"El ruido de nuevas cadenas". Criptomonedas y blockchains, otro sueño emancipatorio fugaz

Santiago Fernando Druetta[1]*

Introducción

Este trabajo pretende analizar una forma de relación social relativamente novedosa llamada Bitcoin. En cuanto objeto de estudio, esta blockchain nos ofrece la posibilidad de cotejar algunos discursos que la construyeron conceptualmente, con la objetividad de las prácticas asociadas a ella.

El nacimiento de la blockchain de Bitcoin está fuertemente asociado a grupos libertarios, anarquistas de derecha (Cypherpunk), identificados con las tecnologías digitales, la economía de los datos y el oxímoron de una sociedad sin instituciones.

Sin pretensiones de hacer de la blockchain un Aleph, ella puede inspirarnos algunas reflexiones sobre la tensión entre los discursos que la presentan como una socialidad ideal, y su rumbo efectivo, que parece seguir dócilmente la lógica del valor.[2]

Como objeto de estudio la blockchain parece sugerir que aun si la era digital necesitara sortear los límites de un capitalismo ya retardatario y su política neoliberal, nada estaría prometiendo una ruptura con la lógica del

1 Licenciado en Comunicación Social (FCC) y Magíster en Ciencias Sociales (FCS) por la Universidad Nacional de Córdoba. Profesor Titular del Instituto Académico Pedagógico de Ciencias Humanas de la Universidad Nacional de Villa María y de la Facultad de Ciencias de la Comunicación de la Universidad Nacional de Córdoba.

2 Tomo estrictamente la categoría marxista de valor y el desarrollo que de ella hacen, profundizando y desplegando sus implicancias políticas y epistemológicas, autores como Alfred Sohn Rethel (2001), Moishe Postone (2006) o Anselm Jappe (2014), entre otros.

* UNVM / UNC - santiagodruetta@gmail.com

valor, ni la irrupción de prácticas emancipatorias, y menos aún la felicidad siempre prometida.

Asumo que es muy temprano para aspirar a alguna certeza al respecto de estas cuestiones y quizás ni siquiera sea factible aún formular las preguntas adecuadas. Pero creo que el análisis del fenómeno blockchain, sus utopías fundacionales, su incipiente institucionalización y sus proyecciones hoy visibles, pueden darnos al menos algún austero punto de referencia.

Espejismos de mercado

En los primeros días de abril de 2022 se realizó en Miami la tercera edición de la conferencia "Guns N' Bitcoin" ("Armas y Bitcoin"),[3] que en su nombre reúne dos elementos aparentemente complementarios: "Bitcoin para defender tu dinero, armas para defender tu libertad".

De hecho, además de la exposición comercial y mesas temáticas, hubo también un acto de homenaje a JSTARK1809, seudónimo del "Santo patrono de las armas impresas en 3D".[4]

Bitcoin y blockchain

Bitcoin es un sistema contable que registra e informa transacciones comerciales o financieras de forma anónima e inviolable, mediante la tecnología blockchain. Como parte de este sistema, se emite la moneda del mismo nombre.

Blockchain es una tecnología de información-comunicación relativamente novedosa. En 1991 aparece el primer trabajo que propone la utilización de cadenas de bloques basada en criptografía para efectuar registros seguros en internet y, en poco más de un lustro, ya se la propone como una solución descentralizada de pagos electrónicos basada en criptografía. La criptografía no sólo confiere seguridad al sistema sino también brinda el carácter anónimo de todas las transacciones. La privacidad es una ban-

3 https://www.criptonoticias.com/comunidad/eventos/asi-fue-conferencia-reunio-bitcoin-armas-fuego/
4 https://www.recoilweb.com/jstark1809-tribute-the-patron-saint-of-3d-printed-guns-171086.html

dera del movimiento Cypherpunk,[5] que lleva en su nombre lo punk, lo tecnológico y la criptografía.

Sin embargo, no será sino hasta 2008 que la blockchain salte a la fama con el sistema Bitcoin que promete administrar de manera segura todo tipo de transacciones económicas sin necesidad de instituciones de mediación o control. Sin bancos, sin estados y con una unidad monetaria propia.

La cadena Bitcoin se presentó como una herramienta descentralizada y segura para llevar registros comerciales y financieros, aunque pronto quedó claro que no era lo único, ni lo más relevante que puede registrar.

Aquí habría que hacer un llamado a la paciencia de lectores y lectoras, para intentar comprender su funcionamiento y seguir la génesis de Bitcoin hacia otras formas sucesoras. El esfuerzo se justifica para alcanzar una visión más clara de este sistema literalmente críptico.

Un libro contable

La cadena Bitcoin es como un libro donde se asientan las transferencias (ingresos y egresos) tal como lo hace cualquier sistema contable al restar los gastos de la cuenta de quien paga y sumarlos en la de quien cobra.

Cada bloque de la cadena puede pensarse como una página de ese libro. Más precisamente un archivo de texto, con capacidad de un megabyte de información, que al completarse ingresa a la cadena, mientras los registros continúan en un nuevo bloque.

Ese registro de datos no existe necesariamente unificado en un lugar y, por eso su control no depende de un grupo que pudiera ser presa de malas intenciones, sino de la acción simultánea de todos los que participan de la elaboración de la cadena de bloques. Se trata de una red descentralizada de tipo P2P.

La red descentralizada

Todos los interesados en participar conectan sus dispositivos en red mediante un software específico. Cada uno es un nodo y en principio no hay jerarquías entre ellos. Así, nadie se adueña de la información y, si cualquier nodo se cae o es hackeado, nada se pierde. Este tipo de redes se

5 Para ver el manifiesto Cypherpunk: https://www.activism.net/cypherpunk/manifesto.html

denomina "peer to peer" (P2P) y en la cosmovisión de este cripto mundo, sus foros, declaraciones y notas periodísticas, el sujeto autónomo y la propiedad privada tienden a aparecer como sus pilares fundamentales.

En el evento "Guns N' Bitcoin", también se homenajeó a varios referentes. Uno de ellos, cuyo seudónimo es Echonoalchimist, declaró a la prensa:

> […] todos los gobiernos están inclinándose hacia la tiranía y están tratando de restringir los movimientos populares [sic], están tratando de eliminar la autonomía corporal, están tratando de hacer del dinero un arma y así, mientras más personas puedan retomar el poder en sus propias manos a través de la minería de Bitcoin desde casa, buscarán la forma de atacarla porque esta soluciona problemas del mundo real. (Esparragoza, 2022)

En estas miradas, una libertad abstracta tiende a confluir con la figura de los propietarios privados en relaciones mercantiles. Y aunque podrá objetarse que la conferencia "Armas y Bitcoins" pertenece a un selecto grupo radicalizado, hay toda una profusión de discursos que parecen asociar a las cadenas de bloques con ciertas perspectivas libertarias y lógicas mercantiles.

Su funcionamiento

La seguridad de la cadena Bitcoin no depende de las armas de fuego sino de un *protocolo de consenso* que permite, a todos sus miembros, verificar la validez de los datos que la cadena registra y que asegura su permanente inalterabilidad: la *prueba de trabajo* (PoW, por sus siglas en inglés).

Explicar este mecanismo supone todas las dificultades imaginables y sólo es posible abordarlo aquí de manera muy elemental.[6] Así voy a intentarlo: una transacción es una operación entre dos nodos[7] (imaginemos que Luis paga dos bitcoins a María), esta y todas las demás transacciones

6 Por más detalles ver https://academy.bit2me.com/que-es-proof-of-work-pow/. También https://academy.bit2me.com/mineria-bitcoin-como-se-crea-un-bloque/#:~:text=Cuando%20un%20nodo%20minero%20logra,para%20que%20estos%20puedan%20validarlo. Acerca del *root hash* ver https://academy.bit2me.com/que-es-un-root-hash/

7 Por más precisión sobre transacciones ver: https://academy.bit2me.com/transacciones-bitcoin/

se van listando en la red y los nodos la toman de allí para verificar su validez, tal como hace el banco o la tarjeta de crédito cuando emitimos un pago, solo que el registro identifica a las partes mediante una clave de identidad muy difícilmente asociable a la persona física que la utiliza. Es anónimo.

A medida que los nodos llamados *mineros* van recopilando las transacciones realizadas y verificándolas, las cargan en el archivo que se propondrá como nuevo bloque en la cadena. Pero la verificación no se hace letra a letra, ya que un algoritmo específico[8] transforma todo el contenido del bloque en un código llamado *hash* y cuyo aspecto es del tipo: 9480ec-00934c3b42725685f6f69b6560163fa503.

La modificación de un solo carácter en el bloque, transformaría a todo el *hash*. Pero, además, como cada bloque lleva en sí el *hash* del bloque precedente (de allí la noción de cadena), cualquier modificación en un bloque no sólo cambia su *hash* sino los de toda la cadena y con ellos el *hash* general (*root hash*).[9]

Aun así, para la seguridad del sistema eso no es suficiente. Todavía se impone a los nodos mineros la búsqueda del *nonce*. Esto se denomina "la dificultad" y conviene recordarlo porque será relevante para el debate. Imaginemos al sistema hablando a los nodos mineros: "Muy bien, aquí están todos ustedes ofreciendo sus registros para el nuevo bloque de la cadena, pero yo sólo aceptaré un bloque cuyo *hash* se inicie con cuatro ceros". A partir de ese momento, todos los postulantes tienen el desafío de agregar, en el bloque que se acaba de completar, un número cuyo efecto sea la modificación solicitada en el *hash* y esto sólo puede hacerse mediante ensayo error. En eso consiste el *minado* que no se hace manualmente, sino en un proceso automático cuya eficiencia depende de la potencia computacional de la que disponga cada nodo.

El primero que lo logre, gana "el premio mayor"; es decir, que cierra el bloque, lo agrega a la cadena y cobra una recompensa jugosa que se abona en la moneda nativa de la cadena (en nuestro caso bitcoins). "Extrae el oro", según la metáfora del sistema, de la que surgen las figuras de "minería" y "nodos mineros".

8 SHA256 es el algoritmo de consenso de blockchain

9 Para más información ver https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp

Cualquier disidencia en los registros, o en algún criterio de trabajo, genera dos bloques distintos que bifurcan la cadena (*fork*) lo que no es un problema sino el principio democrático de acción, en especial ante decisiones de gobernanza. La bifurcación se deja correr, dando por supuesto que crecerá más rápidamente la línea donde siga trabajando la mayoría, mientras que la minoría rezagada, viendo que los bloques y los premios avanzan por el otro camino, terminará "volviendo al redil". Ante los *forks*, la cadena legítima es siempre la más larga.

De la contabilidad a la socialidad

Lo expuesto hasta aquí dista de ser claro y preciso, pero, aun así, ya nos permite una aproximación a las formas de relación que esta tecnología prefigura. Dijimos que, con frecuencia se la presenta como una concreción de la democracia liberal en su versión más pura: propietarios privados, libres e iguales, que tejen sus vínculos con más firmeza y beneficios recíprocos mientras más fieles se mantienen a su interés individual.

No obstante, el "trabajo de estos Robinson" está automatizado y, por lo tanto, ya la idea de sujetos trabajando se torna esquiva. Pero, además, con el propósito de mejorar su potencia de cálculo (minado), los nodos tendieron rápidamente a asociarse sumando equipos y repartiendo premios. Y como la valorización de la criptomoneda fue en aumento, en poco tiempo grandes grupos de inversión -especialmente capitales de riesgo- crearon "granjas de minado", tal como se denominan los inmensos galpones de dispositivos interconectados cuya potencia computacional se infiere de su consumo energético que, en algunos casos, llegó a ser un problema de Estado.

O sea, vemos que los míticos protagonistas individuales van dando paso a clases de agentes, diferencialmente situados en una estructura. Consecuentemente, estas formas diferenciadas de propiedad y/o control de los recursos de minado, ponen en cuestión el supuesto de gobernanza democrática por la bifurcación de la cadena ya que la rama más larga no sería la de la mayoría, sino la de mayor concentración de potencia informática. Así, la sociedad Bitcoin se aleja no sólo del principio liberal de competencia perfecta sino también del de igualdad ciudadana.

El interés individual

La distinción en torno a los recursos de minado, debe complementarse con la división del trabajo que tiene lugar en la blockchain donde, al menos analíticamente, pueden distinguirse nodos mineros que responden a incentivos económicos directos mientras otros trabajan e invierten sin un retorno evidente. Tal el caso de los nodos completos que hacen cumplir todas las reglas del protocolo Bitcoin o los supernodos que operan de forma pública e ininterrumpida como reaseguro del sistema.[10]

De lo dicho no resulta evidente cuál es el interés de los principales responsables de sostener la cadena y menos aún por qué hay tanta gente bien dispuesta. Sin embargo, no es extraño encontrar declaraciones del tipo: "Muchas organizaciones y usuarios voluntarios están ejecutando nodos completos de Bitcoin como una forma de ayudar al ecosistema de Bitcoin" (Binance Academy, 2018).

Esas expresiones parecen remitir a un cierto *activismo* político (incluida la antipolítica), asociadas a una disposición voluntarista con tintes emancipatorios. Otras perspectivas menos generosas, en cambio, señalan que el carácter anónimo de las transacciones permitió su uso en operaciones ilegales y especialmente lavado de dinero, lo que podría justificar, aunque sea en parte, su enorme éxito.

Como hipótesis adicional y sin pretender alentar enfoques "conspiranoicos", cabría mencionar que el sistema Bitcoin fue presentado en la web y firmado con un seudónimo, el 31 de octubre de 2008, en plena crisis de las hipotecas subprime. Justo dos semanas después de que en Bruselas se pidiera una cumbre para reformar el sistema financiero mundial y a treinta días de que la cámara de representantes de los EE.UU. rechazara por escandaloso un plan de rescate del sistema financiero americano, aunque finalmente lo aprobó. Justo entonces, bajo el seudónimo de Satoshi Nakamoto, alguien nos obsequia este fabuloso modelo capaz de operar por fuera del sistema bancario y las regulaciones que pudieran surgir luego del desastre.

Vale recordar que en el año 1933 entró en vigor en EE.UU. la ley Glass-Steagal que separaba la banca de depósito de la banca de inversión, tratando de poner límites a la especulación financiera para prevenir otra crisis como la de 1929. La ley fue objeto de una enconada resistencia de

10 https://academy.binance.com/es/articles/what-are-nodes

sectores financieros que no pudieron contra ella sino hasta los últimos días de 1999. Logro que, menos de una década después de la derogación, derivó en otra burbuja como la que había motivado aquella ley.

¿Sería absurdo pensar que ante la posibilidad de que irrumpiera alguna legislación comparable con la Glass-Steagal, ciertos sectores del mundo financiero, poniendo la barbas en remojo, lanzaron un sistema que les permitía eludir ya no a los bancos sino a las posibles restricciones como la padecida durante tres cuartos de siglo? Si como hipótesis no parece absurda, tampoco alcanza como principio explicativo del masivo interés y aceptación mundial del sistema.

No obstante, entre todas las hipótesis, la menos plausible me parece la de una espontánea adhesión de individuos aislados, impelidos por sus intereses particulares que, ejerciendo su libertad y acrecentando su riqueza, posibilitan el bienestar general en el marco de un nuevo y prístino orden social sin instituciones. En todo caso, al menos pueden señalarse sin temor a equívocos algunas cuestiones claves sobre los difundidos atributos de este sistema.

Primero: la tecnología P2P no funda una comunidad de individuos en un nuevo planeta. La cadena es un sistema de relaciones entre propietarios de equipos informáticos interconectados como nodos de una red que opera sobre la web. Y la web antecede a la cadena, condicionándola.

Segundo: los nodos que la conforman no responden necesariamente a idénticos propósitos e intereses, de modo que la noción de paridad de sus miembros es insostenible.

Tercero: la "comunidad" no es una suma de individuos aislados que en el proceso de reproducir su vida personal van tomando decisiones, consensuando y construyendo paulatinamente un orden. Hay una estructura pre existente, descrita y pautada minuciosamente en el Whitepaper firmado por el fantasmal Satoshi Nakamoto.

Cuarto: esos nodos -agentes idealizados como individuos- pueden y suelen ser organizaciones en sí mismas. Lo que nos expulsa del individualismo metodológico hacia complejas relaciones inter organizacionales.

Quinto: la dependencia tecnológica de estas redes excede con creces la electricidad y el hardware ya que, al operar sobre internet, el sistema es parte y depende de los gigantes de la informática y las telecomunicaciones. Pero por eso mismo también, de instancias reguladoras e, indirectamente, de varias ramas industriales, procesos de comercialización de los insumos

y, en fin, de todas las disputas, acuerdos y estrategias que involucran a esos ámbitos.

Sexto: la cadena de bloques "descentralizada, abierta y democrática" recibe libremente a cualquier participante, pero entendiendo que se trata de "cualquiera" en condiciones de adquirir el equipamiento, que disponga de los conocimientos para operarlo, el tiempo para hacerlo y las disposiciones a actuar en este ámbito.

Séptimo: es dable suponer que la participación está marcada por algún interés que, en el caso de los nodos mineros y los nodos ligeros (clientes) es fácil de imaginar. No tanto así el de aquellos que sostienen la estructura, aunque a veces la distinción puede ser más analítica que fáctica.

El dinero

Hasta aquí los nodos mineros no plantearon mayor dificultad de comprensión respecto del interés que los agita: ganar dinero. Pero no conviene soslayar la pregunta acerca de si el bitcoin es realmente dinero. Como afirma Marx: "La mercancía que funciona como medida del valor y, por consiguiente, sea en persona o por medio de un representante, también como medio de circulación, es el dinero" (1978, p.158)

La sal en algunas sociedades, en otras el cacao y también el oro. Todos productos obtenidos por medio del trabajo y que "prestan su cuerpo" para que el resto de las mercancías lo utilicen como medida de su propio valor. Y, para simplificarlo más aún y no andar con oro en los bolsillos, opera por medio de un representante, "patrón de cuentas", que es una unidad arbitraria: pesos, dinares, rupias, da lo mismo. Signos de valor que no valen por sí mismos, sino por un consenso que los referencia a la mercancía oro por ejemplo y, a través del oro, a cualquier otra mercancía en proporción equivalente.

Podría objetarse que desde hace medio siglo la economía mundial ha abandonado el patrón oro, pasando al dinero fiat, que depende de cierto consenso sobre su valía. Sí, pero siempre está en cierta relación con la riqueza social objetiva. Ese no es el caso de Bitcoin que vuelve al concepto del oro según se expresa en el documento fundacional: "La adición estable de una constante de monedas nuevas es análoga a los mineros de oro que consumen recursos para añadir oro a la circulación" (Nakamoto, s.f., p. 4). Eso suena convincente y, sin embargo, el mítico californiano que baja de

la montaña con su bolsa repleta de pepitas de oro, ha pasado días buscando y extrayendo el mineral. Ha trabajado y ese oro (el de su bolsa y no el que está bajo la tierra) vale por el trabajo de extracción que en él se objetiva.

En la sociedad Bitcoin, "el oro" recibido por el minero no es una expresión de la magnitud de su trabajo ya que entre todos los nodos que "trabajan" intentando cerrar el bloque, sólo recibirá los bitcoins quien encuentre el *nonce*. Algo así como si en una fábrica, al finalizar el día, se patearan penales para elegir a cuál de todos los operarios se le pagará el jornal.

La lógica del valor sería respetada, aun así, si el que anota más goles se llevara la paga de todos los jornaleros y, en ese caso, sólo habría una injusticia distributiva. Pero, aunque aceptáramos que, en la blockchain, lo pagado a uno es lo trabajado por todos, la equivalencia está por demostrarse aún, considerando que mediante la dificultad (cantidad de ceros iniciales del *hash*) el sistema mantiene constante la cantidad de trabajo necesario para el minado (un bloque cada diez minutos), al tiempo que reduce la remuneración sistemáticamente (cincuenta por ciento cada cuatro años). Y precisamente, cuando la productividad de la red tiende a aumentar, el sistema automáticamente eleva la dificultad para mantener el tiempo de trabajo constante. Es decir que exige más ceros en el *hash*.

Dicho claramente, la cantidad de trabajo medida en tiempo, se mantiene constante por cada bloque mientras la remuneración es decreciente, independientemente de los esfuerzos realizados por los nodos.

Asumo que podrían agregarse aún varias objeciones en favor del carácter dinerario del bitcoin y su debate demandaría decenas de páginas, de modo que, para evitarlo, me limitaré a señalar que el mismo sistema de minado (PoW) ya ha sido reemplazado en muchas cadenas de bloques eliminando la función de los mineros.

Entonces, se infiere que, dentro de la cadena, el valor del bitcoin sólo representa la creencia de los participantes. Mientras que, afuera de la cadena, expresa la creencia del sistema financiero en su juego de inversiones al comprarlo y venderlo contra monedas de curso legal en *exchanges* y en la bolsa de valores como ETFs (Exchange Traded Found).

Al comprarlos pagando con monedas de curso legal, los bitcoins valen, así como valen las fichas del casino. Antes de que alguien pague dólares o euros por el bitcoin, vale tanto como los billetes del Monopoly.

El discurso

Pese a los delicados debates posibles aun, creo que lo dicho alcanza para abrir muchos interrogantes sobre la potencia performativa de un régimen discursivo de época, capaz de omitir, sin costo alguno, las innumerables determinaciones que pesan sobre este sistema, para realizar sin más, el paraíso mercantil de la equivalencia aquí en la tierra, sin esfuerzo ni fundamentos.

Sustanciando y naturalizando el valor, se llega al punto de fetichizar un registro digital contable, como si se tratara de un elemento químico: el oro. Pero como en nuestro "mundo marketing" siempre hay una promoción, el discurso laudatorio nos ofrece, por única vez y sin costo adicional, el mismísimo reino de la libertad.

Una mirada a la red Ethereum será el mejor modo de poner la libertad en perspectiva.

La libertad

Ethereum es también una cadena de bloques que funciona con principios similares a Bitcoin, pero metafóricamente podríamos decir que es su "salto evolutivo":

> […] con Ethereum pasamos del concepto de Base de Datos Distribuida al de Computación Distribuida[11] […] Ethereum es una Blockchain programable que no sólo proporciona "operaciones" predefinidas y estandarizadas, sino que también permite a los usuarios crear sus propias "operaciones" […] permite crear diferentes tipos de aplicaciones Blockchain descentralizadas que no se limitan necesariamente a las criptomonedas […] Ethereum es un sistema complejo de Turing que permite a los desarrolladores crear aplicaciones que se ejecutan en el "EVM". (Innovación Digital 360, 2023)

La explicación de esto es tan ineludible como dificultosa y en estas líneas asumo el imperativo de mediar entre la claridad y el rigor. Hecha la salvedad diré que Ethereum es una blockchain sobre la que pueden correr

11 De hecho, el sistema habla de EVM como la Máquina Virtual Ethereum; una hiper computadora definida por toda la potencia informática conectada a su red.

cadenas secundarias[12] y contener programas informáticos capaces de auto ejecutarse cuando se cumplen ciertas condiciones, lo que posibilita inimaginables aplicaciones descentralizadas (Dapps)[13] o *smart contracts*.

Probablemente porque el sistema blockchain se impuso con una perspectiva financiera, se tiende a pensar a los *smart contracts* casi exclusivamente en términos de acuerdos "de negocios", pero ellos pueden accionar sentencias que pongan en marcha diversos flujos de trabajo, del tipo "si sucede X, active el comando Z". Es decir, que pueden provocar efectos dentro del universo digital y fuera de él, tales como los que podría lograr cualquiera con un ordenador conectado a la red y los recursos necesarios. Algo así como hacer sonar el himno nacional si el calendario indica la fecha de alguna conmemoración patriótica, o poner en movimiento una línea de producción cuando queden solo quinientas unidades en stock, o dar inicio a un bombardeo si los sensores registran movimientos de vehículos blindados en la frontera occidental.

Aunque la última aplicación parece de ciencia ficción, vale el mal gusto de mencionarla para sugerir que las imbricaciones entre el mundo digital y el extra digital pueden ser más intensas de lo que solemos suponer, y estos contratos inteligentes son claves para tender puentes entre ambos mundos. Si se piensa en las cadenas de bloques como un elemento exclusivo del mundo financiero, será difícil dimensionar los enormes alcances de esta tecnología.[14]

Una marca digital basta, por ejemplo, para que -cadena de bloques mediante-, se registren todos los pasos en una línea de suministros alimentarios, de controles sanitarios, de sistemas de mantenimiento industrial, de control de legitimidad de objetos, marcas y procesos, etc. Seguimiento que cualquiera de las partes -incluidos los usuarios o consumidores finales- pueden verificar en todo momento.

Existe una aplicación orientada a evitar la pesca comercial ilegal, que registra en cadena de bloques el origen de cada lote de productos. Así, el consumidor final, junto al freezer del supermercado puede escanear un

12 https://learn.bybit.com/es/blockchain/blockchain-layer-1-vs-layer-2/.
13 Por más detalles sobre las Dapps asociadas a Ethereum ver: https://www.ig.com/es/estrategias-de-trading/las-10-dapp-principales-de-ethereum-201113#:~:text=Las%20DApp%20(descentralised%20applications)%2C,muchas%20de%20las%20criptomonedas%20rivales.
14 Por más datos sobre los usos de la tecnología blockchain ver: https://101blockchains.com/es/usos-de-la-tecnologia-blockchain/

código de verificación para saber si el atún que lleva fue pescado conforme a la legislación vigente.[15]

Quedan libradas a la imaginación del lector todas las implicaciones posibles, dada la magnitud del sistema de registros que una sociedad compleja requiere. La tecnología blockchain podría ser la vía más segura y eficiente para mantener siempre actualizadas, accesibles e inalterables las historias clínicas de una población, registros de estado civil, certificaciones de formación escolar, de trayectoria laboral, de infracciones de tránsito, de desempeño laboral, de denuncias o juicios, de premios o reconocimientos de cualquier tipo.

Además, en la cadena de bloques, los certificados de nacimiento podrían estar acompañados de un informe completo del ADN de los recién llegados y su certificación. Las historias clínicas pueden guardarse en plataformas de la nube, linkeadas a la filmación de las intervenciones a la que es sometido el enfermo y los resultados de todos sus estudios.

Los documentos de habilitación de un edificio pueden estar acompañados de audiovisuales que testimonien momentos críticos de la construcción, detalles de las instalaciones y, eventualmente, mediante la internet de las cosas (IoT), esa habilitación podría suspenderse e incluso debitar automáticamente el valor de una multa, si se omite recargar oportunamente los extinguidores de incendio o se posterga el control de los ascensores.

La internet de las cosas permitiría el automático seguimiento, control, y administración del mantenimiento de todo tipo de maquinarias. Informes en tiempo real de desgaste y reparaciones que a los fabricantes y distribuidores les permitiría planificar su actividad y reducir costos de stock. Los mismos registros permitirían mejoras en la performance de esos equipamientos.

No parece delirante imaginar un mercado de cadenas de bloques orientados a necesidades específicas, como por ejemplo el informe de trayectorias laborales, donde las personas que se postulan para ciertos trabajos estarán listadas junto a su respectivo currículum vitae. Pero quizás también se adjunte un informe de desempeños precedentes y un historial de conflictos laborales, incluyendo demandas a sus empleadores o antecedentes de actividad sindical.

15 https://www.criptonoticias.com/aplicaciones/blockchain-lucha-combatir-pesca-ilegal/.

No parece delirante imaginar entonces, que en grandes y complejos grupos sociales pudiera recuperarse ese intenso control social propio de las pequeñas aldeas ya que, para poder brindar estos servicios, el anonimato deberá ser sacrificado. Y no será el único sacrificio necesario.

El trilema de blockchain

A esta altura la pregunta que se impone es quién o quiénes tendrán semejante poder en sus manos y la respuesta de los divulgadores fervientes dice que "Nadie, gracias a la descentralización" porque, supuestamente, se trata de redes P2P, donde nadie podría hacerse con el control del sistema y sus datos. Aunque tampoco resistirlo.

Y si ya vimos que la descentralización no es efectivamente "entre pares" hay que agregar ahora que tampoco es incondicionalmente sostenible. Como suele suceder, el éxito y aceptación del sistema blockchain trajo aparejado el problema de su "escalabilidad", o sea poder registrar más transacciones en menos tiempo, sin afectar la seguridad de la red. Sólo para darnos una idea de la magnitud del desafío, diremos que mientras la cadena Bitcoin difícilmente podía registrar más de siete transacciones por segundo (TPS), el sistema de la tarjeta de crédito Visa estaba registrando un promedio de casi dos mil TPS y podría superar las veinte mil (Porro, 2021). Pero crecer tiene su precio.

Vitalik Buterin, el fundador de Ethereum, acuñó el término "trilema de la escalabilidad" para referirse a la capacidad de una blockchain de combinar tres propiedades orgánicas: Seguridad. Escalabilidad. Descentralización. El trilema enuncia que cualquier tecnología blockchain solo puede presentar dos propiedades a la vez y nunca las tres juntas. Así, la tecnología blockchain actual siempre deberá ceder ante una de las propiedades fundamentales. (Bybit Learn, 2021)

El lector perspicaz podrá imaginar hacia dónde tiende la solución, en la medida que el uso de la blockchain se oriente hacia las aplicaciones que hemos mencionado. Una de las primeras decisiones tomadas en ciertas cadenas, fue abandonar el protocolo PoW o de minado.

Las nuevas cadenas fueron optando por la llamada prueba de stake (PoS) que, en vez de hacer competir a los nodos, los elige por sorteo. Claro que las probabilidades de cada uno son proporcionales al volumen de

criptoactivos que ofrece en caución y el tiempo que propone mantenerlo.[16] La igualdad te la debo.

Esto refuerza no sólo la idea de "clases" de nodos y distribución desigual, sino que pone blanco sobre negro el hecho de que, lo obtenido por cerrar un bloque, no equivale al trabajo necesario. Con esta nueva modalidad, la emisión de las criptomonedas tiende a parecer un retorno financiero antes que el producto del trabajo minero.

Pero si aun así el tiempo apremia, el sistema podrá salvaguardar la seguridad, renunciando a la descentralización en pos de la escalabilidad. He ahí la salida del trilema.

Propiedad privada

Bitcoin como Ethereum, igual que las seguidoras Dash, Monero y tantas otras, son blockchain públicas. Esto no significa "estatales" (vade retro) sino que cualquiera puede integrarse a ellas, al menos formalmente, como ya se sugirió. Es un sistema abierto y transparente. Pero como "el ojo del amo engorda al ganado", las grandes empresas asumieron que podrían lograrse mejores resultados mediante blockchain privadas o concesionadas, y así resolvieron el trilema, sacrificando la descentralización. Grandes y seguras, por lo tanto, privadas.

Las blockchain privadas dependen de una unidad central que controla todas las acciones; tanto el acceso de los usuarios como sus funciones y permisos. Conservando todas las ventajas de la modalidad P2P, lo que cambia es el status de los nodos que dependen ahora de la organización. Así, la empresa regula el acceso al sistema y a la información registrada. El mantenimiento económico depende ahora del propietario o del concesionario.[17] Ni minado ni monedas, a menos que estas últimas deban cumplir alguna función específica y conveniente.

Correlativamente queda abolida también la "resolución democrática de todo diferendo" según el principio de la cadena más larga, porque la

16 Bitcoin mantiene el sistema de PoW, Ethereum transita hacia un sistema dual y las diferentes cadenas públicas que han venido desarrollándose optan mayormente por PoS o alguna de sus muchas variantes.

17 https://academy.bit2me.com/cuantos-tipos-de-blockchain-hay/#:~:text=Un%20ejemplo%20de%20este%20tipo,desarrollar%20o%20mejorar%20los%20mismos

incorporación de cada nuevo bloque es verificada por la autoridad central, eliminando la posibilidad de bifurcaciones (*forks*).

Las empresas que usan cadenas de bloques también pueden tercerizar la tarea en plataformas específicas que les brindan la infraestructura, el *know how* y asistencia técnica.[18] Lejos de ser abolida por las cadenas de bloques, la banca JP Morgan desarrolló Juno y luego Quorum,[19] cadenas de bloques adecuadas a sus necesidades específicas, construidas sobre Ethereum. Linux por su parte, ha creado Hyperledger, también sobre Ethereum. Se trata de un proyecto de código abierto para la adopción empresaria del sistema blockchain. Allí IBM desarrolló la división IBM Food Trust en alianza con Walmart, para la mejora de la trazabilidad de productos frescos. Amazon, que en su diversificada economía ha creado AWS (plataforma de la nube), se vale también del proyecto Hyperledger para contar con Amazon Managed Blockchain.

Queda aún por ver cómo irá vinculándose este tipo de aplicaciones con la inteligencia artificial, pero mientras tanto, los bancos centrales avanzan ya hacia la creación de los CBDC, sus propias monedas, pero en versión digital, operando sobre cadenas de bloques y con *smart contracts*, que posibilitarán un seguimiento en tiempo real de cada centavo, y permitirán fijar las posibilidades, imposibilidades, plazos y destinos de todo gasto. El sueño de Big Brother.

Como se ve, los modos de apropiación y uso de la blockchain no parecen augurar libertades, ni entrar en contradicción con el modo de acumulación capitalista, ni abolir necesariamente la institucionalidad asociada a él. No al menos hasta ahora. O sea que no parece razonable, por lo tanto, imputarle un carácter revolucionario de ningún cariz.

Sin embargo, retorna la pregunta sobre las condiciones de posibilidad, la eficacia y rápida pregnancia de un discurso a veces liberal y otras veces libertario, para presentar como emancipatorio a este sofisticado sistema de control y potencial dominación.

---

18 https://geekflare.com/es/finance/blockchain-platforms-for-finance-applications/

19 https://es.cointelegraph.com/news/jpmorgans-blockchain-products-explained-by-ex-jpm-tech-leads

Un fantasma recorre la red

Quizás pudiera pensarse en la cadena de bloques como herramienta para algunas formas de resistencia política, pero sólo tanto como pueden serlo otras tecnologías de información y comunicación, siempre limitadas por las relaciones asimétricas de poder en que se opere.

En cambio, sus aportes y posibilidades en el marco del desarrollo capitalista probablemente justifican un exhaustivo análisis que excede las posibilidades de estas líneas, pero que no puede omitirse sin más, porque allí precisamente aparecen nuevos interrogantes para las Ciencias Sociales. Intentaré solo dar una pista.

Una unidad de observación privilegiada es la industria del *gaming* que a nivel global facturó más de 150 mil millones de dólares en 2019 (Asociación Española de Videojuegos [AEVI], s.f.). En este universo se impone aceleradamente la tecnología blockchain: "[…] las cadenas aportan dos formas de valor a los juegos, por un lado, ofrecen la posibilidad de intercambiar activos digitales entre los distintos juegos, y por otro, permiten realizar trueques de dichos activos entre los jugadores" (Rodríguez Canfranc, 2019).

La idea es que, mediante marcas digitales, los jugadores puedan identificar y acreditar la propiedad de elementos del juego y registrarlos junto a las trayectorias de desempeño. Avanzar en un juego y obtener recompensas equivale en ese caso a contar con el registro de esos logros y el reconocimiento del sistema, que autoriza a "negociar" y comercializar lo creado y obtenido. Así, por ejemplo, tras construir una choza en un juego, se puede contar con algo así como la escritura digital del inmueble (NFT) para usarlo, venderlo o alquilarlo a otros jugadores. Lo mismo vale para el carbón o la leña obtenidos en los juegos de construcción de aldeas, o para las armas o herramientas recibidas al ascender de nivel. Esto ha dado pie a los "play to earn", juegos en los que se puede ganar dinero y en los que, por lo tanto, para no perder tiempo durmiendo (*time is money*), se suelen establecer alianzas entre jugadores de muy distintos husos horarios (como las camas calientes de la Inglaterra industrial) e incluso contratar empleados-jugadores para no interrumpir la partida.

Esto borra el límite entre trabajo, tiempo libre y entretenimiento. Más aún, cuando el jugador transforma el escenario construyendo algún elemento, o "criando animales" en una granja virtual, está aportando valor

al interior de la plataforma. No sólo porque pueden hacerlos circular allí como mercancías, sino también porque en tanto valores de uso virtuales, muchos de esos elementos van enriqueciendo el escenario (algo parecido a las mejoras de la tierra arrendada). Las empresas propietarias de las plataformas no sólo no remuneran al jugador por eso, sino que obtienen dinero de él como condición de acceso al espacio y sus recursos. Una simpática parodia de la economía feudal.

Como las transacciones se realizan en criptomonedas, el desafío por venir para esas plataformas es interconectarse con otros escenarios (y por lo tanto con las respectivas blockchain) unificando todo el registro de las transacciones y, especialmente, reconociendo recíprocamente las distintas formas de valor. Así es posible vender lo que se gana aquí para comprar lo que se necesita allá. Y, suponiendo que fuera de las plataformas se acepten pagos con esas criptomonedas como de hecho sucede, resulta entonces que podríamos comprar una camisa "de verdad" con el "dinero" virtual obtenido al vender la espada mágica que se recibió al ascender de nivel en un videojuego. Claro, siempre y cuando la creencia sobre el valor de ese tipo de objetos se sostenga.

Esto no es una posibilidad del futuro sino algo que ya acontece de este lado de las pantallas, y se potenciaría hasta lo inimaginable si se pasa del mundo de los juegos a esa espacialidad y temporalidad que prefiguran sitios como Decentraland o Sandbox. Mundos virtuales donde las grandes empresas ya hablan de instalar sucursales y la república de Barbados alguna vez prometió abrir una embajada.[20] De eso se trata el metaverso que pareció inminente durante la pandemia y luego se ralentizó, quizás porque los flujos de inversión privilegian ahora la IA.

Valga aclarar que no estoy proponiendo abolir la diferencia entre realidad y simulación digital, especialmente porque la "parte del león" de todo este mundo digital no se lo llevan los fabricantes de la virtualidad sino los fabricantes de chips, al menos si se tienen en cuenta los índices bursátiles más recientes. El mundo digital no reemplazará al analógico, al menos mientras no podamos sacarnos de encima el cuerpo biológico sin morir en el intento. Pero el mundo analógico carga con un antes y un después de la digitalización y las categorías teóricas con que hemos tratado de interpretarlo y transformarlo no parecen suficientes. O, peor aún, sucumben

20 https://www.infobae.com/america/america-latina/2021/11/17/barbados-anuncio-que-abrira-una-embajada-en-el-metaverso/

a banales afirmaciones de sentido común, a veces dogmáticas como el intento de reducir todo al mercado, o a veces sencillamente delirantes, como la creencia en la condición plana de la tierra.

En este camino las Ciencias Sociales y las categorías teóricas tienen hoy un desafío enorme. O tal vez sólo el desafío de siempre, pero de manera más imperiosa: "[…] la lucha inseparablemente teórica y práctica por el poder de conservar o de transformar el mundo social conservando o transformando las categorías de percepción de ese mundo." (Bourdieu, 1990. p. 35).

(In)conclusión

Como pudimos ver, en cuanto la tecnología blockchain dio muestra de su potencial, las empresas y los Estados hicieron de ella una herramienta de administración y control, prácticamente opuesta a las "anarcofantasías" fundacionales.

Vimos también que la cadena de bloques -entre otras *innovaciones*- tensiona al *paradigma tecno económico* y su marco socio institucional que ha ordenado nuestro presente (Pérez, 2004). Urge entonces preguntarnos por los límites y las posibilidades del neoliberalismo hoy, como patrón de acumulación y marco socio institucional efectivo, atentos a que, nuestro horizonte más probable, es el de una nueva fase de acumulación de tipo industrial digital, que propone enormes interrogantes. Uno de ellos, y no el menor, acerca de los nuevos regímenes discursivos que puedan darle inteligibilidad y cohesión a la realidad.

Referencias

Asociación Española de Videojuegos (AEVI) (s.f.). *El videojuego en el mundo.* https://www.aevi.org.es/la-industria-del-videojuego/en-el-mundo/

Bybit Learn (8 de septiembre de 2021). *Capa 1 vs. Capa 2 de la blockchain, lo que debes saber.* https://learn.bybit.com/es/blockchain/blockchain-layer-1-vs-layer-2/

Binance Academy (29 de noviembre de 2018). ¿Qué son los nodos? Actualizado el 17 de agosto de 2023. https://academy.binance.com/es/articles/what-are-nodes

Bourdieu, Pierre (1990). Espacio social y génesis de clase. En Bourdieu, Pierre, *Sociología y cultura.* México: Grijalbo.

Esparragoza, Luis (22 de abril de 2022). *El mago de la minería de Bitcoin desde casa: entrevista con Econoalchemist.* Criptonoticias. https://www.criptonoticias.com/entrevistas/mago-mineria-bitcoin-casa-entrevista-econoalchemist/

Innovación Digital 360 (24 de abril de 2023). *Ethereum: qué es, cómo se creó, cómo funciona y áreas de aplicación.* https://www.innovaciondigital360.com/blockchain/ethereum-que-es-como-se-creo-como-funciona-areas-de-aplicacion-precios-de-eth-y-graficos-actualizados-en-tiempo-real/

Jappe, Anselm (2014). *El absurdo mercado de los hombres sin cualidades.* Logroño: Pepitas de Calabaza Ed.

Marx, Karl (1978). *El capital.* México: Ed. Siglo XXI.

Nakamoto, Satoshi (s.f.). *Bitcoin Whitepaper.* https://www.bitcoin.com/satoshi-archive/whitepaper/

Pérez, Carlota (2004). *Revoluciones tecnológicas y capital financiero.* México: Siglo XXI Editores.

Porro, Jesús (14 de julio de 2021). *La limitación tecnológica del Bitcoin le impide ser alternativa como medio de pago.* Investing.com. https://es.investing.com/analysis/la-limitacion-tecnologica-del-bitcoin-le-impide-ser-alternativa-como-medio-de-pago-200445012

Postone, Moishe (2006). *Tiempo, trabajo y dominación social.* Barcelona: Marcial Pons Ed.

Rodríguez Canfranc, Pablo (16 de septiembre de 2019). *Blockchain y videojuegos, una relación prometedora.* Telos. https://telos.fundaciontelefonica.com/la-cofa/blockchain-y-videojuegos-una-relacion-prometedora/

Sohn Rethel, Alfred (2001). *Trabajo manual y trabajo intelectual.* Barcelona: Ed. El viejo topo.