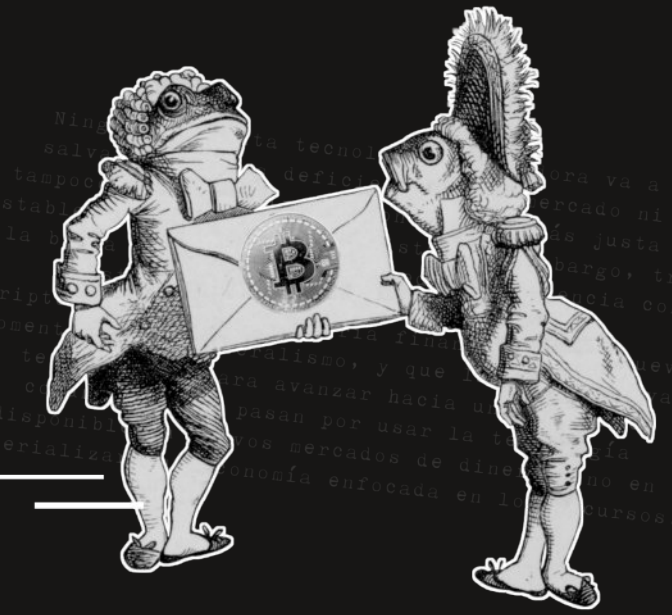
>_

¿Sueñan los liberales con monedas eléctricas?

Una crítica a las ilusiones de las criptomonedas

Colectivo Disonancia

"Ninguna presunta tecnología innovadora va a salvarnos de las deficiencias del mercado ni tampoco un nuevo tipo de moneda hará más justa y estable una economía capitalista. Sin embargo, tras la bruma de las ilusiones queda en evidencia con bastante claridad que la verdad de las criptomonedas es una euforia financiera y un nuevo momento del neoliberalismo, y que las alternativas tecnológicas para avanzar hacia un horizonte comunitario no pasan por usar la tecnología disponible en nuevos mercados de dinero sino en materializar una economía enfocada en los recursos."



colectivo disonancia

¿Sueñan los liberales con monedas eléctricas?

Una crítica a las ilusiones de las criptomonedas

Colectivo Disonancia

"¿Sueñan los liberales con monedas eléctricas? Una crítica a las criptomonedas" es un texto publicado por Colectivo Disonancia el 9 de diciembre de 2021.

Edición y diagramación por Colectivo Disonancia, 2021

colectivodisonancia.net
@cdisonancia

La copia comparte cultura.

Puedes descargar el Fanzine aquí:

https://colectivodisonancia.net/zines

https://cloud.disroot.org/s/ezoecDQFdBdwCzy

https://gitlab.com/cdisonancia/fanzine

Esta obra está bajo
Licencia de Producción de Pares

Descarga este fanzine en:

- https://colectivodisonancia.net/zines
- https://cloud.disroot.org/s/ezoecDQFdBdwCzy
- https://gitlab.com/cdisonancia/zines

O accediendo al enlace en este QR

aquella esperanza que cabía en un dedal
evidentemente no cabe en este sobre
con sucios papeles de tantas manos sucias
que me pagan, el lógico, en cada veintinueve
por tener los libros rubricados al día
y dejar que la vida transcurra,
gotee simplemente
como un aceite rancio.

Sueldo
Mario Benedetti

este siglo, podremos construir ese futuro que, por ahora, es solo el esbozo de una humanidad posible.

con una sociedad comunitaria y libre. Un ejemplo posible es el uso tecnológico para promover una economía centrada en la creación de recursos en vez de tratar de elaborar un nuevo mercado de dinero digital, que es el caso de las criptomonedas. Si una comunidad emplea colectivamente la tecnología, dentro de condiciones de cooperación y de evaluación del impacto ambiental, puede empezar a producir, mantener y planificar sus propios recursos según sus necesidades. No hay nada que impida que el desarrollo tecnológico autónomo no pueda ayudar a contribuir a la producción de alimentos, energías y otros recursos para el bienestar colectivo; humano, animal y ambiental.

En términos digitales tenemos la experiencia de las auténticas redes P2P —o redes de pares—, como el intercambio de archivos por torrent, que puede servir de analogía. Al haber abundancia relativa de los contenidos intercambiados y un acceso colectivo a los medios para producirlos y distribuirlos, las redes de pares son un ejemplo de un intercambio gratuito basado en una propiedad colectiva, en la cual la motivación de intercambio es simplemente la contribución generosa a las redes de cooperación. Por ende, la construcción de un horizonte de autonomía tecnológica es una forma de pensar cómo enfrentar las relaciones de dominación presentes en la DST por medio del uso de la capacidad técnica para promover una economía enfocada en los recursos. Ahora bien, el problema nunca ha sido la falta de estas herramientas, sino la voluntad y fuerza política de los sectores dominantes que impiden ese futuro. Para evitar la capacidad emancipadora que contiene la tecnología al servicio de la comunidad, el capital y la tecnocracia no tienen límite para su violencia que llaman "paz y orden social", por lo que, si queremos hacer posible ese futuro, debemos estar dispuestos a enfrentar esa lucha. Si reunimos la fuerza y destreza suficientes para ganarles, atravesando los complejos problemas a los que estamos abocados en

Índice

indicador indiscutible de poder, al punto de que quien controla la más alta tecnología puede obligar al resto de la sociedad a reorganizarse económica y políticamente en beneficio propio. La historia del capital y la tecnología industrial, por ejemplo, muestra cómo los sectores o clases dominantes de la sociedad moderna, poseedores de dicha tecnología, crearon condiciones ventajosas para extender su dominación y explotación por el mundo, redefiniendo la División Social del Trabajo —DST— a nivel global. La industrialización creó nuevas formas de trabajo, producción, distribución y consumo que consolidaron el poder del capitalismo. En ese sentido, el que existan clases sociales depende, de hecho, de que un sector social controle los medios técnicos con los cuales los demás deben trabajar y mantener sus vidas.

Por consiguiente, para elaborar una crítica radical al lugar que tiene la tecnología en las posibles alternativas económicas, tiene sentido pensar el problema de quién controla la DST. De hecho, no es de extrañar que para autores del pensamiento radical clásico, como Karl Marx o Piotr Kropotkin, el problema político de fondo en la dominación capitalista fuera la DST[38]. Por ende, avanzar en un horizonte de autonomía tecnológica en el cual las comunidades toman control de la tecnología para ponerla al servicio de las necesidades e intereses colectivos contribuye a socavar el poder con el cual el capitalismo puede obtener ventaja de la producción social y de la DST. Esto no se trata, desde luego, de eliminar la especialización del trabajo sino de que colectivamente podamos tomar control tecnológico de la producción para poder decidir sobre nuevas formas de trabajo no salarial, la duración de la jornada laboral, el impacto ambiental y el tipo de tecnologías compatibles

[38] En ambos pensadores, se puede encontrar una reflexión y crítica a la División Social del Trabajo en "La ideología alemana", en el caso de Marx, y en "Campos, fábricas y talleres, en Kropotkin.

lado, permitir criticar qué hay en común en el carácter virtual o abstracto del dinero en general y, por otro lado, pensar qué lugar puede ocupar la tecnología en esa crítica. ¿Estamos obligados a reproducir mercados artificiales con la tecnología cuando intentamos usarla para transformaciones económicas?

Es curioso que uno de los fundadores del liberalismo económico, Adam Smith, pensara que el origen de todo valor es el trabajo y no el mero intercambio comercial: "El trabajo fue el primer precio, la moneda de compra primitiva que se pagó por todas las cosas. Toda la riqueza del mundo fue comprada al principio no con oro ni con plata sino con trabajo"[37]. Si bien el intercambio económico puede generar cambios de precio sobre los cuales obtener ganancias por la ventaja de vender barato y comprar caro; la economía de una sociedad se sostiene por lo que es capaz de producir el trabajo, principalmente al generar recursos materiales y los servicios básicos para el funcionamiento social, es decir, el Valor del Trabajo Social. Siguiendo a Smith, el dinero no es más que una forma de hacer dinámico el intercambio económico debido a la progresiva división del trabajo[37], la condición en la cual se crean distintas labores, cada vez más especializadas, para mantener la producción social. En otras palabras, en la medida en que los trabajos en la sociedad se especializan cada vez más, la única forma en la que los integrantes de la sociedad consiguen lo que necesitan es usar un patrón común para intercambiar el producto de los distintos trabajos especializados. Entonces, el punto crítico para el Poder no es necesariamente controlar el tipo de dinero sino controlar la división del trabajo, es decir, controlar los medios técnicos que hacen posible y determinan la especialización del trabajo y la producción.

El desarrollo tecnológico y su control siempre ha sido un

[37] Adam Smith, "La Riqueza de las naciones" (1776).

Una breve consideración antes de una larga explicación

Las esperanzas contenidas en la idea de que las criptomonedas revolucionarán la economía —que en el fondo es un proyecto propiamente neoliberal— se sostienen en la premisa de que el tipo de procedimiento o de tecnología de intercambio, como el dinero, es el centro de la actividad económica o, al menos, uno de sus elementos decisivos. Desde esta perspectiva tendría sentido emplear nuestros esfuerzos en diseñar y crear nuevas tecnologías que mejoren este intercambio. Sin embargo, como se ha visto, esto no evita que se reproduzcan las lógicas del mercado y la concentración de capitales existentes en las economías no digitales. Además, el uso de alta tecnología en estos casos solo agrega una nueva capa de abstracción al ya abstracto sistema monetario. En este sentido, la crítica a las criptomonedas muestra que éstas no tienen un grado de virtualidad distinto a la de cualquier tipo de dinero, digital o no, razón por la cual las características del mercado capitalista se reproducen y mantienen plenamente en estas nuevas divisas. Esta reflexión debiese poder abrir dos perspectivas, por un

Hasta hace no mucho, la expresión "cripto" hacía directa alusión a la criptografía, la técnica matemática que permite ocultar el contenido de los mensajes y que es la base para enfrentar la vigilancia digital. Actualmente, con el aumento de la popularidad de las criptomonedas y su difusa promesa de transformación radical de la economía, lo "cripto" pasó a convertirse en el sinónimo casi exclusivo de estas tecnologías monetarias y su presunta revolución. Al parecer, como anuncian los emisarios de esta gran transformación, se habría descubierto una solución técnica para enfrentar los problemas centrales que aquejan a la economía. Esta solución sería poner en circulación una moneda digital descentralizada, dando por hecho que los problemas centrales de la economía derivarían del tipo de moneda en circulación y la tecnología para crearla.

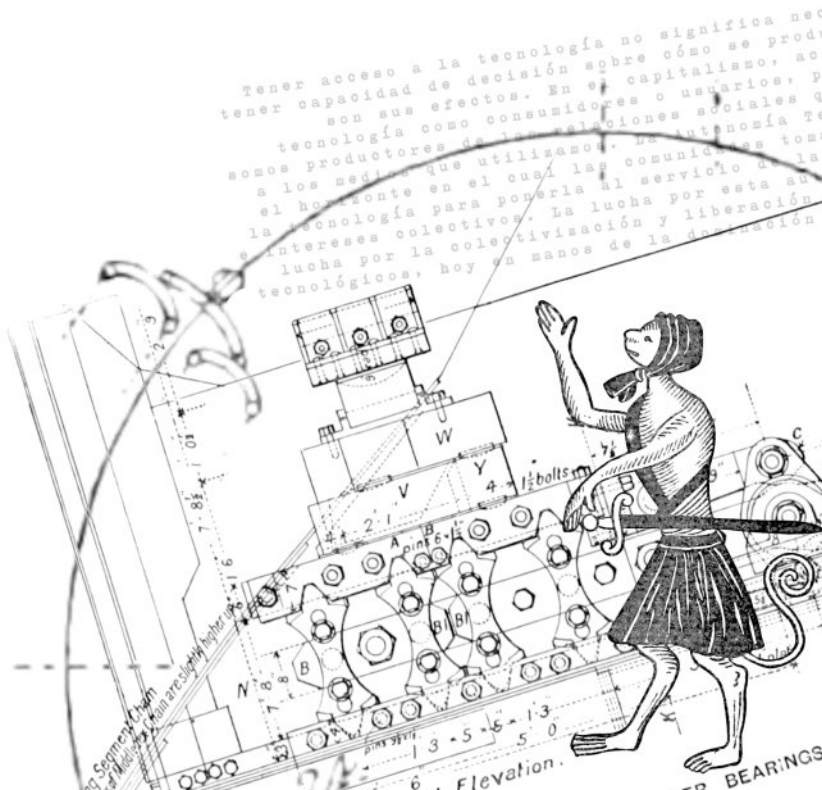
Debido a la apertura de los bancos al uso de las criptomonedas, la utilización legal del Bitcoin por parte del Estado de El Salvador y el creciente interés sobre estas divisas, incluso en sectores

progresistas, se hace relevante abordar la tecnología que sustenta esta iniciativa económica para considerar si acaso son un aporte a la construcción de una sociedad más libre y descentralizada. Luego de analizar el funcionamiento y las propuestas asociadas a estas soluciones económicas no es difícil advertir que las criptomonedas son en gran parte ilusiones. Ninguna presunta tecnología innovadora va a salvarnos de las deficiencias del mercado ni tampoco un nuevo tipo de moneda hará más justa y estable una economía capitalista. Sin embargo, tras la bruma de las ilusiones queda en evidencia con bastante claridad que la verdad de las criptomonedas es una euforia financiera y un nuevo momento del neoliberalismo, y que las alternativas tecnológicas para avanzar hacia un horizonte comunitario no pasa por usar la tecnología disponible en nuevos mercados de dinero sino en materializar una economía enfocada en los recursos.

Por desgracia, como las ilusiones de las criptomonedas tienen un impacto mucho mayor que el real el aporte económico y tecnológico, se requiere profundizar detalladamente en los sueños eléctricos de este liberalismo tecnológico, lo que nos ha obligado a realizar un texto extenso que, dependiendo de los conocimientos del lector, permite saltarse algunas secciones. La primera parte es una descripción de la propuesta del Bitcoin y el impacto de las criptomonedas. La segunda es una crítica a las ilusiones de las criptomonedas a partir de 4 contradicciones que poseen. Y la tercera y cuarta parte son los análisis políticos y tecnológicos sobre la efectividad de las criptomonedas y el esbozo de una alternativa técnica comunitaria y autónoma.

Esbozo de una alternativa:

Autonomía tecnológica y una economía de recursoso



¡Un liberal salvaje ha aparecido!

Satoshi y el misterio de las monedas eléctricas

mostrado anteriormente, las iniciativas de mercado tienden a la concentración de capitales y a desarrollar contradicciones respecto de sus propuestas, por lo que los postulados neoliberales en realidad tienden a beneficiar a algunas corporaciones y a crear Estados fuertes y comprometidos con precarizar la organización laboral y social. Sin embargo, por muy delirante que parezca, y a pesar de sus evidentes contradicciones, las criptomonedas podrían materializar este anhelo de Hayek, en el que estaríamos compitiendo por acertar cuál es la moneda de turno más rentable para nuestra subsistencia, intentando sobrevivir a la proliferación de burbujas en medio de un cementerio de tulipanes. En resumen, dejando de lado las ilusiones, las criptomonedas sí tienen un futuro posible de la mano de políticas neoliberales y de las eventuales burbujas financieras que anuncian, bajo nuevos nombres, las torpezas del pasado. La verdad de las criptomonedas es el neoliberalismo de alta tecnología. En cambio, para una lucha anticapitalista, lo que nos concierne es pensar qué alternativas tecnológicas podrían contribuir a transformaciones económicas que no impliquen crear un mercado ficticio de dinero.

[36] El problema no consiste en usar o no critpomonedas sino en qué proyectos se utilizan y cuán significativo resulta para un horizonte de transformación radical y cómo se asume la contradicción con el neoliberalismo.

Por ejemplo, la cooperativa Faircoop cuenta con una criptomoneda propia, el faircoin, como parte de una iniciativa para la construcción un mercado de cooperación global. Sin embargo, la posible fuerza de su proyecto dependerá realmente de cómo funcione la cooperativa y no de lo innovador de su moneda, que no deja de estar dentro de los márgenes de Hayek.

En cuanto a ejemplos sobre financiamiento, proyectos importantes como Wikileaks o Sci-hub dependen de las donaciones en criptomonedas debido a la persecución legal de sus cuentas bancarias convencionales. En esos casos mientras no se consoliden otras redes de apoyo de trabajo y financiamiento, ese sistema se hace necesario, produciendo como defecto el depender de la volatilidad de estos mercados.

los principales exponentes de la escuela austriaca de economía y del pensamiento neoliberal promovido por la sociedad Mont Pelerin[26]. Hayek, buscando una solución de mercado a la inflación y a la depreciación del dinero *fiat* por parte de los bancos centrales, postuló, en 1976, que era preferible quitar el monopolio del dinero al Estado y dejar que la banca u otras iniciativas privadas crearan su propio dinero y lo pusiera en circulación[35]. El objetivo es que exista un mercado de dinero en el que todas las posibles formas de monedas o divisas compitan entre sí, sin regulación pública y asumiendo el riesgo de su volatilidad. Como proponen los liberales extremos, para sorpresa de nadie, este sistema sería viable porque la competencia del mercado regularía estas monedas. Si se analiza detenidamente, aunque no se lo propongan, el contenido político de todas las criptomonedas y sus partidarios es intentar construir este excéntrico proyecto neoliberal y, de un modo subyacente, estas premisas ya están en la publicación original de Nakamoto. Incluso los proyectos cooperativos basados en criptomonedas no hacen sino reforzar el mercado de monedas en competencia entre sí dado que una iniciativa financiera local y solidaria, pero integrada al mercado global, es perfectamente administrable por las grandes concentraciones de capital. Las iniciativas que busquen desarrollar propuestas comunitarias basadas en criptomonedas o que se financien por medio de ellas deben asumir esta contradicción y considerar cuánto afecta en sus horizontes de transformación social; sin esto, simplemente se está jugando dentro de los márgenes controlados por el neoliberalismo[36].

Desde luego, la propuesta de Hayek es solo el anhelo de un ultraliberal soñando con monedas eléctricas en un inexistente mercado descentralizado sin regulación del Estado. Como se ha

[35] Friedrich Hayek, "La desnacionalización del dinero" (1976).

El Bitcoin, la criptomoneda originaria, se dio a conocer en 2008 con la publicación "Bitcoin: un sistema de [dinero] efectivo electrónico entre pares" de Satoshi Nakamoto[1], seudónimo de la persona o grupo que desarrolló y publicó el código sobre el cual empezó a operar la red. El objetivo de la publicación era proponer y crear un sistema de pagos que no necesitara de ninguna verificación ni confianza externa a la red para garantizar el valor de la moneda y la seguridad de la transacción. En teoría, consiste en un sistema de pagos en el que las personas pueden comprar y vender entre sí sin intermediarios; ni de bancos ni de Estados que vigilen y controlen la transacción: el soñado "libre mercado". Para que un sistema así sea viable debe tener dos características centrales: por un lado, una red segura y funcional, y por otro, la confianza de los usuarios para que le atribuyan valor a la moneda digital.

[1] Satoshi Nakamoto. Bitcoin: un sistema de efectivo electrónico entre pares, (2008). Disponible en Español: https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf e Inglés: https://bitcoin.org/bitcoin.pdf

Explicado de manera simple, la primera característica es desarrollada en la publicación de Nakamoto y consiste en proponer un sistema en donde usuarios especiales, bajo ciertas reglas, verifiquen el correcto funcionamiento de la red y sus transacciones. Estos usuarios especiales llamados "mineros" compiten entre sí para resolver un problema matemático propuesto por la red Bitcoin. Los usuarios que más recursos inviertan —en energía y capacidad de cómputo de sus máquinas— tienen más probabilidad de éxito en resolver rápidamente el problema. Cuando un minero resuelve el puzzle matemático, valida la transacción de bitcoins y la registra en un libro de contabilidad del cual todos en la red tienen una copia de la versión más actualizada. Realizado esto, se repite el ciclo de competencia y verificación. El incentivo de los "mineros" para realizar esta labor, además del cobro de una comisión por validación, es que, con cierta frecuencia y probabilidad, se les premia con la aparición de un nuevo bitcoin para su propiedad. Este premio es cada vez más difícil de conseguir porque el diseño de la red hace que con el aumento de su tamaño la competencia sea más difícil, y con el paso del tiempo la frecuencia de creación de nuevas monedas es menor. Este sistema es llamado "Prueba de Trabajo" —PoW por su sigla en inglés— en el sentido de que los mineros que mejor compitan gastando recursos tiene más probabilidad de demostrar "su trabajo" hacia la red y por ello de merecer la recompensa. El objetivo práctico de este intrincado sistema es que las transacciones no dependan de la "confianza" que tienen los usuarios entre sí sino de los algoritmos matemáticos que rigen las reglas que deben cumplir los mineros. Es decir, no dependería de arbitrariedades humanas.

El libro de contabilidad en donde se registra la serie de transacciones se denomina blockchain o cadena de bloques por la lógica serial con que se almacena y verifica cada transacción. La información de esta cadena es pública por lo que toda la red puede

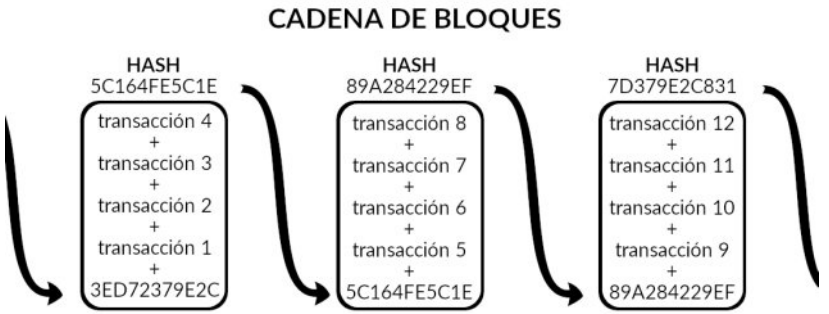
Bitcoin funciona, hasta ahora, como tulipanes digitales que elevan su precio debido a la promesa de un valor aún mayor. No se trata ni del nuevo oro —el que al menos tiene propiedades metálicas inherentes— ni de una revolución tecnológica, como ya se ha visto. Su volatilidad diaria no lo hace confiable para mantener una economía estable, por lo que la recepción cada vez mayor que tiene depende en gran medida de su burbuja. Habrá que ver si la especulación desaparece antes de que se emitan todos los Bitcoin disponibles —los 21 millones— y descubramos qué pasará cuando los mineros pierdan uno de sus principales incentivos: conseguir nuevas monedas. Sin embargo, como muestra la historia de la euforia financiera, no sería de extrañar que, una vez desinflada la burbuja, vuelvan a aparecer las mismas promesas omitiendo el pasado. Ahora bien, este frenesí financiero ha promovido el desarrollo del blockchain y la creación de miles de criptomonedas distintas, pero no necesariamente condena estos desarrollos al destino de la burbuja especulativa. El dinero digital es ya una realidad desde hace décadas con la digitalización de las cuentas bancarias y la progresiva incorporación de cadenas de bloques y criptomonedas al sistema bancario[17]. Puede ocurrir que la desaparición de la burbuja del Bitcoin produzca desconfianza en las tecnologías similares, pero ese no es el único escenario posible. Quizás, lo que necesitan las criptomonedas y el solucionismo del blockchain para consolidarse en un neoliberalismo 2.0 es precisamente que se acabe la especulación de la moneda de Nakamoto y alcanzar así una cierta nivelación de precios que convenza a la mayoría de usar estas divisas en un mercado cotidiano.

Pensando en este futuro, si se extiende su uso y sobreviven a la burbuja del Bitcoin, no es de extrañar que las criptomonedas empiecen a hacer real uno de los sueños de Friedrich Hayek, uno de

ni en propiedades convencionales, sino que en nada menos que tulipanes[34]. Los tulipanes llegaron a Europa occidental en el siglo XVI, pero con el tiempo su valoración empezó a incrementarse, generando un particular frenesí en Holanda, en la década de 1630. El aumento progresivo de precio hizo crecer las expectativas sobre el valor de estas flores y, con ello, aumentar aún más su precio. En 1636, un bulbo de tulipán llegó a equivaler a "un carruaje nuevo de dos caballos tordos y un arnés completo" y su venta ya contaba con un mercado especializado en la Bolsa de Valores de Amsterdam[34]. Como en toda euforia especulativa, muchos se hicieron ricos súbitamente, lo que hizo pensar a la mayoría de los holandeses, y a inversores de distintos lugares de Europa, que los tulipanes marcaban el inicio de una historia de riqueza en permanente crecimiento. No obstante, en 1637, como en todo proceso especulativo, algunos empezaron a vender masivamente sus flores, lo que desencadenó la histeria por la venta y, en consecuencia, el derrumbe del mercado, haciendo quebrar a todos quienes habían mantenido su riqueza invertida en estos peculiares tulipanes[34]. A pesar de lo ridículo que resulta hoy pensar en las motivaciones que llevaron a una sociedad a elevar el precio de unas flores al punto de hacer quebrar su economía, no es una situación tan lejana a lo que ocurre cuando le atribuimos valor al papel moneda o a unos cuantos bits almacenados en una cadena de bloques. La economía capitalista esconde en su fundamento el germen de la locura financiera que se repite cíclicamente con las mismas características: genios financieros que incitan a los demás a hacerse ricos con un nuevo procedimiento que cambiará toda la economía. Y con la misma rapidez con que los precios crecen, desaparece también la frágil memoria financiera de estos acontecimientos una vez pasada la euforia.

[34] John Kenneth Galbraith, "Breve historia de la euforia financiera" (1994).

ver cuántas transacciones se han realizado y con qué monto. A pesar de que esta cadena de registros es pública, en principio, no puede ser alterada arbitrariamente, ya que cada vez que se registra una transacción, automáticamente adquiere una firma criptográfica[2], como si se tratase de una huella dactilar que la hace única. Cada registro de una nueva transacción debe partir de un cálculo de la firma o huella de la transacción anterior, por lo que alterar un solo bloque obligaría a los eventuales mineros maliciosos a tener que modificar permanentemente todo el libro de registro posterior, situación que es muy difícil de mantener en el tiempo. En otras palabras, si un minero falsifica una transacción para su beneficio, se crea un bloque con una firma o huella distinta a la verificada por los demás mineros. Esto produce que entren en competencia dos versiones distintas del libro de contabilidad, uno con el dato alterado y otro con el correcto. Para mantener la falsificación, el minero malicioso tendrá que competir contra la capacidad de cálculo de todos los demás para resolver el siguiente problema antes que ellos, lo que es prácticamente imposible.



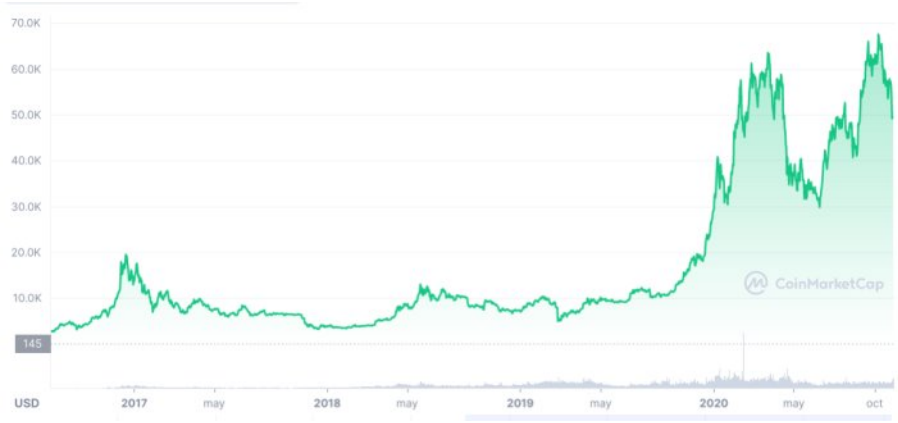
El “Hash” o firma digital es la huella criptográfica que valida cada bloque u hoja del registro. Cada nueva firma incluye en su cálculo la firma anterior.

[2] El cifrado o encriptación consiste en la capacidad de almacenar o comunicar alguna información dentro de un código solo legible por el destinatario o por el programa que utilicemos. Para conocer una historia del cifrado y sus usos puede revisarse Introducción a la criptografía digital: https://colectivodisonancia.net/herramientas/introduccion-a-la-criptografia-digital/

Por consiguiente, al final, la red de la mayoría de los mineros verificará la cadena correcta y más larga, descartando el libro alterado y haciendo perder al minero malicioso sus ganancias. Esto quiere decir que la red ha logrado el "consenso" que se sostiene en la prueba de trabajo y en su capacidad descentralizada de validación.

La segunda característica, el valor de la moneda, depende principalmente de tres factores. Primero, la red Bitcoin solo emitirá un número limitado de monedas: 21 millones —ya se ha emitido más de 18 millones—. Por esto la moneda tenderá a la escasez por ser un elemento finito y, con ello, se espera que aumente su valor. Segundo, dado que hay una escasez progresiva de la moneda y expectativa de aumento de valor, la competencia de los mineros, que es cada vez más difícil y costosa, implica también que la ganancia tiene cada vez más valor por su escasez, lo que aumenta el incentivo en la minería y en la seguridad de la red. Y tercero, la confianza o expectativa de valor —o valor futuro— que las personas puedan darle a la moneda, si consideran verosímil que el Bitcoin pueda usarse en una economía cotidiana; es el sustento final de todo su precio.

De hecho, si se observa el "valor" histórico del Bitcoin hasta ahora, comparado con el dólar, se puede observar que sí ha



Precio histórico de Bitcoin en dólares. Consultado el 4 de dic. De 2021: https://coinmarketcap.com/es/currencies/bitcoin/

Una vez descartadas las ilusiones, ¿qué queda de las criptomonedas? Al observar la fascinación de la mayoría de los entusiastas de estas divisas digitales, principalmente en Bitcoin, se nota que su motivación no es realmente transformar la economía ni establecer un sistema de validación descentralizado; sino que simplemente los motiva la esperanza de hacerse millonarios por una vía fácil. Ha habido casos de este tipo y, como ya se mencionó, efectivamente es posible aprovechar la variación de precios para comprar barato y vender caro[5]. Lo que habría que considerar es si este modelo de actividad económica permite realmente mantener una economía estable o si es simplemente una burbuja financiera que sirve a algunos inversores y se encamina hacia el deterioro económico del resto. Para esto, existe un antecedente histórico ejemplar que es interesante revisar.

En el siglo XVII se vivió un momento espectacular en la historia humana: el primer entusiasmo moderno por una especulación financiera que de hecho no estuvo centrada en dinero

acumulado su "precio" a largo plazo, independiente de su volatilidad diaria. Del mismo modo, a pesar del incremento en la dificultad de obtener recompensas en el minado, la red sigue funcionando porque siguen habiendo usuarios dispuestos a invertir recursos en esa competencia.

A simple vista, la red de Nakamoto va tomando forma, lo que sirve de aliciente para quienes postulan que el Bitcoin muestra la posibilidad efectiva de una moneda descentralizada, sin bancos ni Estados. Este mismo estímulo ha sido acompañado de una vasta proliferación de criptomonedas de diverso tipo —ya existen más de 10.000 distintas[3]— y de nuevas aplicaciones para la cadena de bloques, como la existencia de contratos programables y descentralizados que son verificados por la red y no por los "firmantes"[4], sugiriendo, al parecer, la consolidación de una nueva economía autónoma. Ahora bien, las promesas de las criptomonedas dependen exclusivamente de la premisa de que la creación y circulación de dinero es un agente central y decisivo en la economía, así como también de creer que una nueva aplicación tecnológica es suficiente para hacer las transformaciones que se prometen. No obstante, el mercado capitalista es una institución mucho más compleja que un simple sueño liberal y las criptomonedas, vistas desde cerca, muestran sus contradictorias ilusiones y las limitadas opciones que tienen de ser una real alternativa económica y tecnológica.

[3] https://forbes.co/2021/06/23/economia-y-finanzas/tokens-criptoactivos-y-criptomonedas-que-son-y-cuales-son-sus-diferencias/

[4] Smart contract o contratos inteligentes en Ethereum https://ethereum.org/es/developers/docs/smart-contracts/

Un cementerio de tulipanes:

Jugando a las burbujas con el neoliberalismo

Excepto el Capital, todo el dinero es virtual:

4 contradicciones en las criptomonedas

complejo es. Simplemente como en el fondo desprecian la complejidad de las interacciones humanas, asumen como evidente que una nueva aplicación de cadenas de bloques es preferible a cualquier alternativa existente. En suma, las cadenas de bloques son una tecnología deseosa de encontrar, o inventar, problemas que resolver con simples soluciones técnicas: la sociedad sería una máquina que requiere solo mejores algoritmos para aumentar su precisión.

* * *

Los principales argumentos en defensa de la "revolución" de las criptomonedas poseen, como se ha visto, suficientes contradicciones para evidenciar que, al final, se tratan solo de ilusiones. Se esperaba que estas monedas digitales fueran una gran transformación económica pero se ha visto que solo son una forma de transacción económica que no va más allá de un alto consumo eléctrico, de una progresiva centralización, una sencilla integración con bancos y Estados y un solucionismo tecnológico con pretensiones de innovación. No suponen una alternativa ni más radical ni mejor al dinero convencional y eso se debe a que, si lo consideramos detenidamente, todo el dinero es virtual; las criptomonedas no son sustancialmente distintas al valor imaginado que tiene el dinero. Ninguna moneda tiene valor intrínseco sino que su valor es una virtualidad que depende de su contexto social. En nuestro caso, en una sociedad capitalista, son las relaciones de poder del Mercado, como institución, las que le dan contenido y sentido a los enigmáticos símbolos que identificamos como dinero. Es el Capital y no el papel moneda o los bits el que determina el carácter centralizado y catastrófico de nuestra economía. Solo nos queda pensar, más allá de las ilusiones, qué hay de real en las criptomonedas y qué hacer frente a este tipo de tecnología.

productores no siempre pueden rechazar o negociar si tienen como única alternativa vender su trabajo a estas corporaciones[32]. Del mismo modo, la cadena de bloques podría facilitar el mantener registros descentralizados de vigilancia o crédito social, sin que eso contribuya a ningún "gobierno abierto". En una situación de explotación y opresión, más tecnología no es indicio directo de mayor emancipación, sino que puede contribuir a hacer más eficiente una situación de dominación. Incluso en el caso de que existan legítimos intercambios sociales y formas públicas de administración que requieran técnicas de validación, existen tecnologías tan antiguas como internet que aún siguen vigentes y en permanente perfeccionamiento, como las redes P2P al estilo torrent o el clásico cifrado de llaves que, además de su utilidad, se sostienen en última instancia en la confianza de las redes humanas que las mantienen funcionando. Sin embargo, como no tienen un nombre grandilocuente o alguna artificiosa agencia de marketing creando expectativas, pasan desapercibidas como innovación.

En el fondo, la curiosa fiebre innovadora en la que una tecnología como el blockchain sería la solución a nuestros principales problemas es lo que Evgeny Morozov llama "solucionismo tecnológico", a saber, la creencia en que para cada problema social y político existe una solución tecnológica simple, dando por hecho que el problema inicial era la ausencia de esa tecnología[33]. Los partidarios de las criptomonedas en general y los del blockchain en particular confían en que siempre es preferible una solución que entregue la validación y seguridad a un algoritmo antes de evaluar siquiera la raíz del problema que enfrentan o cuán

[32] Grupo ETC. La insostenibilidad de la agricultura 4.0 (2021) https://www.etcgroup.org/sites/www.etcgroup.org/files/files/la_insostenible_agricultura_4.0_rev_2021.pdf

[33] Evgeny Morozov, "La locura del solucionismo tecnológico" (2013).

Entre algunas de las promesas que circulan en torno a las criptomonedas, y que sostienen los partidarios más fervientes, es el hecho de que pueden ser un mecanismo para enriquecerse rápidamente debido a la expectativa de crecimiento de su valor, por lo que si se compra a un precio bajo y luego se vende en el momento en que aumenta su precio, habría una ganancia asegurada. De hecho, esto es real, ya que ha habido casos, incluso anecdóticos, en donde tempranos compradores de Bitcoin han terminado siendo millonarios[5]. Sin embargo, esto no es una propiedad exclusiva de las criptomonedas; en cualquier mercado con ciertos niveles de capacidad especulativa se puede comprar barato y vender caro. Más allá de este sueño acelerado de tecno-emprendimiento, lo que habría que evaluar como aporte de las criptomonedas son las propuestas de

[5] Es el caso de Kristoffer Koch, quien compró 5000 bitcoins el 2009 a US$22 sin muchas expectativas, pero al enterarse del aumento de su "valor" en 2013 descubrió que sus criptomonedas equivalían US$850.000: https://www.bbc.com/mundo/ultimas_noticias/2013/10/131029_ultnot_noruega_bitcoins_millonario_lav

alternativas a la economía actual. Al respecto hemos escuchado, incluso hasta el cansancio, que estas divisas digitales traerían un nuevo mercado más descentralizado, independiente de bancos y Estados, sumado a una gran transformación tecnológica de la mano de la innovación que supone su sistema de cadena de bloques; pero ni la novedad ni las estrategias de marketing pueden ocultar las notorias contradicciones que tienen estas ilusiones al ser revisadas.

Autovalidación y el problema del consumo eléctrico

Las criptomonedas que usan la Prueba de Trabajo, como Bitcoin, necesitan este procedimiento para garantizar un sistema de validación descentralizado y seguro. A su vez, esta validación realizada de manera autónoma por la red es requerida para no depender de terceros e instituciones que verifiquen las transacciones, es decir, que la red misma llegue a consenso sin intermediarios externos. El problema notorio con la Prueba de Trabajo es que mantiene una competencia entre usuarios que requiere consumir progresivamente cada vez más recursos eléctricos para mantener la red en funcionamiento. Según la estimación de un estudio de la Universidad de Cambridge[6], Bitcoin consume anualmente 116,78TW hora al año. Si fuese un país, estaría en el puesto 32 de los que más consumen en el mundo, encontrándose por encima de los Países Bajos o Chile, y consumiendo más del doble que Israel. Este enorme costo de mantenimiento de la red resulta más grave aún considerando la crisis climática y energética que enfrentamos actualmente[7], en donde lo que necesitamos, de haber posibles

[6] Consumo eléctrico de Bitcoin, consultado el 4 de diciembre de 2021: https://cbeci.org/index Comparación: https://cbeci.org/index/comparisons

[7] El Panel Intergubernamental del Cambio Climático (IPCC) señaló que el calentamiento global, ocasionado por las emisiones acumuladas de CO2, generará daños y efectos catastróficos irreversibles si la temperatura global supera los 1,5°C por sobre el periodo

lo mantiene. Por ende, las soluciones tecnológicas basadas en blockchain suelen ser peores que otras alternativas existentes ya que, partiendo de una premisa equivocada, por un lado, intentan desconocer el valor de la confianza social para mantener los distintos sistemas funcionando y, en segundo lugar, aumentan el riesgo de dichos sistemas puesto que solo están respaldados en aspectos técnicos falibles[30]. Un sistema confiable y seguro no es el que use más criptografía, sino el que posea mejor capacidad social de reorganización y reacción en escenarios adversos, y para eso se requiere de una comunidad humana validando sus acciones con distintos grados de confianza mutua. El blockchain no reemplaza la confianza humana que hace posible la validez de nuestras acciones e intercambios, por lo cual es simplemente una falsa innovación y una tecnología prescindible.

Ahora bien, independientemente del riesgo implicado y de la incoherencia del blockchain respecto de sus premisas, habría que preguntarse si sus diversas aplicaciones siguen siendo útiles o innovadoras. En el caso de los NFT, ¿tiene algún aporte cobrar por el certificado de la autoría de una obra digital? Solo como una excentricidad acaso atendible, como ocurre con la especulación en las galerías de arte, pero en ningún caso se puede hablar de innovación. En cuanto a las demás aplicaciones de las cadenas de bloques, como los contratos inteligentes y el "Gobierno abierto", omiten que los problemas económicos y políticos no tienen que ver principalmente con tener o no un registro inmutable de acciones y transacciones, sino con el poder que tiene el capital y el Estado y que, por muchas buenas voluntades existentes, las soluciones tecnológicas no son una respuesta única ni suficiente para abordar el problema del poder. Varias empresas ya están soñando con digitalizar la cadena de cultivo y distribución de productos agrícolas utilizando blockchain, imponiendo contratos inteligentes que los

resolver la coordinación y comunicación de una red descentralizada; sin la subjetividad humana de por medio se solucionaría el problema. No obstante, al igual que en las contradicciones ya revisadas, esta innovación es más retórica que real. Para Bruce Schneier, un reconocido criptógrafo dedicado a la seguridad digital, el blockchain es en realidad una tecnología bastante inútil para solucionar los problemas que intenta resolver[30]. Según él, Nakamoto y sus herederos tienen una idea estrecha de confianza que se reduce solo a la validación institucional y omiten el hecho de que se requiere una fuerte confianza por parte de las personas para que puedan funcionar las cadenas de bloque y tengan "valor" las criptomonedas[30]. De hecho, hay un caso ejemplar al respecto. El 2016 ocurrió un ataque a la red Ethereum aprovechando una vulnerabilidad en el código de un contrato inteligente, lo que tuvo como consecuencia el robo de 50 millones de dólares en criptomonedas y que la Fundación Ethereum se viera obligada a reemplazar todo su sistema blockchain por una nueva versión[31]. A pesar de esto, los poseedores de esta moneda siguen confiando en su red y Ethereum se mantiene aún como la segunda moneda con mayor "valor" luego de Bitcoin. Esto muestra que las criptomonedas y el blockchain, como todo factor económico y tecnológico, dependen fuertemente de la confianza social y la capacidad de terceros para sostener dicha confianza, invalidando el argumento central de que su aspecto innovador es prescindir de la confianza de los participantes; a Ethereum lo salvó la red de confianza social que

[30] Bruce Schneier, "No hay una buena razón para confiar en la tecnología Blockchain". 2 de junio del 20219. https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/

[31] La fundación Ethereum tuvo que realizar un hard fork o un clon de toda la red para correir el problema e indemnizar a los afectados: https://www.coindesk.com/tech/2016/07/20/ethereum-executes-blockchain-hard-fork-to-return-dao-funds/

soluciones tecnológicas, es reducir el impacto ambiental en lugar de incrementarlo. Incluso, curiosamente, parte del objetivo de Satoshi Nakamoto al crear la red Bitcoin era reducir el costo de las transacciones derivado de la mediación de terceros[1] —el costo de la transacción bancaria y los impuestos estatales—, pero al parecer su prueba de trabajo solo ha desplazado el costo al consumo energético de la validación autónoma.

Las defensas de los partidarios de la moneda de Nakamoto son, por un lado, que el aumento en la eficiencia tecnológica y el uso de energías renovables resolverán el problema a largo plazo y, por otro lado, que la emisión del dinero fiat —el generado por instituciones estatales como los bancos centrales— consumiría comparativamente mayores recursos. En el primer caso, si bien es cierto que podría mejorar la eficiencia técnica en el gasto de recursos, eso no quiere decir necesariamente que se reduzca de manera efectiva el consumo de esos recursos. La paradoja de Jevons[8] sugiere que cuando mejora la eficiencia tecnológica al usar un recurso, manteniéndose el mismo modelo de demanda, es probable que el consumo de ese recurso aumente en vez de disminuir; haciendo que el gasto sea mayor. En el caso del Bitcoin, dadas las condiciones de competencia de la red, los mineros usarán la eficiencia tecnológica para invertir más electricidad en su capacidad de cálculo en vez de reducirla. En

preindustrial https://www.ipcc.ch/site/assets/uploads/sites/2/2019/09/IPCC-Special-Report-1.5-SPM_es.pdf.

El mismo IPCC ha advertido en agosto del 2021 sobre la intensificación del delterioro climático y la posibilidad de sobrepasar el grado y medio laa próximas décadas https://www.ipcc.ch/site/assets/uploads/2021/08/IPCC_WGI-AR6-Press-Release-Final_es.pdf.Además, el 2021 se ha producido una crisis energética por la escasez de energía y el consiguiente aumento de su precio: https://www.theguardian.com/business/2021/oct/12/global-energy-crisis-how-key-countries-are-responding

[8] Una revisión detallada de las posibles consecuencias ecológicas de la paradoja de Jevons se puede encontrar en el artículo de Blake Alcott "Jevons' paradox"(2005) doi:10.1016/j.ecolecon.2005.03.020. Disponible en sci-hub.

cuanto al segundo argumento, podría ocurrir que sea cierto, pero no hay forma certera de hacer la comparación, ni siquiera es posible delimitar qué cosas incluyen el gasto involucrado en la emisión del dinero fiat; si solo se trata de lo que pasa dentro del banco central o si son acaso todas las relaciones sociales que hacen posible la emisión y circulación de las monedas convencionales. El mismo problema se puede aplicar a las criptomonedas, en donde no se ha estimado el costo en fabricación del hardware o el impacto de los desechos electrónicos. En este punto, el gasto de las criptomonedas solo es evaluable si lo que ofrecen como solución económica es preferible al sistema bancario centralizado, elementos que se abordarán en los siguientes puntos; pero sí sabemos con certeza que la Prueba de Trabajo presenta un problema inherente de gasto eléctrico de carácter progresivo y perjudicial.

Aun así, las criptomonedas tienen alternativas para enfrentar este problema. Entre los distintos tipos de mecanismos de validación que actualmente existen[9], hay algunos que no dependen de la Prueba de Trabajo, como, por ejemplo, la denominada Prueba de Participación —Proof of Stakes o PoS—. En su versión simple, esta prueba consiste en que los usuarios pueden elegir congelar en una "bóveda" parte de sus monedas para aumentar la posibilidad de convertirse en verificadores de los bloques de la red. Mientras más monedas inviertan tienen más posibilidades de convertirse en validadores y, con ello, recibir la recompensa de la validación. El riesgo, además de no poder usar las monedas que han congelado por un tiempo determinado, es que, si actúan de manera maliciosa al alterar los bloques, pueden perder el dinero invertido cuando los demás participantes de la red detecten los bloques alterados. La

[9] Una revisión general de los distintos algoritmos de consenso y sus diferencias se pueden encontrar en "A review on consensus algorithm of blockchain" (2021) de Du Mingxiao y otros. doi:10.1109/smc.2017.8123011. Disponible en sci-hub.

infinitas copias que se pueden hacer del archivo, el propietario puede vender el "certificado" que valida su propiedad a otro usuario de la red y con ello el nuevo propietario, independiente de la cantidad de copias exactas que existan, puede certificar que es el dueño auténtico de... un archivo jpg. Por ejemplo, el gif Nyan Cat ha sido vendido como NFT por 590 mil dólares[28], pero esa venta no impide se puedan seguir haciendo copias o que cualquier pueda seguir utilizando el gif; lo que compró el nuevo propietario es el certificado que indica que "su" gif es el original. Pero las curiosidades no se detienen ahí. Algunos tecno-optimistas han aprovechado el entusiasmo para proponer iniciativas a problemas administrativos y políticos. Las propuestas llamadas E-Goverment o Gobierno Abierto —Open Government para los "emprendedores" de turno— son sistemas de administración pública en donde, por medio de contratos inteligentes, los Estados podría llegar a prescindir de la burocracia para encontrar maneras rápidas y descentralizadas de resolver sus comunicaciones y registros al delegar en las cadenas de bloques la validación de este tipo de acciones administrativas[29]. Así, bajo esta nueva promesa, se podría dejar de confiar en gobiernos y Estados puesto que los algoritmos solucionarían los problemas políticos y administrativos asociados.

Con estos ejemplos, el blockchain pareciera ser a todas luces una gran innovación, particularmente al intentar descartar la necesidad de confianza humana en favor de mecanismos criptográficos que serían más seguros y certeros respecto a cómo

[27] Los NFT en palabras del banco BBVA: https://www.bbva.com/es/que-son-los-ntfs-los-tokens-para-el-coleccionismo-de-bienes-digitales/

[28] Historia de Nyan Cat y su venta como NFT: https://knowyourmeme.com/memes/nyan-cat

[29] El uso de Blockchain en el gobierno según IBM https://www.ibm.com/blockchain/industries/government

imparcialidad de los cálculos criptográficos ha seducido de manera peculiar a tecnócratas, políticos y crédulos de todos los tipos. Habría, por fin, una tecnología que soluciona las fallas, desconfianzas y los costos de diversos tipos de intercambios y registros que realiza la sociedad. En este sentido, el blockchain de Ethereum es uno de los ejemplos principales ya que, además de validar su criptomoneda, permite realizar Contratos Inteligentes[4]. A diferencia de los contratos convencionales en donde la realización de las acciones y pagos establecidos depende de la confianza mutua de las personas involucradas en un contrato —por ejemplo en la confianza futura que requiere un contrato de trabajo para asumir que se harán los pagos de los salarios—, los contratos inteligentes son básicamente programas informáticos que ejecutan una acción cuando ocurre una determinada validación en la cadena de bloques. A modo de ejemplo, uno de estos contratos puede realizar el pago a algún proveedor solo cuando una entrega se ha realizado y validado en la cadena, o también hacer una distribución proporcionada de recursos según las acciones y labores realizadas en alguna empresa. Estos programas suponen la idea de que ya no es necesario confiar en las palabras de las personas que están realizando una transacción, sino en las condiciones programadas en el contrato que, una vez "firmado", no puede ser desconocido ni alterado por alguna de las partes porque los pagos o criptomonedas en juego quedan retenidos o condicionados por el contrato inteligente.

Este tipo de transacciones ha generado una gran variedad de iniciativas, como el registro de propiedades materiales en cadenas de bloques o, más curioso aún, como validar la propiedad de algún archivo digital. Esta peculiar forma de propiedad llamada NFT —o Token No Fungible— consiste en que una persona puede crear un contenido digital, por ejemplo un dibujo en un archivo .jpg, y validar su propiedad dentro de la cadena bloques[27]. Con esto, a pesar de las

ventaja evidente es que este procedimiento no requiere necesariamente de la competencia de gasto de recursos de la Prueba de Trabajo —o lo requiere en menor grado— haciendo que efectivamente se reduzca considerablemente el consumo eléctrico. Este procedimiento lo usan, con alguna variación, monedas como Peercoin y ADA, así como una nueva versión de Ethereum, la segunda criptomoneda con mayor capitalización. No obstante, Bitcoin, la principal criptodivisa, no utiliza este sistema de validación y, mientras se mantenga operativa su red, sigue siendo un grave problema ambiental.

Ahora bien, en el caso ideal de que se desechara Bitcoin en beneficio de monedas más eficientes, la Prueba de Participación introduce un problema que Nakamoto precisamente quería evitar al proponer una validación que dependiera de una competencia de recursos. Ese problema es la progresiva concentración en la capacidad de validación, ya que quienes más invierten tienen más posibilidad de ganar recompensas y luego de volver a repetir el ciclo de inversión, generando con ello, una centralización permanente en el funcionamiento de la red.

La falsa descentralización

Una de las declaraciones más frecuentes para promover las criptomonedas es la supuesta descentralización de su funcionamiento, ya sea por la estructura de las redes que las sostienen o también porque su precio o emisión no dependen de instituciones centralizadas. Esta característica produciría, según algunos, una descentralización de la economía en general y, a su vez, daría paso a una economía más democrática[10]. Sin embargo, el tipo

[10] Por ejemplo, en este artículo sobre el efecto descentralizador de las criptomonedas: https://www.elsaltodiario.com/el-jornal-andaluz/la-descentralizacion-de-la-economia

de moneda en circulación no es el principal factor económico que determina la centralización de la economía y, como era de esperar, hoy difícilmente se puede hablar de una descentralización real en las criptomonedas.

Respecto de la concentración de riquezas, en el caso de Bitcoin, gracias a que es público su libro de contabilidad —su blockchain— sabemos que el 40% de las monedas generadas en la red son propiedad de aproximadamente 1000 personas[11], por lo que la descentralización en la emisión del dinero no evita la concentración de la riqueza. Esto se debe a que, como todo mercado, quienes hayan comprado la moneda al inicio de su puesta en marcha o que cuenten actualmente con capital para comprar grandes cantidades, pueden iniciar un proceso de acumulación de capital, con las posibles consecuencias negativas como especular con el valor de la moneda o emplear las riquezas para crear las ya conocidas formas de explotación y desigualdad.

Independiente de la concentración de riqueza, un aspecto que sí debiese expresar una desconcentración en las criptomonedas es el control efectivo que los usuarios pueden tener sobre la propiedad de su dinero. A diferencia del sistema bancario en el cual el banco es el custodio del dinero de las personas, lo que les permite controlar las transacciones y especular con el dinero deposito al entregar créditos, las redes de criptomonedas poseen monederos digitales —o wallets— que entregarían mayor autonomía a los usuarios ya que serían estos los que almacenarían su propio dinero en sus cuentas personales y autogestionadas. No obstante, esta esperanza de Nakamoto está cada vez más lejana. Lo que ha ocurrido es que los

[11] bloomerg.com "Las ballenas de Bitcoin: 1.000 personas poseen el 40% del mercado". 8 de diciembre, 2017
https://web.archive.org/web/20211021105424/https://www.bloomberg.com/news/articles/2017-12-08/the-bitcoin-whales-1-000-people-who-own-40-percent-of-the-market

almacenamiento de dinero y de transacciones realizadas, perfectamente pueden llegar a operar como un nuevo tipo de banca De manera similar, las cadenas de bloque que funcionan con delegación de prueba de participación —Delegated Proof of Stake o DpoS—, que operan eligiendo delegados para validar los bloques, introducen de manera incipiente una lógica de gobierno electo y plutocrático[9]. Sin embargo, si el problema de la validación oscila entre la centralización, incluyendo Estados y bancos, y el excesivo gasto de recursos, al menos queda el blockchain como herramienta innovadora para solucionar distintos problemas del mercado con autonomía y emprendimiento... ¿o no?

Innovación y solucionismo

Entre las ideas habitualmente mencionadas por los partidarios de las criptomonedas es posible destacar, más allá de las promesas de ascenso económico, las que aluden a la revolucionaria innovación que supone la tecnología de la cadena de bloques, el blockchain. Recordemos que este sistema consiste en un libro o registro digital que en principio mantiene el detalle de transacciones, registro al cual todos los usuarios de la red pueden acceder. Este libro es validado de manera descentralizada y "sellado" con criptografía, lo que impide que pueda ser modificado de modo posterior o arbitrario. En palabras de Satoshi Nakamoto, es un sistema que se autovalida ya que está "basado en pruebas criptográficas en vez de confianza", es decir, no depende de la confianza que tengamos en instituciones o terceros que indiquen si algo es válido, sino que son los participantes de la red y sus dispositivos los que se "ponen de acuerdo" y validan sus transacciones por medio de procedimientos matemáticos, en teoría, objetivos e incuestionables.

Esta idea de una tecnología que busca reemplazar la confianza mutua que tengamos los participantes de una acción por la

capa tecnológica ha permitido que estas instituciones utilicen la moneda de Nakamoto de la manera tradicional en que se usa el dinero fiat: con sistema fraccionario, custodio de valores y potenciales corralitos. A pesar de la sorpresa de los entusiastas de las criptomonedas, no es extraño en la historia encontrar que las transformaciones del mercado necesitaron de un estrecho vínculo con las instituciones ya establecidas. Los mercaderes y la banca emergente del siglo XIV y XV mantuvieron una fuerte cercanía con los soberanos de los reinos y principados, así como también con el poder papal, vínculo que estabilizó y fomentó el poder del capitalismo incipiente[25]. De manera mucho más explícita y reciente, está el caso de la acción promotora y correctiva que han tenido los Estados en la implementación de las políticas neoliberales. Muy lejos de la ingenua idea de un mercado autorregulado, los Estados han resultado ser uno de los principales actores en la precarización laboral y en la entrega de garantías a las empresas privadas[26].

El asunto de fondo es que solo cambiando el tipo de moneda no se puede evitar el hecho de que el propio mercado es también una institución, es decir, una relación social que adquiere una inercia propia e histórica que no depende ni se desarrolla según la voluntad de quienes la crearon. Y en ese sentido, el mercado, del tipo de dinero que sea, requiere a su vez de otras instituciones centralizadoras para funcionar, como lo son el Estado y la banca tradicional. Y cuando estas instituciones de apoyo no existen, las crea; como ocurre con la función bancaria cada vez más evidente de los exchanges que, debido al grado de concentración de

[25] Una revisión histórica de las funciones políticas de los mercaderes y banqueros de la Baja Edad Media se puede encontrar en el libro "Mercaderes y banqueros de la Edad Media" (1969), de Jacques Le Goff.

[26] Un análisis de la historia del neoliberalismo y de la paradójica función del Estado promotor de este pensamiento puede encontrarse en "Breve Historia del Neoliberalismo" (2005) de David Harvey.

usuarios de criptomonedas, en vez de utilizar los complejos mecanismos para mantener un monedero propio, han optado por la facilidad de uso que ofrecen los "Exchanges", las plataformas intermediarias que permiten cambiar criptomonedas por dinero fiat. Estos servicios, además de permitir la compra y venta de monedas, ofrecen monederos fáciles de gestionar alojados en sus sitios, lo que ha ocasionado una notoria concentración en transacciones y almacenamiento. Un estudio del 2021 para la categorización de la concentración en los blockchain públicos[12] encontró que en Bitcoin 7 exchanges acaparan el 97% de las transacciones globales, lo que supone una abrumadora concentración en cómo funciona este mercado. De hecho, estos exchanges, que ni siquiera son más seguros dado que no han evitado el riesgo de robos y "hackeos" millonarios[13], al ser en la mayoría de los casos los custodios del dinero de los usuarios, tienen pleno control sobre sus recursos, quebrando las ilusiones de la autonomía financiera. Este problema radica en que los exchanges comprometen la base criptográfica de estas divisas digitales. Las criptomonedas utilizan procedimientos de cifrado no solo para verificar la validez de las transacciones sino también para verificar al usuario propietario de cada monedero. Mientras el usuario tenga bajo su resguardo su "llave de cifrado"[14], nadie puede robar o controlar su dinero, así como tampoco especular

[12] Taxonomía de la centralización en sistemas públicos de blockchain: una revisión sistemática de la literatura" (2021) de Ashish Rajendra Sai y otros. Disponible en Sci-hub. sci-hub.se/10.1016/j.ipm.2021.102584

[13] BBC. "Las verdaderas víctimas de los masivos robos cibernéticos de criptomonedas". 1 de septiembre, 2021. https://www.bbc.com/mundo/noticias-58344057

[14] El cifrado de llaves, o cifrado asimétrico, es un tipo de encriptación en la cual el usuario posee un archivo digital, llamado "llave privada", con el cual puede desencriptar sus mensajes y documentos. Mientras sea el único poseer de la copia de su llave privada, es el único con el control completo de su información; condición que se vulnera en los exchanges. Una explicación más extensa sobre este tipo de cifrado puede encontrarse aquí: https://colectivodisonancia.net/herramientas/introduccion-a-la-criptografia-digital/#id6

con la cantidad que tiene guardada, lo que es precisamente la motivación para la existencia de los "wallets". Al ser los reales custodios de las criptomonedas, teniendo por ello pleno control de las llaves de cifrado del usuario, los exchanges pueden manipular o impedir el retiro de todos los fondos –los clásicos corralitos bancarios– cuando los usuarios prefieran sacar sus monedas, como ha ocurrido en algunas ocasiones[15]. Además, en los casos en que los exchanges utilicen tecnologías sin un código público, podrían incluso especular con el monto real que tienen almacenado, tal como puede hacerlo la banca, como se verá más adelante.

Otro aspecto de descentralización frustrada es el sistema de validación distribuida. En el caso de la minería de Prueba de Trabajo, la competencia creciente por el aumento de la capacidad de cálculo tiende a la concentración de quienes cuentan con la inversión suficiente para mantener una elevada capacidad de cálculo en sus equipos. En Bitcoin, 4 piscinas de minado —o agrupaciones de mineros— concentran el 50,36% de capacidad de validación de la red y en Ethereum las 4 principales piscinas concentran el 63,04% del poder de validación[12]. En el caso de los blockchain que usan pruebas de participación o validación por autoridad, como ya se mencionó, introducen una lógica de centralización en las cuales usuarios, o grupos de ellos, con condiciones específicas como una mayor acumulación de monedas tienen más posibilidades de ser validadores y seguir acumulando dinero, evidenciándose su tendencia a la concentración de manera mucho más explícita que en los mecanismos de competencia. Se podrían seguir señalando otras capas técnicas que también muestran signos de centralización en las

[15] Infotechnology.com "Coinbase y Binance están caídos y frenaron los retiros ante la fuerte caída de Bitcoin". 20 de mayo, 2021. https://www.infotechnology.com/finanzas-digitales/coinbase-y-binance-estan-caidos-y-frenaron-los-retiros-ante-la-fuerte-caida-de-bitcoin/

empresa BitGo para el desarrollo y mantenimiento de la plataforma y de la aplicación Chivo Wallet[23] con que los salvadoreños pueden acceder al monedero entregado por el Estado. Lo que ocurre técnicamente es que el gobierno del Salvador, con la ayuda de BitGo, ha elaborado una segunda capa, que opera por fuera y es anterior a la cadena de bloques, para darle viabilidad al uso de la criptomoneda en una economía nacional, pero a su vez esta segunda capa opera también como un filtro que opaca la realidad de las transacciones. Como la plataforma y el monedero no tienen público su código, no hay garantías para saber cómo funciona realmente, ni siquiera si los usuarios tienen realmente la cantidad de monedas que se les asegura tener. En rigor, lo que los salvadoreños tienen en sus monederos es un token, solo una promesa de bitcoin; y mientras se mantengan en la red Chivo, el propietario y custodio real de los Bitcoin es el banco central. Respecto de esta situación, se le ha pedido al Banco de Desarrollo de El Salvador que detalle qué ha hecho con el fideicomiso de 150 millones de dólares y a qué cuentas se depositaron los Bitcoin comprados, pero el banco se ha negado a dar información[24].

En resumen, el caso de El Salvador muestra que las criptomonedas no suponen un mercado autónomo del Estado y la banca tradicional y, de hecho, la propia necesidad de escalar las transacciones facilita la centralización y la participación de estas instituciones. En el caso de Bitcoin, incluso con mineros validando de manera descentralizada la red, la necesidad de crear una segunda

[23] forbes.mx "El Salvador aprovecha un unicornio de las criptomonedas en su debut con el bitcoin". 7 de septiembre, 2021. https://www.forbes.com.mx/el-salvador-unicornio-criptomonedas-debut-bitcoin/

[24] elsalvador.com "Bandesal niega información sobre compras de Bitcoin y cuentas en las que se han depositado" 18 de octubre, 2021. https://www.elsalvador.com/noticias/negocios/bandesal-niega-informacion-bitcoin/891119/2021/

principales criptomonedas, pero como son muchas es preferible revisar directamente el estudio antes mencionado[12] para ver la larga lista que muestra el fracaso de la descentralización de las criptomonedas.

Los partidarios de estas divisas continúan buscando combinaciones o variantes de blockchain que, sin consumir muchos recursos, no tiendan a la centralización; pero probablemente estén buscando una solución a un problema inherente a cualquier mercado. De hecho, el mercado, por medio de la acumulación de capitales, tiende a la concentración de poder que influye y determina la estructura del propio mercado. Aunque aumente el volumen de quienes participan o se distribuyan ciertas riquezas, esta tendencia a la concentración es un resultado de la competencia capitalista, y la producción del dinero digital, en cualquiera de sus formas, no está exenta de esta fuerza. Dicha situación deja el camino abierto para la estrecha relación con el Estado y la banca, dos instituciones que presuntamente quedarían excluidas por las criptomonedas.

La aparente autonomía frente a la banca y el Estado

Una de las promesas de las criptomonedas que ha atraído, curiosamente, a sectores políticos diametralmente opuestos de manera simultánea es la esperada independencia respecto a dos instituciones: los Estados y los bancos. Como la tecnología de cadena de bloques permite validar la emisión y transacción de estas monedas digitales sin necesidad de depender de una institución externa, en principio, no se necesita la función reguladora del Estado que, por medio del banco central, crea y valida el dinero de curso legal, es decir, el dinero fiat. De hecho, en el proceso de creación y circulación de las criptomonedas, los bancos no tendrían cabida ya que se dificultan dos de sus funciones principales: el custodio y el crédito. Los usuarios de las cadenas de bloques pueden almacenar

Network o segunda capa[19] que consiste, de manera sucinta, en una plataforma de almacenamiento e intercambio temporal de gran capacidad entre dos o más usuarios de Bitcoin, antes de entrar en acción la cadena de bloques. Una vez realizadas las transacciones en esta plataforma, el intercambio finaliza y es validado por los mineros. Utilizando una analogía, funciona como un simulador de transacciones que, una vez finalizado, ejecuta la transacción real y su posterior adición a la cadena. Esto permite que las criptomonedas que tienen un sistema de validación lento puedan escalar potencialmente a un mercado global; pero también se presta para que un intermediario controle el intercambio por sobre el mecanismo de validación del blockchain. El caso ejemplar, que involucra al Estado, es lo que ocurre en el Salvador.

El 8 de junio del 2021 se aprobó en El Salvador la Ley Bitcoin[20] que establece la divisa de Nakamoto como moneda de curso legal y la obligatoriedad de recibir pagos en Bitcoin si es ofrecido en una transacción. Bajo el argumento de ampliar el acceso a las transacciones digitales a la población del país sin cuentas bancarias —dos tercios de los salvadoreños—, el gobierno de Nayib Bukele, autodenominado "el dictador más cool del mundo"[21], creó una reserva o fideicomiso de 150 millones de dólares para darle convertibilidad al Bitcoin dentro del país[22]. Además, contrató a la

[19] Joseph Poon y Thaddeus Dryja. "La Lightning Network Bitcoin: pagos instantáneos escalables fuera de la cadena" (2016) https://lightning.network/lightning-network-paper.pdf

[20] Asamblea legislativa de El Salvador. "Ley Bitcoin", 8 de junio, 2021. https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/27F0BD6F-3CEC-4F52-8287-432FB35AC475.pdf

[21] Nayib Bukele, "El dictador más cool del mundo": https://web.archive.org/web/20210922001740/https://twitter.com/nayibbukele/

[22] forbes.co "El Salvador crea fideicomiso de US$150 millones para conversión al bitcoin". 31 de agosto, 2021. https://forbes.co/2021/08/31/actualidad/el-salvador-crea-fideicomiso-de-us150-millones-para-conversion-al-bitcoin/

sus recursos en sus propios monederos digitales y, a su vez, como la cantidad exacta de monedas emitidas es de conocimiento público, solo es posible prestar el dinero que se tiene; a diferencia de la banca, cuyos créditos pueden entregarse a partir de dinero inexistente. Por consiguiente, la cadena de bloques de las criptomonedas pareciera estar creando un sistema de emisión de dinero que en efecto no dependería de estas instituciones.

De hecho, si se considera en detalle, no les faltan razones a los partidarios de las criptomonedas en atacar a estas dos instituciones por su capacidad de manipular el mercado. El dinero fiat, creado por los bancos centrales, actualmente no tiene ningún respaldo salvo la acreditación institucional. Esto permite, en un mercado de banca desregulada, emplear un sistema fraccionario; dicho de manera sencilla, permite que los bancos conserven solo una fracción del dinero que tienen como depósito, prestando lo demás como crédito, por lo cual nunca está guardada la totalidad del dinero depositado. La apuesta de los bancos es que las personas nunca retirarán simultáneamente sus depósitos, lo que dejaría en evidencia la insolvencia de la banca. A su vez, el Estado en determinadas situaciones, por medio del banco central, puede emitir dinero de la nada con el objetivo de solventar deudas bancarias o para financiar políticas públicas. En estas situaciones, ambas instituciones poseen el control y la capacidad de alterar la cantidad de dinero en circulación para beneficio propio, a riesgo de inestabilidades económicas. En cambio, en el sistema de dinero que se desprende de la propuesta de Nakamoto, la emisión de criptomonedas está condicionada por la Prueba de Trabajo o la participación de los usuarios de la red, lo que impediría la emisión arbitraria de dinero. Además, como el dinero almacenado en los wallets está registrado de manera pública en las cadenas de bloques, no podría haber banca fraccionaria que especule con fondos depositados. Sin embargo, incluso si aceptamos esta

alternativa, la prometida autonomía frente a las instituciones es cada vez más ilusoria.

La banca tradicional ha tomado la iniciativa y, al mismo nivel que los exchanges, ha empezado a abrir cuentas de criptomonedas para sus clientes[16], en donde el banco es el custodio de las llaves de cifrado y, por ende, tiene pleno control de las monedas del usuario. Además, como el usuario no tiene acceso y control efectivo de su monedero, no hay garantía de que realmente sea propietario de la cantidad que el banco le indique y de que no se esté fraccionado su reserva para crear crédito. Es decir, el sistema bancario tradicional es perfectamente compatible con la tendencia centralizadora de las criptomonedas, incluso si su sistema de validación pretende no serlo. De hecho, los bancos ya han empleado un sistema propio de cadena de bloques, llamado Ripple, para optimizar sus transacciones[17] y de paso han creado una criptomoneda bancaria: XRP[18].

Ahora bien, el problema de la institucionalización de las criptodivisas no solo ocurre por el acercamiento de la banca, sino también por la aplicación de una tecnología complementaria al Bitcoin para hacerlo viable a escala global. La situación es que en la moneda de Nakamoto la red solo punede validar 7 transacciones por segundo, lo que la hace inviable en una economía real con miles de intercambios en el mismo período de tiempo. Para solucionar esto se optó por desarrollar una nueva tecnología llamada Lightning

[16] bbva.com "BBVA Suiza abre el servicio de bitcoin a todos sus clientes de banca privada". 18 de junio, 2021. https://www.bbva.com/es/bbva-suiza-abre-el-servicio-de-bitcoin-a-todos-sus-clientes-de-banca-privada/

[17] bbva.com "BBVA realiza transferencias internacionales en tiempo real entre Europa y México con Ripple". 17 de mayo, 2018. https://www.bbva.com/es/bbva-realiza-transferencias-internacionales-tiempo-real-europa-mexico-ripple/

[18] Sorbre la criptomoneda XRP se puede consultar el sitio del proyecto: "XRP: The Best Digital Asset for Global Payments" https://ripple.com/xrp/