UNA CADENA PARA ATARLAS A TODAS

Apuntes sobre cómo la tecnología blockchain determina la cultura

G. Carbonell
2ª Prueba de Evaluación Continua
Culturas políticas, ciudadanía y democracia: procesos de transformación
Máster en Comunicación, cultura, sociedad y política
UNED, 2020

ÍNDICE DE CONTENIDOS

LA GÉNESIS DE UN FACTOR DIFERENCIAL

¿Cómo puede cambiar la sociedad a través de la tecnología? Implicados en una revolución de la conectividad sin precedentes antes del siglo XX, la pregunta se enfoca en cómo la redefinición de los protocolos de la red tecnológica pueden suscitar cambios en los protocolos de la red social[1] con la que interactúa.

En 1994, Timothy C. May, uno de los fundadores del movimiento *cypherpunk*, escribía en su *Cyphernomicon* —un compendio de notas sobre el porqué de la criptografía y su epifenómeno social, la criptoanarquía—:

> Algunos de nosotros creemos que diversas formas de criptografía fuerte causarán el declive del poder del estado, quizá incluso colapse con bastante rapidez. Creemos que la expansión en el ciberespacio, con comunicaciones seguras, dinero digital, anonimidad y pseudoanonimidad, y otras interacciones crypto-mediadas, cambiarán profundamente la naturaleza de las economías y las interacciones sociales.[2]

Nos encontramos en un momento crucial de la génesis de internet, en el que se discute sobre qué efectos de la conectividad en red terminarán siendo hegemónicos. En términos jurídicos, entre la *High Performance Computing Communication Act* de 1991, que liberó el desarrollo comercial de internet, y la *Telecommunications Act* de 1996, que liberalizó el mercado de las telecomunicaciones y relajó los límites de la propiedad cruzada de medios y canales de comunicación.

Es un momento en el que son palpables tanto el celo de los hackers por mantener internet en forma de espacio colaborativo como el celo empresarial por ganar relevancia comercial dentro del ecosistema emergente. Es en 1996 cuando John Perry Barlow publica su *Declaración de independencia del ciberespacio*[3], y alrededor del año 2000 cuando crece y estalla la "Burbuja Puntocom"[4]. Napster nacerá en 1999 como una propuesta descentralizada de consumo cultural, como "el primer sistema P2P para intercambio de archivos masivo[, y] la presión judicial [conseguirá] cerrar la plataforma [...] en 2002"[5]; mientras, Steve "Jobs se [convertirá] en el intermediario de dos enemigos mortales[, las discográficas y los internautas,] con una plataforma de música digital [...] completamente centralizada, cuantificada y registrada por Apple"[6].

Empezamos a percibir roces entre las partes implicadas, intuyendo dilemas en torno al derecho de autor, la propiedad privada, la privacidad, etcétera. Queda patente que el diseño de las soluciones informáticas influye y se relaciona con las instituciones humanas. Cabe

[1] No confundir aquí una red entre personas (una *red social*) con una "Red Social", entendida como una plataforma dentro de internet que aloja perfiles de personas a las que pretenden conectar (*conectividad*) dentro de esa misma plataforma.
[2] May, 1994. 2.13.1
[3] Barlow, 1996.
[4] El País. 2010, March 10.
[5] Peirano 2018, p. 149
[6] Peirano 2018, p. 168-169.

preguntarse entonces, como hará Jaron Lanier[7], en qué medida los diseños tecnológicos condicionan el futuro de las sociedades en las que se implementan, y de qué forma las decisiones pretéritas de una sociedad respecto a su consumo de tecnología acotan sus opciones futuras (los bloqueos en las opciones futuras, que él llama *lock-ins*):

> Merece la pena intentar descubrir cuándo las filosofías nos limitan al software bloqueado [*locked-in*]. Por ejemplo, ¿la anonimidad generalizada o la pseudoanonimidad son algo bueno? Es una pregunta importante, porque las filosofías correspondientes sobre cómo los humanos pueden expresar el significado han estado tan arraigadas en los diseños de software entrelazados de Internet que es posible que no podamos deshacernos de ellos por completo, o incluso recordar que las cosas podrían haber sido diferentes.[8]

Parafraseando al letrado y ciberactivista Laurence Lessig, que "la arquitectura en el ciberespacio es la verdadera protectora de la expresión; constituye la *Primera Enmienda en el ciberespacio*"[9] y que, por lo tanto, desatender a cómo las relaciones humanas se redefinen a través de la tecnología es sinónimo de desatender los derechos civiles mismos; equivale dejar al arbitrio de los ingenieros el *ethos* de los ingenios.

En este sentido, Eric Hughes ya acuñó en su *Manifiesto Cypherpunk* de 1993 el famoso lema "cypherpunks write code"[10]. Si bien se puede discutir que el vector tecnológico sea el único factor determinante de la propuesta de éxito de un movimiento, dada la capacidad de la tecnología pretérita para condicionar la futura, es indudable que construir las herramientas que potencialmente definirán el futuro es una propuesta coherente si el objetivo es un presente asegurado por las comunicaciones cifradas.

Llegados a este punto, cabe preguntarnos por las implementaciones técnicas que, en forma de contrarrespuesta a la tendencia centralizadora de internet, hayan tenido un calado cultural suficiente como para enmarcarse dentro de un cambio de paradigma.

Cuando hablamos de sistemas cifrados descentralizados, me refiero a sistemas de votación, consumo, expresión, almacenamiento, etcétera, distribuidos entre todos los usuarios de la red; en oposición a conglomerados de servidores con un propietario único al que los usuarios acuden demandando fracciones de sus datos. ¿Pero cómo puede tener calado social un proyecto tecnológico de descentralización de la información? Estas implementaciones son posibles, aunque deben compensar la pérdida de eficiencia con actores en red más activos y con mayor inteligencia operativa que las que encontraríamos en un paradigma centralizado, donde un único dueño de la información arbitra las demandas del resto de miembros. Como ha sido también el caso del estudio de las "redes neuronales", las limitaciones de conectividad en red y la capacidad de cómputo de los actores han supuesto una frontera técnica que hemos ido ampliando conforme la informática se ha desarrollado en las últimas tres décadas.

[7] Lanier, 2011, 2014, 2019.
[8] Lanier, 2011, p. 13.
[9] Peirano 2018, p. 152. Cit. Lessig, Laurence, *El Código 2.0*.
[10] Trad. inglés: "Los cypherpunk escriben código".

En su mismo manifiesto de 1994, pese a ser propositivo, May calificaba el dinero digital de “material exótico”[11]. Hablaba de un sistema de transmisión de valor sin bancos centrales ni nacionales; una tecnología construida sobre internet que permitiese a los poseedores de dicho dinero operar al margen de cualquier estado o institución. Pese a las limitaciones técnicas de las que era consciente, es un requerimiento que repite en exceso, llegando a clarificar que los “agentes y objetos dentro de un sistema informático seguramente necesiten seguridad, credenciales, robustez e incluso dinero digital para transacciones”[12]. Su compañero Hughes[13] también subrayó que “debemos juntarnos y crear sistemas que permitan que transacciones anónimas tengan lugar”. En 1991, el ingeniero Phil Zimmermann ya había implementado y regalado al mundo la tecnología de encriptación PGP (*Pretty Good Privacy*), que supuso un cambio sin parangón en la comunicación entre dos puntos dentro de una red monitorizada, por lo que era esperable que sucesivas aportaciones se relacionasen con más victorias en pro de la privacidad.

Guiado por este espíritu de anonimidad y descentralización, en 2008, alguien con el pseudónimo de Satoshi Nakamoto envió a una lista de correo sobre criptografía en metzdowd.com un artículo titulado *Bitcoin: A Peer-to-Peer Electronic Cash System*[14].

BLOCKCHAIN: EL FACTOR DIFERENCIAL

Tal y como proponía Satoshi Nakamoto en su artículo, la tecnología Bitcoin se definiría como “una versión puramente entre personas [*Peer-to-Peer*] de dinero electrónico [que] permitiría que los pagos se enviasen directamente de una parte a otra sin las cargas que implica hacerlo a través de una institución financiera”[15].

Sin desmerecer el haber sido la primera criptodivisa implementada, el aporte más relevante de Bitcoin fue dar con un sistema de certificación de transacciones entre iguales. Si el dinero avalado por los estados-nación lo está además por los bancos centrales en una relación de jerarquía, quienes permiten además a los bancos comerciales un entramado contable que consiste en traducir el dinero fiduciario en dinero anotado, y las relaciones de crédito o tenencia se ven afectadas por productos financieros, especulación y secretismo; la tecnología que propuso Bitcoin otorga la igualdad a cualquier tenedor: todos los actores tienen el mismo tipo de dinero, todos conocen las acciones de todos, ningún actor tiene más poder que otro para limitar el uso del dinero dentro de la red. En otras palabras, la implementación de Bitcoin no reinventa el dinero sino que inaugura el concepto de *blockchain*: una cadena de bloques (u operaciones) con una naturaleza común, compartida por todos los miembros de una misma operativa.

En términos computacionales, “definimos una moneda electrónica como una cadena de firmas digitales”[16]. Dando por hecho que el patrón oro ya no representa el dinero impreso por un estado, podemos extrapolar que una criptodivisa no tiene por qué representar, tampoco, un

[11] May, 1994 5.4.1.
[12] May, 1994 6.8.1.
[13] Hughes, 1993.
[14] Nakamoto, 2008, November 1.
[15] Nakamoto, S. (2008)
[16] Nakamoto, S. (2008), p. 2.

activo material como podría ser un metal precioso. Los “bitcoins” propiamente señalados como monedas son cantidades acuñadas colectivamente a través de la actividad de algunos nodos que se comportan como “mineros” dentro de la red Bitcoin. De hecho, una cantidad dada de criptomonedas se relaciona con las llaves criptográficas que permiten anotar operaciones legítimas con dicha cantidad en el registro compartido; no con la tenencia de cierto volumen de monedas en sí. Así, se puede entender una criptodivisa como una serie de registros compartidos confiables adscritos a una forma también confiable de alterarlos.

En esta tesitura, una “cadena de bloques” (o *blockchain*) implementada no se ve en la necesidad de servir a un fin monetario. Si bien Bitcoin y otras criptodivisas (Ripple, Litecoin, Monero, Dash, Dogecoin, etc.) han articulado su funcionamiento en torno a la idea de que cualquier actor en su sistema pueda fiscalizar las acciones del resto de actores, un *blockchain* no presupone como condición indispensable definir una divisa. Es, incluso, frecuente que las acciones se asocien a un mero *token*[17]; que o bien representa una acción puntual o bien señala a otro *blockchain* con otra divisa.

De esta forma, un *blockchain* se convierte en un objeto tecnológico cuya ontología es compartida y cuya teleología es testimonial; es compartido por todos sus poseedores y cada operación se anota para que todos los miembros de la red conozcan lo que así ha ocurrido. Cuestiona el *status quo* hasta el presente, porque hasta este momento no existía tal connivencia de fuerzas; capaces de colectivizar los hechos con protocolos estandarizados que publiciten la información mediante un soporte de datos descentralizado fuera del error humano. La postura es opuesta a la idea de centralizar la información en un servidor cerrado al público y servirla a conveniencia de los clientes que la demandan. En esta tesitura, cualquier poseedor ostenta una copia de todo lo acontecido y puede tomar la acción siempre que haya otros nodos en la red dispuestos a actuar como testigos; no hay acciones veladas para el resto de miembros; y los conflictos se resuelven mediante procesos, no mediante política.

APLICACIONES DE *BLOCKCHAINS* Y SUS CAMBIOS DE PARADIGMA

Habiendo ya introducido la pugna entre centralización y descentralización en el desarrollo de internet; y dejando claro que la búsqueda de sistemas criptográficos frente a las amenazas de la centralización ha dado, entre otros frutos, con la tecnología *blockchain*, llega el momento de aventurar las posibles implementaciones de dicha tecnología y cómo estas pueden alterar las estructuras sociales que las adopten[18]. Volvemos a la pregunta sobre cómo puede cambiar la sociedad a través de la tecnología.

La primera respuesta a esta incógnita es más que evidente: el surgimiento de criptodivisas no reguladas ha creado un ecosistema especulativo sobre el valor de estas, similar al mercado FOREX de monedas. A diferencia de la banca y la inversión tradicionales, estos sistemas son discretos (y con frecuencia anónimos), por lo que sirven a los especuladores como un contexto para sus prácticas alejadas del intervencionismo estatal. En

[17] Trad. inglés: ficha, vale, testimonial.
[18] Rosic, 2017, March 7. Daley, 2018, December 5. Viens, 2019, November 5.

este sentido, el mercado de criptodivisas representa una contraparte; donde antes teníamos estados de derecho gestionando sus monedas, ahora sumamos un entorno donde no hay más forma de gestionar el valor de las divisas que la propia homeostasis del sistema. Ambos escenarios parecen retroalimentarse, pues existen agentes de cambio que permiten comprar criptomonedas con dinero bancario y viceversa; y los indicios sugieren que los cambios sociales (en un contexto de crisis, por ejemplo) se reflejan en las valoraciones de cualquier divisa, independientemente de su naturaleza. Así, el mercado especulativo de las criptomonedas sirve de vía de escape al mercado regulado cuando sus condiciones estatales no son favorables, como el mercado regulado sirve de refugio de las inversiones cuando el entorno descentralizado se vuelve demasiado volátil. La *Mano Invisible* de Adam Smith estrecha la Mano del Estado a conveniencia, poniendo en jaque cualquier paradigma que abogue por decantarse por uno u otro modelo como solución última.

En este sentido, también hay que considerar cómo afecta al individuo la tenencia y uso de una criptodivisa. En las socialdemocracias liberales, la Hacienda Pública tiene poder para conocer el secreto bancario y embargar las cuentas de la ciudadanía, con tal de garantizar el cobro de impuestos y de vehicular las disposiciones de la judicatura. Este entramado se sustenta en la cooperación de instituciones en distinto orden de jerarquía, desde los Poderes Públicos hasta los bancos comerciales, quienes han de acatar las demandas del estado. Si retomamos las ideas de que la criptodivisa se maneja a través de una llave cifrada (que no necesita adscribirse a un número de identificación fiscal) y que las transferencias no requieren de organismos oficiales que las certifiquen, podemos afirmar que el uso generalizado de una criptodivisa cuestiona el poder estatal para fiscalizar y actuar en materia económica. Si bien los impuestos se han podido considerar como un acto de voluntariedad frente a la sociedad en que se vive, no es menos cierto que el pacto de la socialdemocracia se ha sustentado en el control estatal más allá del mero monopolio de la violencia; también lo empodera la vigilancia. Con una ciudadanía cuyo valor monetario escapa de la capacidad del estado para cobrarse el impuesto adeudado, infiero que una adopción en masa de esta forma de dinero legaría el pago de tributos a la buena voluntad, poniendo en jaque el sostenimiento de todo el aparato construido con dinero público.

Hasta el momento, la presencia de una forma anónima de pago, sumada a la implementación de otras tecnologías como The Onion Router[19] y PGP, ha dado por finalizada la "Cruzada contra las drogas". Poco pueden hacer las fuerzas del orden si el tráfico se traslada de la calle a los domicilios, siendo el agente que traslada las sustancias un operario de correos y el volumen de correo tal que la inspección de todos los envíos se mantiene como un problema irresoluble. Los pedidos se tramitan dentro de mercados similares a Amazon, donde las plataformas retienen el dinero hasta que ambas partes (ofertante y demandante) quedan satisfechas, y donde los usuarios aún siendo anónimos ven sus avatares evaluados en términos de reputación. Tras un proceso que implica traducir dinero bancario a criptodivisas, conectarse a una red cifrada y comunicar la dirección de envío codificada con una llave criptográfica dispuesta por el vendedor, el consumidor recibe en su buzón un paquete sellado herméticamente, tratado contra perros antidroga, con unas condiciones sobre la pureza de la sustancia y unos precios que no encuentran equivalente en el mercadeo tradicional; donde el

[19] "El Enrutador Cebolla", que establece caminos de comunicación seguros entre pares, incluidos servidores cuya posición geográfica es desconocida.

traficante no muestra referencias de otros compradores y la sustancia puede estar más adulterada.

Con lo dicho, quedan cubiertos tres fenómenos de cambio cultural sustanciales relacionados con la implementación de criptodivisas: la especulación financiera, la relación de contribución de la ciudadanía con el estado, y la reconfiguración del mercado de las drogas hacia un nuevo paradigma que escapa del estado. No obstante, como se ha dicho, el concepto de *blockchain* excede la idea de un mecanismo efectivo de intercambio de valor, extendiéndose hasta la consideración de la fiscalización colectiva de todas las acciones.

Uno de los aspectos más prometedores de las "cadenas de bloques" más allá de la divisa se refiere a los llamados *smart contracts*. Siguiendo nuestra herencia de Derecho Romano, hasta ahora los contratos se han firmado a mano, en cada página y por duplicado. Si bien este formalismo ofrecía garantías en épocas donde los medios de reproducción eran más limitados, hoy en día se puede falsificar una firma o alterar un folio con relativa facilidad. Un registro compartido de contratos elimina el problema de la duplicidad (lo que dice la copia de un contrato frente a lo que dice su supuesta copia en discordancia) mediante redundancia (la constancia del contrato es absoluta en todo el sistema), y cancela el riesgo de pérdida de copias por alguna de las partes. Además, un registro no requiere una equivalencia formal con un contrato; donde el documento ha de explicitar cuanto se firma, una cadena de bloques es dinámica y por lo tanto puede adoptar configuraciones más elásticas en términos jurídicos, como podría ser suscribir una cláusula por registro y valerse de nuevos registros para actualizar cláusulas.

Otra potencial aplicación del *blockchain* tiene que ver con los cuestionados sistemas de votación electrónica. Si el cómputo de los votos depende de que cada una de las terminales haya transmitido la información a un ordenador central, previa comprobación de la identidad de los votantes por términos analógicos-humanos, el sistema queda a merced de la incertidumbre: ¿existe coincidencia entre la identidad declarada y las personas votantes? ¿Es el código de una máquina igual en todas las máquinas, o pudo adulterarse? ¿Existe algún agente intermedio en el proceso de transmisión capaz de alterar el voto? ¿Cómo puede un votante certificar que su voto se computó correctamente? Con un sistema distribuido de votación electrónica, todas las máquinas poseerían una parte o la totalidad del registro de los votos, siendo estos públicos, y el problema del secreto del voto se podría solventar mediante una clave criptográfica personal similar a las que ya expide la administración pública (y que podría estar inscrita en el DNIe).

Esta última idea, que parece relegar a la ciencia ficción la idea de que cada máquina de voto contenga los votos de todo un país (existiendo tantas copias de los votos como cabinas en colegios electorales), no es descabellada. Si cada voto se comprime en un registro de unos 5KB (5120 caracteres, aprox.), la voluntad de un país de cincuenta millones de personas cabe en menos de 240GB. En términos de España, con unas 50.000 mesas de votación[20], cada mesa sería responsable de la producción y transmisión de sólo unos 4.8MB de información, y la contabilización de los votos sería tan inmediata como el cierre de las votaciones. Aunque este proceder plantee otras dudas, como qué sistema impediría consultar el *blockchain* a tiempo real (un equivalente a las encuestas "a pie de urna"), un sistema de votación descentralizado evitaría los fraudes tales como una adición hartera y súbita de votos o los fallos en el conteo.

[20] Riestra, 2014, May 24.

Otro ejemplo de implementación de *smart contracts* alejado del imaginario jurídico tradicional tiene que ver con cómo se podrían financiar los creadores de contenido. Actualmente, un creador de YouTube prevé sus ingresos en función de una fracción de los ingresos por publicidad que generen sus vídeos. Con tecnologías como el BAT (*Basic Attention Token*), que inscribe sus movimientos en el *blockchain* de Ethereum, la relación de fuerzas cambia; los usuarios reciben *tokens* cuando ven anuncios, los creadores reciben *tokens* cuando son vistos y los anunciantes pueden usar *tokens* para promocionarse, pudiendo ser estos tres roles ejercidos por una misma persona. Como citan en su *whitepaper*, BAT supone un sistema "basado en blockchain de anuncios digitales", una manera de medir la atención e intercambiarla como un bien. Con esta propuesta, el negocio de internet pasa de ser bicameral (entre quienes se anuncian a través de creadores, y los usuarios que obtienen contenido a cambio de publicidad) a convertirse en una relación retroalimentada. En términos de equivalencia, ya no hay distinción entre una "inversión" en publicidad y decir que un vídeo "te gusta". La naturaleza de la atención, se use como se use (para vender, como creador, como audiencia), es la misma y se representa por un activo común: "el bono básico de atención". Y así las cosas, de cualquier acción, ya sea iniciar una campaña promocional o darle las gracias a un autor, queda fe pública de que sucedió en un registro donde cada firmante tiene una identidad que lo avala (potencialmente anónima, pero concreta). De este modo, se hace también difícil falsificar la actividad en red; pues las cifras son más confiables si no hay un único ente que las gestiona, y se pueden evitar casos como que Facebook mintiese a sus anunciantes sobre el número de visitas de los vídeos subidos a su plataforma[21].

Este paradigma cercena los últimos veinte años de comercio en red. En oposición, los nodos centralizadores (a saber, Facebook, Amazon y Google en mayoría) han construido un negocio que se basa en monitorizar la actividad de los usuarios para venderles bienes y servicios en sus momentos más vulnerables. En el caso de las "redes sociales" y Google, el negocio pasa directamente por alterar el flujo de informaciones para manipular su voluntad. Como explica van Dijk[22]:

> Tal vez irónicamente, mercantilizar las relaciones sociales —convertir *conexión* [humana] en *conectividad* mediante las tecnologías de programación— es exactamente lo que las plataformas corporativas, particularmente Google y Facebook, descubrieron como el huevo dorado que su ganso había producido. Además de generar contenido, la producción colectiva genera un sub-producto que los usuarios no dan intencionadamente: datos conductuales y para perfiles.

En este modelo el dinero solo fluye en una dirección (de anunciantes a plataformas), esperando que se recupere la inversión fuera del canal de promoción. Con la propuesta del BAT, son los propios espectadores quienes costean la atención, poniéndose al nivel de los anunciantes y desoyendo a los intermediarios, obligando a las plataformas a replantear la diferencia entre quienes consumen el contenido y quienes lo costean, y a decidir su lugar dentro del nuevo paradigma. Es más; el hecho de que la atención sea tomada como referencia clave del valor de las interacciones, en lugar de serlo el dinero prometido a través de la esperada atención,

[21] Moore, 2016, September 23.
[22] van Dijk, 2013. La cursiva es mía.

constituye un incentivo para los creadores; que ven sus actos recompensados por un valor directo, no subsidiario de otro. Aunque, con lo dicho, hay que considerar también que la hegemonía la ostentan todavía las plataformas centralizadas, y que este modelo no se ha impuesto, entre otras razones porque en la especificación técnica de internet no se consideró un sistema de remuneración bidireccional desde su inicio (Lanier 2011).

Un sistema parecido es Mediachain, adquirido por Spotify en 2017, que utiliza una tecnología de contratos transparentes y descentralizados con tal de garantizar mayores ingresos para músicos, que además de poder tener una idea clara del contexto en el que firman también ven agilizados los medios de pago. Parece que una industria discográfica circunscrita a los despachos y los cazatalentos, a la idea de "firmar" con una discográfica, es demasiado ineficiente a la hora de gestionar un catálogo de artistas a escala mundial en la sociedad red (en términos de Castells[23], aquella sociedad "cuya estructura social está compuesta de redes potenciadas por tecnologías de la información y de la comunicación basadas en la microelectrónica.").

En otro orden de cosas, debemos considerar el impacto de las tecnologías *blockchain* en contextos donde las acciones de terceras partes deben ser monitorizadas. Es el caso de la industria de seguros, el transporte de mercancías y los dispositivos conectados a internet (*Internet of Things*). En cualquiera de estos escenarios, existen personas interesadas en que otros actores de su red circunscriban su conducta a unas limitaciones de naturaleza funcional o contractual que pueda ser revisada.

Si una agencia de seguros es capaz de certificar las acciones que sus asegurados han hecho públicas en un *blockchain* común, tanto las aseguradoras como los asegurados aumentan sus garantías contractuales y, en el caso de las aseguradoras, se protegen contra el fraude. Una implementación de tal magnitud podría considerar, por ejemplo, que la maquinaria de ciertas industrias comunicase por red cada una de las acciones de sus operadores, de la misma forma que Facebook o Google recopilan información cuando sus usuarios aprietan botones. Una monitorización técnica de todos los riesgos activos y de las acciones que se tomaron permite reconstruir los eventos con mayor certidumbre que la que ofrece un mero testimonio, o incluso una grabación.

Del mismo modo, un *blockchain* puede fiscalizar las acciones de aparatos más pequeños, y no necesita ser compartido fuera de la red de estos aparatos. Pongamos, por caso, una solución domótica donde cualquier dispositivo (persianas, electrodomésticos, puertas, cámaras, telefonillo, etc.) compartan en su red local las acciones que ejecutan. Esto crea una *interfaz* común sin duplicidades, que no depende de la relación de todos con todos sino de todos con un registro compartido. Así, los dispositivos podrían compartir recursos entre sí: encender el calentador cuando se abra la puerta pasadas las ocho de la tarde, pasar el robot aspiradora cuando la alarma no detecta movimiento, utilizar la televisión como disuasión si se ha abierto la puerta de la casa pero no la del portal, etc. La información de cada aparato se guardaría en los demás y su comportamiento sería homeostático, sin depender de un coordinador central como puede ser el teléfono móvil (en el caso de altavoces, iluminantes, etc. controlados por BlueTooth), lo que añade una pátina de seguridad en la medida en que la red domótica se autogestionaría y no necesitaría conectar los dispositivos directamente a internet; y, en el caso de hacerlo, podría mediar otro dispositivo como el teléfono para inscribir órdenes

[23] Castells, 2011, p. 27

en el *blockchain* en lugar de dejar los dispositivos enteros a merced de quien los encuentre. Sería como dejar en casa una lista de recados, y que los aparatos que reconocen tu letra le hiciesen caso conforme se ven capacitados. La alternativa, menos halagüeña, pasa porque cada dispositivo se establezca en la red como un nodo abierto susceptible de ser conectado desde cualquier parte del mundo, sin que las acciones que se le comandan queden inscritas, pudiendo así convertir dispositivos como una cámara en el dormitorio infantil en una herramienta al servicio de actores ilícitos. Si tal cámara transmitiese información cifrada sólo al dispositivo con una llave de cifrado válida, un potencial ladrón necesitaría antes hacerse con el teléfono móvil del atacado y deducir sus contraseñas; hoy en día, los "Google dorks" son instrucciones que se le pueden pasar a Google para descubrir cámaras privadas convertidas en públicas por estar mal configuradas.

A su vez, el comercio internacional puede beneficiarse enormemente de las "cadenas de bloques". Asumamos la inherente complejidad en el entramado de empresas, bienes y transportes a nivel mundial. Hablamos de millones de cargas con infinidad de subproductos dentro, con distintas naturalezas (como por ejemplo, si son perecederos o no), que deben circular por multitud de actores entre sus puntos de origen y destino. Un *blockchain* aplicado a las exportaciones permitiría un seguimiento público de los contenedores, haciendo más fácil localizar extravíos, así como computar almacenamientos compartidos. Un aumento considerable de la trazabilidad significa un aumento considerable de la certidumbre, acrecentada aún más si consideramos que las malas prácticas de algunos comerciantes quedarán a la vista de sus socios. En un contexto definido por diversos idiomas, culturas políticas y empresariales, y agendas secretas, canalizar dichas transacciones en un registro común contrarresta la entropía del sistema.

En cuanto a la censura, los *blockchains* tienen un papel tan protagónico en el movimiento *cypherpunk* como la "encriptación cebolla" de la red TOR. Por una parte hablamos de evitar el borrado de ciertas informaciones, mientras que el otro trata la privacidad de quienes manejan dichas informaciones. Si hablar de TOR significa considerar que cada intermediario entre dos ordenadores añadirá una capa de cifrado al mensaje con tal de ocultar los orígenes de los emisores, una "cadena de bloques" soluciona el problema inverso de este tipo de sistemas: la persistencia. Las tecnologías de cifrado han inaugurado formas de ocultar la información, pero a menudo obvian formas de que no se olvide nunca.

A tal fin, implementaciones como el IPFS (*InterPlanetary File System*) permiten subir archivos a un registro compartido, de forma que ciertos nodos puedan copiar la información y hacerla redundante, en una estructura creciente donde cada vez es más difícil hacer desaparecer algo. Los intentos de censura en dicha red sólo pueden tener dos consecuencias: el olvido de la información, o el "efecto Streisand"; ver la difusión de la información amplificada por los intentos de censura.

Con un sistema de tablas distribuidas, IPFS permite a los usuarios consultar las referencias a otros archivos, e incluso utilizar esas referencias para asociar los datos a otras plataformas que también se valen de tecnologías *blockchain*. Apoyado en otra "cadena de bloques" como Steem, que se define como "un blockchain social que hace crecer comunidades y hace posible el flujo inmediato de reventas para usuarios por premiarlos al compartir contenido", la plataforma D.Tube se postula como la antítesis de YouTube: un sistema de *streaming* de vídeo sin publicidad, curado por la comunidad, regulado por sus propias divisas

(DTC ó DTube Coin, y el VP ó Voting Power), y cuyos servidores están sostenidos por miembros participantes. El valor monetario creado al participar se puede cambiar por dinero bancario, cuando no almacenarlo para generar "Voting Power" (poder de participación) o "destruirlo" oficialmente para canjearlo por promoción dentro de la red. La suma de estos factores crea un sentido de comunidad *junto a* la plataforma, en lugar de *frente a*; desdibujando la idea paternalista de que un usuario se adscribe a una serie de términos legales estipulados por un servidor monolítico e inhumano.

Al contrario que en el "internet de las plataformas", estos modelos distribuidos exigen consigo *compartir*, por lo que la cultura de las empresas y sus usuarios tiende a volverse más altruista. Uno de los primeros ejemplos lo encontramos en las redes de compartición de archivos P2P sin *blockchain*, como pueden ser las redes GNutella y Bittorrent, en las que compartir se volvía un requisito moral, evaluado por el ratio entre la información enviada y la descargada. Una red centralizada se puede mantener mientras se mantengan suficientes conexiones entre el servidor y los usuarios como para mantener los costes del servidor, mientras que una red descentralizada exige del compromiso participativo de sus integrantes, pues son a la vez usuarios y proveedores.

Como último ejemplo, conviene tratar los procesos industriales y su cadena de valor. Pese a que en el sector servicios resulte, con frecuencia, difícil ponderar el valor de las acciones específicas de las empresas, los sectores primario y secundario se regulan por firmes indicadores de eficiencia (en inglés, *Key Performance Indicators*): el volumen de materia prima obtenida o convertida, el porcentaje de materia prima perdida en el proceso, los distintos procesos de construcción de las distintas piezas, el ensamblaje, el almacenado, los costes de estructura, etc. Por lo tanto, los procesos industriales son susceptibles de ser fiscalizados al completo dentro de una estructura que refleje cómo se construye el valor desde la obtención de los recursos para un objetivo y la consecución del objetivo.

De puertas para adentro, ello supone que cualquier empresa deje de depender de un ERP (*Enterprise Resource Planner*) centralizado y lo distribuya. En términos prácticos, la empresa que decida monitorizar sus procesos mediante una "cadena de bloques", en lugar de mediante un servidor central, se libera de que un único actor (la empresa que instaló su ERP) sea la estructura que aloja toda la inteligencia de negocio. Ello se traduce en una mayor facilidad para implementar innovación dentro de la compañía, en la medida en que cualquier tecnología ha de adaptarse a un sistema consensuado de código libre, con protocolos compartidos, en lugar de necesitar adaptar las máquinas a un ERP que podría convertirse más adelante en una limitación debido a su naturaleza privada. Y en otro orden, también permitiría poner en un mismo espacio todos los indicadores estratégicos, lo que facilitaría la correlación de datos con el fin de tomar decisiones. En suma, la empresa pasa a ser dueña de su inteligencia de negocio y a poder poner en común todos sus subsistemas, con el consiguiente ahorro.

Aunque el mayor valor de la tecnología *blockchain* aplicada a la industria se encuentra en considerar el proceso industrial como la suma de la actividad de varias empresas cuyos procesos están interconectados. Los vicios que pueden aparecer en cualquier sector son infinidad: proveedores que no proveen, subcontratas con laxos controles, ahorro en las calidades, utilización conjunta de tecnologías que no se pensaron para trabajar juntas, amaños contables, impagos, accidentes, etc. Pero si un sector en su conjunto decide compartir la

información del proceso que enriquece a todos, una importante cantidad de estos vicios desaparece.

Pongamos, por caso conocido, el de la industria tintométrica; donde hay una disparidad de opciones entre bases para pintura, pigmentos y máquinas. Con frecuencia, algunos tenedores de máquinas que venden pintura al público deciden utilizar pigmentos más económicos que pueden hacer fallar la máquina. Al tiempo, quienes proveen el *software* que opera las máquinas también comercializan los pigmentos más caros. El conflicto surge cuando un vendedor al por menor que intentó ahorrar en los pigmentos pretende que el proveedor de pigmentos al que no le compró le solucione el problema; en algunas ocasiones es un defecto de la máquina, cuando en otras tiene que ver con que la licencia del programa informático con las fórmulas químicas expiró. Sea cual sea el origen del conflicto, el caso es que ambas partes sostienen versiones distintas sobre un acuerdo de negocio definido por elementos claros: máquinas, contratos, pigmentos, *software*.

Si el destino de cada partida de pigmento y pintura base fuese anotado entre los socios comerciales en un registro compartido, al tiempo que cada máquina de pinturas inscribiese en el mismo *blockchain* cada vez que hace pintura, el proceso sería diáfano para todas las partes. Sería posible inspeccionar la “cadena de bloques”, escrutar paso por paso cómo un material ha sido extraído, transportado, tratado, vuelto a transportar, comercializado, recibido, mezclado, etc. No habría forma de intentar convencer a nadie de lo que debió pasar, porque cualquiera podría encontrar un conflicto de intereses inspeccionando las relaciones desde las materias primas hasta el consumidor final. Si una máquina falla y en una parte anterior del *blockchain* no existen registro de que se cargaron pigmentos legítimos, se puede aducir que se usaron materiales sin garantía; si el *software* expira y en el *blockchain* no hay huella de que se hayan usado los pigmentos de quien comercializa dicho *software*, no hay razón empírica que defienda que las licencias se han de renovar.

Sumado a este aumento de la transparencia y por ende de las garantías, cabe la posibilidad de concebir (ahora sí) cada una de esas acciones comunalizadas como la certificación de que se está creando *valor*, en términos monetarios. De esta forma, una empresa del sector primario o secundario podría acuñar una criptodivisa en paralelo a cada acción comercial. Este *token*, en lugar de medir la atención como el BAT o generar monedas resolviendo bloques de cómputo como Bitcoin, reflejaría la actividad industrial; y a mayor actividad, mayor potencial de generar valor, y más moneda creada. Y esta divisa, paralela a la actividad de su sector, podría usarse tanto como un valor especulativo dentro del mercado de las criptodivisas como una alternativa a concertar contratos con dinero bancario (esto es, que las empresas implicadas en procesos similares costearan sus acuerdos con la moneda que ellos mismos generan, cuyo valor se genera bajo criterios previamente consensuados, no arbitrarios).

Y en otra vuelta de tuerca, aún habría espacio para que la venta de las criptodivisas que estas empresas generasen pudiese servir para obtener capitalización en dinero bancario, con el objetivo de reinvertirlo en I+D.

CONCLUSIONES SOBRE LA CULTURA

Al margen de las merecidas consideraciones jurídicas, económicas y técnicas, la finalidad de lo expuesto es tratar los efectos culturales de las tecnologías *blockchain*.

Con lo dicho, cabe añadir que el planteamiento de las "cadenas de bloques" sigue siendo reconsiderado, por lo que no podemos asumir que sus efectos estén asentados. Con todo, sus distintas aplicaciones sugieren que los cambios sucederán en plural y en distintas áreas; no como un cambio unívoco de paradigma sino como una suma emergente de soluciones más eficientes, que irá modificando las relaciones en la medida en que compartir información las modifique.

Lo que queda claro es que, más allá de la complicación técnica de las implementaciones, las distintas aplicaciones humanas del concepto redefinen (y por tanto resignifican) las relaciones entre los actores de una red; mientras se mejoran los procesos y se hacen transparentes las funciones, los actores han de adaptar su efectividad a las exigencias colectivas, ahora compartidas como no lo eran antes. Y si hablamos de sistemas humanos, ello implica que los propios humanos se adapten al nuevo paradigma; en primera instancia, asumiendo que la imposición de una *blockchain* en sus mecanismos de acción obliga a asumir, axiomáticamente, esta tecnología como una nueva "institución cero" que replantea la forma de relacionarse con el medio.

Así, en términos culturales, las "cadenas de bloques" han alterado la forma en la que entendemos y nos relacionamos con el dinero, han puesto en cuestión la idea de valor tras el dinero fiduciario (una de nuestras instituciones hegemónicas), ponen en jaque la relación de los estados para con sus ciudadanos y diluyen el poder de las instituciones económicas para gestionar las divisas, amplían las relaciones civiles amparadas por el secretismo, mejoran las garantías en entornos compartidos, y dan cabida a una gran cantidad de aplicaciones industriales que desafían los aspectos de la cultura empresarial que se apoyan en decisiones políticas (fenómeno que, seguramente, se cobre con una gestión más tecnocrática).

En resumidas cuentas, la aparición de las tecnologías *blockchain* mejora las relaciones humanas en términos de transparencia y garantías.

Y por todo lo dicho, es preciso que nos cuestionemos como civilización el papel protagónico de la tecnología en la determinación de la naturaleza humana; dónde trazamos la frontera entre ser servidos y servir. Como propuesta, la visión crítica y el espíritu constructivo de Lanier (2014, p. 306-307, 362):

> La actitud hacker suele ser algo así: "abrid vuestras vidas a la 'net, vosotros gente ordinaria. El mundo está a punto de volverse transparente y la transparencia será el inicio de una era dorada. Compartir es bueno. *No obstante*, encripta tu vida como un loco. Una VPN, etc. Solo la gente más lista puede ser silenciosa en el bosque digital."
>
> Esta es básicamente una forma de decir que cuanto mayo sea tu habilidad con ordenadores, más derecho tienes de ser un individuo genuinamente en control de su propia vida. Pero nosotros los tecnologistas tenemos el deber de ayudar a la humanidad, en lugar de convertirnos en una clase privilegiada.
>
> [...]

Conforme la tecnología mejora, la economía tendrá que volverse menos abstracta. La Economía solía tratar acerca de los patrones de resultados que emergían de reglas que influenciaban el comportamiento humano en sociedad. Se enfocaba en la forma en la que las políticas engendraban resultados.

Pero cada año que pasa la economía debe enfocarse más y más en tratar el diseño de máquinas que medien en la conducta humana. Un sistema de información guía a la gente de forma más directa, detallada y literal que las políticas. Otra forma de verlo es que la economía debería convertirse en una versión a gran escala, sistémica, del diseño de interfaces de usuario.

FUENTES

Barlow, J. P. (1996) *A Declaration of the Independence of Cyberspace*.

Castells, M., & Bustillo, F. M. (2011). *La sociedad red : una visión globa*l. Alianza.

Daley, S. (2018, December 5). *25 blockchain applications & real-world use cases disrupting the status quo*. Built In. https://builtin.com/blockchain/blockchain-applications

El País. (2010, March 10). Repo/03/10/actualidad/1268209975_850215.htmlrtaje | El día que la burbuja "puntocom" pinchó. *El País*. https://elpais.com/economia/2010

Lanier, J. (2011) *You Are Not A Gadget*. Penguin Books.

Lanier, J. (2014). *Who owns the future?* Simon & Schuster Paperback.

Lanier, J. (2019). *Ten Arguments for Deleting Your Social Media Accounts Right Now*. Random House Uk.

May, C. T.. (1994) *Cyphernomicon*.

Moore, M. (2016, September 23). *Facebook has been lying about some VERY important statistics*. Express.co.uk. https://www.express.co.uk/life-style/science-technology/713624/facebook-lying-video-view-statistics-advertising-figures-discrepancy

Nakamoto, S. (2008, November 1). *Bitcoin P2P e-cash paper*. Www.Mail-Archive.com. https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. http://satoshinakamoto.me/bitcoin-draft.pdf

Peirano, M. (2019). *El enemigo conoce el sistema: manipulación de ideas, personas e influencias después de la economía de la atención*. Debate.

Riestra, L. (2014, May 24). *Lo que debes saber del día de la votación en España*. ABC. https://www.abc.es/elecciones-europeas/20140525/abci-elecciones-europeas-espana-201405241626.html

Rosic, A. (2017, March 7). *17 Blockchain Applications That Are Transforming Society.* Blockgeeks. https://blockgeeks.com/guides/blockchain-applications/

van Dijck, J. (2013). *The Culture of Connectivity*. Oxford University Press.

Viens, A. (2019, November 5). *Exploring the Practical Applications of Blockchain Technology*. Visual Capitalist. https://www.visualcapitalist.com/exploring-the-practical-applications-of-blockchain-technology/