirmaciones, y así sucesivamente. Para el caso de Bitcoin, esperar por seis confirmaciones (~1 hora), es lo que se recomienda para concluir que esa transacción es inmutable. Si un atacante desea cambiarla, debe resolver otro reto matemático, en el bloque que incluya la versión alterada de la transacción y en los bloques consecutivos de una forma más rápida que el resto de mineros, ya que los nodos construyen sobre la cadena que contiene mayor prueba de trabajo acumulada. Realizar cambios en el *blockchain* de Bitcoin, requiere comprometer recursos en forma de equipo computacional y electricidad, por lo tanto, económicamente, lo que es rentable, es actuar de acuerdo a los incentivos.

Pensemos en el caso en que Alicia quiere defraudar a Bob, o sea, efectuar un doble gasto: ella crea una transacción de 1.000 satoshis hacia Bob y la comunica a un nodo que llamaremos X y, simultáneamente, también crea otra transacción donde ella se paga a sí misma los mismos 1000 satoshis y comunica esta transacción a un nodo que llameros Y. El nodo X verifica la transacción y la propaga a través de la red, de la misma forma el nodo Y. Como consecuencia existirán dos versiones, supongamos que la mitad de los nodos de la red tendrán en su mempool la versión de la transacción del nodo X y la otra mitad de la red habrá incluido en su mempool la transacción propagada por el nodo Y. También pensemos en el caso de que existan nodos que escucharon las dos transacciones que, al ser contradictorias, van a verificar una y rechazar la otra, por este motivo es que asumimos que las *mempool* tendrán solo una de las dos versiones, en la versión X Alicia le paga a Bob y en la versión Y Alicia se paga a sí misma.

Ahora, entran los mineros en escena. Supongamos que la mitad de los mineros de la red tiene en su mempool la transacción de la versión X y la otra mitad la transacción de la versión Y. Imaginemos que un minero con la versión Y resuelve el reto matemático antes que los demás. Entonces, el bloque sobre el que se construirá la cadena, tiene solo una versión de la transacción, en este caso, el pago de Alicia a sí misma. Por lo tanto, la billetera digital de Bob no le mostrará confirmaciones de la transacción que esperaba recibir.

Consideremos el caso en que un minero con la versión X y otro con la versión Y resuelven "simultáneamente" el reto. En este escenario, existirán dos bloques candidatos propagándose por la red, que

[41] Es una "sala de espera" donde se almacenan temporalmente las transacciones pendientes. Cada nodo tiene su propio mempool. Ver https://mempool.space/

serán contradictorios entre sí. Imaginemos que la mitad de los nodos de la red incluye en su *blockchain* la versión X y la otra mitad de los nodos la versión Y. Esto se conoce como una "bifurcación de consenso", ya que hay dos realidades en la red, dos cadenas con versiones inconsistentes entre sí. Tanto la billetera de Alicia como la de Bob mostrarán una confirmación.

Suponga que un minero que tiene la versión Y del *blockchain* crea un bloque que construye sobre esta cadena y resuelve el reto antes que los demás mineros. Cuando este bloque se propague por la red, los nodos con la versión X concluirán que su *blockchain* es incorrecta, porque ahora existe una cadena con mayor prueba de trabajo construida sobre una versión de la realidad que ellos no poseen. Por lo tanto, desecharán su bloque con la versión X, conocido como bloque huérfano, y adoptarán la cadena construida con la versión Y. La billetera de Alicia mostrará dos confirmaciones y la de Bob cero. Es por lo anterior que se recomienda al usuario esperar aproximadamente seis confirmaciones, porque estas bifurcaciones de consenso pueden ocurrir. Y así es como Nakamoto resuelve el problema del doble gasto sin la necesidad de intermediarios.