

El impacto del blockchain en nuestras vidas será tan significativo
como el que representó la aparición de internet



LA REVOLUCIÓN BLOCKCHAIN

DESCUBRE CÓMO
ESTA NUEVA TECNOLOGÍA
TRANSFORMARÁ
LA ECONOMÍA GLOBAL

DON TAPSCOTT

Autor del bestseller Wikinomics

ALEX TAPSCOTT

*Posiblemente el mejor tratado
escrito hasta el momento
sobre blockchain.*

Del prólogo de ENRIQUE DANS,
profesor de innovación en IE Business School

DEUSTO

Índice

Portada

Dedicatoria

Citas

Prólogo, por Enrique Dans

Primera parte. Digamos sí a la revolución

Capítulo I. El protocolo fiable

Capítulo II. El futuro reiniciado: siete principios esenciales de la economía blockchain

Segunda parte. Transformaciones

Capítulo III. Reinventar los servicios financieros

Capítulo IV. Reformar la empresa por dentro y por fuera

Capítulo V. Nuevos modelos de negocio: ganar dinero con las blockchains

Capítulo VI. El "registro de las cosas": dar vida al mundo físico

Capítulo VII. La paradoja de la prosperidad: inclusión económica y empresa

Capítulo VIII. Reconstruir el Estado y la democracia

Capítulo IX. Una cultura libre con las blockchains: suena a gloria

Tercera parte. Promesa y peligro

Capítulo X. Superar obstáculos: diez desafíos que hay que afrontar

Capítulo XI. El liderazgo de la era que viene

Agradecimientos

Notas

Créditos

Gracias por adquirir este eBook

Visita [Planetadelibros.com](https://planetadelibros.com) y descubre una nueva forma de disfrutar de la lectura

¡Regístrate y accede a contenidos exclusivos!

Primeros capítulos

Fragmentos de próximas publicaciones

Clubs de lectura con los autores

Concursos, sorteos y promociones

Participa en presentaciones de libros

PlanetadeLibros

Comparte tu opinión en la ficha del libro
y en nuestras redes sociales:



Explora

Descubre

Comparte

*A Ana Lopes y Amy Welsman por haber hecho posible este libro y
por entender que «todo está en las blockchains»*

«Una obra maestra que analiza hábilmente el potencial que tiene la tecnología blockchain para hacer frente a los más importantes retos globales.»

HERNANDO DE SOTO, economista y presidente del Instituto para la Libertad y la Democracia, Perú.

«El sistema blockchain es a la confianza lo que internet a la información. Igual que el internet original, las cadenas de bloques tienen la capacidad de transformarlo todo. Leed este libro y lo entenderéis.»

JOICHI ITO, director del MIT Media Lab.

«En este extraordinario viaje a las fronteras de las finanzas, los Tapscott arrojan una luz nueva sobre el fenómeno blockchain y nos convencen de la necesidad de entender mejor su poder y su potencial.»

DAVE MCKAY, presidente y consejero delegado del Royal Bank de Canadá.

«*La revolución blockchain* analiza pormenorizadamente en qué consisten la promesa y el peligro del sistema blockchain de una manera a la vez accesible y erudita, permitiendo al lector echar una mirada privilegiada al futuro.»

ALEC ROSS, escritor, autor de *The Industries of the Future*.

«Si alguna vez ha habido un tema que clamaba por explicaciones, ese tema son las blockchains. Los Tapscott las explican de un modo comprensible y transmitiendo la emoción, el potencial y la importancia del fenómeno.»

BLYTHE MASTERS, consejera delegada de Digital Asset Holdings.

«Este libro tiene la capacidad de predicción de *1984* de Orwell y la visión de Elon Musk. Leedlo o extinguiólos.»

TIM DRAPER, fundador de Draper Associates, DFJ y Draper University.

«Las blockchains son como una gran ola tecnológica, y Tapscott, como siempre hace, esta vez con su hijo Alex, ha salido bien temprano a navegar. Magnífica travesía.»

YOCHAI BENKLER, catedrático Berkman de Derecho Empresarial de la Facultad de Derecho de la Universidad de Harvard.

«Si sois hombres de negocios o gobernantes, tenéis que entender la revolución blockchain. Nadie ha investigado mejor ni escrito un libro más interesante sobre el tema que los Tapscott.»

ERIK BRYNJOLFSSON, catedrático del MIT y coautor de *La carrera contra la máquina*.

«Un libro indispensable y actualizadísimo en el que se explica cómo la tecnología en la que se basa bitcoin podría —y debería— hacer posible una economía digital que distribuya realmente la riqueza.»

DOUGLAS RUSHKOFF, autor de *Present Shock* y *Throwing Rocks at the Google Bus*.

«Cambios tecnológicos que se desarrollaban a lo largo de una generación ocurren ahora en un abrir y cerrar de ojos, y nadie cuenta mejor esta historia que los Tapscott.»

ERIC SPIEGEL, presidente y consejero delegado de Siemens USA.

«Pocos líderes nos permiten ver lo que está a la vuelta de la esquina como lo hace Don Tapscott. Con *La revolución blockchain*, él y su hijo Alex nos instruyen, nos desafían y nos muestran una forma completamente nueva de pensar en el futuro.»

BILL MCDERMOTT, consejero delegado de SAP SE.

«*La revolución blockchain* es una excelente mezcla de historia, tecnología y sociología que abarca todos los aspectos del protocolo de las blockchains, un invento que con el tiempo puede revelarse tan trascendental como la imprenta.»

JAMES RICHARDS, autor de *Currency Wars* y *The Death of Money*.

«*La revolución blockchain* es como una guía de carreteras que nos permite movernos por el mundo del dinero digital, y que, a la vez que explica magistralmente el panorama actual, nos dirige hacia un sistema financiero global más justo, eficaz y conectado.»

JIM BREYER, consejero delegado de Breyer Capital.

«*La revolución blockchain* es la guía definitiva e indispensable para moverse por esta tecnología que cambiará el mundo.»

JERRY BRITO, director ejecutivo de Coin Center.

«Es realmente increíble. El análisis que los Tapscott hacen del sistema blockchain como modelo inclusivo en un mundo cada vez más centralizado es, a la vez, matizado y extraordinario.»

STEVE LUCZO, presidente y consejero delegado de Seagate Technology.

«Una vehemente defensa de la capacidad del blockchain de aumentar la transparencia pero también de asegurar la privacidad. En palabras de los autores, “el internet de la cosas necesita un archivo de la cosas”.»

CHANDRA CHANDRASEKARAN, consejero delegado y director gerente de Tata Consultancy Services.

«¡El epicentro de la confianza se extiende! La exposición definitiva de las posibilidades revolucionarias de un sistema descentralizado basado en la confianza.»

FRANK D’SOUZA, consejero delegado de Cognizant.

«Este libro identifica un nuevo movimiento tecnológico y lo conecta con la más profunda de las necesidades humanas: la confianza. Una investigación minuciosa y una escritura provocativa. Todos los hombres de negocios y políticos serios tienen que leerlo.»

BRIAN FETHERSTONHAUGH, presidente y consejero delegado de
OgilvyOne Worldwide.

«*La revolución blockchain* da las claves de un progreso tecnológico que no ha hecho más que empezar.»

FRANK BROWN, director gerente y jefe de operaciones de
General Atlantic.

«Un libro que hay que leer. Adquiriréis un profundo conocimiento de por qué el blockchain está convirtiéndose rápidamente en una de las más importantes tecnologías emergentes después de internet.»

PERIANNE BORING, fundadora y presidenta de la Cámara de
Comercio Digital.

«Cuando una tecnología generacional cambia el mundo en el que vivimos, tenemos mucha suerte de contar con cartógrafos como Don Tapscott y ahora su hijo Alex que nos expliquen hacia dónde vamos.»

RAY LANE, socio gerente de GreatPoint Ventures y socio
emérito de Kleiner Perkins.

«Don y Alex han escrito la guía definitiva para aquellos que quieran cruzar esta nueva y prometedora frontera.»

BENJAMIN LAWSKY, exsuperintendente de los Servicios
Financieros del estado de Nueva York y consejero delegado de
The Lawsky Group.

«*La revolución blockchain* es un importantísimo y esclarecedor manifiesto de la era digital que viene.»

DAN PONTEFRACCT, autor de *The Purpose Effect* y previsor jefe
de TELUS.

«El mejor y más completo libro de investigación sobre el descubrimiento tecnológico más apasionante que ha habido después de internet. Una obra de una claridad y una profundidad excepcionales.»

ANDREAS ANTONOPOULOS, autor de *Mastering Bitcoin*.

«*La revolución blockchain* explica e ilumina estupendamente el nuevo mundo feliz del dinero descentralizado que puede prescindir de la confianza.»

TYLER WINKLEVOSS, cofundador de Gemini and Winklevoss
Capital.

«Una visión fascinante —y tranquilizadora— de una tecnología que tiene el poder de transformar por completo la economía global. ¡Un gran libro!»

PAUL POLMAN, consejero delegado de Unilever.

Prólogo

Todo es blockchain. O al menos, todo lo será. Resulta relativamente sencillo llegar a esa conclusión a partir de una sencilla revisión de las noticias: a lo largo de los últimos meses, sin ir más lejos, podemos encontrar menciones sobre el papel fundamental y crucial de esta tecnología en las empresas de generación de energía, en la redefinición de la industria de la música, en la seguridad de la cadena de conservación de alimentos en distribución, en el futuro de la industria aseguradora, en el sector inmobiliario, en la eliminación de la corrupción en la política o, por supuesto, en la banca, entre muchas otras. Blockchain se ha convertido en la tecnología de infinitos usos, en el elemento a incorporar a todos los procesos, y en el cimiento sobre el que se edificará todo nuestro futuro. No importa a qué se dedique, su nivel de responsabilidad o la compañía para la que trabaje: de una manera u otra, puede estar seguro de que muchos de los elementos que manejará en su relación con el mundo estarán contruidos sobre la base de la tecnología blockchain.

Para una tecnología conceptualizada por primera vez en el año 2008 y vinculada originalmente a una aplicación tan difícil de aprehender como una criptomoneda digital, el bitcoin, el nivel de atención y de relevancia resulta completamente inusitado. En cierto sentido, la tarea más compleja que blockchain como tecnología ha tenido que superar es la de ser capaz de desprenderse de la complicada herencia que la vincula con bitcoin y ver cómo era rápidamente adoptada para aplicaciones de todo tipo. Y es que la idea de una criptomoneda no es simplemente compleja en apariencia, sino que además, cuestiona como tal la esencia de algo tan central en nuestras vidas como el dinero y los elementos que hacen que un billete de cien euros valga eso, cien euros, y no sea simplemente un pedazo de papel sin ninguna importancia. Tratar de explicar bitcoin a una audiencia, independientemente de su nivel intelectual, es en realidad muchísimo más difícil que explicarles el funcionamiento de una base de datos conectada, distribuida y descentralizada en miles o millones de ordenadores personales.

Blockchain es una revolución perfectamente comparable a la aparición del ordenador personal, o al desarrollo y popularización de internet. Es, posiblemente, uno de los cambios más importantes y fundamentales que vayamos a ver en nuestras vidas, con el potencial de cambiarlo todo. Uno de esos cambios que otorgan innumerables ventajas a aquellos capaces de entenderlo, de hacerse a la idea de sus implicaciones. En muy poco tiempo, he tenido la oportunidad de conocer a emprendedores y de evaluar ideas que aplican blockchain a temas tan absoluta y radicalmente variados como un registro de tierras en Ghana, un protocolo de seguridad para los dispositivos conectados a la internet de las cosas, o un sistema que convierte en obsoleto el sistema de patentes tal y como lo conocemos. Con un detalle adicional: esta tecnología une a su capacidad disruptiva, unas barreras de entrada sumamente bajas, que permiten que prácticamente cualquier

compañía, independientemente de su tamaño o sus recursos, pueda plantearse construir sobre ella. A estas alturas, con más de veintiséis años trabajando en innovación, creo que sé reconocer una disrupción cuando la veo. Y si blockchain no es una revolución, es que nunca hemos visto ninguna.

En muy poco tiempo, blockchain ha pasado de recibir la etiqueta de disruptiva, a pasar a considerarse la semilla fundamental para una nueva internet más segura, a ser capaz de crear el mayor superordenador jamás construido en la historia, o directamente, a cambiar el mundo tal y como lo conocemos. En un futuro no muy lejano, utilizaremos bases de datos descentralizadas y basadas en blockchain para cuestiones que irán desde decidir la hora a la que nos levantamos de la cama, pagar por el agua caliente que consumimos en la ducha, garantizar la seguridad de todos los aparatos conectados en nuestro hogar a la internet de las cosas, negociar con el robot que nos corta el césped del jardín, identificarnos en un vehículo autónomo que nos lleve a trabajar, hacer transacciones económicas de todo tipo con total seguridad y trazabilidad, enviar dinero a un amigo... la centralidad de blockchain en el mundo transaccional va a ser absoluta, hasta el punto de que no seremos capaces de plantearnos cómo de imperfecta, insegura e incómoda era nuestra vida antes de que esta tecnología viese la luz. De hecho, no sería de extrañar que, a medida que este papel central se va consolidando con mayor claridad, el desarrollo de blockchain como tecnología se hiciese acreedor de alguno de los grandes reconocimientos que identifican los elementos verdaderamente importantes que cambian el mundo, como un premio Nobel.

¿Le parece futurista? El mejor consejo que puedo darle es que no se quede con esa idea. Cada día más, los cambios más fundamentales e insospechados se incorporan a nuestras vidas con una velocidad vertiginosa, y se asimilan como si hubiesen estado siempre ahí, como si formasen parte del paisaje. La exclusión digital es ya mucho peor que el ostracismo. Pero es que además, en este caso, ni siquiera existe la posibilidad de considerarse excluido: en este caso, hablamos de una tecnología que formará parte de nuestras vidas lo queramos o no. En el futuro, no importará si estamos almacenando información en la red, firmando un contrato de cualquier tipo, asegurándonos la propiedad de una tecnología o votando en unas elecciones... en todos los casos, estaremos utilizando blockchain.

¿Cómo asimilar una tecnología con un potencial tan brutal como para afectar a directivos de cualquier industria, políticos o a todos los seres humanos sin excepción? ¿Qué resulta tan importante entender sobre ella, y cómo es posible que en tan poco tiempo se le atribuya el potencial de convertirse en la base de toda la economía digital, con elementos tan importantes como el incremento de la transparencia y el respeto a la privacidad? ¿Cómo enfrentarse a ideas que cuestionan y redefinen algunos de los que consideramos elementos básicos y fundacionales en los negocios, en las transacciones o en la confianza? ¿Cómo entender que una tecnología ha sido capaz de resolver todos los problemas inherentes a cualquier transacción, y ha conseguido que cualquiera pueda crear confianza gracias a un proceso de autenticación garantizado por la colaboración de muchos?

La primera cuestión es fundamental: entienda de qué estamos hablando. En ese sentido, el libro que tiene entre manos es, muy posiblemente, el mejor tratado escrito hasta el momento sobre blockchain a un nivel de comprensión razonablemente accesible. Pero no se limite a leerlo: además, trate de proyectar su actividad, su experiencia y sus conocimientos sobre lo que va leyendo y asimilando. Se encontrará un texto didáctico plagado de ejemplos, que explora no solo los hechos y sus consecuencias, sino también los problemas existentes, cómo se pueden resolver y las implicaciones de cada caso, de cada aplicación. Es, en realidad, un auténtico tratado, en toda la extensión de la palabra, un mapa para orientarse en la que es, sin duda, la tecnología emergente más relevante desde la aparición de internet.

Mire a su alrededor. A poco que consulte las fuentes adecuadas, se dará cuenta de que no es necesario que un profesor de innovación venga a contarle la relevancia de blockchain y las implicaciones que tendrá en el futuro: basta con que lea las noticias, con que hable con emprendedores o con que haga una simple búsqueda en internet. Sin embargo, pasar de la constatación de que algo es importante a entenderlo, a ver algo más que una nebulosa que envuelve todos los conceptos conocidos requiere algo más, un esfuerzo intelectual consciente. Para entender algo es fundamental querer entenderlo, partir de una voluntad sólida y de una disposición que permita enfrentarse sin desmayo a cuestiones que ha considerado prácticamente invariables desde las etapas más tempranas de su educación, desde el mismísimo parvulario. Y además, hace falta un mapa, una guía bien escrita y accesible que, partiendo de los elementos conocidos, le permita adentrarse en aquellos que no lo son tanto.

Considere este libro una especie de viaje iniciático cuyos frutos en términos de aprendizaje, va a valorar mucho en el futuro. Enfoque su lectura con rigor, con voluntad, con la decisión necesaria de quien acepta que le van a mover el suelo bajo sus pies. Cuanto antes sea consciente de ello, menos desprevenido se encontrará, más preparado estará, y más confianza tendrá en lo que se nos avecina. El futuro, más que nunca, es de los que invierten en comprenderlo.

ENRIQUE DANS
Profesor de Innovación en IE Business School

PRIMERA PARTE

Digamos sí a la revolución

Capítulo I

El protocolo fiable

Parece que el genio de la tecnología ha salido otra vez de la botella. Convocado por una o varias personas por motivos poco claros en algún momento de la historia, el genio se ha puesto ahora a nuestro servicio para dar un nuevo salto hacia delante: transformar el sistema del poder económico y el viejo orden de los asuntos humanos en algo mejor. Si es que queremos.

Expliquémonos.

Las primeras cuatro décadas de internet nos han traído el correo electrónico, la red informática global (*world wide web*), las empresas electrónicas, los medios sociales, la red móvil, el almacenamiento en la nube y los primeros días del «internet de las cosas». Internet ha servido para reducir los costes de investigar, colaborar e intercambiar información. Ha permitido la aparición de nuevos medios de comunicación y entretenimiento, de nuevas formas de comerciar y de organizar el trabajo, y de empresas digitales como nunca las ha habido. Gracias a la tecnología de sensores, ha incorporado inteligencia en nuestras carteras, en nuestra ropa, en nuestros automóviles, en nuestros edificios, en nuestras ciudades y hasta en nuestra biología. Está ocupando tanto nuestro entorno que pronto no será necesario «acceder» a la red porque trabajaremos y viviremos inmersos en una tecnología omnipresente.

En general, internet ha posibilitado muchos cambios positivos —para los que pueden acceder a la red—, pero tiene serias limitaciones para los negocios y la actividad económica. *The New Yorker* pudo publicar de nuevo la viñeta de Peter Steiner de 1993 en la que un perro le dice a otro: «En internet, nadie sabe que eres un perro». En línea, seguimos sin poder establecer de una manera fiable la identidad del otro ni confiar en él para intercambiar dinero sin el aval de un tercero, que suele ser un banco o el gobierno. Los mismos intermediarios almacenan nuestros datos e invaden nuestra intimidad por motivos de lucro o de seguridad nacional. Incluso con internet, los costes estructurales de dichos intermediarios excluyen a 2,5 millones de personas del sistema financiero global. Pese a la promesa de un mundo igualitario, los beneficios económicos y políticos han resultado ser asimétricos, y el poder y la prosperidad van para aquellos que ya los tienen, incluso si han dejado de buscarlos. El dinero hace más dinero del que hace mucha gente.

La prosperidad que la tecnología crea ya no es mayor que la intimidad que destruye. Con todo, en la era digital en la que estamos, la tecnología está en el centro de casi todo, para bien y para mal. Nos permite valorar y violar los derechos del prójimo como nunca antes ha ocurrido. El auge de la comunicación y del comercio en línea está creando más posibilidades para el cibercrimen. La «ley de Moore» de la duplicación anual de la

capacidad procesadora duplica el poder de defraudadores y ladrones —«Moore's Outlaws» o «Los forajidos de Moore»—,¹ por no hablar de emisores de correo basura (*spammers*), suplantadores de identidad (*phishers*), ciberespías, zombis, hackers, ciberacosadores y *datanappers* —delincuentes que lanzan *ransomware* y piden rescates por la información secuestrada— y demás.

En busca del protocolo fiable

En una fecha tan temprana como 1981 ya había expertos tratando de resolver con criptografía los problemas de privacidad, seguridad e inclusión que internet planteaba. Reformaran como reformasen el proceso, siempre se producían filtraciones, porque había terceras partes implicadas. Pagar con tarjeta de crédito en internet no era seguro porque los usuarios tenían que proporcionar mucha información personal, y las comisiones por pagos pequeños eran muy altas.

En 1993, un brillante matemático llamado David Chaum creó eCash, un sistema de pago digital que era «un producto técnicamente perfecto que permitía pagar por internet de manera segura y anónima... Servía perfectamente para enviar peniques y céntimos electrónicos por internet».² Era un sistema tan perfecto que Microsoft y otros pensaron en incluirlo en su software.³ El problema fue que a los compradores en línea no les preocupaba entonces la privacidad y seguridad en la red. La compañía neerlandesa de Chaum, DigiCash, quebró en 1998.

Por la misma época, uno de los socios de Chaum, Nick Szabo, escribió un artículo titulado «El protocolo de Dios», parafraseando la expresión «la partícula de Dios» con la que el premio Nobel Leon Lederman se refería a la importancia del bosón de Higgs en la física moderna. En su artículo, Szabo reflexionaba sobre la creación de un protocolo tecnológico ideal en el que Dios fuera el mediador fiable de todas las operaciones: «Todas las partes enviarían la información a Dios. Dios manejaría esa información y devolvería el resultado. Como Dios es la suma de la discreción y la confidencialidad, ninguna de las partes sabría de las demás más de lo que sabe de sí misma».⁴ Era una idea muy interesante: hacer negocios por internet requiere mucha fe. Como la infraestructura carece de la seguridad suficiente, muchas veces no tenemos más remedio que tratar con los intermediarios como si fuera dioses.

Una década después, en 2008, el sistema financiero global se hundió. Quizá aprovechando el momento, una persona o serie de personas, con el pseudónimo de Satoshi Nakamoto, esbozaron el protocolo de un nuevo sistema de pago electrónico directo y entre iguales (*peer-to-peer* o P2P) que usaba una criptomoneda llamada «bitcoin». Las criptomonedas (monedas digitales) se diferencian de la moneda tradicional en que no las crean ni las controlan los países. Este protocolo establece una serie de normas —en forma de computación distribuida— que garantiza la *integridad* de la información intercambiada entre esos miles de millones de ordenadores *sin pasar por terceros*. Esta circunstancia aparentemente sutil ha estimulado, asombrado y, en definitiva, cautivado la imaginación de los informáticos, efecto que se ha extendido

rápidamente a los negocios, a los gobiernos, a los defensores de la privacidad, a los activistas sociales, a los teóricos de los medios de comunicación y a los periodistas, por mencionar sólo unos pocos ámbitos.

«Todo el mundo exclama: “¡Dios mío, ya está! ¡Es el gran salto! Es lo que estábamos esperando”», dice Marc Andreessen, cocreador del primer navegador comercial, Netscape, y gran inversor en proyectos tecnológicos. «“Ha resuelto todos los problemas. Sea quien sea, merece el premio Nobel, porque es un genio.” ¡Esto es! Ésta es la red fiable distribuida que hacía falta en internet.»⁵

Hoy, gente sesuda de todo el mundo se pregunta por las implicaciones de un protocolo que capacita a simples mortales para crear confianza mediante códigos inteligentes. Esto nunca había ocurrido antes: nunca había habido transacciones fiables entre dos o más partes, autenticadas por la colaboración de muchos y posibilitadas por intereses colectivos, no por grandes empresas que buscan su beneficio.

Una plataforma global con la que podamos operar de modo seguro no será el Dios Todopoderoso, pero sí es algo muy grande. Lo llamaremos «protocolo fiable».

Este protocolo es el fundamento de un creciente número de registros globalmente distribuidos llamados *cadena de bloques (blockchain)*, el más grande de los cuales es bitcoin. Aunque el aspecto tecnológico es complicado y la expresión «blockchain» suena rara, la idea es sencilla. Las cadenas de bloques nos permiten enviar dinero de manera directa y segura de una persona a otra sin pasar por un banco, una tarjeta de crédito o PayPal.

Más que un internet de la información, es un internet del valor o del dinero. También es una plataforma que permite a todo el mundo saber lo que es verdad, al menos con respecto a la información que se registre de manera estructurada. En su forma más básica, es un código fuente libre: todo el mundo puede descargárselo gratuitamente, ejecutarlo y usarlo para desarrollar nuevas herramientas de gestión de transacciones en línea. Como tal, nos da la posibilidad de crear infinidad de aplicaciones nuevas y de cambiar muchas cosas.

El funcionamiento del registro mundial

Los grandes bancos y algunos gobiernos están usando cadenas de bloques a modo de registros distribuidos con la idea de revolucionar la manera de almacenar información y realizar transacciones. Sus aspiraciones son loables: mayor velocidad, menores costes, más seguridad, menos errores y eliminación de puntos centrales que puedan atacarse o fallar. Estos modelos no suponen necesariamente el uso de criptomonedas.

Sin embargo, las blockchains más importantes y de mayor alcance se basan en el modelo de Satoshi. Veamos cómo funciona este modelo.

El bitcoin o cualquier otra moneda digital no se guarda en archivos que estén en un lugar concreto; está representado por transacciones que se registran en una cadena de bloques, que es una especie de hoja de cálculo o registro que usa los recursos de una amplia red entre iguales para verificar y aprobar todas y cada una de las transacciones hechas en bitcoin. Todas las cadenas de bloques, como la que usa bitcoin, están

distribuidas, es decir, se ejecutan en ordenadores que ofrecen voluntariamente personas de todo el mundo; no hay una base de datos central que pueda atacarse. La blockchain es *pública*: todo el mundo puede verla cuando quiera porque reside en la red, no en una determinada institución que se encargue de auditar las transacciones y llevar registros. Y además está *encriptada*: usa una encriptación que incluye claves públicas y privadas (en lugar de los sistemas de dos claves de las cajas fuertes) que garantizan una total seguridad. No tenemos que preocuparnos porque Target o Home Depot tengan malos *firewalls* o haya un miembro del personal de Morgan Stanley o del gobierno federal de Estados Unidos que sea un ladrón.

Cada diez minutos, como si fuera el ritmo cardiaco de la red del bitcoin, todas las transacciones realizadas se comprueban, ordenan y almacenan en un bloque que se une al bloque anterior, creándose así una cadena. Cada bloque debe referirse al bloque anterior para ser válido. Esta estructura registra exactamente el momento de las transacciones y las almacena, evitando que nadie pueda alterar el registro. Si queremos robar un bitcoin, tenemos que reescribir toda la cadena de bloques a la vista de todos, lo que es prácticamente imposible. Por eso las blockchains son un registro distribuido y suponen la conformidad de la red con todas las transacciones que se han realizado. Igual que la red informática global de la información, esto es el «registro informático global» del valor: un registro distribuido que todo el mundo puede descargar y ejecutar en su ordenador personal.

Algunos estudiosos han afirmado que la invención de la contabilidad por partida doble permitió el nacimiento del capitalismo y de la nación-Estado. Este nuevo registro digital de transacciones económicas puede programarse para asentar prácticamente todo lo que tenga valor e importancia para la humanidad: partidas de nacimiento y defunción, permisos de matrimonio, escrituras y títulos de propiedad, grados académicos, informes financieros, procedimientos médicos, demandas de seguros, votos, origen de los alimentos y cualquier otra cosa que pueda codificarse.

La nueva plataforma permite combinar registros digitales sobre casi cualquier cosa en tiempo real. De hecho, pronto habrá miles de millones de cosas inteligentes que percibirán, responderán, se comunicarán, comprarán su propia electricidad y compartirán información importante, en fin, que lo harán todo, desde proteger nuestro medio ambiente hasta cuidar de nuestra salud. Este «internet de todo» necesita un «registro de todo». Negocios, comercio y economía necesitan una computación digital.

¿Por qué preocuparnos, pues? Nosotros creemos que la verdad *puede* hacernos libres y que la confianza distribuida afectará profundamente a todos los aspectos de nuestra vida, tanto si somos amantes de la música que queremos que los artistas se ganen la vida con su arte, como consumidores que queremos saber de dónde viene la carne de la hamburguesa que nos comemos, inmigrantes hartos de pagar comisiones altísimas por enviar dinero a nuestros seres queridos en nuestra tierra ancestral, mujeres saudíes que queremos publicar nuestra propia revista de moda, trabajadores humanitarios que necesitamos identificar los títulos de propiedad de los propietarios para reconstruir sus casas después de un terremoto, ciudadanos cansados de la falta de transparencia y responsabilidad de los políticos, usuarios de medios sociales que valoramos nuestra

privacidad y pensamos que la información que generamos podría sernos provechosa. En este mismo momento, hay innovadores que están creando aplicaciones basadas en blockchains que sirven para todo esto. Y es sólo el comienzo.

Un entusiasmo razonable por las blockchains

No cabe duda de que la tecnología blockchain tiene profundas implicaciones en muchas instituciones. Esto explica el entusiasmo que ha despertado en muchas personas listas e influyentes. Ben Lawsky dejó su trabajo de superintendente de servicios financieros en el estado de Nueva York y fundó una asesoría del ramo. «En cinco o diez años, el sistema financiero será irreconocible... Y yo quiero formar parte del cambio», dice.⁶ Blythe Masters, que fue directora financiera y de Global Commodities del banco de inversiones JP Morgan, creó una empresa de tecnología blockchain con la idea de cambiar la industria. En la portada de *Bloomberg Markets* de octubre de 2015 aparecía Masters con un titular que decía: «Las blockchains son todo». Ese mismo mes, *The Economist* publicaba un reportaje titulado «La máquina fiable», en el que se decía que «la tecnología en la que se basa bitcoin podría cambiar el funcionamiento de la economía».⁷ Para *The Economist*, la tecnología blockchain es «el mejor modo de estar seguro de las cosas». Bancos de todo el mundo contratan a los mejores expertos en tecnología para que investiguen los nuevos modelos. A los banqueros les gusta que las transacciones sean seguras, fáciles e instantáneas, pero algunos retroceden ante la idea de un sistema abierto, descentralizado y con nuevas modalidades monetarias. La industria de los servicios financieros ya ha rebautizado y privatizado la tecnología blockchain y la llama «tecnología del registro distribuido», en un intento por reconciliar lo mejor de bitcoin —seguridad, rapidez y bajos costes— con un sistema completamente cerrado cuyo uso requiere el permiso de los bancos o las entidades financieras. Consideran que las blockchains constituyen bases de datos más fiables que las que antes tenían, y que permiten a los principales actores —compradores, vendedores, depositarios y reguladores— llevar registros compartidos e indelebles, con la consiguiente reducción de costes, disminución de riesgos y eliminación de puntos centrales susceptibles de fallo.

Invertir en empresas de tecnología blockchain está de moda, como lo estuvo invertir en empresas electrónicas en los noventa. Los inversores de riesgo muestran un grado de entusiasmo que haría palidecer a un inversor en empresas electrónicas de los noventa. Sólo en 2014 y 2015 más de 1.000 millones de dólares de capital de riesgo fueron a parar al incipiente sistema blockchain, y las inversiones casi se duplican cada año.⁸ «Estamos seguros», dice Marc Andreessen en una entrevista para *The Washington Post*, «de que dentro de veinte años hablaremos de esta tecnología como ahora hablamos de internet».⁹

Los reguladores se han puesto en guardia y han formado grupos de trabajo para estudiar qué tipo de legislación puede aplicarse. Gobiernos autoritarios como el de Rusia han prohibido o limitado drásticamente el uso de bitcoins, como lo han hecho Estados democráticos que deberían haber escarmentado, como Argentina, que ha tenido varias crisis monetarias. Gobiernos occidentales más alertados están intentando entender cómo la nueva tecnología podría transformar no sólo el sistema de bancos centrales y la

naturaleza del dinero, sino también la actuación de los gobiernos y la naturaleza de la democracia. Carolyn Wilkins, la gobernadora adjunta del Banco de Canadá, cree que es hora de que los bancos centrales de todo el mundo consideren seriamente la posibilidad de pasar todos los sistemas monetarios nacionales a moneda digital. Andrew Haldane, economista jefe del Banco de Inglaterra, ha propuesto la creación de una moneda digital nacional para el Reino Unido.¹⁰

Corren tiempos excitantes. En la creciente legión de entusiastas no faltan oportunistas, especuladores y delincuentes. Lo primero que la mayoría de la gente oye cuando se habla de dinero digital es la historia de la bancarrota de la plataforma de cambio Mt. Gox o la de la condena de Ross William Ulbricht, fundador de la empresa de «criptomercado» o mercado de la «web oscura» (*darknet market*) Silk Road, intervenida por el FBI por tráfico de drogas y armas y pornografía infantil y que usaba la tecnología bitcoin como sistema de pago. El precio del bitcoin ha fluctuado drásticamente y la propiedad de bitcoins sigue estando concentrada. Un estudio de 2013 mostraba que 937 personas poseían la mitad de todos los bitcoins, aunque esto ya está cambiando.¹¹

¿Cómo pasamos de la pornografía y del «esquema Ponzi» a la prosperidad? Para empezar, no es bitcoin, que sigue siendo una moneda especulativa, lo que debería interesarnos, salvo que seamos comerciantes. Este libro versa sobre algo mucho más grande que el dinero. Versa sobre el poder y el potencial de la plataforma tecnológica en la que bitcoin se basa.

Esto no significa que bitcoin o las criptomonedas no sean importantes en sí mismas, como han dicho algunos que quieren desvincular sus proyectos de los escandalosos negocios del pasado. Estas monedas son fundamentales para la revolución de las blockchains, que consiste en la posibilidad de intercambiar valor, sobre todo dinero, de manera directa y entre iguales.

La confianza en la era digital

En el mundo de los negocios la confianza consiste en esperar que la otra parte se comporte de acuerdo con los cuatro principios de la integridad: honradez, consideración, responsabilidad y transparencia.¹²

La **honradez** no es sólo una prenda moral; se ha convertido en un factor económico. Para establecer relaciones de confianza con empleados, socios, clientes, accionistas y público, las empresas han de ser veraces y escrupulosas y facilitar la información en todo momento. No deben mentir omitiendo datos, ni confundir creando complejidad.

La **consideración** en los negocios significa muchas veces un intercambio justo de beneficios o perjuicios entre unas partes que operan de buena fe. Pero la confianza requiere un genuino respeto por los intereses, deseos y sentimientos ajenos, y que las partes puedan relacionarse con buena voluntad.

La **responsabilidad** significa contraer compromisos claros con las partes implicadas y atenerse a ellos. Tanto los individuos como las instituciones deben demostrar que cumplen sus compromisos y responden ante las promesas que quebrantan, permitiendo

que esas mismas partes implicadas o expertos independientes verifiquen sus operaciones. No pueden escurrir el bulto ni entrar en un cruce de acusaciones.

La **transparencia** significa operar abiertamente, a la luz del día. La pregunta «¿qué esconden?» es señal de poca transparencia que lleva a desconfiar. Claro está que las empresas tienen derecho legítimo al secreto empresarial y demás formas de información confidencial. Pero cuando se trata de información que parecería pertinente a clientes, accionistas, empleados y demás actores, una transparencia activa es fundamental para ganarse su confianza. Más que taparse para tener éxito, las empresas deben destaparse para eso mismo.

La confianza en los negocios y en otras instituciones es, en general, menor que nunca. Según un estudio de 2015 realizado por la empresa de relaciones públicas Edelman, la confianza en las instituciones, sobre todo en las empresas, ha caído a niveles como los existentes en el peor momento de la gran recesión de 2008. Edelman observa que incluso la industria tecnológica, sector en otro tiempo intachable y que sigue siendo el que más confianza inspira, registra, por primera vez, caídas en la mayoría de los países. Los consejeros delegados y los funcionarios estatales siguen siendo las fuentes de información menos fiables, a mucha distancia de los expertos procedentes del ámbito académico o industrial.¹³ Igualmente, Gallup, en su encuesta de 2015 sobre la confianza de los estadounidenses en las instituciones, informó de que los «negocios» ocupaban el segundo lugar más bajo de las quince instituciones estudiadas; menos del 20 por ciento de los encuestados decían que tenían un nivel medio o alto de confianza. Sólo el Congreso estaba por debajo.¹⁴

En el mundo anterior a la tecnología blockchain, la confianza en las transacciones venía de individuos, intermediarios u otras entidades que actuaban con integridad. Como muchas veces no podemos conocer a la otra parte, ni menos aún si es íntegra, tenemos que fiarnos de terceros no sólo para que respondan de desconocidos, sino también para que registren las transacciones y operen con la lógica propia del comercio en línea. Estos poderosos intermediarios —bancos, gobiernos, PayPal, Visa, Uber, Apple, Google y otros grupos empresariales— se llevan gran parte del valor.

En el incipiente mundo de las blockchains la confianza viene de la red e incluso de objetos que hay en esa red. Carlos Moreira, de la empresa de seguridad criptográfica WISEKey, dice que las nuevas tecnologías delegan la confianza incluso en cosas físicas. «Si un objeto, tal como el sensor de una torre de comunicaciones, una bombilla o un cardiógrafo, no es fiable y puede no funcionar bien o no pagar por los servicios que recibe, será rechazado por los demás objetos automáticamente.»¹⁵ El registro mismo es el fundamento de la confianza.¹⁶

Para ser claros, digamos que la «confianza» se refiere a la compraventa de bienes y servicios y a la integridad y protección de la información; no significa confianza en todo tipo de negocios. Pero, como veremos a lo largo de este libro, un registro global de información fidedigna puede contribuir a que nuestras instituciones sean más íntegras y el mundo más seguro y fiable. En nuestra opinión, las empresas que realicen parte de sus operaciones o todas ellas en el sistema blockchain verán aumentar rápidamente su cotización. Accionistas y ciudadanos querrán que todas las empresas y organismos

públicos gestionen sus fondos, como mínimo, en el sistema blockchain. Con el incremento de la transparencia, los inversores sabrán si un consejero delegado merece o no la pingüe prima que recibe. Los contratos inteligentes que este sistema establezca exigirán que las partes cumplan con sus compromisos y los votantes verán si sus representantes son honrados o actúan con integridad fiscal.

El regreso de internet

La primera era de internet arrancó con la energía y el espíritu de un joven Luke Skywalker: con la creencia de que cualquier niño procedente de un planeta desértico podía derrotar un imperio del mal y crear una nueva civilización lanzando una empresa electrónica. Cosa ilusa, sin duda, pero mucha gente, incluidos los que esto escriben, esperaron que internet, tal como lo encarnaba la red informática mundial, transformaría un mundo industrial en el que el poder lo tenían unos pocos y cuyas estructuras eran difíciles de escalar y aún más difíciles de derribar. A diferencia de los viejos medios de comunicación, centralizados y controlados por fuerzas poderosas, y cuyos usuarios eran pasivos, los nuevos medios estaban distribuidos y eran neutrales, y todo el mundo era un participante activo en lugar de un receptor pasivo. Unas comunicaciones baratas y entre iguales contribuirían a socavar las tradicionales jerarquías y a incluir en la economía global a ciudadanos de países en vías de desarrollo. El valor y la reputación se fundarían en la calidad de lo que cada cual aportara, no en su condición socioeconómica. Si en la India había una persona lista y con ganas de trabajar, por su mérito ganaría una buena reputación. El mundo sería más llano, más meritocrático, más flexible y más fluido. Y, lo más importante, la tecnología contribuiría a la prosperidad de todos, no a la riqueza de unos pocos.

Algo de esto ha ocurrido. Ha habido colaboraciones masivas como Wikipedia, Linux o Galaxy Zoo. Modelos de negocio en red y la contratación externa han permitido a gentes de países en vías de desarrollo participar más en la economía global. Hoy día, dos mil millones de personas colaboran como si fueran socialmente iguales. Todos tenemos acceso a la información como nunca antes la habíamos tenido.

Pero el imperio del mal contraataca. Ya está claro que una serie de poderes concentrados en negocios y gobiernos han sometido a su voluntad la original estructura democrática de internet.

Ahora, grandes instituciones controlan y poseen estos nuevos medios de producción y de interacción social: su infraestructura subyacente, los masivos y crecientes tesoros de datos, los algoritmos que gobiernan cada vez más los negocios y la vida cotidiana, el mundo de las aplicaciones, las extraordinarias capacidades incipientes, el aprendizaje automático y los vehículos autónomos. Desde Silicon Valley y Wall Street hasta Shanghái y Seúl, esta nueva aristocracia usa su privilegiada posición para explotar la más extraordinaria tecnología jamás concebida y hacer de las personas actores económicos, adquirir fortunas espectaculares y reforzar su poder e influencia sobre economías y sociedades.

Muchos de los peores temores que los primeros pioneros de la era digital tuvieron se han hecho realidad.¹⁷ Vemos que en la mayoría de los países desarrollados el producto interior bruto (PIB) crece pero sin que se produzca el correspondiente crecimiento del empleo. Vemos que se crea cada vez más riqueza y que la desigualdad social crece también cada vez más. Empresas tecnológicas poderosas han pasado mucha actividad de la red abierta, distribuida e igualitaria, a aplicaciones cerradas o patentadas que sólo permiten la lectura y que, entre otras cosas, impiden la colaboración. Determinadas empresas se han apropiado de muchas de estas tecnologías abiertas y democráticas y están usándolas para obtener un enorme beneficio.

Una consecuencia, al menos de todo ello, es que el poder económico se ha vuelto más suspicaz, se ha concentrado y atrincherado más. En vez de hacer que los datos se distribuyan más general y democráticamente, los acumulan y explotan unas pocas entidades que, a menudo, los usan para controlar más y adquirir más poder. Si uno acumula información y el poder que esa información conlleva, puede fortalecer más su posición mediante la producción de conocimiento patentado. Este privilegio tiene ventaja sobre el mérito, venga de donde venga.

Además, poderosos «conglomerados digitales», como Amazon, Google, Apple y Facebook —que al principio fueron empresas emergentes de internet— están apoderándose de esos tesoros de datos que ciudadanos e instituciones generan muchas veces en «silos» privados en lugar de en la red. Esto, aunque beneficia mucho a los consumidores, tiene como consecuencia que esa información se convierta en una nueva clase de activo financiero, y que nuestra idea tradicional de la privacidad y la autonomía individual se vea subvertida.

Gobiernos de todas clases usan internet para mejorar operaciones y servicios, pero ahora también emplean la tecnología para controlar y hasta manipular a los ciudadanos. En muchos países democráticos los gobiernos utilizan las tecnologías de la información y de la comunicación para espiar a los ciudadanos, cambiar la opinión pública, favorecer sus intereses particulares, limitar derechos y libertades y, en general, mantenerse en el poder. Gobiernos represores como los de China e Irán limitan el uso de internet y lo utilizan para atacar a la disidencia y movilizar a los ciudadanos en defensa de sus objetivos.

Esto no significa que la red esté acabada, como algunos han sostenido. La red es vital para el futuro del mundo digital y todos nosotros deberíamos apoyar a los que se esfuerzan por defenderla, como hace la Fundación World Wide Web, que lucha por mantenerla abierta, neutral y en constante evolución.

Ahora, con la tecnología blockchain, se ha abierto un mundo de nuevas posibilidades que pueden invertir estas tendencias. Ahora disponemos de una plataforma verdaderamente igualitaria que hace posibles todas esas apasionantes cosas de las que hablamos en este libro. Cada cual puede ser dueño de su identidad y de sus datos personales. Podemos realizar transacciones, crear e intercambiar valor sin que intermediarios poderosos hagan de árbitros del dinero y la información. Miles de millones de personas excluidas podrán incorporarse pronto a la economía global. Podemos proteger nuestra intimidad y rentabilizar nuestra propia información. Podemos estar

seguros de que los creadores son retribuidos justamente por su propiedad intelectual. En lugar de querer resolver los problemas de la creciente desigualdad social mediante la redistribución de la riqueza solamente, podemos empezar cambiando el modo como la riqueza se *distribuye*: cómo se crea en origen, porque gentes de todas clases, desde granjeros hasta músicos, pueden beneficiarse más de la riqueza que crean. Se abren horizontes que parecen ilimitados.

Es más Yoda que Dios. Pero este nuevo protocolo, si no es divino, nos permite colaborar con confianza en un mundo que lo necesita, y eso ya es mucho. Estamos entusiasmados, sí.

Nuestro avatar personal y la caja negra de la identidad

En el transcurso de la historia, cada nuevo medio de comunicación ha permitido a la humanidad trascender el tiempo, el espacio y la mortalidad. Esta —nos atrevemos a decir— divina capacidad suscita una y otra vez, inevitablemente, la cuestión existencial de la identidad: ¿Quiénes somos? ¿Qué significa ser humano? ¿Cómo nos conceptuamos a nosotros mismos? Como Marshall McLuhan observó, el medio acaba convirtiéndose en el mensaje. Las personas damos forma al medio y éste nos da forma a nosotros. Nuestro cerebro se adapta. Nuestras instituciones se adaptan. La sociedad se adapta.

«Hoy necesitamos que un organismo con derechos nos preste una identidad, en forma de tarjeta bancaria, tarjeta de pasajero frecuente o tarjeta de crédito», dice Carlos Moreira, de WISeKey.¹⁸ Nuestros padres nos pusieron un nombre, la obstetra o la comadrona que nos trajo al mundo nos tomó las huellas del pie para identificarnos, registró nuestro peso y altura y dio fe de la hora, fecha y lugar de nuestro nacimiento firmando nuestra partida de nacimiento. Ahora pueden registrar esta partida de nacimiento en una blockchain y vincular con él avisos natalicios y una cuenta de ahorro para cuando vayamos a la universidad. Parientes y amigos pueden contribuir con bitcoins a nuestra enseñanza superior. Desde ese momento, nuestros datos empiezan a circular.

En los albores de internet, Tom Peters escribió: «Somos nuestros proyectos».¹⁹ Quería decir que nuestras afiliaciones corporativas y condición laboral ya no nos definían. Igual de verdad es decir hoy: «Somos nuestros datos». El problema, dice Moreira, es que «esa identidad es ahora nuestra, pero los datos que genera la interacción de esta identidad con el mundo los poseen otros».²⁰ Así es como la mayoría de las empresas e instituciones nos ven, por la estela informativa que dejamos en internet. Reúnen esa información y forman una imagen virtual de nosotros, y a este «yo virtual» nuestro le ofrecen nuevas y extraordinarias prestaciones que nuestros padres no habrían imaginado ni en sus mejores sueños.²¹ Pero estas ventajas tienen un precio: la privacidad. Los que dicen que «la privacidad ha muerto, olvidémosla» se equivocan.²² La privacidad es el fundamento de las sociedades libres.

«La gente tiene una idea muy simple de la identidad», dice el teórico de las blockchains Andreas Antonopoulos.²³ Usamos la palabra *identidad* para referirnos al yo, a la proyección de ese yo en el mundo y a todos los atributos que asociamos con ese yo o con una de sus proyecciones. Estas proyecciones pueden venir de la naturaleza, del

Estado, de organizaciones privadas. Podemos tener uno o más roles y una serie de atributos ligados a esos roles, y los roles pueden cambiar. Pensemos en nuestro último trabajo. ¿Cambió nuestro rol de manera natural a causa de los cambios que había que hacer en el trabajo o porque se revisó la descripción de nuestro trabajo?

¿Y si nuestro «yo virtual» —nuestro avatar personal— lo poseyéramos en realidad nosotros y «viviera» en la caja negra de nuestra identidad de manera que pudiéramos rentabilizar el flujo de nuestra información y revelar sólo lo que quisiéramos revelar cuando hiciéramos valer un derecho concreto? ¿Por qué nuestro carné de conducir contiene más información de la que supone haber aprobado el examen correspondiente y demostrado que somos capaces de conducir? Imaginemos una nueva era de internet en la que nuestro avatar personal manejara y protegiera el contenido de nuestra caja negra. Este fiel criado informático podría dar solamente el detalle o la cantidad que se nos pidiera en cada situación y al mismo tiempo limpiar las migajas de información que dejáramos al navegar por el mundo digital.

Esto puede sonar a ciencia ficción como la que se ve en películas como *Matrix* o *Avatar*. Pero hoy la tecnología blockchain lo hace posible. Joseph Lubin, consejero delegado de Consensus Systems, se refiere a esta idea llamándola «identidad digital persistente e imagen» en una blockchain. «Yo doy una imagen de mí mismo cuando estoy con mis amigos de universidad y otra cuando hablo en el Banco de la Reserva Federal de Chicago», dice. «En la economía digital en línea representaré los varios aspectos de mi persona, e interactuaré en ese mundo desde una plataforma de diferentes imágenes de mí mismo.» Lubin espera tener una «imagen canónica», la versión de sí mismo que paga impuestos, obtiene préstamos y contrata seguros. «Podré tener también una imagen de hombre de negocios y una imagen de familia para separar los intereses que yo decida vincular con mi imagen canónica. Puedo tener una imagen de jugador que no quiera asociar a mi imagen de hombre de negocios. Incluso podría tener una imagen en la web oscura que nunca pudiera vincularse a las otras.»²⁴

Nuestra caja negra puede incluir información como el carné de identidad, el número de la seguridad social, información médica, cuentas de proveedores de servicios, cuentas bancarias, diplomas, licencias profesionales, partidas de nacimiento y demás credenciales, así como información personal que no queramos revelar pero sí rentabilizar, como nuestras preferencias sexuales o nuestra condición médica, en una encuesta o una investigación. Podríamos dar esta información para determinados usos por parte de determinadas entidades durante periodos de tiempo determinados. Podríamos enviar parte de nuestros atributos a nuestro médico de cabecera y otra parte al fondo de inversión en el que quisiéramos invertir. Nuestro avatar podría contestar preguntas de sí o no sin revelar quiénes somos: «¿Tienes veinte años o más? ¿Has ganado más de 100.000 dólares anuales en los últimos tres años? ¿Es normal tu índice de masa corporal?»²⁵

En el mundo físico, nuestra reputación es local: nuestro tendero, nuestro jefe, los amigos con los que cenamos tienen cierta opinión de nosotros. En la economía digital, la reputación de las varias identidades de nuestro avatar será portátil. Esto contribuirá a incorporar a gente de todo el mundo a la economía digital. Africanos con una cartera y un avatar digitales podrán adquirir la reputación necesaria para, por ejemplo, pedir un

préstamo con el que montar un negocio. «Mirad: toda esta gente me conoce y responde por mí. Soy de fiar, financieramente hablando. Soy un ciudadano emancipado y formo parte de la economía digital global.»

La identidad es sólo una parte de esto. Lo demás es una nube —una identidad nubosa— de partículas poco o muy vinculadas a nuestra identidad. Si intentamos registrar todas estas partículas en una blockchain, un registro inmutable, perdemos no sólo el matiz de la interacción social sino también el don de olvidar. Nunca deberíamos ser definidos por nuestro peor día.

Un plan de prosperidad

En este libro leerá el lector decenas de historias sobre iniciativas posibilitadas por este protocolo de confianza que crea nuevas oportunidades para un mundo más próspero. Prosperidad, por encima de todo, significa elevar el nivel de vida. Para ello, la gente necesita disponer de medios, herramientas y oportunidades para crear riqueza material y crecer económicamente. Pero nosotros creemos que incluye más cosas: seguridad personal, salud, educación, sostenibilidad medioambiental, oportunidades para labrarnos y controlar nuestro destino y participar en la economía y en la sociedad. Para prosperar, un individuo necesita tener, como mínimo, acceso a alguna forma de servicio financiero básico que le permita acumular y mover valor con seguridad, capacidad de comunicación, herramientas transaccionales con las que conectarse a la economía global, seguridad, protección y garantía del derecho a la tierra y a otros bienes que posea legalmente.²⁶ Esto y más es lo que prometen las blockchains. Las historias que el lector leerá pintarán un futuro en el que haya prosperidad para todos, no sólo más riqueza y poder para los ricos y los poderosos. Quizá incluso sea un mundo en el que cada cual será dueño de sus datos y podrá proteger su privacidad y seguridad personal. Un mundo abierto en el que todos podremos contribuir a crear nuestra propia infraestructura tecnológica, en lugar de un mundo de «jardines vallados» (*walled gardens*) en los que grandes compañías ofrezcan aplicaciones patentadas. Un mundo en el que miles de millones de personas excluidas podrán participar en la economía global y beneficiarse de su liberalidad. Veamos cómo sería.

Una economía realmente igualitaria

Los expertos se refieren a menudo a Airbnb, Uber, Lyft, TaskRabbit y otras plataformas como «economía colaborativa» (*sharing economy*). Es una bonita idea: que personas iguales creen valor y participen de él. Pero estas empresas tienen poco que ver con la idea de colaborar y compartir. De hecho, triunfan precisamente porque no comparten: agregan. Es una economía de agregación. Uber es una empresa de 65.000 millones de dólares que agrega servicios de transporte. Airbnb, la preferida de Silicon Valley, que vale 25.000 millones de dólares, agrega viviendas. Otros agregan herramientas y gente mañosa a través de sus plataformas centralizadas y patentadas y luego las revenden. En el proceso, recaban información con fines de explotación comercial. Ninguna de estas compañías

existía hace una década porque no se daban las condiciones tecnológicas para ello: omnipresentes teléfonos inteligentes, GPS y sistemas de pago sofisticados. Ahora existe una tecnología —la blockchain— que nos permitirá reinventar de nuevo estas industrias. Los grandes revolucionarios de hoy están a punto de ser revolucionados.

Imaginemos que, en lugar de la empresa centralizada Airbnb, tenemos una aplicación distribuida —que podemos llamar «blockchain Airbnb» o «bAirbnb»—, que es esencialmente una cooperativa cuya propiedad es de sus miembros. Cuando queremos alquilar algo, el software de bAirbnb repasa la blockchain y muestra aquello que responde a nuestros criterios. Como la red crea un registro de la transacción en la cadena, una opinión positiva de un usuario mejora nuestra reputación y establece nuestra identidad, sin ningún intermediario. Dice Vitalik Buterin, fundador de la blockchain Ethereum: «Mientras que la mayoría de las tecnologías tiende a automatizar a los trabajadores para que hagan tareas serviles en la periferia, las de blockchain automatizan las operaciones para que el centro desaparezca. En lugar de echar a un taxista de un trabajo, el sistema blockchain echa a Uber y permite que el taxista trabaje directamente con el cliente».²⁷

Un sistema financiero más rápido e incluyente

La industria de los servicios financieros hace que nuestra economía global hierva de actividad, pero el sistema está hoy plagado de problemas. Por ejemplo, es seguramente la industria más centralizada del mundo y la última que siente los efectos transformadores de la revolución tecnológica. Bastiones del viejo orden financiero, como los bancos, hacen lo imposible por defender sus monopolios y muchas veces obstaculizan las innovaciones reformadoras. Además, el sistema financiero funciona con una tecnología obsoleta y se regula por leyes que se remontan al siglo XIX. Abunda en contradicciones y evoluciona desigualmente, lo que lo hace a veces lento, muchas veces inseguro y, casi siempre, opaco a muchos de los que participan en él.

La tecnología del registro distribuido puede liberar muchos servicios financieros de la jaula de las viejas instituciones, así como promover la competencia y la innovación. Esto es bueno para el usuario final. Incluso estando conectadas al viejo internet, miles de millones de personas están excluidas de la economía por la simple razón de que las instituciones financieras no ofrecen servicios como el bancario porque serían clientes poco rentables y que suponen un riesgo. Con el sistema blockchain, estas personas no sólo están conectadas, sino —y más importante— incluidas en la actividad financiera, y capacitadas para comprar, prestar, vender y, en fin, medrar en la vida.

Otras instituciones como éstas pueden transformarse a sí mismas gracias a la tecnología blockchain, siempre que tengan la voluntad de hacerlo. La tecnología es una gran promesa de revolución de la industria para bien, desde bancos a bolsas, desde compañías de seguros a asesorías contables, pasando por agencias de corretaje, microprestamistas, redes de tarjetas de crédito, agencias inmobiliarias y demás. Cuando todo el mundo comparte el mismo registro distribuido, las operaciones no tardan días, se

verifican instantáneamente y todos podemos verlo. Miles de millones de personas se beneficiarán de ello, y este cambio puede liberar y ayudar a emprendedores de todo el mundo.

Protección global de los derechos económicos

Los derechos de propiedad están tan inseparablemente unidos a nuestro sistema de democracia capitalista que en el primer borrador de la Declaración de Independencia de Estados Unidos que escribió Thomas Jefferson figuraban como derechos inalienables del hombre «el derecho a la vida, el derecho a la libertad y el derecho a la búsqueda de la *propiedad*», no de la felicidad.²⁸ Aunque estos grandes principios sentaron las bases de la economía y la sociedad modernas de las que disfrutamos en muchos países desarrollados, hasta ahora gran parte de la población mundial no se ha beneficiado de ellas. Y aunque se han hecho progresos en los capítulos de la vida y la libertad, la mayoría de los propietarios del mundo ven cómo unos funcionarios corruptos les confiscan sus casas o sus tierras arbitrariamente, con sólo darle a una tecla de sus ordenadores conectados a la base de datos centralizada del Estado. Sin una prueba de titularidad, los propietarios de tierra no pueden pedir préstamos, conseguir una licencia de obras ni vender la propiedad, y pueden ser expropiados, todo lo cual es un serio impedimento para la prosperidad.

El economista peruano Hernando de Soto, presidente del Instituto para la Libertad y la Democracia y una de las mentes más destacadas en el terreno de la economía, afirma que al menos 5.000 millones de personas en todo el mundo están impedidas de participar plenamente en el valor que la globalización crea porque los derechos de propiedad de sus tierras están poco garantizados. El sistema blockchain, dice, puede cambiar esto. «La idea fundamental de este sistema es que los derechos de propiedad pueden ser comercializados, tanto si son bienes financieros como bienes raíces o ideas. La meta es registrar no simplemente la parcela de tierra sino los derechos unidos a ella, de manera que no puedan ser violados.»²⁹ Unos derechos de propiedad universales pueden sentar las bases de un nuevo modelo de justicia global, crecimiento económico, prosperidad y paz. En este nuevo paradigma los derechos están protegidos no por armas, ni por milicias, ni por soldados, sino por la tecnología. «El sistema blockchain es para un mundo gobernado por cosas reales, no por cosas ficticias. Y creo que eso es bueno»,³⁰ dice De Soto. Y es un sistema descentralizado. No hay una autoridad central que lo controle, todo el mundo sabe lo que está ocurriendo y todo queda grabado para siempre.

El fraude de los giros postales

Casi todos los informes, artículos y libros que hablan de los beneficios de las criptomonedas ponen en duda el sentido de los giros postales. Y con mucha razón. El mayor flujo de dinero que llega a los países en vías de desarrollo no es de ayuda extranjera ni de inversiones directas de otros países, sino de dinero girado a los países pobres por los miembros de sus diásporas. El proceso de poner un giro requiere tiempo,

paciencia y, a veces, valor para ir todas las semanas al mismo barrio de mala muerte en el que está la oficina y pagar el mismo 7 por ciento de comisión. Hay una forma mejor de hacerlo.

Abra y otras compañías están construyendo redes de pago con el sistema blockchain. La idea de Abra es convertir a todos sus usuarios en cajeros de banco. Todo el proceso — desde que el dinero sale de un país hasta que llega a otro— tarda una hora y no una semana, y la comisión es del 2 por ciento y no del 7 por ciento y más. Abra espera que los usuarios de su red superen en número a todos los cajeros automáticos del mundo. Western Union tardó ciento cincuenta años en tener 500.000 agentes en todo el mundo. Abra tendrá un número igual de cajeros en su primer año.

Burocracia y corrupción de la ayuda extranjera

¿Podría el sistema blockchain resolver los problemas de la ayuda extranjera? El terremoto de Haití de 2010 fue uno de los desastres naturales más mortíferos que se conocen. Entre cien mil y doscientas mil personas murieron. Tras el terremoto, el gobierno de Haití resultó ser un lastre. La comunidad mundial donó más de 500 millones de dólares a la Cruz Roja, organización muy conocida. Una investigación posterior reveló que parte del dinero se malgastó o desapareció de una u otra forma.

El sistema blockchain puede mejorar la entrega de ayuda extranjera suprimiendo a los intermediarios que reciben la ayuda antes de que llegue a su destino. En segundo lugar, como es un registro inmutable del flujo de capital, el sistema blockchain obliga a las instituciones a responsabilizarse más de sus acciones. Imaginemos que pudiéramos seguir cada dólar que damos a la Cruz Roja desde que sale de nuestro teléfono hasta que llega al beneficiario. Podríamos dejar nuestro dinero en depósito e ir donando conforme la Cruz Roja fuera cumpliendo objetivos.

Ayuda a los que crean valor

En la primera generación de internet muchos creadores de propiedad intelectual dejaron de recibir las debidas compensaciones por ella. Los primeros fueron los músicos y compositores que tenían contratos con casas discográficas que no habían imaginado cómo afectaría internet a la industria del ramo. No fueron capaces de apuntarse a la era digital y reinventar sus modelos de negocio, y poco a poco fueron cediendo el control a distribuidores en línea innovadores.

Fijémonos en la reacción que tuvieron las grandes casas discográficas con Napster, la plataforma de música compartida lanzada en 1999. Las grandes empresas de la industria musical se unieron para demandar a la plataforma, a sus fundadores y a *dieciocho mil usuarios*, y la plataforma se desmanteló en julio de 2001. Alex Winter, realizador de un documental sobre Napster, declaró a *The Guardian*: «No me gusta pensar en términos de blanco o negro cuando se trata de grandes cambios culturales... En el caso

de Napster, había mucho gris entre la postura de los que decían: “Puedo compartir todo aquello que he comprado” y la de los que decían: “Eres un delincuente incluso si compartes uno solo de los archivos que hayas comprado”». ³¹

Estamos de acuerdo. Crear con los consumidores suele ser un negocio más sostenible que demandarlos. El caso puso el foco en la industria de la música y dejó ver lo anticuado de sus prácticas comerciales, la ineficiencia de las grandes distribuidoras y lo que algunos calificaron de políticas contra los músicos.

Muy poco ha cambiado desde entonces. Hasta ahora. Pensamos en el nuevo sistema musical que está surgiendo con el protocolo de las cadenas de bloques, encabezado por la cantautora británica Imogen Heap, la violonchelista Zoë Keating y desarrolladores y emprendedores de tecnología blockchain. Todas las industrias culturales están listas para la revolución, y la promesa es que los creadores serán plenamente compensados por el valor que creen.

Una empresa reinventada como motor del capitalismo

Con la creación de una plataforma igualitaria y global en la que podamos proteger nuestra identidad, tener confianza, adquirir una reputación y realizar transacciones, podremos por fin reformar profundamente las estructuras empresariales a fin de innovar, crear valor compartido y posiblemente generar prosperidad para muchos y no sólo riqueza para unos pocos. Esto no significa que las empresas serán más pequeñas en lo que a ingresos o impacto se refiere. Al contrario, estamos hablando de crear empresas del siglo XXI, que podrán producir una riqueza masiva y ser poderosas en sus mercados respectivos. Pensamos que las empresas serán más como redes que como las jerarquías verticales de la era industrial. Por eso tendremos la posibilidad de distribuir (no redistribuir) la riqueza de una manera más democrática.

También pasaremos al lector por el asombroso mundo de los contratos inteligentes, los nuevos agentes económicos autónomos y lo que nosotros llamamos «las empresas autónomas distribuidas» en las que un software inteligente se ocupa de administrar y organizar muchos recursos y funciones, desplazando en muchos casos a las empresas. Los contratos inteligentes permiten crear lo que nosotros llamamos «empresas reticulares abiertas», que se basan en nuevos modelos de negocio o en modelos viejos pero reinventados con el sistema blockchain.

Objetos vivos y en acción

Tecnólogos y escritores de ciencia ficción llevan mucho tiempo imaginando un mundo en el que una red global de sensores conectados por internet registrara todos los sucesos, acciones y cambios que se produjeran en el mundo. La tecnología blockchain permitirá que las cosas colaboren, intercambien unidades de valor —energía, tiempo y dinero— y reconfiguren cadenas de suministros y procesos de producción según la información compartida sobre demanda y capacidad. Podemos incorporar metadatos a dispositivos

inteligentes y programarlos para que reconozcan otros objetos por los metadatos de éstos y actúen o reaccionen ante determinadas circunstancias sin riesgo de error o manipulación.

A medida que el mundo físico cobre vida, todos podremos prosperar, desde el modesto y remoto granjero australiano que necesita electricidad para su negocio hasta propietarios de viviendas de todo el mundo que pueden participar de una red eléctrica distribuida con tecnología de cadenas de bloques.

Los empresarios de tecnología blockchain

Los empresarios son esenciales para que la economía crezca y la sociedad prospere. Se suponía que internet iba a liberarlos, facilitándoles las herramientas y prestaciones que tienen las grandes compañías y evitándoles muchos de sus lastres, como son la cultura heredada, los procesos anquilosados y los pesos muertos. Pero el prometedor éxito de empresas electrónicas multimillonarias esconde una inquietante verdad: el número de empresas y nuevos negocios ha descendido constantemente en muchas economías desarrolladas en los últimos treinta años.³² En el mundo desarrollado, internet ha hecho poco por facilitarles las cosas a los nuevos empresarios, que han de soportar pesadas burocracias estatales. Internet tampoco ha liberado las herramientas financieras necesarias para emprender negocios que podrían montar miles de millones de personas. No todos tenemos que convertirnos en empresarios, claro, pero incluso a las personas normales y corrientes que quieren ganarse un sueldo decente, la falta de instrumentos financieros y el mucho papeleo se lo ponen muy difícil.

Es una cuestión compleja, pero el sistema blockchain puede contribuir al fomento de la empresa y, en consecuencia, a la prosperidad de muchas e importantes formas. Una persona normal que viva en un país en vías de desarrollo sólo necesita un dispositivo con acceso a internet para disponer de un depósito de valor fiable y de la posibilidad de hacer negocios más allá de su comunidad. Tener acceso a la economía global significa tener acceso a nuevas formas de crédito, financiación, proveedores, socios y oportunidades de inversión. Ningún talento ni recurso es tan pequeño que no pueda rentabilizarse con el sistema blockchain.

Un gobierno del pueblo para el pueblo

Preparémonos también para ver grandes cambios en los gobiernos y en las formas de gobierno. La tecnología blockchain ya está revolucionando los mecanismos de gobierno y haciendo posible que rindan mejor y más barato, así como creando nuevas posibilidades de cambiar la democracia misma, al permitir que los gobiernos sean más abiertos, estén más libres del control de los grupos de presión y se comporten con arreglo a los cuatro principios de la integridad. Pensamos que las tecnologías blockchain pueden cambiar lo que significa ser ciudadano y participar en el proceso político, desde votar y acceder a los

servicios sociales hasta resolver muchos de los grandes y arduos problemas que tiene la sociedad, pasando por pedir cuentas a nuestros representantes de las promesas por las que los elegimos.

Promesa y peligro de la nueva plataforma

Si hay seis millones de personas en la «ciudad desnuda»,³³ entonces hay seis millones de obstáculos para que esta tecnología desarrolle plenamente su potencial. Además, tiene algunos peros preocupantes. Hay quien dice que esta tecnología no está hecha para el común de los mortales; que es difícil de usar, y que ya empiezan a surgir las llamadas «aplicaciones asesinas» (*killer applications*). Otros critican la ingente cantidad de energía que se gasta en alcanzar consenso sólo en la red de bitcoin: ¿qué pasará cuando miles o incluso millones de blockchains interconectadas procesen cada una miles de millones de transacciones diarias? ¿Son los incentivos tan grandes como para que la gente participe y actúe correctamente, sin que acabe intentando apoderarse de la red? ¿Acabará la tecnología blockchain con el empleo?

Estas cuestiones tienen que ver con el liderazgo y la capacidad de gestión, no con la tecnología. La primera era de internet arrancó porque sus principales actores —gobiernos, organizaciones civiles, desarrolladores y gente normal y corriente— tuvieron visión e intereses comunes. El sistema blockchain requiere un liderazgo parecido. En este libro hablamos largo y tendido de la necesidad de que los líderes de este nuevo paradigma distribuido lo defiendan y provoquen una ola de innovación económica e institucional a fin de que esta vez la promesa se cumpla. Invitamos al lector a que forme parte de este movimiento.

Este libro surgió del programa Redes para Soluciones Globales de la Facultad de Administración y Dirección de Empresas Rotman de la Universidad de Toronto, dotado con 4 millones de dólares. Financiado principalmente por grandes empresas tecnológicas, además de por las fundaciones Rockefeller y Skoll, el Departamento de Estado estadounidense e Industry Canada, el programa exploraba nuevas formas de resolución de problemas y de gestión globales. Los dos nos ocupamos de llevar a cabo el programa (Don lo creó, Alex dirigió el proyecto en criptomonedas). En 2014 lanzamos una iniciativa que duró un año sobre la revolución que suponía el sistema blockchain y las consecuencias que tenía en los negocios y la sociedad, iniciativa que culminó en este libro. En él hemos tratado de considerar con perspectiva la promesa y el peligro de la nueva plataforma.

Si hombres de negocios, gobiernos e innovadores de la sociedad civil lo hacen bien, pasaremos de un internet regido principalmente por los costes decrecientes de investigar, coordinar, recabar información y tomar decisiones —en el que lo más importante era controlar, mediar y rentabilizar información y transacciones en la red— a un internet regido por los costes decrecientes de negociar, controlar y hacer cumplir los acuerdos sociales y comerciales, en el que lo más importante será la integridad, la seguridad, la colaboración, la privacidad de todas las transacciones y la creación y distribución de valor. Es un cambio de estrategia de ciento ochenta grados. El resultado puede ser una

economía igualitaria con instituciones realmente distribuidas, inclusivas y participativas, o sea, legítimas. Si cambiamos radicalmente lo que podemos hacer en línea, la manera de hacerlo y la forma de participación de las personas, la nueva plataforma puede incluso crear las condiciones que nos permitan afrontar algunos de nuestros más serios desafíos sociales y económicos.

Si lo hacemos mal, la tecnología blockchain, que encierra tantas promesas, será frenada e incluso impedida. Peor aún, podría convertirse en un instrumento que usaran instituciones poderosas para proteger su riqueza o, si los gobiernos se apoderasen de ella, en una nueva forma de control social. Las tecnologías de software distribuido, criptografía, agentes autónomos e incluso inteligencia artificial, estrechamente relacionadas entre sí, podrían írsenos de las manos y volverse contra nosotros, sus creadores humanos.

Es posible que esta nueva tecnología se vea dificultada, detenida, poco utilizada o algo peor. El sistema blockchain y las criptomonedas, en particular bitcoin, están ahora en pleno auge, pero no podemos predecir si triunfarán o no, ni con qué rapidez lo harán, si fuera el caso.³⁴ Hacer predicciones siempre es arriesgado. Dice el teórico tecnológico David Ticoll: «Muchos nos equivocamos al predecir el impacto que tendría internet. No supimos ver fenómenos perversos como el Estado Islámico, y algunas de las grandes predicciones optimistas resultaron falsas». Y añade: «Si el sistema blockchain es tan grande y universal como la red, también nos equivocaremos si predecimos sus pros y sus contras».³⁵

Por eso, en lugar de predecir el futuro de este sistema, abogamos por él. Decimos que debe triunfar porque puede ayudarnos a entrar en una nueva era de prosperidad. Creemos que la economía funciona mejor cuando funciona para todos, y esta nueva plataforma es un motor de inclusión. Reduce drásticamente los costes de traspasar dinero, por ejemplo, con giros postales. Facilita tener una cuenta bancaria, obtener crédito e invertir. Apoya la empresa y la participación en el comercio global. Cataliza un capitalismo distributivo, no un capitalismo redistributivo.

Todos deberíamos dejar de oponernos a él y hacer lo posible por impulsarlo. Aprovechemos esta fuerza no para el beneficio inmediato de unos pocos, sino para el duradero beneficio de muchos.

Hoy, los que esto escriben están entusiasmados con el potencial que ofrece esta nueva fase de internet. Nos apasiona la gran ola de innovación que está desencadenándose y la posibilidad que da de conseguir un mundo más próspero y mejor. Con este libro queremos que el lector se interese, entienda esta nueva ola y actúe para que estas promesas se cumplan.

¡Conque agárrese el lector y siga leyendo! Estamos en una de esas tesituras cruciales de la historia humana.

Capítulo II

El futuro reiniciado: siete principios esenciales de la economía blockchain

«La libertad se basa en la privacidad», dijo Ann Cavoukian, directora ejecutiva del Privacy and Big Data Institute de la Universidad de Ryerson. «Esto lo aprendí hace treinta años en Alemania, cuando empecé a asistir a conferencias. No es casualidad que Alemania sea el primer país del mundo en protección de la privacidad y la información. Tuvieron que sufrir los abusos del Tercer Reich y la total supresión de las libertades, que empezó con la total eliminación de su privacidad. Cuando terminó, dijeron: “Nunca más”.»³⁶

Por eso es irónico —o muy lógico— que una de las primeras plataformas informáticas descentralizadas e igualitarias que garantizan la privacidad del usuario se llame Enigma, que es como se llamaba la máquina desarrollada por el ingeniero alemán Arthur Scherbius para transcribir información codificada. Scherbius diseñó Enigma para uso comercial: con este aparato, las compañías mundiales podían comunicarse rápida y seguramente secretos comerciales, instrucciones bursátiles y demás información confidencial. En pocos años, el ejército alemán empezó a fabricar su propia versión de Enigma para enviar por radio mensajes en clave a las tropas. Durante la guerra, los nazis usaron Enigma para comunicar planes estratégicos, dar detalles de objetivos y coordinar ataques. Fue un instrumento de sufrimiento y opresión.

Nuestro Enigma de hoy es un instrumento de libertad y prosperidad. Diseñado por Guy Zyskind y Oz Nathan en el Media Lab del Instituto Tecnológico de Massachusetts (MIT), el nuevo Enigma combina las virtudes del registro público de las blockchains, cuya transparencia «da fuertes incentivos para comportarse honradamente», con algo conocido como *cifrado homomórfico y computación participativa segura*.³⁷ Dicho lisa y llanamente: «Enigma coge nuestra información —cualquier información—, la trocea y la cifra en unidades de datos que distribuye al azar por los nodos de la red. No está en un único lugar», dice Cavoukian. «Enigma usa la tecnología blockchain para incrustar los datos y rastrear todas las unidades de información.»³⁸ Podemos compartirla con terceros y estos terceros pueden usarla en computaciones sin tener que descifrarla.³⁹ Si funciona, podría cambiar por completo la manera de gestionar nuestra identidad en línea. Tendríamos una caja negra con nuestra información personal que sólo nosotros controlaríamos y a la que sólo nosotros tendríamos acceso.

Por muy bonito que parezca, la criptografía es un terreno por el que hay que andar con pies de plomo. Primero, porque se necesita crear una vasta red de participantes. Segundo, porque «la criptografía es un ámbito en el que más vale no echar las campanas al vuelo, porque la historia nos enseña que algoritmos que todo el mundo cree seguros y

llevan usándose cuatro o cinco años, de pronto resulta que un científico inspirado dice que tienen un fallo y todo se viene abajo», decía Austin Hill, de Blockstream. «Por eso preferimos ser cautos y usar algoritmos bien establecidos cuya validez esté demostrada. Esto tiene mucho mucho futuro, y bitcoin se diseñó con eso en mente.»⁴⁰

Con todo, la idea merece ser tomada muy en serio, porque tiene profundas consecuencias en la privacidad, la seguridad y la sostenibilidad. «Enigma ofrece lo que, según ellos, garantiza la privacidad», dice Cavoukian. «Esto es decir mucho, pero es lo que necesitamos cada vez más en este mundo conectado e interconectado.»⁴¹

En nuestra investigación nos encontramos con muchos proyectos iniciados con tecnología blockchain cuyos desarrolladores tenían las mismas aspiraciones de hacer valer derechos humanos básicos: no sólo el derecho de la privacidad y de la seguridad, sino también el derecho de la propiedad, del reconocimiento de nuestra condición legal de personas, de la participación en el gobierno, la economía y la cultura. Imaginemos una tecnología que pudiera preservar nuestra libertad de elegir por nosotros mismos y por nuestras familias, de expresar esas elecciones en el mundo y de controlar nuestro destino, independientemente del lugar en el que vivamos o nacimos. ¿Qué nuevas herramientas y trabajos podríamos crear con estas capacidades? ¿Qué nuevos negocios y servicios? ¿Cómo podría crear oportunidades? Las respuestas están ahí delante, gracias a Satoshi Nakamoto.

Los siete principios esenciales

Creemos que esta era que viene podría inspirarse en la visión de Satoshi Nakamoto, que gira en torno a una serie de principios implícitos y que el espíritu colaborativo de muchos apasionados e igualmente talentosos líderes de la comunidad ha materializado.

Su gran visión se limitaba al dinero y no tenía el objetivo más grande de crear una segunda generación de internet. La cuestión no era reinventar la empresa, cambiar nuestras instituciones ni transformar la civilización. Sin embargo, la visión de Satoshi era asombrosa por su sencillez, originalidad e intuición de la humanidad. Todos los que leyeron el artículo de 2008 tuvieron claro que iba a empezar una nueva era de la economía digital. Si la primera era de la economía digital nació por una combinación de la informática y de las tecnologías de la comunicación, esta segunda sería resultado del inteligente concurso de la ingeniería informática, las matemáticas, la criptografía y la economía del comportamiento.

El cantante de folk Gordon Lightfoot cantaba: «Si pudieras leer mi mente, amor, ¡lo que mis pensamientos te dirían!». Satoshi lleva sin dar señales de vida desde 2011 (aunque su nombre sigue apareciendo de cuando en cuando en los foros de debate), pero nosotros creemos que el protocolo fiable que él concibió responde a los principios que pueden guiarnos para reconfigurar nuestras instituciones y nuestra economía.

Todas las personas con las que hemos hablado han querido compartir con nosotros sus ideas sobre el sistema blockchain. En todas las conversaciones, libros blancos, diálogos de foros han surgido una serie de temas de los que nosotros hemos extraído unos principios generales que pueden guiarnos a la hora de crear software, servicios, modelos

de negocio, mercados, organizaciones y hasta gobiernos con tecnología blockchain. Satoshi nunca escribió sobre estos principios, pero están implícitos en la plataforma tecnológica que él creó. Creemos que son los principios que informarán la siguiente era de la economía digital, una era de confianza renovada.

Si el lector es nuevo en este campo, esperamos que estos principios le ayuden a entender los fundamentos de la revolución de las blockchains. Si es un redomado escéptico respecto del sistema blockchain bitcoin, dichos principios pueden servirle si en el futuro se propone ser un empresario, inventor, ingeniero o artista que busque colaboración creativa con gente afín, o un propietario o inversor en activos de cualquier tipo, o un ejecutivo que quiera replantearse su función en esta incipiente economía de las blockchains.

1. Integridad en la red

Principio: La confianza es intrínseca, no extrínseca. La integridad está cifrada en todas y cada una de las etapas del proceso y distribuida, y no depende de cada miembro individualmente. Los participantes pueden intercambiar valor directamente, confiados en que los demás actuarán con integridad. Esto significa que los valores de la integridad — honradez de palabra y de acción, respeto por los intereses ajenos, responsabilidad por las consecuencias de nuestras decisiones y actos y transparencia a la hora de tomar decisiones y obrar— están codificados en derechos de decisión, estructuras de incentivos y operaciones de tal manera que comportarse sin integridad o es imposible, o cuesta mucho más tiempo, dinero, energía y reputación.

Problema que hay que resolver: En internet la gente no ha podido hacer transacciones o negocios directamente por la simple razón de que el dinero no es como otros bienes de información o de propiedad intelectual. Podemos enviar el mismo selfie a todos nuestros amigos, pero no debemos dar a un amigo nuestro un solo dólar que ya hayamos dado a otra persona. El dinero debe salir de nuestra cuenta e ir a la de nuestro amigo. No puede existir en los dos sitios, y no digamos en muchos sitios. Con lo cual existe el riesgo de que gastemos una unidad de dinero digital en dos sitios y uno de ellos nos lo devuelva como si fuera un cheque falso. A esto lo llamamos el «problema del doble gasto» (*double-spend problem*). Esto les va bien a los defraudadores que quieren gastar dos veces su dinero. Les va mal al destinatario del dinero devuelto y a nuestra reputación. Tradicionalmente, cuando hacemos pagos en línea, resolvemos el problema del doble gasto recurriendo a la base de datos de uno o varios terceros que autorizan la operación, como agencias de giros postales (Western Union), bancos comerciales (Citicorp), organismos gubernamentales (Commonwealth Bank of Australia), compañías de tarjetas de crédito (Visa) o plataformas de pago en línea (PayPal). La operación puede tardar días y hasta semanas en algunos lugares del mundo.

Posible solución: Satoshi usó una red distribuida entre iguales que ya existía y un poco de criptografía inteligente para crear un *mecanismo de consenso* que podría resolver el problema del doble gasto tan bien o mejor que un tercero fiable. En el sistema blockchain, la red registra el momento en el que se hace la primera transacción en la que

gastamos una unidad monetaria concreta y rechaza las transacciones subsiguientes en las que intentamos gastar esa misma unidad, con lo que impide que la gastemos dos veces. Los participantes de la red que ejecutan nodos de bitcoin plenamente operativos —llamados «mineros» (*miners*)— reúnen transacciones recientes, las registran en forma de bloque de datos y repiten el proceso cada diez minutos. Todos los bloques deben referirse al bloque anterior para ser válidos. Los protocolos incluyen un método que reserva espacio en el disco para que todos los nodos puedan almacenar la blockchain completa. Por último, las cadenas son públicas. Todo el mundo puede ver las transacciones que se realizan en el mismo momento en que se realizan. Nadie puede esconder ninguna, lo que hace que bitcoin pueda seguirse mejor que el dinero en efectivo.

Satoshi no sólo quería prescindir de la mediación de los bancos centrales, sino también eliminar la ambigüedad y las interpretaciones conflictivas de lo que ocurría. Que el código hable por sí mismo. Que la red busque algorítmicamente consenso sobre lo ocurrido, lo cifre y lo registre en forma de blockchains. El mecanismo para lograr consenso es fundamental. «El consenso es un proceso social», dice en su blog Vitalik Buterin, pionero de la blockchain Ethereum. «A los seres humanos se nos da bien llegar a acuerdos... sin tener que recurrir a algoritmos.» Explica que, cuando un sistema supera la capacidad de los individuos, la gente recurre al software. En redes de iguales, el algoritmo de consenso reparte el derecho a actualizar el estado de la red, es decir, de someter la verdad a votación. El algoritmo distribuye este derecho entre un grupo de iguales que constituye un «grupo económico», un grupo que se juega el pellejo, por así decirlo. Según Buterin, lo importante de este grupo económico es que sus miembros están distribuidos de manera segura: ninguno de ellos, ni solo ni con otros, debería poder superar a la mayoría, ni siquiera teniendo los medios y los incentivos para ello.⁴²

Para lograr consenso, la red bitcoin usa un mecanismo llamado «prueba de trabajo». Esto puede parecer complicado pero la idea es muy simple. Como no podemos basarnos en la identidad de los mineros para decidir quién crea el siguiente bloque, creamos un acertijo muy difícil de resolver (que cuesta mucho *trabajo* resolver), pero que es fácil de verificar (todo el mundo puede comprobar la solución muy rápidamente). Los participantes deciden de común acuerdo que el primero que resuelva el acertijo cree el siguiente bloque. Los mineros han de emplear recursos (hardware informático y electricidad) para encontrar el *hash* correcto —que es una especie de huella dactilar única de cada texto o archivo de datos— y resolver el acertijo. Por cada bloque que encuentran, los mineros reciben bitcoins de premio. El acertijo se genera matemáticamente para que sea imposible resolverlo mediante un atajo. Por eso, cuando el resto de la red ve la respuesta, sabe que ha costado mucho trabajo llegar a ella. Además, este proceso de resolución de acertijos es continuo («del orden de 500.000 trillones de hashes por segundo», según Dino Mark Angaritis). Los mineros «buscan un hash que coincida con el objetivo. Estadísticamente debe ocurrir cada diez minutos. Es un proceso de Poisson, por lo que a veces tarda un minuto y otras una hora, pero, de media, tarda diez minutos». Angaritis explica cómo funciona: «Los mineros reúnen todas las transacciones pendientes que encuentran en la red y procesan la información mediante una función criptográfica llamada “algoritmo de hash seguro” (*secure hash algorithm* o SHA-256), que da como

resultado un *valor de hash* de 32 bits. Si el valor de hash está por debajo de cierto objetivo (establecido por la red y ajustado cada 2.016 bloques), el minero ha encontrado la solución del acertijo y ha “resuelto” el bloque. Desafortunadamente para el minero, encontrar el valor de hash correcto es muy difícil. Si ese valor no es correcto, el minero ajusta la información entrante y lo intenta de nuevo. Cada intento produce un valor de hash *completamente distinto*. Los mineros deben intentarlo muchas veces para dar con la solución. Hasta noviembre de 2015, el número de intentos ha sido de unos 350 millones de billones. ¡Eso es mucho trabajo!».⁴³

El lector quizá haya oído hablar de otros mecanismos de consenso. La primera versión de Ethereum —Frontier— también usa el de la prueba de trabajo, pero los desarrolladores de Ethereum 1.1 tienen intención de sustituirlo por el mecanismo de la «prueba de participación». En este mecanismo, los mineros tienen que invertir y quedarse con algún depósito de valor (por ejemplo, la moneda original de la blockchain, como Peercoin, NXT, etc.). No tienen que gastar energía en votar. Otras blockchains, como Ripple y Steller, recurren a las redes sociales para lograr consenso y pueden recomendar que los nuevos participantes (es decir, los nuevos nodos) generen una *lista de nodos única* de al menos cien nodos en los que confían al votar sobre el estado de los negocios. Este tipo de prueba está sesgada: los recién llegados necesitan inteligencia social y reputación para participar. Otro mecanismo es el de la «prueba de actividad», que combina el de la prueba de trabajo y el de la prueba de participación, en el que un número al azar de mineros debe suscribir el bloque usando una clave cifrada antes de que el bloque sea oficial.⁴⁴ El mecanismo de la «prueba de capacidad» requiere que los mineros asignen al minado un espacio considerable de sus discos duros. La idea del mecanismo de la «prueba de almacenamiento» es parecida y requiere que los mineros asignen y compartan espacio del disco en una nube distribuida.

Lo del almacenamiento es importante. Los datos de las blockchains difieren de los datos de internet en una cosa fundamental. En internet, la mayor parte de la información es maleable y fugaz, y la fecha y la hora exactas de su emisión no son esenciales para la información pasada o futura. En el sistema blockchain el movimiento de bitcoins por la red queda registrado en todo momento, desde que se acuñan. Para que un bitcoin sea válido, debe remitirse a su propia historia y a la historia de la blockchain. En consecuencia, la cadena debe preservarse en su integridad.

Tan importante es el proceso de minado —juntar un bloque de transacciones, gastar recursos, resolver el problema, alcanzar consenso, guardar una copia de todo el registro— que hay quien considera que la blockchain de bitcoin es un servicio público como internet, que requiere apoyo público. Paul Brody, de Ernst & Young, piensa que todos nuestros aparatos deberían prestar su capacidad procesadora para mantener un sistema blockchain: «Nuestro cortacésped o lavavajillas vendrá con una CPU probablemente miles de veces más potente de lo que necesita, conque ¿por qué no ponerlo a minar? No para hacer dinero, sino para mantener nuestra parte del sistema blockchain», dice.⁴⁵ Independientemente de cuál sea el mecanismo de consenso usado, este sistema garantiza la integridad porque usa códigos inteligentes y no porque los seres humanos decidan comportarse bien.

Implicaciones para la economía de blockchain: En lugar de fiar a grandes compañías y gobiernos la verificación de la identidad de la gente y de su reputación, podemos fiarlo a la red. *Por primera vez disponemos de una plataforma que garantiza transacciones seguras y mucha información grabada sin que importe cómo actúa la otra parte.*

Las consecuencias que esto tiene en la mayor parte de la actividad social, política y económica son enormes. Ya no se trata de quién se casa con quién, quién vota a quién, quién paga a quién, se trata de que cualquier actividad requiere de registros fiables y transacciones seguras. ¿Quién es el propietario de esto? ¿Quién tiene los derechos de esta propiedad intelectual? ¿Quién es licenciado en Medicina? ¿Quién ha comprado armas? ¿Quién ha fabricado estas zapatillas Nike, este dispositivo Apple o esta leche infantil? ¿De dónde proceden estos diamantes? La confianza es la condición *sine qua non* de la economía digital, y una plataforma que permite la colaboración segura y fiable de mucha gente encierra grandes posibilidades de conseguir una nueva forma de organización social.

2. Poder distribuido

Principio: El sistema distribuye poder por una red de iguales sin que haya ningún punto de control. Las partes no pueden apagar el sistema por sí solas. Si una autoridad central lograra inhabilitar o expulsar a un individuo o a un grupo, el sistema sobreviviría. Si la mitad de la red intentara dominar al conjunto, todo el mundo lo vería.

Problema que hay que resolver: En la primera era de internet todas las grandes instituciones con bases de usuarios bien asentadas, fueran empleados, ciudadanos, clientes u otras organizaciones, se preocuparon poco por su contrato social. Una y otra vez, los poderes centrales han demostrado su voluntad y su capacidad de pasar por alto a los usuarios, almacenar y analizar sus datos, suministrar información al gobierno sin su conocimiento y realizar cambios importantes sin su consentimiento.

Posible solución: Los costes energéticos de controlar la blockchain bitcoin superarán los beneficios. Satoshi ideó un método del tipo de la prueba de trabajo que exige que los usuarios empleen mucha capacidad de procesamiento (que gasta mucha electricidad) para defender la red y acuñar nuevas monedas. Se inspiraba en Hashcash, la solución que encontró el criptógrafo Adam Back para reducir el spam o correo basura y los ataques llamados de «denegación de servicio». El método de Back requería que los remitentes hicieran una prueba de trabajo cuando enviaban un correo electrónico. El sistema marcaba el email como «correo especial» para señalar la relevancia que el mensaje tenía para su remitente. «Este correo es tan importante que he gastado toda esta energía para enviártelo.» El sistema incrementa los costes de enviar correo basura o programas malintencionados como malware y ransomware.

Cualquiera puede descargarse gratis el protocolo bitcoin y tener una copia de la blockchain. El protocolo usa la técnica del *bootstrapping*, que permite instalar el programa en el ordenador o dispositivo móvil de un usuario siguiendo unas sencillas

instrucciones que hacen funcionar el resto del programa. Es la técnica usada en una red de usuarios como BitTorrent, que es una base de datos de propiedad intelectual que reside en cientos de miles de ordenadores de todo el mundo.

Esto protege la red del control del Estado, lo que puede ser bueno o malo dependiendo del caso: no es lo mismo el de un disidente de un país totalitario que lucha por los derechos de las mujeres que el de un delincuente de un país democrático que extorsiona. Los regímenes totalitarios no podrían congelar cuentas bancarias ni apropiarse del dinero de activistas políticos. Los Estados no podrían confiscar arbitrariamente activos de un sistema blockchain como hizo la administración de Franklin Delano Roosevelt mediante el decreto 6102 que obligaba a los ciudadanos a entregar al gobierno «monedas de oro, lingotes de oro y certificados de oro» so pena de multa o prisión.⁴⁶ Josh Fairfield, de la Universidad Washington & Lee, lo dice claramente: «Ya no tenemos que buscar intermediarios».⁴⁷ La blockchain reside en todas partes. Los usuarios la mantienen actualizando su copia y prestando las unidades de procesamiento que le quedan libres para las operaciones de minado. No hay chanchullo que valga. Todas las acciones y transacciones se difunden por toda la red para su verificación y validación. No hay terceros ni servidores que centralicen ni almacenen nada.

Satoshi distribuyó también la «casa de la moneda» vinculando la acuñación de bitcoins con la creación de un nuevo bloque en el registro, con lo que puso la capacidad de batir moneda en manos de la red de iguales. El minero que primero resuelva el acertijo y se someta a una prueba de trabajo recibirá cierta cantidad de bitcoins nuevos. No hay «reservas federales» ni bancos centrales ni haciendas públicas que controlen la circulación de moneda. Es más, todos y cada uno de los bitcoins contienen enlaces directos que llevan al bloque en el que se registró su creación y a todas las transacciones subsiguientes.

No se necesitan intermediarios, pues. El sistema funciona con la mejor colaboración de la gente. Tenemos poder sobre nuestros datos, nuestras propiedades y nuestro nivel de participación. Es poder informático distribuido que proporciona poder humano distribuido y colectivo.

Implicaciones para la economía de blockchains: Una plataforma como ésta podría proporcionar modelos de creación de riqueza nuevos y distribuidos. Nuevas formas de colaboración entre iguales podrían resolver los problemas sociales más importantes de la humanidad. Podríamos solucionar la crisis de confianza e incluso de legitimidad de las actuales instituciones traspasando poder real a los ciudadanos, dándoles verdaderas oportunidades de prosperar y participar en la sociedad, en lugar de dedicarnos a hacer malabarismos propios de un relaciones públicas.

3. El valor como incentivo

Principio: El sistema hace coincidir los incentivos de todos los participantes. El bitcoin o alguna ficha de valor es parte esencial de esta coincidencia y correlativo a la reputación. Satoshi programó el software para premiar a los que trabajaran en él y para que

perteneciera a los que poseen y usan sus fichas, de suerte que todos lo cuidaran. Especie de última versión del Tamagotchi, el sistema blockchain es como una mascota globalmente distribuida.⁴⁸

Problema que hay que revolver: En la primera era de internet la concentración de poder de las empresas, combinada con su gran tamaño, complejidad y opacidad, les permitió sacar cantidades desproporcionadas de valor de las mismas redes que las dotaron de derechos. Los grandes bancos explotaron el sistema financiero hasta el límite porque «las estructuras de incentivos estaban diseñadas para que la mayoría de los altos ejecutivos y muchos de los encargados de los préstamos actuaran con falta de visión y mucho riesgo», según el economista Joseph Stiglitz. Eso incluía «cebarse con los estadounidenses más pobres». Así resume el problema: «Si damos malos incentivos a la gente, se comportará mal, y se comportó exactamente como uno esperaba».⁴⁹

Grandes empresas electrónicas ofrecían servicios gratis de venta, búsqueda y medios sociales a cambio de los datos del usuario. Según un estudio de Ernst & Young, casi dos terceras partes de los directivos encuestados dijeron que recababan información de los consumidores para hacer negocios, y casi el 80 por ciento reconocía haber aumentado las ganancias gracias al aprovechamiento de esta información. Pero cuando los piratas informáticos atacan esas empresas y roban las tarjetas de crédito y la información bancaria de los consumidores, son éstos los que pagan el pato. No sorprende que, según la misma encuesta, casi la mitad de los consumidores dijeran que habían negado acceso a sus datos en los siguientes cinco años y más de la mitad dijera que ahora proporcionaban menos datos, incluso censurándose a sí mismos en los medios sociales, que en los cinco años anteriores.⁵⁰

Posible solución: Satoshi esperaba que los participantes actuaran en interés propio. Entendía la teoría de juegos. Sabía que las redes sin protección eran vulnerables y habían recibido ataques llamados «Sybil», que hacen que los nodos forjen múltiples identidades, los derechos se difuminen y el valor de la reputación se deprecie.⁵¹ La integridad de la red de iguales y la reputación de sus usuarios se ve menoscabada cuando no sabemos tanto si estamos tratando con tres partes, como si estamos tratando con una parte que usa tres identidades. Por eso Satoshi programó el código fuente de manera que, por muy egoístamente que actuemos, nuestras acciones beneficiaran al sistema en su conjunto y aumentaran nuestra reputación, nos identificáramos como nos identificásemos. La exigencia de recursos del mecanismo de consenso, unida a la idea de premiar con bitcoins, podría persuadir a los participantes a comportarse correctamente y a resultar fiables en el sentido que se esperaba. Los ataques Sybil serían económicamente inviables.

Satoshi escribió: «Por norma, la primera transacción de un bloque es una transacción especial que da comienzo a una nueva moneda que pertenece al creador del bloque. Esto constituye un incentivo para que los nodos sostengan la red».⁵² Bitcoin ofrece incentivos para que los mineros creen un bloque y lo vinculen con el bloque anterior. Los primeros que completan un bloque se llevan cierta cantidad de bitcoins como premio por su esfuerzo. El protocolo de Satoshi premiaba a los primeros que lo hacían generosamente: durante los primeros cuatro años, los mineros recibieron 50 bitcoins (BTC) por cada bloque. Cada cuatro años, el premio fue disminuyendo la mitad: 25 BTC, 12,5 BTC, y así

sucesivamente. Como ahora poseen bitcoins, tienen un incentivo para garantizar el éxito duradero de la plataforma, comprando los mejores programas para ejecutar operaciones de minado, gastando energía lo más eficientemente posible y manteniendo el registro. Bitcoin no sólo nos incentiva para participar en la labor de minado y en las transacciones con otros, sino que nos da derecho a la propiedad de la plataforma misma. Las cuentas de usuario distribuidas son el elemento más básico de la infraestructura criptográfica de la red. Poseyendo y usando bitcoins, estamos financiando el desarrollo de la cadena.

Satoshi decidió que el grupo económico fuera el de los *propietarios de capacidad procesadora*. Esto requiere que esos mineros consuman un recurso externo a la red, principalmente electricidad, si quieren participar en el sistema de premios. A veces, varios mineros encuentran dos bloques igualmente válidos de igual extensión, y los demás mineros deben elegir uno para seguir construyendo la cadena. Normalmente eligen el que creen que ganará y no los dos, pues si eligieran los dos se verían obligados a dividir su capacidad procesadora entre dos cadenas, lo que significaría que perderían valor. La cadena más larga supone la mayor cantidad de trabajo y, por lo tanto, los participantes la eligen como el estado canónico de la cadena. Por su parte, Ethereum decidió que su grupo económico fuera el *propietario de moneda*, y Ripple and Stellar que lo fuera la red social.

La paradoja de estos esquemas de consenso es que, actuando en interés propio, estamos sirviendo a la red de iguales, lo que a su vez afecta a nuestra reputación como miembros del grupo económico. Antes de que existieran las tecnologías blockchain, la gente tenía difícil rentabilizar el valor de su reputación en línea. No era sólo a causa de los ataques Sybil, por los que un ordenador podía desempeñar múltiples roles. La identidad tiene muchas facetas y matices y es efímera. Poca gente ve todos los lados, y no digamos las sutilezas y la historia de nuestra identidad. En diferentes contextos, tenemos que presentar algún documento u otra cosa que atestigüe nuestra identidad con cierto detalle. La gente «sin papeles» se ve obligada a colaborar con su círculo social. En blockchains como Stellar, éste es un excelente comienzo, una forma de crear una presencia digital permanente y de establecer una reputación que puede llevarse mucho más allá de nuestra comunidad geográfica.

Otra forma de preservar valor es la *política monetaria* que hay programada en el software. «Todas las monedas que ha usado la humanidad han sido inseguras por una u otra razón», dice Nick Szabo. «Esta inseguridad se ha manifestado de muchas maneras, desde la falsificación al robo, pero la más perniciosa de todas ha sido seguramente la inflación.»⁵³ Satoshi impuso un techo de suministro de bitcoins de 21 millones, que tenían que emitirse a lo largo del tiempo para evitar una inflación arbitraria. Dado que cada cuatro años el número de bitcoins minados en un bloque se reduce a la mitad y que el ritmo actual de minado es de seis bloques por hora, esos 21 millones de bitcoins deberían estar en circulación en 2140. No puede haber hiperinflación ni devaluación como las que causan las burocracias incompetentes o corruptas.

Las monedas no son los únicos activos con los que podemos negociar en el sistema blockchain. «No hemos hecho más que rascar la superficie de lo posible», dice Hill, de Blockstream. «Seguimos en el punto en el que estábamos en 1994 en lo que respecta a

aplicaciones y protocolos que exploten a fondo la red y le digan al mundo: “Esto es lo que puedes hacer y es pasmoso”.»⁵⁴ Hill piensa que habrá variados instrumentos financieros que nos permitirán, por ejemplo, autenticar activos y propiedades. También cree que habrá aplicaciones de bitcoin en el Metaverso (un mundo virtual) para que podamos convertir bitcoins en kongbucks y pagar a Hiro Protagonist para que nos piratee alguna información.⁵⁵ O enchufarnos a OASIS (un mundo de muchas utopías virtuales), donde podemos descubrir el huevo de Pascua, ganar la herencia de Halliday, vender los derechos de posicionamiento virtual de OASIS a Google y comprar un coche automático para recorrer Toronto.⁵⁶

Y, por supuesto, tenemos el internet de la cosas, en el que podemos registrar nuestros dispositivos, asignarles una identidad (Intel ya está haciéndolo) y coordinar pagos entre ellos usando bitcoins en lugar de las monedas tradicionales. «Podemos definir todos los nuevos negocios que queramos emprender y hacer que interoperen dentro de la red, y usar la infraestructura de la red sin tener que iniciar una nueva blockchain sólo para nosotros», dice Hill.⁵⁷

A diferencia de las monedas tradicionales, cada bitcoin puede dividirse en ocho lugares decimales. Esto permite a los usuarios combinar y dividir valor a lo largo del tiempo en una sola transacción, lo que significa que un *input* puede tener múltiples *outputs* a lo largo de múltiples periodos de tiempo, algo mucho más eficaz que hacer una serie de transacciones. Los usuarios pueden establecer contratos inteligentes para medir el uso de un servicio y hacer pagos en pequeñas fracciones a intervalos regulares.

Implicaciones para la economía de blockchains: En la primera era de internet nada de esto era posible. Ahora tenemos una plataforma en la que la gente y aun las cosas disponen de verdaderos incentivos financieros para colaborar eficazmente y crear casi cualquier cosa. Imaginemos unos foros de debate en línea en los que los participantes tienen reputaciones que quieren mejorar, en parte porque comportarse mal les resultará económicamente costoso. Los troles absténganse. Imaginemos una red de paneles solares cuyos propietarios son retribuidos en tiempo real en la blockchain por generar energía sostenible. Imaginemos un proyecto de software de código abierto en el que la comunidad de desarrolladores compense a los que hacen grandes contribuciones de códigos aceptables. Imaginemos que no haya países. No es difícil de conseguir.⁵⁸

4. Seguridad

Principio: Las medidas de seguridad están integradas en la red sin puntos flacos y no sólo garantizan la confidencialidad, sino también la autenticidad de todas las actividades y la imposibilidad de que nos sean denegadas. Todo el que quiera participar debe usar criptografía —no es posible optar por lo contrario— y las consecuencias de comportarse mal sólo las sufre la persona que se comporta mal.

Problema que hay que resolver: Piratería, robo de identidad o de información, fraude, ciberacoso, correo basura, programas maliciosos, todo esto socava la seguridad del individuo en la sociedad. La primera era de internet, en lugar de traer transparencia y reducir las infracciones, parece que ha hecho poco por aumentar la seguridad de las

personas, las instituciones y la actividad económica. El usuario normal de internet tiene que recurrir casi siempre a débiles contraseñas para proteger su correo electrónico o sus cuentas porque los proveedores de servicios no le ofrecen nada mejor. Pensemos en el típico intermediario financiero: no se especializa en tecnología de seguridad, sino en innovación financiera. El año que Satoshi publicó su artículo, el número de delitos informáticos en entidades financieras como BNY Mellon, Countrywide o GE Money ascendió al 50 por ciento de todos los robos de identidad registrados ese año, según el Identity Theft Resource Center.⁵⁹ En 2014 esta cifra había descendido al 5,5 por ciento en el sector financiero, pero los delitos en los sectores de la sanidad subieron al 42 por ciento del total del año. IBM informó de que el coste medio de un delito informático es de 3,8 millones de dólares, lo que significa que estos delitos han costado al menos 1.500 millones de dólares en los últimos dos años.⁶⁰ El coste medio para una víctima de robo de identidad en el sector de la sanidad ronda los 13.500 dólares, y estos delitos van en aumento. Los consumidores no saben qué aspecto de sus vidas va a verse atacado la próxima vez.⁶¹ Si la siguiente etapa de la revolución digital supone traspasarse dinero directamente entre partes, ese traspaso debe poder hacerse sin riesgo de pirateo informático.

Posible solución: Satoshi requería que los participantes usaran infraestructuras de clave (PKI, por sus siglas en inglés) para crear plataformas seguras. PKI es una forma avanzada de criptografía «asimétrica» por la que los usuarios disponen de dos claves que no desempeñan la misma función: una es para encriptar y la otra para desencriptar. De ahí que sean asimétricas. La plataforma bitcoin constituye hoy el mayor despliegue de PKI del mundo, y el segundo de Estados Unidos después del sistema de acceso común del Departamento de Defensa.⁶²

Creada en los años setenta,⁶³ la criptografía asimétrica cobró fuerza en los noventa en forma de programas de encriptación de correo electrónico como Pretty Good Privacy. Este programa es bastante seguro, y también bastante complicado de usar porque requiere que todos los miembros de la misma red lo usen, y que tomen nota de sus dos claves así como de las claves públicas de todos los demás. No hay posibilidad de cambiar la contraseña. Si la olvidamos, tenemos que empezar desde el principio. Según Virtru Corporation, «la encriptación del correo electrónico está en auge. Con todo, sólo el 50 por ciento de los correos se encriptan en tránsito, y la encriptación de extremo a extremo aún es más infrecuente».⁶⁴ Algunos usan *certificados digitales*, unos códigos que protegen los mensajes sin necesidad de encriptarlos y desencriptarlos, pero los usuarios deben solicitar (y pagar por ellos una cuota anual) sus certificados individuales, y los proveedores de servicios de correo electrónico más comunes —Google, Outlook y Yahoo!— no los soportan.

«Los sistemas pasados fracasaron porque no tenían incentivos, y la gente nunca consideró la privacidad un incentivo lo bastante fuerte como para proteger esos sistemas», dice Andreas Antonopoulos.⁶⁵ La cadena bitcoin resuelve prácticamente todos estos problemas porque da incentivos para adoptar PKI en todas las transacciones de valor, no sólo en el uso de bitcoin sino también en los protocolos bitcoin compartidos. No tenemos que preocuparnos de si los firewalls son débiles, hay empleados ladrones o piratas

informáticos. Si dos personas usan bitcoin, si pueden almacenar e intercambiar bitcoins con seguridad, entonces pueden almacenar e intercambiar información confidencial y activos digitales con seguridad en el sistema blockchain.

La cosa funciona así. La moneda digital no se almacena en un archivo propiamente dicho. La representan una serie de transacciones indicadas por un hash criptográfico. Los usuarios tienen las criptoclaves de su dinero y lo intercambian directamente entre sí. Esta seguridad trae consigo la responsabilidad de mantener privadas nuestras claves.

Los patrones de seguridad son importantes. La blockchain bitcoin funciona con el conocido y asentado SHA-256, publicado por el Instituto Nacional de Patrones y Tecnología de Estados Unidos como Patrón Federal de Procesamiento de la Información. Las muchas repeticiones de este cálculo matemático que se necesitan para encontrar la solución de un bloque obligan al dispositivo informático a consumir una considerable cantidad de electricidad para resolver el acertijo y ganar un bitcoin nuevo. Otros algoritmos, como el de la prueba de participación, gastan mucha menos energía.

Recordemos lo que decía Austin Hill al principio de este capítulo sobre que nunca había que echar las campanas al vuelo en cuestión de algoritmos. Hill, que trabaja con el criptógrafo Adam Back en Blockstream, no se fía de las criptomonedas que no usan pruebas de trabajo. «Creo que la prueba de participación no funciona a la larga. Para mí, es un sistema en el que el rico se hace más rico y los que tienen fichas deciden lo que es el consenso, mientras que el sistema de la prueba de trabajo no deja de ser algo físico. Me gusta porque se parece mucho al sistema del oro.»⁶⁶

Por último, la cadena más larga suele ser la más segura. La relativa antigüedad de la blockchain de Satoshi y su ya asentada base de usuarios y mineros de bitcoins aumentan su seguridad.

Atacarla requeriría más capacidad procesadora que atacar cadenas cortas. Hill dice: «Siempre que se inaugura una de estas nuevas redes con una cadena completamente nueva, hay un montón de gente que coge su capacidad procesadora latente, todos los ordenadores y CPU que no tienen minando bitcoins, y la dirigen contra estas nuevas redes para manipularlas y atacarlas.»⁶⁷

Implicaciones para la economía de blockchain: En la era digital, la tecnología digital es obviamente la condición previa de la seguridad de una persona en la sociedad. Hoy día, los bits pueden atravesar nuestros firewalls y nuestras carteras. Los ladrones pueden meter la mano en nuestros bolsillos y secuestrarnos el coche desde la otra punta del mundo. Como operamos cada vez más con herramientas y plataformas digitales, estas amenazas se han multiplicado en formas que la mayoría de nosotros no entendemos. Con la blockchain bitcoin, con su diseño más seguro y su transparencia, podemos hacer transacciones de valor y proteger nuestra información.

5. Privacidad

Principio: La gente debería poder controlar sus propios datos. Punto. Debería tener el derecho de decidir sobre su identidad, y cuándo, cómo y cuánta compartir con los demás. Respetar el derecho a la privacidad no es exactamente lo mismo que respetar la

privacidad. Necesitamos las dos cosas. Al eliminar la necesidad de confiar en los otros, Satoshi eliminó la necesidad de conocer la verdadera identidad de esos otros para interactuar con ellos. «He hablado con muchos ingenieros y científicos de la información y todos me han dicho: “Pues claro que podemos integrar la privacidad en la estructura de la información, en el diseño de los programas”», dice Ann Cavoukian.⁶⁸

Problema que hay que resolver: La privacidad es un derecho humano fundamental en una sociedad libre. En los últimos veinte años de internet las bases de datos centrales, tanto del sector público como del privado, han acumulado toda clase de información confidencial sobre individuos e instituciones, a veces sin conocimiento de éstos. Para preocupación de muchos, las empresas sondean el mundo digital en busca de esa información y crean lo que podríamos llamar *ciberclones* de esos individuos e instituciones. Incluso hay gobiernos democráticos que están creando naciones vigilantes, como ha demostrado recientemente el caso de la Agencia Nacional de Seguridad de Estados Unidos, que, extralimitándose en su derecho a la vigilancia, ha realizado un injustificado espionaje en internet. Son atentados contra la privacidad por partida doble, primero por reunir y usar nuestros datos sin nuestro conocimiento ni nuestro permiso, y segundo por no proteger ese tesoro de los piratas informáticos. «Tenemos que abandonar la idea de que lo que ganamos por una parte lo perdemos por otra, de que es una cosa o la otra. Eso, para mí, ya es pasado y es contraproducente», dice Cavoukian. «Nosotros apostamos por un modelo que une las dos cosas, que nos permite tener privacidad y a la vez dar información.»⁶⁹

Posible solución: Satoshi no incorporó ningún requisito de identidad en la capa de red misma, con lo que nadie tiene que proporcionar nombre, dirección de correo electrónico ni ninguna otra información personal para descargarse y usar el programa de bitcoin. La blockchain no necesita saber quiénes somos. (Y Satoshi no necesita recabar la información de nadie para comercializar otros productos. Su software de código abierto era el último grito en el mercado de liderazgo intelectual.) Así es como funciona la Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT, por sus siglas en inglés); si pagamos en efectivo, por lo general SWIFT no nos pide que nos identifiquemos, aunque suponemos que muchas oficinas de la sociedad tienen cámaras, y que las entidades financieras deben cumplir los requisitos contra el blanqueo de dinero o de conocimiento del cliente (requisitos AML/KYC, por sus siglas en inglés) para formar parte de la sociedad y poder usar sus servicios.

Además, las capas de identificación y verificación están separadas de la de transacción, lo que significa que la parte A emite la transferencia de bitcoins desde la dirección de la parte A a la de la parte B. No hay referencia alguna a la identidad de nadie en esa transacción. Entonces la red confirma que la parte A no sólo controla la cantidad de bitcoins especificada, sino que también autoriza la transacción, y luego registra la cantidad emitida por la parte A como una cantidad no gastada (*unspent transaction output*) asociada a la dirección de la parte B. Sólo cuando la parte B se dispone a gastar esa cantidad comprueba la red que ahora es esta parte la que lo controla.

Comparemos esto con el modelo de las tarjetas de crédito, que se basan en la identidad. Por eso se roban direcciones y números de teléfono de millones de personas cada vez que se piratea una base de datos. Veamos el número de registros asociados a algunos de los más recientes robos de datos: T-Mobile, 15 millones de registros; JP Morgan Chase, 76 millones; Anthem Blue Cross Blue Shield, 80 millones; eBay, 145 millones; Office of Personal Management, 37 millones; Home Depot, 56 millones; Target, 70 millones, y Sony, 77 millones, y ha habido también ataques menores contra compañías aéreas, universidades, compañías de gas y electricidad y hospitales, que forman parte de nuestras infraestructuras más valiosas.⁷⁰

En el sistema blockchain los participantes pueden elegir mantener un cierto grado de anonimato en el sentido de que no necesitan asociar ningún otro detalle a su identidad ni guardar esos detalles en una base de datos central. No insistiremos bastante en lo importante que es esto. *En el sistema blockchain no hay tesoros de información personal.* Los protocolos de este sistema nos permiten elegir el nivel de privacidad que queremos en cada transacción o entorno. Nos ayuda a administrar mejor nuestras identidades y nuestra interacción con el mundo.

Una empresa emergente llamada Personal BlackBox Company se propone ayudar a las grandes empresas a tratar de otra manera la información del cliente. Su director comercial, Haluk Kulin, nos confiesa: «Compañías como Unilever o Prudential vienen y nos dicen: “Queremos gestionar mejor nuestra información. ¿Puede sernos útil vuestra plataforma? Queremos aliviar la carga que nos supone la información”. Están viendo que la información es un activo tóxico cada vez más grande para las grandes corporaciones».⁷¹ Esta plataforma permite a sus clientes acceder a información anónima —como en los experimentos clínicos, en los que los médicos sólo conocen los aspectos más relevantes de la salud de los pacientes— sin correr ningún riesgo. Algunos clientes pueden dar más información a cambio de bitcoins u otras ventajas. En última instancia, la plataforma de Personal BlackBox usa PKI, con lo que sólo los clientes tienen acceso a sus datos con sus claves privadas. Ni siquiera la empresa tiene acceso a esos datos.

Las blockchains permiten varias formas flexibles de autenticación selectiva y anónima. Austin Hill lo compara con internet. «Las direcciones TCP/IP no se identifican con identidades públicas. La misma capa de red lo ignora. Cualquiera puede conectarse a internet, conseguir una dirección IP y empezar a enviar y recibir paquetes libremente en todo el mundo. Como sociedad, hemos visto un gran beneficio en permitir ese grado de anonimato... Bitcoin opera casi exactamente así. La misma red no depende de la identidad. Esto es bueno para la sociedad y para el buen diseño de la red.»⁷²

Así pues, mientras que las blockchains son públicas —todo el mundo puede verlas en cualquier momento porque residen en la red, no en ninguna institución centralizada que audite las transacciones y guarde registros—, la identidad de los usuarios es anónima. Esto significa que tenemos que triangular mucha cantidad de datos para averiguar quién posee una clave pública concreta. El emisor puede proporcionar solamente los metadatos que el receptor necesita conocer. Y, lo que es más, todos podemos poseer varios conjuntos de claves públicas y privadas, igual que podemos tener varios dispositivos o puntos de acceso a internet y múltiples direcciones electrónicas con varios pseudónimos.

Dicho esto, proveedores de servicios de internet como Time Warner, que asignan direcciones IP, guardan registros que vinculan las identidades a las cuentas. Del mismo modo, si compramos una cartera bitcoin en una bolsa autorizada como Coinbase, esta bolsa está obligada a cumplir con los requisitos AML/KYC. Por ejemplo, ésta es la política de privacidad de Coinbase: «Guardamos la información que nos envías desde tu ordenador, teléfono móvil u otros dispositivos. Esta información puede incluir tu dirección IP, información sobre el dispositivo, incluyendo identificador, nombre del dispositivo y tipo, sistema operativo, ubicación, información sobre la red móvil y sobre uso del servidor, así como el tipo de navegador, tráfico que entra y sale de nuestro sitio y las páginas a las que accedes en él».⁷³ Por lo tanto, los gobiernos pueden reclamar esta información de usuario a los proveedores de servicios de internet. Pero no pueden reclamar la blockchain.

Es importante saber también que podemos establecer niveles más altos de transparencia para cada conjunto de transacciones, aplicación o modelo de negocio si todos los interesados están de acuerdo. En determinadas situaciones, veremos nuevas prestaciones en las que es muy importante que haya una gran transparencia. Cuando las compañías dicen la verdad a los clientes, accionistas o socios, crean confianza.⁷⁴ Esto es, privacidad para los individuos y transparencia para las organizaciones e instituciones públicas y privadas.

Implicaciones para la economía de blockchain: El sistema blockchain nos permite frenar la carrera con la que vamos hacia una sociedad de la vigilancia. Pensemos en lo que significa que las empresas tengan enormes bases de datos con información detallada sobre nosotros. Llevamos veinte años de internet global y sólo es el comienzo del acceso de las empresas a nuestra más íntima información. Pronto lo tendrán también a la información sobre nuestra salud y condición física, sobre nuestros movimientos diarios, sobre la vida en nuestro hogar, etc. Mucha gente sencillamente ignora la cantidad de pactos fáusticos que hace todos los días en la red. Simplemente por usar un sitio, los usuarios autorizan a los propietarios de ese sitio a convertir simples rastros digitales en detallados mapas que se usan para obtener beneficios comerciales.

Salvo que nos pasemos al nuevo paradigma, no es ciencia ficción prever cientos de millones de avatares bullendo en los centros de datos del mañana. Con la tecnología blockchain, cada cual puede poseer sus avatares personales como ocurre en el mundo virtual de Segunda Vida, pero con consecuencias en el mundo real. Nuestro yo virtual puede proteger nuestra información personal, dar sólo la que se nos pide en los intercambios económicos o sociales y garantizar que recibimos la debida retribución por cualquiera de nuestros datos que tenga valor para un tercero. Es pasar de los «grandes datos» a los datos privados, o «datos pequeños», si queremos.

6. Derechos preservados

Principio: Los derechos de propiedad son transparentes y legítimos. Las libertades individuales están reconocidas y son respetadas. Nosotros pensamos que es una verdad evidente que todos nacemos con una serie de derechos inalienables que deben y pueden

ser protegidos.

Problema que hay que resolver: En la primera fase de la economía digital la cuestión era buscar maneras de ejercer esos derechos más eficazmente. Internet se convirtió en un medio para desarrollar nuevas formas de arte, información y entretenimiento, para establecer derechos de autor de poemas, canciones, historias, fotografías y grabaciones de sonido y vídeo. Podíamos aplicar el Uniform Commercial Code para hacer en línea lo que el código ya permitía en el espacio físico, que era eliminar la necesidad de negociar y firmar contratos por cada artículo, como un tubo de pasta dentífrica, por poco que costara. Incluso así, teníamos que confiar en intermediarios que controlaran las transacciones y que podían denegarlas, retrasarlas, retener el dinero en sus propias cuentas (los banqueros llaman a esto *float*, «dinero flotante»), o autorizarlas para luego revertirlas. Daban por sentado que un porcentaje de la gente engañaría y que cierto grado de fraude es inevitable.

En esta gran eclosión de eficiencia, los derechos legítimos fueron pisoteados; no sólo los derechos de privacidad y seguridad, sino también los de libre expresión, reputación y participación equitativa. La gente podía criticarnos, difamarnos y bloquearnos con poco coste o riesgo. Directores de cine cuyos ingresos dependían de agencias, alquiler de vídeos, ventas de DVD y derechos de televisión por cable de las películas emitidas hace unas décadas, ven cómo sus ingresos disminuyen porque sus fans suben a la red archivos digitales que otros se descargan gratuitamente.

Posible solución: La prueba de trabajo requerida para acuñar monedas también registra el momento en el que se hacen las transacciones, de manera que sólo se autoriza la primera vez que se gasta una moneda. Combinado con PKI, el sistema blockchain no sólo impide el doble gasto, sino que también confirma la propiedad de todas y cada una de las monedas en circulación, y cada transacción es inmutable e irreversible. En otras palabras, no podemos negociar con lo que no es nuestro, sea una propiedad real, una propiedad intelectual o un derecho de la persona, como tampoco podemos negociar con lo que no estamos autorizados a negociar en nombre de otra persona, en calidad de agente, como abogado o director de empresa. Y tampoco podemos suprimir la libertad de expresión, asociación o religión.

Haluk Kulin, de Personal BlackBox, lo dice mejor: «En miles de años de interacción humana, siempre que le hemos quitado el derecho de participación a la gente, ésta ha vuelto por sus fueros y ha acabado con el sistema. Estamos viendo que tampoco en el mundo digital es sostenible obviar su consentimiento».⁷⁵ Como «registro de todo», el sistema blockchain puede usarse a modo de archivo público con herramientas como Proof of Existence, un sitio que crea y registra criptográficamente acciones, títulos, recibos o licencias en una blockchain. Este sitio no guarda copia de documentos originales; el hash del documento se crea en el dispositivo del usuario, no en el sitio de Proof of Existence, con lo que se asegura la confidencialidad. Incluso si una autoridad central elimina el sitio, la prueba permanece en la blockchain.⁷⁶ Este sistema, pues, permite demostrar la propiedad de algo y conservar registros sin censura.

En internet no siempre podíamos hacer valer nuestros derechos contractuales o ver si se respetaban. Y así, para el caso de transacciones más complejas en las que intervienen muchos derechos y muchas partes, ahora tenemos los «contratos inteligentes» (*smart contracts*), unos códigos especiales que ejecutan conjuntos complejos de instrucciones en blockchain. «La intersección de descripciones legales y programas informáticos es fundamental, y los contratos inteligentes son el primer paso dado en esa dirección», dice Steve Omohundro, presidente del *think tank* o laboratorio de ideas Self-Aware Systems. «Cuando se entiendan los principios de la codificación digital de las leyes, creo que todos los países empezarán a hacerlo... Cada jurisdicción codificará sus leyes, exacta y digitalmente, y habrá programas de traducción que las traduzcan... Evitar los conflictos entre leyes será una gran ventaja económica.»⁷⁷

Un contrato inteligente permite que una parte ceda derechos de uso a otro parte, por ejemplo un compositor que cede los derechos de uso de una canción a un editor musical. El código del contrato podría incluir el término o duración de la concesión, la cantidad de dinero que pasará de la cuenta del editor a la del compositor en concepto de derechos de autor, y algunas cláusulas de rescisión de contrato, como, por ejemplo, la de que si la cuenta del compositor recibe menos de un cuarto de bitcoin en los siguientes treinta días, todos los derechos vuelven automáticamente al compositor y el editor deja de tener acceso a la obra de ese compositor registrada en la blockchain. Para hacer que este contrato inteligente entre en vigor, el compositor y el editor —y quizá representantes financieros y legales de este último— firmarán usando sus claves privadas.

Un contrato inteligente también permite que los propietarios de activos unan sus recursos y creen una sociedad en la blockchain. El contrato incluye, codificadas, unas cláusulas de admisión que especifican claramente los derechos de esos propietarios. Los contratos de agencias de empleo asociados podrían definir los derechos de las empresas codificando lo que pueden y no pueden hacer con los recursos de la sociedad sin permiso de los propietarios.

Los contratos inteligentes son un método sin precedentes de garantizar el cumplimiento del contrato, incluyendo los contratos sociales. «Si realizamos una gran transacción con una estructura de control específica, podemos predecir el resultado en cualquier momento dado», dice Antonopoulos. «Si realizamos una transacción firmada y verificada por una serie de firmas en una cuenta multifirma, podemos predecir si la red verificará la transacción. Y si la red puede verificar la transacción, entonces esa transacción puede liquidarse y de una manera irreversible. Ninguna autoridad central o tercera parte puede revertirla, ni nadie puede anular el consenso de la red. Esta idea es nueva tanto en el derecho como en las finanzas. El sistema de bitcoin proporciona un altísimo grado de certidumbre sobre el resultado de un contrato.»⁷⁸

Nadie puede apoderarse del contrato, suspenderlo o redirigirlo a una dirección bitcoin diferente. Sólo tenemos que transmitir la transacción firmada a cualquiera de los nodos de la red desde cualquier parte y por cualquier medio. Dice Antonopoulos: «Aunque apagaran internet, seguiríamos pudiendo transmitir la transacción por radio de onda corta usando el código Morse. Aunque una agencia gubernamental intentara censurar nuestra comunicación, seguiríamos pudiendo transmitir la transacción por Skype

con una serie de emoticonos. Mientras que al otro lado haya alguien que pueda decodificar la transacción y registrarla en la blockchain, siempre podremos ejecutar el contrato inteligente. Así, hemos convertido algo que, en derecho, es casi imposible de garantizar, en algo que puede verificarse con certeza matemática».⁷⁹

Pensemos en los derechos de propiedad, tanto de bienes como intelectuales: «La propiedad es sólo el reconocimiento por parte de un gobierno o de una agencia de que somos los propietarios de algo y de que defenderán nuestro derecho a esa propiedad», dice Stephen Pair, consejero delegado de BitPay. «Es sólo un contrato que puede firmar cualquier autoridad que defienda por nosotros nuestros derechos y que firma en nombre de nuestra identidad, y una vez que tenemos eso, y que la propiedad está registrada, podemos transferirla a otra gente. Esto es muy directo.»⁸⁰ Comunidades que compartan recursos podrían considerar un espectro de derechos, tomados de la pirámide de derechos de la economista y premio Nobel Elinor Ostrom, que es una especie de jerarquía de derechos. En el nivel más bajo, hay usuarios autorizados que sólo pueden acceder y retirar recursos; demandantes que tienen esos derechos pero también pueden negar el acceso a otros; propietarios que tienen derechos de administración además de los de acceso y exclusión, y propietarios que pueden acceder, usar, excluir a otros, administrar y vender el recurso (a saber, que tienen derecho de enajenación).⁸¹

Consideremos ahora los derechos de privacidad y publicidad: «Nuestro modelo consiste en aplicar realmente los derechos al mercado», dice Kulin, de Personal BlackBox. Su compañía usa tecnología de blockchain para representar y hacer valer el derecho que tienen los individuos de rentabilizar sus datos personales. «El sistema blockchain pone a nuestra disposición a un grupo de personas que tienen el mismo objetivo y usan la misma tecnología, lo que nos permite crear diferentes formas para que las empresas aprovechen estos conjuntos de datos únicos en lugar de proteger sus silos de datos.»⁸² Dicho lisa y llanamente, la gente crea mejor información de la que una empresa puede extraer de ella, y los consumidores se identifican emocionalmente mejor con marcas e influyen más en sus iguales que las empresas.

Implicaciones para la economía de blockchain: Un principio económico general es que para aplicar derechos debemos empezar por aclarar en qué consisten esos derechos. En el campo de la dirección y administración de empresas, la holocracia es un ejemplo interesante, aunque controvertido, de cómo los miembros de una organización definen el trabajo que hay que hacer y asignan derechos y la responsabilidad de hacer ese trabajo como parte de un todo.⁸³ ¿Quién acordamos que debe tomar esta serie de decisiones y ocuparse de estas actividades en nuestra compañía? La respuesta a esta pregunta puede codificarse en un contrato inteligente e integrarse en la blockchain de manera que las decisiones, los pasos dados hacia la meta y los incentivos sean todos transparentes y consensuados.

Esto, claro está, no es sólo tecnología. Es mucho más que una cuestión de activos físicos, de propiedad intelectual o de instrumentos de privacidad de Personal BlackBox con módulos sobre derechos publicitarios de las hermanas Kardashian. Necesitamos que haya más educación sobre derechos y que se desarrollen nuevas formas de entender los sistemas de gestión de esos derechos. Tendremos sistemas de gestión de los derechos de

voto y sistemas de gestión de los derechos de propiedad. Habrá empresas que creen una especie de indicadores de derechos que midan nuestro nivel de compromiso cívico, con índices, por ejemplo, de ejercicio de voto, donación de capacidades, reputación, tiempo, bitcoin o libre acceso a nuestra propiedad física o intelectual. Nada más y nada menos.

7. Inclusión

Principio: La economía funciona mejor cuando funciona para todos. Eso significa eliminar obstáculos que dificulten la participación. Significa crear nuevas plataformas que hagan posible un *capitalismo distribuido*, no simplemente un capitalismo redistribuido.

Problema que hay que resolver: La primera era de internet dio muchas sorpresas a mucha gente. Pero, como hemos señalado, la mayoría de la población mundial sigue estando excluida, no sólo del acceso a la tecnología sino también del acceso al sistema financiero y a las oportunidades económicas. Además, la promesa de que este nuevo medio de comunicación traerá prosperidad para todos ha quedado en agua de borrajas. Es verdad que ha ayudado a las empresas del mundo desarrollado a dar trabajo a millones de personas de economías en vías de desarrollo, que ha facilitado la empresa y ha dado a los más desfavorecidos nuevas oportunidades y acceso a información básica.

Pero no es suficiente. Sigue habiendo 2.000 millones de personas ⁸⁴ sin una cuenta bancaria, y en el mundo desarrollado la prosperidad disminuye a la vez que la desigualdad social no cesa de aumentar. En las economías en vías de desarrollo el teléfono móvil es muchas veces el único medio de conectarse que las personas pueden permitirse. La mayoría de las instituciones disponen de aplicaciones de pago para móviles que combinan cámaras y códigos QR. Sin embargo, las comisiones necesarias para mantener a estos intermediarios hacen que los micropagos sean poco factibles. Los consumidores de la base de la pirámide siguen sin poder permitirse tener el balance de cuenta mínimo, la cantidad de pago mínima, ni las comisiones que se cobran por transacción, con lo que de nada les sirve el sistema, cuyos costes hacen que los micropagos y las microcuentas sean inviables.

Posible solución: Satoshi diseñó el sistema para que funcionara con los protocolos más elementales de internet (TCP/IP), pero también podía funcionar sin internet si fuera necesario. Satoshi imaginó que una persona normal interactuaría con las blockchains a través de lo que él llamó «verificación de pago simplificada» (SPV, por sus siglas en inglés), que puede funcionar en teléfonos móviles para activar esas cadenas. Ahora, con un móvil de esos que se abren y se cierran, cualquiera puede participar en la economía o en un mercado como productor o consumidor. No se necesita ni cuenta bancaria, ni certificado de ciudadanía, ni partida de nacimiento, ni dirección domiciliaria, ni moneda local estable para usar las tecnologías de blockchain. El sistema blockchain abarata muchísimo los costes de girar dinero, facilita el tener una cuenta bancaria, obtener crédito e invertir y fomenta la empresa y la participación en el comercio global.

Esto era parte de la visión de Satoshi. Entendía que para las personas de economías en vías de desarrollo la situación era peor. Cuando burócratas corruptos o incompetentes de Estados fallidos necesitaban fondos para ejercer su gobierno, sus bancos centrales o

sus tesoros simplemente emitían más moneda para aprovecharse de la diferencia entre los costes de fabricación y el valor nominal de la moneda. Eso se llama «señoreaje». El incremento de la masa monetaria devalúa la moneda. Si la economía del país decae — como ocurrió en Argentina y Uruguay, y más recientemente en Chipre y Grecia—, estos organismos centrales pueden congelar las cuentas de todos aquellos que no pueden permitirse sobornar. Dada esta posibilidad, los ricos pueden trasladar su dinero a países con más seguridad jurídica y monedas más estables.

Pero no los pobres. Tengan la moneda que tengan, ésta pierde su valor. Los funcionarios pueden desviar fondos de ayuda extranjera y bloquear sus fronteras con montañas de papeleo, dificultando la ayuda que pudiera querer prestarse a su gente: madres e hijos que necesitan comida y medicinas, víctimas de la guerra, de una sequía prolongada y de otras calamidades naturales.

El servicio de micropagos australiano mHITS (sigla de Mobile Handset Initiated Transactions) ha lanzado un servicio nuevo, BitMoney, que permite a clientes de más de cien países recargar sus teléfonos móviles enviando un mensaje de texto a mHITS especificando una cantidad de bitcoins.⁸⁵ Según el desarrollador de Bitcoin Gavin Andresen: «No vemos todas las transacciones, sino sólo las que nos interesan. No confiamos nuestro dinero a otros usuarios como nosotros, sólo les pedimos que nos den la información que circula por la red».⁸⁶

«El potencial que tiene el uso del sistema blockchain para registrar propiedades en los países en vías de desarrollo, donde es una cuestión muy importante ligada a la pobreza, es muy considerable», dice Austin Hill. «No hay una entidad de confianza que administre los títulos de propiedad de tierras, y por eso conseguir que la gente pueda decir: “Esta propiedad es mía” y luego usarla como aval para mejorar su situación personal y familiar es algo fundamental.»⁸⁷

En un comentario técnico, Andresen se refiere a la ley de Nielsen sobre el ancho de banda, según la cual el ancho de banda de los usuarios con mayor ancho de banda aumenta un 50 por ciento cada año, mientras que el de las mayorías tiende a retrasarse en dos o tres años. El ancho de banda va por detrás de la capacidad procesadora, que aumenta en torno al 60 por ciento anual (según la ley de Moore). O sea, el ancho de banda es el factor clave, según Jakob Nielsen.⁸⁸ Interfaces, sitios web, productos digitales, servicios, organizaciones y demás tendrán que diseñarse para que se adapten a la tecnología de las mayorías si quieren beneficiarse de las redes. Por lo tanto, la inclusión significa considerar todo el espectro de uso, no sólo el de los usuarios mejor conectados, sino también el de quienes tienen tecnologías lentas o sufren cortes de energía en regiones remotas de países pobres.

Implicaciones para la economía blockchain: Más adelante hablamos de la paradoja de la prosperidad: aunque la primera era de internet benefició a muchos, la prosperidad en el mundo occidental no ha crecido para la mayoría de la gente. El fundamento de la prosperidad es la inclusión, y el sistema blockchain puede ayudar. Aclaremos que la inclusión tiene muchas dimensiones. Significa acabar con la hegemonía social, económica y racial, con la discriminación basada en la salud, el género y la

identificación o preferencia sexual. Significa acabar con las barreras que impone el lugar en el que uno vive, el hecho de haber pasado una noche en la cárcel o lo que votamos, pero también acabar con los «techos de cristal» y con todas las formas de «amiguismo».

Diseñar el futuro

Nuestra conversación con Ann Cavoukian nos animó a investigar la promesa alemana del «Nunca más». Descubrimos lo que dijo el presidente alemán Joachim Gauck el día de la conmemoración del Holocausto: «Nuestras obligaciones morales no se agotan con el recuerdo. También existe dentro de nosotros una profunda y perdurable certeza de que el recuerdo nos encomienda una misión. Esa misión consiste en proteger y conservar la humanidad. Consiste en proteger y conservar los derechos de todos los seres humanos».⁸⁹ ¿Se refería al genocidio en Siria, Iraq, Darfur, Srebrenica, Ruanda o Camboya, después de que el pueblo alemán jurara «Nunca más»?

Nosotros creemos que la tecnología blockchain puede ser un instrumento importante para proteger a la humanidad y conservar los derechos de todos los seres humanos, un medio de comunicar la verdad, repartir prosperidad y —como la red deniega transacciones fraudulentas— extirpar esas primeras células cancerosas de una sociedad que pueden crecer hasta ser mortales.

Reconocemos que es decir mucho. Siga leyendo el lector y juzgue por sí mismo.

Desde un punto de vista más prosaico y más práctico, estos siete principios pueden servir como guía para crear la siguiente generación de empresas, organizaciones e instituciones innovadoras y de alto rendimiento. Si creamos cosas pensando en la integridad, el poder, el valor, la privacidad, la seguridad, los derechos y la inclusión, estaremos reinventando nuestra economía y nuestras instituciones sociales para que sean fiables. Centremos ahora nuestra atención en lo que deberíamos hacer para lograrlo.

SEGUNDA PARTE

Transformaciones

Capítulo III

Reinventar los servicios financieros

El sistema financiero global mueve billones de dólares al día, sirve a miles de millones de personas y sostiene una economía global de más de 100 billones de dólares.⁹⁰ Es la industria más poderosa del mundo, el fundamento del capitalismo global y sus líderes son los Amos del Universo. Visto más de cerca, es como una máquina de Rube Goldberg de desarrollo desigual y curiosas contradicciones. Para empezar, el aparato lleva mucho tiempo sin modernizarse. Nuevas tecnologías se han acoplado como buenamente han podido a unas infraestructuras obsoletas. Pensemos en esos bancos que permiten operar por internet pero siguen emitiendo cheques de papel y usando ordenadores centrales de los años setenta del siglo pasado. Cuando un cliente de estos bancos pasa su tarjeta de crédito por un lector para pagar un café con leche en Starbucks, su dinero pasa por no menos de cinco intermediarios antes de llegar a la cuenta bancaria de Starbucks. La transacción se realiza al momento, pero el pago tarda días.

Además, las grandes multinacionales como Apple o General Electric tienen que mantener cientos de cuentas bancarias en moneda local en todo el mundo para facilitar sus operaciones.⁹¹ Cuando una empresa de este tipo necesita mover dinero entre dos sucursales de dos países distintos, el director de una sucursal envía un giro bancario de la cuenta de esa sucursal a la cuenta de la otra. Estas transferencias son complicadísimas y tardan días, a veces semanas en liquidarse. Durante ese tiempo, ninguna de las dos sucursales puede usar ese dinero para financiar operaciones o invertir, pero los intermediarios pueden cobrar intereses. «Lo que la tecnología hizo fundamentalmente fue convertir un proceso basado en el papel en un proceso semiautomático y semielectrónico, pero la lógica seguía dependiendo del papel», dice Vikram Pandit, exconsejero delegado de Citigroup.⁹²

En todas partes vemos otra curiosa paradoja: los comerciantes compran y venden títulos en todas las bolsas del mundo en cuestión de nanosegundos; sus operaciones se realizan al instante pero tardan tres días completos en liquidarse. Los gobiernos locales usan no menos de diez agentes diferentes —asesores, abogados, aseguradoras, banqueros, etc.— para conseguir emitir un bono municipal.⁹³ Un jornalero de Los Ángeles cobra el cheque de su sueldo pagando un 4 por ciento de comisión; luego, con su puñado de dólares, hace un giro a su familia en Guatemala y lo sablean de nuevo en concepto de comisiones, tasas de cambio y otros costes ocultos. Cuando los muchos miembros de su familia se reparten el dinero, ninguno tiene para abrir una cuenta bancaria o conseguir crédito. Forman parte de los 2.200 millones de personas que viven con menos de dos dólares al día.⁹⁴ Los pagos que éstos tienen que hacer son muy pequeños, demasiado

pequeños como para que puedan hacerse por redes de pago convencionales como las de las tarjetas de débito y crédito, cuyas comisiones mínimas imposibilitan los llamados micropagos. Para los bancos, servir a esta gente no es una «idea rentable», según reza un estudio reciente de la Facultad de Negocios de la Universidad de Harvard.⁹⁵ De manera que la máquina del dinero no es realmente global ni por su escala ni por su alcance.

Los responsables de la política monetaria y de la regulación de los mercados muchas veces ignoran por completo lo que ocurre, por culpa de la deliberada opacidad de muchas grandes operaciones financieras y de la compartimentación de los controles. La crisis financiera global de 2008 fue un buen ejemplo. La excesiva especulación, la falta de transparencia y una sensación de complacencia causada por incentivos sesgados impidieron que nadie viera el problema hasta que casi fue demasiado tarde. «¿Cómo va a funcionar nada, de la policía al sistema monetario, si no tenemos números ni localizaciones?», se pregunta Hernando de Soto.⁹⁶ Los reguladores siguen tratando de manejar esta máquina con leyes pensadas para la era industrial. En el estado de Nueva York las leyes sobre transferencia de dinero se remontan a la guerra de Secesión, cuando el principal medio de transporte del dinero eran los caballos y los coches.

El sistema financiero es una especie de monstruo a lo Frankenstein, compuesto de contradicciones e incongruencias. ¿Por qué, por ejemplo, necesita Western Union 500.000 puntos de venta en todo el mundo cuando más de la mitad de la población mundial tiene un teléfono inteligente?⁹⁷ Erik Voorhees, uno de los pioneros de bitcoin y destacado crítico del sistema bancario, dice: «Es más fácil enviar a China un yunque por correo postal que dinero por el sistema bancario. ¡Eso es absurdo! El dinero ya es digital, ¡no tienen que enviar dinero contante y sonante cuando hacemos un giro!». ⁹⁸

¿Por qué es tan ineficiente? Según Paul David, el economista que acuñó la expresión «paradoja de la productividad», superponer tecnologías nuevas a infraestructuras ya existentes «no es infrecuente en las transiciones históricas de un paradigma tecnológico a otro». ⁹⁹ Por ejemplo, las fábricas tardaron cuarenta años en usar electricidad comercial frente a la fuerza del vapor, y muchas veces ambos sistemas funcionaron a la vez hasta que los fabricantes se pasaron definitivamente al primero. Durante ese periodo de reequipamiento, la productividad decayó. En el sistema financiero, por su parte, el problema se agrava porque no ha habido una transición clara de una tecnología a la siguiente; hay muchas tecnologías heredadas, algunas de una antigüedad secular, que nunca acaban de funcionar con todo su potencial.

¿Por qué? En parte, porque las finanzas son un monopolio. Opinando sobre la crisis financiera, el premio Nobel Joseph Stiglitz escribió que los bancos «hacían todo lo que podían por aumentar los costes de las transacciones». Añadía que, incluso en el comercio al por menor, los pagos por bienes y servicios básicos «debían costar fracciones de peniques». «Pero ¿cuánto costaban?», se preguntaba. «El uno, dos o tres por ciento del valor de lo vendido y más. El capital y la magnitud de las operaciones, unidos a que tienen licencia regulatoria y social para operar, permiten a los bancos sacar todo lo que pueden de todos los países, especialmente de Estados Unidos, con beneficios de miles de millones.» ¹⁰⁰ Históricamente, las oportunidades de los grandes intermediarios centralizados han sido enormes. No sólo bancos tradicionales (como el Bank of America),

sino también compañías de tarjetas de crédito (Visa), bancos de inversión (Goldman Sachs), bolsas (la de Nueva York), cámaras de compensación (CME), compañías de giros y transferencias de dinero (Western Union), aseguradoras (Lloyd's), asesorías legales (Skadden, Arps), bancos centrales (la Reserva Federal estadounidense), gestorías de inversión (BlackRock), asesorías contables (Deloitte), consultorías (Accenture) y comerciantes de materias primas (Vitol Group) han creado este enorme leviatán. Los engranajes del sistema financiero —intermediarios poderosos que consolidan capital e influencia y muchas veces imponen economías monopolistas— hacen que el sistema funcione, pero también lo ralentizan, aumentan los costes y obtienen exorbitantes beneficios. Debido al monopolio que estos intermediarios ejercen, muchas grandes empresas no encuentran incentivos para perfeccionar sus productos, incrementar la eficiencia, mejorar la experiencia del consumidor ni atraer a la siguiente generación.

Un nuevo «look» para la segunda profesión más vieja del mundo

Los días de este sistema financiero están contados porque la tecnología blockchain promete hacer de la década que viene un tiempo de grandes cambios, pero también de inmensas oportunidades para quienes sepan aprovecharlas. La industria de los servicios financieros tiene hoy mil problemas: está anticuada, se basa en una tecnología obsoleta que desentona de este mundo digital nuestro que avanza a pasos de gigante, y muchas veces lo frena. Es exclusivo y deja a miles de millones de personas sin acceso a mecanismos de financiación básicos. Está centralizado y expuesto a robos de datos y otros ataques, o a la quiebra pura y dura. Y es monopolista, lo que refuerza el *statu quo* y asfixia la innovación. El sistema blockchain promete resolver estos problemas y muchos más porque innovadores y empresarios pueden elaborar nuevas formas de crear valor con esta poderosa plataforma.

Hay seis razones fundamentales por las que la tecnología blockchain traerá profundos cambios a esta industria, acabará con el monopolio financiero y ofrecerá a individuos e instituciones la posibilidad real de crear y administrar valor como ellos quieran. Que tomen nota los participantes de la industria de todo el mundo.

- **Autenticación:** Por primera vez en la historia, dos partes que ni se conocen ni confían la una en la otra pueden hacer negocios. Verificar la identidad y crear confianza ha dejado de ser el derecho y el privilegio del intermediario financiero. Y, lo que es más, en el contexto de los servicios financieros el protocolo fiable cobra un doble significado. El sistema blockchain también puede crear confianza cuando ésta se necesita verificando la identidad y la capacidad de cualquiera de las partes con una combinación de historial de transacciones (en la blockchain), reputación basada en opiniones acumuladas y otros indicadores sociales y económicos.
- **Coste:** En el sistema blockchain la red a la vez realiza y liquida transferencias de valor entre iguales y lo hace continuamente, de suerte que el registro está siempre actualizado. Para empezar, si los bancos aprovecharan este recurso, podrían ahorrar unos 20.000 millones de dólares en gastos de oficina *sin cambiar su modelo de*

negocio básico, según afirma el banco español Santander, aunque la verdadera cifra es, sin duda, mucho mayor.¹⁰¹ Con unos costes mucho más bajos, los bancos podrían ofrecer a individuos e instituciones mayor acceso a los servicios financieros, mercados y capital en comunidades con déficit de servicios. Esto sería un gran beneficio no sólo para las grandes empresas sino también para personas ambiciosas y empresarios de todo el mundo. Cualquiera, en cualquier parte, con un teléfono móvil y una conexión a internet, podría sumarse a la gran corriente de las finanzas globales.

- **Velocidad:** Hoy, los giros de dinero tardan de tres a siete días en liquidarse. Las transacciones bursátiles tardan de dos a tres días, y las de préstamos bancarios una media de nada menos que veintitrés días.¹⁰² La red SWIFT gestiona quince millones de órdenes de pago entre diez mil entidades financieras de todo el mundo, pero tarda días en realizarlas y liquidarlas.¹⁰³ Lo mismo ocurre con el sistema de la Cámara de Compensación Automatizada (ACH, por sus siglas en inglés), que maneja billones de dólares anuales de pagos en Estados Unidos. La red bitcoin tarda unos diez minutos en realizar y liquidar todas las transacciones hechas en ese espacio de tiempo. Otras redes de blockchain son aún más rápidas, y nuevas innovaciones, como la Bitcoin Lightning Network, aspiran a aumentar mucho más la capacidad de la blockchain bitcoin y reducir el tiempo de liquidación de las transacciones a fracciones de segundo.¹⁰⁴ «En el sistema bancario tradicional, donde tenemos al remitente en una red y al destinatario en otra, hay que pasar por muchos registros, muchos intermediarios, muchos saltos. Algo puede fallar en el proceso. Tiene todas las papeletas para ello», dice Chris Larsen, consejero delegado de Ripple Labs.¹⁰⁵ Además, el paso a un sistema de transferencias de valor instantáneo y expedito liberará, para desgracia de los que se aprovechan del *float*, un capital que, de otra manera, permanecería atrapado en el camino.
- **Gestión del riesgo:** La tecnología blockchain promete reducir varias formas de riesgo financiero. El primero es el *riesgo de liquidación*, que consiste en que nuestra transacción nos sea devuelta por algún fallo técnico del proceso. El segundo es el *riesgo de la otra parte*, que consiste en que la parte con la que hemos hecho la transacción quiebre antes de liquidar el pago. El más importante es el *riesgo sistémico*, la suma de todos los riesgos graves que se corren en el sistema con la otra parte. Vikram Pandit llama a éste *riesgo Herstatt*, por alusión al banco alemán que no pudo cumplir con sus obligaciones y quebró: «En la crisis financiera hemos visto que uno de los riesgos era: si comercio con alguien, ¿cómo puedo saber que la otra parte me pagará?». Según Pandit, los pagos instantáneos del sistema blockchain podrían eliminar este riesgo. Los contables podrían examinar el funcionamiento interno de una empresa en todo momento y ver qué transacciones están haciéndose y cómo las registra la red. La irreversibilidad de las transacciones y la verificación instantánea del historial financiero eliminarían un aspecto del *riesgo del agente* o del intermediario, que consiste en que unos administradores sin escrúpulos aprovechen el papeleo y la dilación para ocultar malas prácticas.

- **Innovación del valor:** La blockchain bitcoin fue diseñada para mover bitcoins, no para manejar otro tipo de activos financieros. Pero la tecnología es de código abierto y se presta a la experimentación. Algunos innovadores están desarrollando un tipo de blockchains llamadas «altcoins» para gestionar otras cosas. Otros quieren aprovechar el tamaño y la liquidez de la blockchain bitcoin para crear monedas «derivadas» en las llamadas «cadenas laterales» que pueden «colorearse» para representar cualquier activo o pasivo, física o digital: una acción de bolsa o un bono, un barril de petróleo, un lingote de oro, un coche, una cuota de un coche, una orden de cobro o de pago y, por supuesto, una moneda. Las cadenas laterales son blockchains con características y funciones distintas de la cadena bitcoin pero que funcionan con la red y la infraestructura de ésta sin menoscabo de la seguridad. Las cadenas laterales interactúan con la blockchain mediante un mecanismo de «vinculación bidireccional» (*two-way peg*), un medio criptográfico de transferir activos de la blockchain a las laterales y viceversa sin mediación de terceros. Otros están tratando de eliminar la moneda o ficha definitivamente, creando plataformas de intercambio en blockchains privadas. Las entidades financieras están ya usando la tecnología blockchain para registrar, intercambiar y negociar activos y pasivos, y podrían acabar usándola en lugar de las formas de intercambio tradicionales y los mercados centralizados, con lo que subvertirían nuestra forma de entender el valor y de venderlo y comprarlo.
- **Código abierto:** La industria de los servicios financieros es como una altísima pila de sistemas tecnológicos que han ido superponiéndose y amenazan con desmoronarse. Cambiar algo cuesta porque cada mejora debe ser compatible con todo lo anterior. El sistema blockchain, siendo de código abierto como es, permite la innovación y la mejora constantes, basadas en el consenso de la red. Estas ventajas —autenticación, costes bajísimos, velocidad, pocos riesgos, gran innovación de valor, adaptabilidad— pueden no sólo transformar las formas de pago, sino también el mercado de valores, la banca de inversión, la forma de contabilidad y auditoría, el capital de riesgo, los seguros, la gestión de riesgos empresariales, la banca comercial y otros pilares de la industria. Sigamos adelante.

Los ocho pilares: cómo cambiará el sector de los servicios financieros

Éstas son las ocho funciones que creemos que darán un vuelco radical al mundo financiero. También figuran resumidas en la tabla de la página 101.

- 1. Autenticar la identidad y el valor:** Hoy dependemos de intermediarios poderosos que den confianza y verifiquen nuestra identidad en una transacción financiera. Estos intermediarios son los árbitros últimos del acceso a servicios financieros básicos como cuentas bancarias y préstamos. El sistema blockchain rebaja y a veces elimina por completo el factor confianza en ciertas transacciones. Asimismo, la tecnología permitirá a los usuarios establecer una identidad que sea verificable, sólida y criptográficamente segura, y crear confianza cuando se necesite.

2. **Mover valor:** El sistema financiero mueve a diario dinero por todo el mundo, asegurándose de que ningún dólar se gasta dos veces: desde los noventa y nueve céntimos de una canción en iTunes hasta los miles de millones de dólares que una empresa transfiere internamente, con los que se compra un activo o se adquiere otra empresa. El sistema blockchain puede convertirse en la forma estándar de mover cualquier cosa de valor —monedas, acciones, bonos, títulos— en cantidades pequeñas o grandes, a lugares cercanos o lejanos, con destinatarios conocidos o desconocidos. El sistema blockchain puede ser al movimiento del valor lo que los contenedores estándar hicieron por el movimiento de bienes: reducir mucho los costes, acelerar el intercambio, disminuir los riesgos y estimular el crecimiento y la prosperidad.
3. **Almacenar valor:** Las instituciones financieras son las depositarias del valor para la gente, las instituciones y los gobiernos. En el caso de una persona normal y corriente, un banco guarda valor en cajas fuertes, en cuentas de ahorro o en cuentas corrientes. Las grandes instituciones que quieran liquidez con la garantía de un pequeño rendimiento de sus equivalentes de efectivo optarán por inversiones sin riesgo, como fondos de mercado de dinero o bonos del tesoro. Los individuos no tienen por qué depender en primer lugar de los bancos para que les guarden sus valores o les proporcionen cuentas corrientes y de ahorro, y las instituciones dispondrán de un mecanismo más eficaz para comprar y guardar activos financieros sin riesgo.
4. **Prestar valor:** De préstamos hipotecarios a bonos del tesoro, las instituciones financieras facilitan el crédito en forma, por ejemplo, de tarjetas de crédito, hipotecas, bonos de empresa, bonos municipales, obligaciones del Estado y valores respaldados por activos. El negocio del préstamo ha generado una serie de industrias auxiliares que verifican, puntúan y califican créditos. En el caso de un individuo, lo puntúan; en el caso de una institución, la califican, de bonos de inversión a bonos basura. En el sistema blockchain todos podremos emitir, negociar y liquidar herramientas de deuda tradicionales directamente, con lo que reduciremos los riesgos y las dificultades al aumentar la rapidez y la transparencia. Los consumidores podrán obtener préstamos de otros consumidores. Esto es particularmente importante para las personas que no tienen cuentas bancarias y para los empresarios de todo el mundo.
5. **Intercambiar valor:** Los mercados facilitan diariamente y a nivel mundial el intercambio de billones de dólares de activos financieros. Comerciar consiste en comprar y vender activos y herramientas financieras con objeto de invertir y especular, así como liquidar las operaciones y almacenar el valor. El sistema blockchain acorta los plazos de liquidación de todas las transacciones de días y semanas a minutos y segundos. Esta rapidez y eficiencia crea oportunidades para que las personas sin cuenta bancaria o con una cuenta bancaria precaria participen en la creación de riqueza.

- 6. Financiar e invertir:** Invertir en un activo, compañía o nueva empresa da a las personas la posibilidad de obtener un rendimiento, en forma de revalorización del capital, dividendos, intereses, rentas o alguna combinación de éstos. La industria crea mercados, haciendo que los inversores sean empresarios y dueños de negocios en todas las etapas del crecimiento, desde «ángeles» hasta salidas a bolsa. Hacer dinero suele requerir intermediarios: bancos de inversión, inversores de riesgo y juristas, por mencionar unos pocos. El sistema blockchain automatiza muchas de estas funciones, habilita nuevos modelos de financiación entre iguales y podría hacer que registrar dividendos y pagar cupones fuera más eficiente, transparente y seguro.
- 7. Asegurar el valor y gestionar el riesgo:** La gestión del riesgo, de la que la seguridad forma parte, está destinada a proteger a individuos y compañías de pérdidas y quiebras. Más en general, la gestión del riesgo en los mercados financieros ha dado lugar a una miríada de productos derivados y otras herramientas financieras cuyo objeto es proteger el dinero de contingencias imprevisibles o incontrolables. Según las últimas estimaciones, el valor de todos los derivados extrabursátiles asciende a 600 billones de dólares. El sistema blockchain soporta modelos de seguro descentralizados, que hacen que el uso de derivados para gestionar el riesgo sea mucho más transparente. Utilizar sistemas de reputación basados en el capital social y económico de una persona, sus actos y otros factores de reputación permite a las aseguradoras hacerse una idea más clara del riesgo actuarial y tomar decisiones más informadas.
- 8. Contabilidad para crear valor:** La contabilidad consiste en medir, procesar y comunicar información financiera de entidades económicas. Es un industria multimillonaria controlada por cuatro grandes auditorías: Deloitte Touche Tohmatsu, PricewaterhouseCoopers, Ernst & Young y KPMG. Las prácticas de contabilidad tradicionales no sobrevivirán a la rapidez y complejidad de las finanzas modernas. Los nuevos métodos de contabilidad que usen registros distribuidos de blockchain harán que la auditoría e información financiera sea transparente y ocurra en tiempo real. También mejorará muchísimo la capacidad de reguladores y otras partes interesadas de examinar las operaciones financieras de las empresas.

De intercambiar acciones a intercambiar bloques

«Wall Street ha despertado de verdad», dijo Austin Hill, de Blockstream.¹⁰⁶ Se refería al profundo interés que la industria financiera mostraba por las tecnologías blockchain. Pensemos en Blythe Masters, una de las personas más poderosas de Wall Street. Convirtió el departamento de derivados y productos de JP Morgan en un gigante global y fue pionera en el mercado de derivados. Tras retirarse por un tiempo, entró como consejera delegada en una empresa emergente con sede en Nueva York, Digital Asset Holdings. La decisión sorprendió a muchos. Blythe entendió que el sistema blockchain transformaría su sector igual que internet transformó otras industrias: «Me lo tomaré tan en serio como tendríamos que habernos tomado la idea de internet en los noventa. Es una gran cosa que cambiará el funcionamiento del mundo financiero».¹⁰⁷

TABLA Los ocho pilares: Las transformaciones que producirán las blockchains en los servicios financieros

Función	Impacto de las blockchains	Actores
1. Autenticar la identidad y el valor	Identidades verificables y sólidas, criptográficamente seguras	Agencias de calificación, análisis de datos, comercialización, banca comercial, banca general, redes de tarjetas de pago, reguladores
2. Mover valor: pagar, transferir dinero y comprar bienes y servicios	Transferir valor en grandes y en pequeñas cantidades sin intermediarios reducirá los costes y aumentará la rapidez de los pagos	Banca comercial, banca general, redes de tarjetas de pago, servicios de transferencia de dinero, telecomunicaciones, reguladores
3. Almacenar valor: monedas y productos y activos financieros son modos de almacenar valor. Cajas fuertes, cuentas de ahorro o cuentas corrientes. Fondos del mercado del dinero o bonos del tesoro	Mecanismos de pago combinados con depósitos de valor seguros y fiables reducen la necesidad de recurrir a servicios financieros típicos; las cuentas de ahorro y corrientes quedarán obsoletas.	Banca comercial, corredores de bolsa, banca de inversión, gestión de activos, telecomunicaciones, reguladores
4. Prestar valor: tarjetas de crédito, hipotecas, bonos de empresa, bonos municipales, obligaciones del Estado, bonos respaldados por activos y otras formas de crédito	La deuda puede emitirse, negociarse y liquidarse en el sistema blockchain; aumenta la eficiencia, reduce dificultades y riesgo sistémico. Los clientes pueden usar su reputación para acceder a préstamos de otros clientes; importante para las personas sin cuenta bancaria y para empresarios	Banca general, comercial y minorista, finanzas públicas, micropréstamos, micromecenazgo, reguladores, agencias de calificación, fabricantes de software de calificación crediticia

5. Intercambiar valor: especular e invertir, hacer corresponder órdenes de compra y venta, liquidar operaciones, gestionar y evaluar avales, liquidar y custodiar valores	Las blockchains reducen el tiempo de liquidación de las transacciones de días y semanas a minutos y segundos. Esta rapidez y eficiencia crea oportunidades para que las personas sin cuenta bancaria o con una cuenta bancaria precaria participen en la creación de riqueza	Inversión, banca general, comercio internacional, fondos de inversión y de pensiones, corretaje minorista, cámaras de compensación, mercados de acciones, futuros y materias primas; corretaje de materias primas, bancos centrales, reguladores
6. Financiar e invertir en activos, compañías, empresas emergentes; revalorización del capital, dividendos, intereses, rentas o una combinación de éstos	Nuevos modelos de financiación entre iguales, registro de operaciones de empresas, como pago de dividendos, hecho automáticamente por contratos inteligentes. Registro de derechos para reclamaciones automatizadas de ingresos por alquileres y otras formas de renta	Banca de inversión, capital de riesgo, juristas, auditorías, gestión de la propiedad, bolsas, micromecenazgo, reguladores
7. Asegurar valor y gestionar el riesgo: proteger activos, casas, vidas, salud, propiedad y prácticas mercantiles, productos derivados	Las aseguradoras que usen sistemas de reputación calcularán mejor el riesgo actuarial, creación de mercados de seguros descentralizados. Derivados más transparentes	Seguros, gestión del riesgo, banca general, corredores de bolsa, cámaras de compensación, reguladores
8. Contabilidad para crear valor: una nueva forma de gestión empresarial	El registro distribuido hará que la auditoría y la información financiera sea inmediata y transparente, y mejorará muchísimo la capacidad de los reguladores para examinar las operaciones financieras de las empresas	Auditoría, gestión de activos, protección de accionistas, reguladores

Masters no se había creído lo que al principio se decía de bitcoin, sistema del que se aprovechaban los narcotraficantes, que usaban los jugadores y que celebraban los libertarios por suponerlo capaz de crear un nuevo mundo. Esto cambió en 2014. Masters nos cuenta: «Hubo un momento en que me dije: “¡Ajá!” y empecé a valorar las posibles consecuencias de la tecnología en un mundo que yo conocía bien. Si aplicar al dinero digital la tecnología de registros distribuidos ya era interesante y tenía consecuencias en el sistema de pagos, la tecnología misma de bases de datos en la que se basaba aún tenía más consecuencias».¹⁰⁸ Según Masters, el sistema blockchain podría aumentar la eficiencia y reducir los costes «al permitir que muchas partes funcionaran con la misma información en vez de tener que duplicarla, repetirla y ajustarla una y otra vez». Como mecanismo para registrar transacciones compartidas, descentralizadas y repetidas, el sistema blockchain es el «código de oro», dice.¹⁰⁹

«Tengamos en cuenta que las infraestructuras de los servicios financieros llevan décadas sin evolucionar. Ha evolucionado la fachada, pero no lo que hay detrás», dice Masters. «Ha habido como una carrera para ver quién invertía más en una tecnología dirigida a acelerar la ejecución de una transacción, de manera que hoy día las ventajas competitivas se miden en fracciones de nanosegundos. Lo irónico es que la infraestructura que procesa esa transacción no ha evolucionado.» «El proceso de liquidar las transacciones financieras y guardar registro de ellas sigue tardando días y en algunos casos semanas.»¹¹⁰

Masters no es la única que está entusiasmada con la tecnología blockchain. Bob Greifeld, consejero delegado de Nasdaq, dice: «Creo firmemente en la capacidad que tiene la tecnología blockchain de producir un cambio fundamental en la infraestructura de la industria de los servicios financieros».¹¹¹ Greifeld está integrando la tecnología del registro distribuido del sistema blockchain en la plataforma de mercados privados de Nasdaq gracias a una plataforma llamada Nasdaq Linq. Las bolsas son mercados centralizados de valores y van a cambiar también. El 1 de enero de 2016 Nasdaq Linq completó su primer intercambio con el sistema blockchain. Según Hill, de Blockstream, uno de los mayores administradores de activos del mundo «tiene más gente dedicada a la innovación en materia de blockchain que nosotros en toda nuestra empresa». La empresa de Hill ha ganado más de 75 millones de dólares y emplea a más de veinte personas. «Esta gente quiere entender en serio cómo podemos usar la tecnología para cambiar la manera de hacer negocios.»¹¹² El NYSE, Goldman Sachs, Santander, Deloitte, RBC, Barclays, UBS y prácticamente todas las grandes entidades financieras del mundo tienen el mismo interés. En 2015 la opinión de Wall Street sobre el sistema blockchain era mayoritariamente positiva: en un estudio, el 94 por ciento de los encuestados dijo que este sistema podría desempeñar un importante papel en las finanzas.¹¹³

Aunque muchas otras aplicaciones despiertan el interés de Wall Street, lo que interesa a los responsables financieros de todo el mundo es la idea de usar el sistema blockchain para procesar todas las operaciones de manera segura desde el principio hasta el final, lo que podría reducir enormemente los costes, incrementar la rapidez y la eficacia y mitigar los riesgos de las operaciones. Masters dice: «Todo el proceso de una operación, su ejecución, la conexión de múltiples intercambios, la comprobación de quién hizo qué

con quién y si están de acuerdo, puede ocurrir en el momento de hacerla, mucho antes de lo que ocurre en el mercado financiero convencional». ¹¹⁴ Greifeld lo dice así: «Actualmente liquidamos operaciones “T+3” (o sea, tres días). ¿Por qué no liquidarlas en cinco o diez minutos?». ¹¹⁵

Wall Street compra y vende riesgo, y esta tecnología puede literalmente reducir el riesgo de la otra parte, el riesgo de liquidación y el riesgo sistémico en todo el sistema. Jesse McWaters, director de innovación financiera del Foro Económico Mundial, dice: «Lo mejor de la tecnología de registros distribuidos es la posibilidad de rastrear todas las operaciones, lo que puede mejorar la estabilidad del sistema financiero». Cree que estas «nuevas herramientas permiten a los reguladores hilar más fino». ¹¹⁶ La índole pública del sistema blockchain —su transparencia y su facilidad de inspección—, más el hecho de que liquide automáticamente todas las operaciones y registre inmutablemente el momento en que se producen, permite a los reguladores ver lo que está ocurriendo e incluso programar alertas para que no se les escape nada.

El pacto del Doctor Fausto

Los bancos y la transparencia rara vez van de la mano. La mayoría de los actores financieros ganan competitividad porque aprovechan las asimetrías de información y el mayor conocimiento que tengan del asunto de que se trate en comparación con la competencia. Pero el sistema bitcoin es, por naturaleza, un sistema transparente. Para los bancos esto significa tener que destaparse, por así decirlo. ¿Cómo reconciliamos, pues, una plataforma abierta con la política de puertas cerradas de los bancos?

Austin Hill lo llama el «pacto fáustico» de Wall Street, que les supone una desventaja considerable. ¹¹⁷ «A la gente le gusta la idea de no tener que esperar tres días para liquidar una transacción, sino hacerlo en unos minutos y saber que es definitivo y que es real —dice Hill—. La contrapartida de eso es que todas las transacciones que se hacen en la blockchain [de bitcoin] son completamente públicas. Esto aterroriza a no poca gente de Wall Street.» ¿La solución? Transacciones confidenciales en las llamadas blockchains «de permiso», también conocidas como blockchains privadas. Mientras que la cadena de bitcoin es completamente abierta y no requiere permisos —esto es, cualquiera puede acceder a ella e interactuar con ella—, las blockchains de permiso exigen que los usuarios tengan ciertas credenciales y una licencia para operar en ellas. Hill ha desarrollado la tecnología por la que sólo unos cuantos participantes ven los varios componentes de una transacción y pueden garantizar su integridad.

A primera vista, las blockchains privadas y de permiso parecen presentar unas cuantas ventajas claras. Por ejemplo, sus miembros pueden cambiar fácilmente las reglas de la cadena si lo desean. Los costes pueden mantenerse bajos porque las transacciones sólo necesitan la validación de sus miembros, sin que sean necesarios mineros anónimos que gasten mucha electricidad. Además, como todas las partes son de confianza, es improbable que se produzca lo que se llama un «ataque del 51 por ciento». Se puede tener la seguridad de que los nodos están bien conectados, pues en la mayoría de los casos son grandes instituciones financieras. Además, son más fáciles de controlar por parte de los

reguladores. Sin embargo, estas ventajas también crean debilidades. Cuanto más fácil es cambiar las reglas, más probable es que algún miembro se las salte. Las blockchains privadas también evitan los efectos de red que hacen que una tecnología se desarrolle rápidamente. Limitar intencionadamente ciertas libertades creando nuevas reglas puede afectar a la neutralidad. Por último, sin innovación abierta la tecnología tiende a estancarse y volverse vulnerable.¹¹⁸ Esto no quiere decir que las blockchains privadas no prosperarán, pero los actores de servicios financieros deben tomarse estas cuestiones muy seriamente.

Ripple Labs, que cada vez cuenta con más crédito en círculos bancarios, está desarrollando otra inteligente forma de tranquilizar a Fausto. «Ripple Labs se dirige a la banca general y usamos un método de consenso en lugar del sistema de prueba de trabajo», dice el consejero delegado Chris Larsen, lo que significa que las transacciones no las validan ni mineros ni nodos anónimos.¹¹⁹ La compañía Chain tiene su propia estrategia. Financiada con 30 millones de dólares por Visa, Nasdaq, Citi, Capital One, Fiserv y Orange, Chain se propone dar soluciones de blockchain pensadas para las empresas, principalmente del sector financiero, con una de las cuales, Nasdaq, ya tiene un acuerdo. «Todos los activos del futuro serán instrumentos digitales que funcionarán en múltiples blockchains», dice Adam Ludwin, consejero delegado de Chain. Pero esto no será el mundo de silos al que Wall Street está acostumbrado, «porque todo el mundo opera en el mismo sistema especulativo abierto». ¹²⁰ Los de Wall Street quizá quieran apoderarse de esta tecnología, pero tendrán que vérselas con la innovación que posibilita, algo que no pueden controlar ni predecir.

Masters también ve las virtudes de las blockchains de permiso. En su opinión, sólo un pequeño grupo de socios comerciales, algunos vendedores y los reguladores tienen que tener acceso. A este grupo de elegidos se les proveerá de credenciales. Según Masters, «los registros de permiso tienen la ventaja de no exponer nunca a una institución financiera regulada al riesgo, ni de operar con una parte desconocida, actividad inaceptable desde el punto de vista de la regulación, ni de crear una dependencia con un proveedor de servicios desconocido, como un procesado de transacciones, cosa igualmente inaceptable desde el punto de vista de la regulación». ¹²¹ Estas blockchains de permiso, o cadenas privadas, atraen a las instituciones financieras tradicionales, que no se fían de bitcoin ni de nada que tenga que ver con bitcoin.

Aunque Blythe Masters es consejera delegada de una empresa emergente, el gran interés que muestra por las nuevas tecnologías es un ejemplo de la participación cada vez mayor de los actores financieros tradicionales en el sector. Esta apuesta por nuevas tecnologías refleja la creciente convicción de que estas empresas tecnológicas emergentes también pueden revolucionar las altas finanzas. Para Eric Piscini, de Deloitte, cuyos clientes han tomado conciencia de estos hechos durante el pasado año, el «repentino interés por esta tecnología es algo que nadie se esperaba». ¹²² El entusiasmo se extiende como una epidemia a algunas de las más antiguas y grandes instituciones financieras del mundo.

Barclays es una de las decenas de instituciones financieras que están explorando nuevas oportunidades en la tecnología blockchain. Según Derek White, director de diseño y digital de Barclays, «tecnologías como la blockchain van a cambiar nuestra industria». White está creando una plataforma de innovación abierta que permitirá a su banco contratar a un gran número de creadores y pensadores en esta industria. «Queremos ser pioneros. Pero también conectar con los pioneros de las tecnologías y los traductores de esas tecnologías», dice.¹²³ Barclays invierte dinero en ello, recortando decenas de miles de puestos de trabajo de áreas tradicionales y aumentándolos en el sector tecnológico, sobre todo con el lanzamiento del Acelerador Barclays. Según White, «tres de cada diez empresas con las que nos hemos asociado últimamente son empresas de blockchain o de bitcoin. Las blockchains son la mayor prueba de que el mundo está pasando de los sistemas cerrados a los sistemas abiertos y pueden cambiar radicalmente el futuro no sólo de los servicios financieros, sino de muchas industrias».¹²⁴ ¡Bancos hablando de sistemas financieros abiertos, *mon Dieu!*

El servicio financiero

En el otoño de 2015 nueve de los mayores bancos del mundo —Barclays, JP Morgan, Credit Suisse, Goldman Sachs, State Street, UBS, Royal Bank of Scotland, BBVA y Commonwealth Bank of Australia— anunciaron un plan para colaborar en la creación de modelos comunes de tecnología de blockchain, conocido como R3 Consortium. Desde entonces, treinta y dos más se han unido al esfuerzo y cada pocas semanas se suma otro grupo de destacadas compañías del sector.¹²⁵ Hay dudas sobre hasta qué punto estos bancos se toman en serio la iniciativa. Después de todo, la condición para unirse al grupo es aportar sólo 250.000 dólares, pese a lo cual el R3 constituye un gran salto hacia delante para la industria. Establecer modelos es fundamental para acelerar la adopción y el uso de una nueva tecnología y por eso somos optimistas respecto de la iniciativa. R3 ha contratado a algunos de los principales visionarios y técnicos del sector. Mike Hearn se sumó en noviembre, uniéndose a un grupo que incluye a Richard Gendal Brown, exdirector ejecutivo de innovación bancaria de IBM, y a James Carlyle, ahora director de ingeniería de R3 y exdirector de ingeniería de Barclays.¹²⁶

En diciembre de 2015, la Fundación Linux, en colaboración con un grupo de grandes empresas, lanzó otro proyecto de blockchain, llamado Hyperledger Project. Este proyecto no hace la competencia a R3; al contrario, uno de los miembros fundadores de Hyperledger Project es R3, además de Accenture, Cisco, CLS, Deutsche Börse, Digital Asset Holdings, DTCC, Fujitsu Limited, IC3, IBM, Intel, JP Morgan, London Stock Exchange Group, Mitsubishi UFJ Financial Group (MUFG), State Street, SWIFT, VMware y Wells Fargo.¹²⁷ Con todo, esto demuestra lo muy en serio que la industria está tomándose esta tecnología y también lo reacia que es a adoptar blockchains completamente abiertas y descentralizadas como bitcoin. A diferencia de R3, Hyperledger Project es un proyecto de código abierto que ha encargado a una comunidad el desarrollo de una «blockchain para hacer negocios». Es, sin duda, loable y puede que funcione muy bien. Pero no nos equivoquemos: es un proyecto de código abierto diseñado para crear

tecnologías *reservadas*, lo que se consigue, por ejemplo, limitando el número de nodos de una red o exigiendo credenciales. Como en el caso de R3, una de las prioridades de Hyperledger es establecer modelos. David Treat, de Accenture, uno de los miembros fundadores del grupo, dice: «Una de las claves del proyecto es crear modelos y compartir plataformas que usen los participantes de la industria».

El sistema blockchain también ha abierto un debate sobre el papel que tienen los gobiernos de supervisar la industria de los servicios financieros. La idea de «servicio» parece implicar la existencia de monopolios muy regulados por el Estado. Sin embargo, como la tecnología blockchain promete reducir riesgos y aumentar la transparencia y la capacidad de respuesta, algunos actores del sector afirman que la tecnología misma funciona como regulación.¹²⁸ Si los reguladores pueden escudriñar en el funcionamiento interno de los bancos y los mercados, seguro que también pueden simplificar unas leyes y abrogar otras, ¿verdad? La pregunta no es fácil de contestar. Por un lado, los reguladores tendrán que replantearse su función de supervisión, dado el vertiginoso ritmo de la innovación. Por otro lado, los bancos suelen actuar sin integridad cuando el Estado no interviene.

¿Van los grandes bancos a dominarlo todo gracias al desarrollo de blockchain sin bitcoin, cogiendo los elementos de la tecnología de registros distribuidos que más les convengan y adaptándolos a los modelos de negocio existentes? R3 es una sola de las muchas señales que hay de que los bancos se mueven en este sentido. El 19 de noviembre de 2015, Goldman Sachs registró una patente de «métodos de liquidación de valores en mercados financieros usando técnicas distribuidas, de iguales y criptográficas», con una moneda patentada llamada SETLcoin.¹²⁹ La ironía de que un banco *patente* una tecnología originalmente pensada como de código abierto y accesible para todos no se nos escapa, ni debería escapársele al lector. ¿Acaso era esto lo que Andreas Antonopoulos temía cuando advertía de que los bancos convertirían bitcoin de «rock punk en *smooth jazz*»?¹³⁰ O quizá los bancos tendrán que competir por los mejores productos y servicios con entidades radicalmente diferentes cuyos dirigentes se oponen a todo lo que esos bancos representan.

El servicio financiero del futuro podría ser un «jardín vallado» y bien cuidado, que una camarilla de interesados influyentes explotara, o podría ser un ecosistema orgánico y vasto, en el que la fortuna económica de las personas crecieran allí donde hubiera luz. El debate está servido, pero si la experiencia de la primera generación de internet nos ha enseñado algo es que los sistemas abiertos funcionan mejor que los cerrados.

La aplicación bancaria: quién ganará en la banca comercial

El Google del capital: eso es lo que está creando Jeremy Allaire, «una empresa de bienes de consumo financieros que ofrece a los consumidores productos para que guarden y envíen dinero, cursen y reciban pagos, los servicios fundamentales que la gente espera que le ofrezca la banca comercial».¹³¹ Él lo ve como un servicio poderoso, instantáneo y

gratuito para cualquiera que disponga de un dispositivo con acceso a internet. Su empresa, Circle Internet Financial, es una de las más grandes y mejor financiadas del sector.

Circle es todo menos una empresa bitcoin. «Amazon no era una compañía HTTP, ni Google era una compañía SMTP. Circle no es una compañía bitcoin», dice Allaire. «Para nosotros, bitcoin es la siguiente generación de protocolos de internet fundamentales que se usan en la sociedad y en la economía.»¹³²

Para Allaire, el sector de los servicios financieros es el último foco de resistencia, y quizá el mayor premio, que ha de ser transformado esencialmente por la tecnología. «Si nos fijamos en la banca comercial, hay tres o cuatro cosas que los bancos comerciales hacen. Una es que proporcionan un lugar donde almacenar valor. Otra es que ofrecen algún tipo de servicio de pago. Además de eso, dan crédito y nos proporcionan un sitio donde almacenar riqueza y generar posibles ingresos.»¹³³ Su visión: «Dentro de cuatro o cinco años, una persona será capaz de descargar una aplicación, almacenar valor digitalmente en la moneda que quiera —dólares, euros, yenes, renminbis o monedas digitales— y hacer pagos inmediata o casi inmediatamente con interoperabilidad global, con un altísimo nivel de seguridad y sin fugas de información privada. Y lo más importante, será gratis».¹³⁴ Igual que internet ha transformado los servicios informativos, así transformará el sistema blockchain los servicios financieros, dando pie a nuevas capacidades hasta el momento inimaginables.

Según Allaire, los beneficios de la tecnología blockchain —liquidación instantánea, interoperabilidad global, altos niveles de seguridad y transacciones casi gratis— benefician a todo el mundo, tanto a las personas como a los negocios. ¿Y qué decir de su idea de que todo sea gratis? ¡Herejía!, claman los banqueros de todo el mundo. ¡Desde luego, Goldman Sachs y la empresa china IDG no han invertido 50 millones de dólares para crear una empresa sin ánimo de lucro o de interés público!¹³⁵ «Si conseguimos crear una franquicia global con decenas de millones de usuarios y ser la plataforma que usen para realizar sus transacciones, entonces será un activo de mucho valor.» Allaire quiere que Circle «tenga la capacidad subyacente de ofrecer otros productos financieros». Aunque no lo dice específicamente, los datos financieros de millones de consumidores podrían ser más valiosos para la empresa que sus activos financieros. «Queremos reinventar la experiencia de los consumidores y su relación con el dinero, así como darles la posibilidad de elegir cómo se usa su dinero y cómo pueden generar más dinero con él.»¹³⁶ Líderes del viejo paradigma, tomad nota.

Empresas como Circle están libres de la carga de la herencia y la cultura de viejos paradigmas. Su planteamiento novedoso puede ser una gran ventaja. Muchos de los grandes innovadores del pasado fueron personas ajenas al sistema. Netflix no lo inventó Blockbuster. iTunes no lo inventó Tower Records. Amazon no lo inventó Barnes & Noble. Ésa es la idea.

Stephen Pair, consejero delegado de BitPay, una de las empresas pioneras del sector, cree que los recién llegados tienen una clara ventaja. «Emitir activos fungibles como acciones, bonos y monedas en el sistema blockchain y crear la infraestructura necesaria para hacer que crezcan y sean rentables no requiere que tengamos currículo de

banqueros», dice. Para empezar, «no necesitamos toda la infraestructura e instituciones heredadas que constituye hoy Wall Street... No sólo podemos emitir estos activos en la blockchain, sino que podemos crear sistemas con los que sea posible hacer transacciones atómicas instantáneas como ésta, por ejemplo: yo tengo acciones de Apple en mi cartera y quiero comprarte algo, pero tú quieres dólares. Con esta plataforma, puedo realizar una transacción atómica (o sea, de todo o nada) y emplear mis acciones de Apple para enviarte dólares». ¹³⁷

¿De verdad es tan fácil? La batalla por reinventar la industria de los servicios financieros no es como la batalla por el comercio electrónico de los primeros días de la red. Para que negocios como el de Allaire prosperen, deben facilitar una de las mayores transferencias de valor de la historia humana, y mover billones de dólares desde millones de cuentas bancarias tradicionales a millones de carteras de Circle. Y esto no es fácil. Los bancos, pese a su entusiasmo por el sistema blockchain, no se fían de estas empresas, porque dicen que son empresas de «alto riesgo». Quizá su resistencia se deba al miedo de acelerar su propia desaparición. Han surgido intermediarios entre el viejo y el nuevo mundo. Vogogo, una empresa canadiense, está ya trabajando con Coinbase, Kraken, BitPay, Bitstamp y otros para abrir cuentas bancarias, cumplir con las normas y permitir que los consumidores transfieran dinero a carteras de bitcoin con métodos de pago tradicionales. ¹³⁸ ¡Qué ironía! Mientras que Amazon puede saltarse a la competencia minorista fácilmente, los líderes de este nuevo paradigma deben respetar a los del viejo.

Quizá necesitamos un banquero que tenga la voluntad de experimentar propia de Silicon Valley. Suresh Ramamurthi tiene todas las papeletas para serlo. Este hindú, exejecutivo de Google e ingeniero de software, sorprendió a muchos cuando decidió comprar el banco CBW, sito en el pueblo de Weir, Kansas, de 650 habitantes. Para él, este pequeño banco local era un laboratorio para usar el protocolo de blockchain y las vías de pago basadas en bitcoin para realizar giros de dinero transfronterizos. En su opinión, los empresarios del sistema blockchain que no conozcan los detalles de los servicios financieros están condenados al fracaso. Dice: «Están haciendo una ventana en el edificio pintándola de bonitos colores. Pero no se puede solucionar el problema desde fuera. Tienes que hablar con alguien de dentro del edificio, que conozca cómo funciona la fontanería». ¹³⁹ En los últimos cinco años, Suresh ha sido consejero delegado del banco, director de información, director de cumplimiento normativo, cajero, portero y, sí, fontanero. Suresh conoce ahora la fontanería bancaria.

Muchos veteranos de Wall Street no ven que haya guerra entre lo viejo y lo nuevo. Blythe Masters cree que hay «al menos tantas maneras de que los bancos mejoren la eficiencia y operaciones de Wall Street como oportunidades de revolución por parte de los nuevos competidores». ¹⁴⁰ Nosotros no podemos evitar creer que lo radicalmente nuevo lleva las de ganar. Por eso las grandes cadenas de televisión no inventaron YouTube, ni los grandes fabricantes de coches inventaron Uber, ni las grandes cadenas de hoteles inventaron Airbnb. Para cuando los magnates de las mil mayores empresas decidan seguir un nuevo camino de crecimiento, un nuevo competidor habrá chocado contra ellos con velocidad, agilidad y mejores ofertas. Independientemente de quién salga

ganando, la colisión entre la imparable fuerza del cambio tecnológico y el inamovible obstáculo de los servicios financieros, la industria más atrincherada del mundo, promete ser violenta.

El traductor Google de los negocios: nuevas formas de contabilidad y administración empresarial

«Las asesorías contables son como champiñones: crecen en la oscuridad y se nutren de basura», dice Tom Mornini, consejero delegado de Subledger, una empresa emergente dedicada al sector contable.¹⁴¹ La contabilidad se ha convertido en el lenguaje de las finanzas, ininteligible para todos excepto para unos cuantos iniciados. Si todas las transacciones pudieran verse en un registro compartido y globalmente distribuido, ¿por qué habríamos de necesitar asesores contables que nos las tradujeran?

La contabilidad moderna nació en la curiosa mente de Luca Pacioli, en Italia, en el siglo XV. Su engañosamente sencilla invención era un método llamado «de partida doble», según el cual todos los participantes en una transacción han de anotar un debe y un haber en el balance, el registro de activos y pasivos. Al codificar estas normas, Pacioli puso orden en unas prácticas arbitrarias que impedían crecer a las empresas.

Ronald Coase piensa que la contabilidad es como un culto. Cuando era estudiante en la Facultad de Economía de Londres, Coase veía «aspectos religiosos» en esta práctica. «Los libros que se confiaban a los contables parecían libros sagrados.» Los estudiantes de contabilidad consideraban las críticas que él hacía «sacrílegas».¹⁴² ¿Cómo se atreve a poner en duda sus «muchos métodos para calcular la amortización, valorar inventarios, asignar gastos y demás, todos los cuales daban resultados diferentes pero todos los cuales eran prácticas contables perfectamente aceptables», y otras prácticas *casi* idénticas que, sin embargo, eran consideradas completamente «indignas de respeto»? Por eso Tom Mornini es el primero que critica la profesión.

Nosotros vemos cuatro problemas con la contabilidad moderna. Primero, el sistema actual depende de que los administradores juren que tienen sus libros en orden. Decenas de casos de primer orden —Enron, AIG, Lehman Brothers, WorldCom, Tyco y Toshiba— demuestran que los administradores no siempre actúan con integridad. La avaricia domina a mucha gente. El amiguismo, la corrupción y la información falsa causan bancarrotas, pérdidas de empleo y crisis de mercado, pero también altos costes y mayor control del capital.¹⁴³

Segundo, la principal causa de los errores contables se debe a fallos humanos, según AccountingWEB. Muchas veces los problemas empiezan cuando alguien teclea mal un número en una hoja de cálculo y, como una mariposa que agita las alas, el pequeño error se convierte en un gran problema cuando pasa a los cálculos del balance.¹⁴⁴ Casi el 28 por ciento de los profesionales afirma que las personas introducen datos erróneos en el sistema informático de sus empresas.¹⁴⁵

Tercero, nuevas leyes como la de Sarbanes-Oxley han hecho poco para acabar con el fraude contable. Si acaso, la creciente complejidad de las empresas, unas transacciones con más facetas y la rapidez del comercio moderno crean nuevas formas de ocultar las

malas prácticas.

Cuarto, los métodos tradicionales de contabilidad no pueden conciliarse con los nuevos modelos de negocio. Pongamos por ejemplo las microtransacciones. La mayoría de los programas de contabilidad permiten dos lugares decimales (esto es, un penique), por lo que no sirven para microtransacciones de ningún tipo.

La contabilidad —la medición, el procesamiento y la comunicación de información financiera— no es el problema. Desempeña una función crítica en la economía actual. Pero el desarrollo de los métodos contables debe ponerse al día con la era moderna. Pensemos que en tiempos de Pacioli se hacían auditorías a diario. Hoy se hacen de uvas a peras. ¿En qué otra industria quinientos años de progreso tecnológico han *aumentado* el tiempo que tarda en ejecutarse una tarea en un 9.000 por ciento?

El «registro mundial»

Hoy, las empresas registran un debe y un haber con cada transacción; dos entradas, es decir, una contabilidad por partida doble. Podrían añadir fácilmente una tercera entrada en el «registro mundial» que sería instantáneamente accesible para quienes necesitaran verla, como accionistas, auditores o reguladores. Imaginemos que cuando una gran empresa como Apple vende productos, compra materias primas, paga a sus empleados o hace balance de activos y pasivos, el registro mundial asentara la transacción y publicara un recibo con fecha y hora en la blockchain. Los informes financieros de una empresa serían un registro vivo, que podría auditarse, revisarse y verificarse. Generar cualquier parte financiero actualizado al minuto debería ser tan sencillo como usar una función de hoja de cálculo, que con pulsar una tecla nos da un informe financiero inmutable, completo, verificable y carente de errores. Puede que las empresas no quieran que todo el mundo vea esos números, para que los ejecutivos sólo den acceso a reguladores, administradores y otros actores clave.

Muchas personas del sector ven las consecuencias que este registro mundial podría tener en la contabilidad. Según Simon Taylor, de Barclays, un registro como éste podría racionalizar el cumplimiento de la regulación por parte de los bancos y reducir riesgos. «Hacemos un montón de trabajo informativo en materia de regulación en el que decimos lo que hemos hecho porque lo que hemos hecho queda archivado en un sistema que nadie más puede ver.»¹⁴⁶ Un registro mundial en el que todo quedara asentado de una manera transparente permitiría que «los reguladores tuvieran acceso a la misma base de datos, lo que conllevaría menos trabajo y menos costes, y la posibilidad de hacer auditorías en tiempo real. Es una gran cosa».¹⁴⁷ Para Jeremy Allaire, de Circle, los más beneficiados son los reguladores. «Los inspectores de bancos tienen que depender de sistemas contables y registros privados y opacos para hacer su trabajo —dice Allaire—. Con un registro público y compartido, los auditores e inspectores de bancos dispondrían de métodos fiscales automatizados para ver hasta qué punto está saneado un balance y es fuerte una empresa, una innovación importante que podría automatizar partes relevantes de la regulación, así como de la auditoría y la contabilidad.»¹⁴⁸

Un registro mundial incorporaría la integridad en el sistema. «Cometer un fraude será mucho más difícil. Hay que cometerlo en un sistema en desarrollo y no podemos volver atrás y cambiar nuestros registros», dice Christian Lundkvist, de Balanc3, una empresa emergente de contabilidad por partida triple basada en Ethereum.¹⁴⁹ Austin Hill afirma: «Un registro público constantemente auditado y verificado significa que no tenemos que fiarnos de los libros de nuestro socio; hay integridad en los informes o en los logaritmos de las transacciones, porque la misma red lo comprueba. Es como una auditoría criptográfica que se realiza de antemano y continuamente. No dependemos de PricewaterhouseCoopers ni de Deloitte. No existe el riesgo de la otra parte. Si el registro dice que es verdad, es que es verdad».¹⁵⁰

Deloitte, una de las cuatro mayores empresas auditoras del mundo, quiere entender el impacto del sistema blockchain. Eric Piscini, que dirige el centro de criptomoneda de Deloitte, les dice a los clientes que el sistema blockchain es «un gran riesgo para nuestro modelo de negocio porque ahora el negocio de la banca es gestionar el riesgo. Si mañana desaparece ese riesgo, ¿qué vamos a hacer?». ¹⁵¹ El negocio de la auditoría está a punto de ser revolucionado, y esta actividad constituye una tercera parte de las ganancias de Deloitte.¹⁵² Piscini añade: «Es toda una revolución de nuestro modelo de negocio. Hoy empleamos muchísimo tiempo auditando empresas y les cobramos la correspondiente tarifa. Mañana, si ese proceso se racionaliza y simplifica porque las blockchains registran el momento exacto de todas las operaciones, cambiará la manera como auditamos empresas».¹⁵³ ¿O quizá acabará con las auditorías mismas?

Deloitte ha desarrollado una solución llamada PermaRec (por «Permanent Record» o registro permanente) con la que «Deloitte registrará esas transacciones en una blockchain que le permitirá auditar a una de las partes o a las dos muy rápidamente, porque las transacciones quedan grabadas».¹⁵⁴ Pero si la tercera entrada de la blockchain — registrada con fecha y hora y que todo el mundo puede ver— se realiza automáticamente, cualquiera, en cualquier parte, puede saber si las cuentas cuadran. Sin embargo, el sector de mayor crecimiento para Deloitte y las otras tres grandes auditorías es el de los servicios de asesoría. Muchos clientes no entienden el fenómeno blockchain. Este desconcierto favorece que las personas recurran a servicios de consultoría.

Mornini, un intrépido empresario que se define a sí mismo como un «eterno optimista», dice que la contabilidad periódica es como «mirar a una persona que baila delante de una luz estroboscópica. Sabemos que está bailando, pero no vemos cómo lo hace. Resulta curioso, pero cuesta imaginarse todos los pasos que hay en medio».¹⁵⁵ La contabilidad periódica es como un resumen. La auditoría es, por definición, un proceso retrospectivo. Dar una idea completa de la salud financiera de una empresa a partir de datos financieros periódicos es como querer convertir una hamburguesa en una vaca.

Según Mornini, las mayores empresas nunca querrán que exista una contabilidad transparente que sea de dominio público y ni siquiera accesible a personas privilegiadas como auditores o reguladores. Las finanzas de una empresa son su secreto mejor guardado. Además, muchas empresas quieren que sus administradores dispongan de cierto grado de flexibilidad a la hora de contabilizar ciertas cosas, considerar un ingreso, amortizar un activo o asentar un cargo de fondo de comercio.

Pero Mornini cree que una mayor transparencia beneficiaría a las empresas, no sólo porque les permitiría racionalizar el departamento de finanzas o reducir los gastos de auditoría, sino porque aumentaría su valor de mercado. Dice: «La primera empresa que adopte este sistema verá aumentar significativamente su cotización, o su relación precio-beneficio, con respecto a otras empresas cuyos inversores han de esperar con impaciencia el goteo de información financiera que les dan trimestralmente». Después de todo, añade, «¿quién va a invertir en una empresa que nos muestra lo que pasa cada tres meses, comparada con una que hace lo propio en todo momento?». ¹⁵⁶

¿Exigirán los inversores que la contabilidad por partida triple sea una norma de la gestión empresarial? La pregunta tiene su sentido. Muchos inversores institucionales, como los del plan de jubilación de los funcionarios de California, han desarrollado unas normas de gestión empresarial estrictas y no invertirán en una empresa que no las cumpla. ¹⁵⁷ La contabilidad por partida triple podría ser la siguiente de esas normas.

La contabilidad por partida triple: la privacidad es para los individuos, no para las empresas

La contabilidad por partida triple tiene sus escépticos. Izabella Kaminska, periodista del *Financial Times*, cree que imponer la contabilidad por partida triple hará que muchas transacciones queden fuera del balance contable de las empresas. «Siempre habrá personas que se nieguen a seguir el protocolo y escamoteen y escondan valores en redes paralelas independientes, lo que llamamos “mercado negro”, “valores fuera de balance” o “banca en la sombra”». ¹⁵⁸

¿Cómo hacer cálculos contables que no estén basados en transacciones, sobre todo cuando se trata de activos intangibles? ¿Cómo contabilizar los derechos de propiedad intelectual, el valor de marca o incluso el prestigio de los famosos, por ejemplo de Tom Hanks? ¿Cuántas películas malas debe hacer este oscarizado actor para que el sistema blockchain empiece a depreciar el valor de la marca Hanks?

Defender la contabilidad por partida triple no es ir contra la contabilidad tradicional. Siempre habrá áreas en las que se necesiten auditores competentes. Pero si la contabilidad por partida triple, puesto que permite registrar, archivar, verificar y auditar transacciones en tiempo real, puede aumentar la transparencia y la inmediatez de la contabilidad de una empresa, entonces el sistema blockchain podría resolver muchos de los mayores problemas contables. Deloitte necesitará a alguien que calcule en tiempo real el valor de activos intangibles y desempeñe otras funciones contables que el sistema blockchain no pueda desempeñar, pero no necesitará a una legión de auditores.

Por último, ¿de verdad es deseable que todo quede registrado indeleblemente? En Europa hay tribunales que fallan a favor del «derecho al olvido» y dan curso a reclamaciones de personas que quiere borrar su historial de internet. ¿No habría que aplicar el mismo principio a las empresas? No. ¿Por qué los conductores de Uber están sujetos a la evaluación de los clientes y no han de estarlo los ejecutivos de una empresa? Imaginemos un mecanismo —una «aplicación de la confianza», digamos— que registre

las opiniones de los clientes en un registro público y establezca una puntuación independiente y rastreable de la integridad de las empresas. En la caja negra de éstas, la luz del sol es el mejor desinfectante.

La contabilidad por partida triple es la primera de las muchas innovaciones en materia de gestión empresarial. Como muchas instituciones de la sociedad, nuestras empresas sufren una crisis de legitimidad. El activista y accionista Robert Monks dice: «El capitalismo se ha convertido en una cleptocracia, pensada por y para el enriquecimiento de los consejeros delegados de las empresas, o lo que yo llamo los “reyes gerentes”». ¹⁵⁹

El sistema blockchain devuelve el poder a los accionistas. Supongamos que una ficha que representa un activo, un «bitshare», viniera acompañada de uno o muchos votos, cada uno de los cuales abogara por una decisión empresarial concreta. La gente podría votar a sus apoderados desde cualquier parte, con lo que las acciones importantes que hubieran de emprender las empresas podrían someterse a una votación más inmediata, más inclusiva y menos susceptible de manipulación. Las decisiones que se tomaran dentro de las empresas requerirían un consenso real y un gran número de firmas, y cada accionista tendría voz y voto a la hora de decidir el futuro de la empresa. Una vez que los votos se han emitido, la decisión y las actas de las juntas de los consejos de administración quedarían registradas con fecha y hora en un registro inmutable.

¿Y no tienen las empresas derecho a cambiar su historial, derecho al olvido? ¹⁶⁰ No. Como productos de la sociedad que son, las empresas tienen responsabilidades inherentes al permiso que se les ha dado para operar. Además, tienen el deber para con la sociedad de hacer pública toda la información que se refiera a sus negocios. Claro está que las empresas tienen el derecho y la obligación de guardar el secreto industrial y proteger la privacidad de sus empleados, personal y demás actores. Pero eso es otra cosa. Aumentar la transparencia es una gran oportunidad para los empresarios de todo el mundo: oportunidad de elevar al máximo los niveles de calidad de la gestión empresarial y erigirse en paladines de la confianza, y todo eso gracias a la adopción de las blockchains.

Reputación: somos el crédito que tenemos

Sea que pidamos nuestra primera tarjeta de crédito, sea que solicitemos un préstamo, lo primero que el banco valorará será cuánto crédito tenemos, nuestra «calificación crediticia». Esta cifra representa nuestra solvencia y, en consecuencia, el riesgo de que no cumplamos. Es el resultado de una serie de factores, que van del plazo de amortización del préstamo al historial de pagos. La mayoría de los préstamos minoristas dependen de esto. Pero este cálculo tiene muchos fallos. Primero, es muy reductivo. Un joven sin antecedentes crediticios puede tener fama de solvente, de cumplir con sus compromisos, o puede tener una tía rica. La calificación crediticia no tiene en cuenta ninguno de estos factores. Segundo, la calificación crea incentivos perversos para los individuos. La gente usa cada vez más la tarjeta de débito, es decir, el dinero que tiene en sus cuentas. Como no tienen calificación crediticia, son penalizados. Sin embargo, las empresas de tarjetas de crédito siguen animando a la gente a que pida tarjetas de crédito. Tercero, las

calificaciones crediticias van con mucho retraso: los datos en que se basan pueden quedar anticuados y ser poco relevantes. Que nos retrasemos en un pago a los veinte años tiene poco que ver con nuestro riesgo crediticio a los cincuenta.

FICO, una agencia estadounidense que antes se llamaba Fair, Isaac and Company, domina el mercado de las calificaciones crediticias en Estados Unidos, pero en sus análisis no tiene en cuenta la información más relevante. Marc Andreessen dice: «PayPal puede dar una calificación en tiempo real y en milésimas de segundos, basándose en nuestro historial de compras en eBay, que resulta ser una fuente de información más fiable que la que usa FICO para calificarnos».¹⁶¹ Estos factores, combinados con datos sobre transacciones y negocios y otros atributos generados por la tecnología blockchain, pueden crear un algoritmo mucho más potente para determinar el riesgo crediticio y de gestión.

¿Qué reputación tenemos? Todos tenemos al menos una. La reputación es un factor esencial de la confianza en los negocios y en la vida cotidiana. Hasta ahora, los intermediarios financieros no han usado la reputación como base para crear confianza entre individuos y bancos. Pensemos en el propietario de un pequeño negocio que quiere pedir un préstamo. Lo más frecuente es que el encargado de turno del banco base su decisión en la documentación que aporta la persona, su identidad considerada desde un solo punto de vista y su calificación crediticia. Por supuesto, un ser humano es mucho más que la suma de su número de la seguridad social, su lugar de nacimiento, su domicilio y su historial de crédito. Pero el banco no sabe, ni le importa, si somos unos empleados cumplidores, unos voluntarios activos, unos ciudadanos comprometidos, o los entrenadores del equipo de fútbol de nuestro hijo. El encargado de conceder el préstamo puede valorar que nos comportemos con integridad, pero el sistema de calificación del banco no. Estos componentes de la reputación son difíciles de formular, documentar y usar tal y como están concebidos los sistemas social y económico actuales. La mayoría de ellos son etéreos y efímeros.

Entonces, ¿qué hacen los miles de millones de personas que no tienen reputación más allá de su círculo social inmediato? Allí donde hay servicios financieros disponibles para los pobres del mundo, muchos no pueden cumplir con los requisitos de identidad exigidos, como presentar un documento de identidad, un certificado de residencia o un historial financiero. Este problema también se da en el mundo desarrollado. En diciembre de 2015, muchos grandes bancos estadounidenses se negaron a aceptar el recién creado documento de identidad de Nueva York como credencial válida para abrir una cuenta bancaria, pese a que más de 670.000 personas lo solicitaron y los reguladores bancarios federales aprobaron su uso.¹⁶² El sistema blockchain puede resolver este problema dando a la gente la posibilidad de crear identidades únicas con varios atributos, entre ellos el historial de transacciones, y alternativas al sistema bancario tradicional.

Sigue habiendo muchos casos —sobre todo en materia de crédito— en los que el sistema blockchain crea confianza entre las partes cuando esa confianza se necesita. La tecnología blockchain no sólo funciona para que el capital prestado vaya al prestatario, sino que también garantiza que éste lo devuelva con intereses. Da poder a las dos partes con sus propios datos, refuerza su privacidad y genera una nueva identidad económica

perdurable basada en factores como el historial económico y el capital social de cada cual. Patrick Deegan, director de tecnología de Personal BlackBox, empresa dedicada a la identidad digital, dice que las personas «formarán y gestionarán algún día su propia identidad y establecerán conexiones de confianza con otros iguales y nodos» gracias a la tecnología blockchain.¹⁶³ Como esta tecnología registra y archiva todas las transacciones en un registro inmutable, todas ellas pueden servir para incrementar nuestra reputación y solvencia. Además, las personas pueden decidir qué identidad quieren que interactúe con esta o aquella institución. Dice Deegan: «Puedo crear diferentes identidades que representen sendos aspectos de mí mismo, y elijo la identidad que quiero que trate con la empresa».¹⁶⁴ Los bancos y otras empresas que operen con el sistema blockchain no deben pedir ni incorporar más información que la que necesitan para prestar sus servicios.

Este modelo ha demostrado que funciona. BTCjam es una plataforma de préstamo entre iguales que usa la reputación como base para conceder créditos. Los usuarios pueden vincular su perfil de BTCjam a Facebook, LinkedIn, eBay o Coinbase para reforzar su reputación. Los amigos pueden recomendarnos desde Facebook. Incluso podemos incluir nuestra calificación crediticia actual como uno de los muchos atributos. Ninguno de estos datos se divulga. Los usuarios de esta plataforma empiezan con una calificación baja. Pero enseguida pueden ganarse una reputación mostrando que son prestatarios fiables. La mejor estrategia es empezar con un «préstamo de reputación» para demostrar que somos de fiar. Como usuarios que piden financiación, tendremos que contestar a una serie de preguntas del inversor. No contestarlas significa que algo pasa y la comunidad dudará en financiarnos. Para nuestro primer préstamo, pidamos una suma razonable y devolvámosla a tiempo. Cuando lo hayamos hecho, nuestra puntuación aumentará y otros miembros de la comunidad podrían dar una opinión positiva sobre nosotros. Hasta septiembre de 2015 BTCjam ha concedido 18.000 préstamos por un total de 14 millones de dólares.¹⁶⁵

El empresario Erik Voorhees pide sentido común: «Con un sistema basado en la reputación, la gente que más puede permitirse comprar una casa será la que más fácilmente la compre. Los que menos puedan permitírsela tendrán difícil conseguir un préstamo». Para él, este método «bajará los costes para los buenos actores y los subirá para los malos, lo que es el mejor incentivo».¹⁶⁶ En sistemas basados en la reputación, nuestra solvencia no derivará de una calificación que dé FICO, sino de un conjunto de atributos que forman nuestra identidad y avalan nuestra capacidad de devolver un préstamo. La calificación crediticia de las empresas también cambiará para incluir la nueva información y los nuevos factores que el sistema blockchain hace posibles. Imaginemos unas herramientas que integren la reputación y rastreen diferentes aspectos de ella, como la solvencia económica, la competencia profesional y la conciencia social. Imaginemos una forma de préstamo basada en valores compartidos, en la que la gente que nos presta dinero valora el papel que desempeñamos en la comunidad y nuestras metas.

La oferta pública de venta del sistema blockchain

La semana del 17 de agosto de 2015 fue una mala semana: la bolsa china se hundió, el índice S&P 500 tuvo la peor caída en cuatro años y los expertos de todo el mundo hablaron de que podía producirse otra recesión económica global y hasta una crisis. Las ofertas públicas de venta fueron retiradas del mercado, las fusiones de empresas se paralizaron y Silicon Valley empezó a ponerse nervioso por la sobrevaloración de sus queridos «unicornios», como se llama a las empresas privadas valoradas en más de 1.000 millones de dólares.

En medio del pánico, una empresa llamada Augur lanzó una de las más exitosas campañas de micromecenazgo o financiación colectiva de la historia. En la primera semana, más de 3.500 personas de Estados Unidos, China, Japón, Francia, Alemania, España, el Reino Unido, Corea, Brasil, Sudáfrica, Kenia y Uganda contribuyeron con un total de 4 millones de dólares. No hubo corretaje, ni banco de inversión, ni bolsa, ni documentación obligatoria, ni regulador, ni abogados. Ni siquiera hubo un Kickstarter ni un Indiegogo. Señoras y señores, bienvenidos a la oferta pública de venta del sistema blockchain.

Poner en contacto a inversores con empresarios es una de las ocho funciones de la industria de los servicios financieros que es más probable que cambien radicalmente. El proceso de reunir capital líquido —mediante inversión privada, ofertas públicas de venta, ofertas secundarias e inversiones privadas en valores públicos (PIPE, por sus siglas en inglés)— no ha cambiado significativamente desde los años treinta del siglo pasado.¹⁶⁷

Gracias a las nuevas plataformas de micromecenazgo, las pequeñas empresas pueden acceder al capital usando internet. Las gafas de realidad virtual Oculus Rift y el reloj inteligente Pebble se financiaron gracias a este modelo. Sin embargo, los participantes no podían comprar acciones directamente. Hoy, la ley «Jumpstart Our Business Startups» (literalmente «Pongamos en marcha nuestra empresa emergente») permite que los pequeños inversores inviertan directamente en campañas de micromecenazgo, pero tanto inversores como empresarios siguen necesitando intermediarios como Kickstarter o Indiegogo, así como un método de pago convencional, normalmente tarjeta de crédito o PayPal, para participar. El intermediario es el último árbitro de todo y decide quién posee qué.

La oferta pública de venta del sistema blockchain va más allá. Ahora, las empresas pueden reunir capital «en el sistema blockchain» emitiendo fichas o criptotítulos que tengan algún valor en la empresa. Pueden ser acciones, bonos o, como en el caso de Augur, títulos de creador de mercados en la plataforma, que da a los inversores el derecho de decidir qué mercados de predicción abrirá la empresa. Ethereum tuvo aún más éxito que Augur y financió el desarrollo de una blockchain completamente nueva mediante la venta masiva de su ficha, el ether. Hoy, Ethereum es la blockchain pública que más rápidamente crece y la segunda más larga. La inversión media de los micromecenas de Augur era de unos 750 dólares, pero pueden hacerse también suscripciones de un dólar e incluso de diez céntimos. Cualquier persona del mundo —incluso del país más pobre y remoto— puede convertirse en un inversor de bolsa.

Overstock, la empresa de venta electrónica, está lanzando la que probablemente sea la iniciativa de criptovalores más ambiciosa que ha habido hasta ahora. Su visionario fundador, Patrick Byrne, cree que el sistema blockchain «puede hacer por el mercado de capitales lo que internet ha hecho por los consumidores». El proyecto, llamado Medici, capacita a las empresas para emitir valores en blockchain y hace poco ha recibido el beneplácito de la comisión del mercado de valores de Estados Unidos, la SEC.¹⁶⁸ La empresa empezó emitiendo sus primeros valores basados en el sistema blockchain, como criptobonos por valor de 5 millones de dólares para una filial de FNY Capital, en 2015.¹⁶⁹ Overstock afirma que muchos servicios financieros y otras empresas han empezado a usar la plataforma. Desde luego, con la tácita aprobación de la SEC, Overstock arranca con ventaja en lo que sin duda es un largo viaje.

Si las ofertas públicas de venta del sistema blockchain siguen teniendo éxito, al final cambiarán muchas de las funciones del sistema financiero global —corredores de bolsa, bancos de inversión y expertos en derecho bursátil— y la naturaleza misma de la inversión. Confiamos en que la combinación de la oferta pública de venta del sistema blockchain con nuevas plataformas de compraventa de valor como Circle, Coinbase (la empresa emergente de compraventa de bitcoins mejor financiada), Smarwallet (un mercado global de todo tipo de valores) y otras empresas emergentes dé lugar a un mercado virtual distribuido. La vieja guardia toma nota. El NYSE invirtió en Coinbase y Nasdaq está integrando tecnología blockchain en su mercado privado. Bob Greifeld, consejero delegado de Nasdaq, empieza discretamente, usando el sistema blockchain para «simplificar los registros y hacerlos al mismo tiempo más baratos y precisos»,¹⁷⁰ pero es evidente que Nasdaq y otras grandes empresas tienen planes más ambiciosos.

El mercado de los mercados de predicción

Augur está creando una plataforma de mercados de predicción descentralizada que premia a los usuarios que predicen certeramente acontecimientos futuros: deportivos, resultados de elecciones, lanzamientos de nuevos productos, sexo de hijos de famosos... ¿Cómo funciona? Los usuarios de Augur pueden comprar y vender acciones del resultado de un acontecimiento futuro, cuyo valor es una estimación de la probabilidad de que ese acontecimiento se produzca. Así, si las probabilidades son las mismas (del 50 por ciento), una acción costará cincuenta céntimos.

Augur se basa en la «sabiduría de los grupos», el principio científico según el cual un gran número de personas suele predecir mejor el desenlace de un acontecimiento futuro que uno o más expertos.¹⁷¹ En otras palabras, Augur pone el espíritu del mercado al servicio de la precisión predictiva. Ya ha habido otros intentos de mercados de predicción centralizados, como el Hollywood Stock Exchange, Intrade y HedgeStreet (ahora Nadex), pero la mayoría han sido suspendidos o abortados por motivos legales, o sea, porque especulaban con contratos de asesinato y futuros de terrorismo.

La tecnología blockchain refuerza el sistema y lo hace más preciso y más resistente al fallo, al ataque, al error, a la coerción, a preocupaciones de liquidez y a lo que Augur llama eufemísticamente «regulación jurisdiccional anticuada». En Augur, las personas

que deciden sobre las cuestiones se llaman árbitros o jueces (*referees*) y su legitimidad deriva de los puntos que tenga su reputación. Por hacer lo correcto —esto es, por dar fe de que un acontecimiento se ha producido, de quién ha ganado un partido o unas elecciones—, reciben más puntos. Mantener la integridad del sistema tiene otros beneficios económicos: cuantos más puntos tenga nuestra reputación, más mercados podemos abrir y en consecuencia más comisión podemos cobrar. En palabras de Augur, «nuestros mercados de predicción eliminan el riesgo de la otra parte, prescinden de servidores centralizados y crean un mercado global que emplea criptomonedas como bitcoin, ether y criptomonedas estables. Todo el capital se guarda por medio de contratos inteligentes y nadie puede robarlo». ¹⁷² Augur soluciona el problema de los contratos poco éticos con una política de tolerancia cero con la delincuencia.

Para los dirigentes de Augur, el único límite de la utilidad de los mercados de predicción es la imaginación humana. En Augur, cualquiera puede hacer una predicción claramente definida sobre cualquier cosa con un plazo exacto, desde predicciones triviales, como «¿Llegarán a divorciarse Brad Pitt y Angelina Jolie?», hasta predicciones trascendentales, como «¿Se disolverá la Unión Europea antes del 1 de junio de 2017?». Las consecuencias para la industria de los servicios financieros, para los inversores, para los actores económicos y para mercados enteros son enormes. Pensemos en un agricultor de Nicaragua o de Kenia que no tenga medios para afrontar el riesgo cambiario, el riesgo político o los cambios de tiempo y clima. Tener acceso a los mercados de predicción permitiría a esa persona mitigar el riesgo de sequía o calamidad. Por ejemplo, podría firmar un contrato de predicción por el que cobrara dinero si una cosecha no alcanza cierto nivel o si en el país llueve menos de una determinada cantidad de lluvia.

Los mercados de predicción son útiles a los inversores que quieren apostar una cantidad al resultado de acontecimientos concretos como «¿Aumentará IBM sus beneficios en al menos diez céntimos este trimestre?». Hoy, la «estimación» oficial de los beneficios de las empresas no es más que la media de las estimaciones que hacen los llamados expertos analistas. Aprovechando la sabiduría de los grupos, podemos hacer predicciones más realistas y generar mercados más eficientes. Los mercados de predicción pueden protegernos de la incertidumbre global y de sucesos como los llamados «del cisne negro»: «¿Se contraerá la economía griega más del 15 por ciento este año?». ¹⁷³ Hoy dependemos de que unos locutores den la voz de alarma; un mercado de predicción sería un sistema más imparcial que avisaría con mayor antelación a inversores de todo el mundo.

Los mercados de predicción podrían complementar y, en última instancia, transformar muchos aspectos del sistema financiero. Pensemos en mercados de predicción en que se negocie con el resultado de operaciones empresariales, como informes de beneficios, fusiones, compras y cambios en la administración. Los mercados de predicción ofrecerían una forma de asegurar el valor y de conjurar los riesgos, pudiendo incluso descartar instrumentos financieros privados como las opciones de compra y venta, las permutas de tasas de interés y las permutas de incumplimiento crediticio.

Desde luego, no todo necesita un mercado de predicción. Tiene que haber suficientes personas que se preocupen por hacerlo líquido para que llame la atención. Pero el potencial es grande, la oportunidad es excelente y todo el mundo puede participar.

De camino a la prosperidad

Las tecnologías blockchain cambiarán todas las formas y funciones de la industria de los servicios financieros, desde la banca comercial y los mercados de capital hasta la contabilidad y la regulación. También nos obligarán a replantearnos el papel que los bancos y las instituciones financieras desempeñan en la sociedad. «En bitcoin no hay rescates, ni días inhábiles, ni controles de divisas, ni congelación de fondos, ni límites de retirada de efectivo, ni horarios de bancos», dice Andreas Antonopoulos.¹⁷⁴

Mientras que el viejo mundo era jerárquico, lento, reacio al cambio, cerrado y opaco, y estaba controlado por intermediarios poderosos, el nuevo orden será horizontal, igualitario, más privado y seguro, transparente, inclusivo e innovador. Habrá sin duda trastorno y desconcierto, pero también es una excelente oportunidad para que los líderes del sector hagan algo. La industria de los servicios financieros se contraerá y a la vez se expandirá en los años venideros; habrá menos intermediarios que ofrezcan más productos y servicios mucho más baratos a mucha más gente. Esto es bueno. La cuestión de si las blockchains cerradas y de permiso tendrán cabida en un mundo descentralizado es discutible. Barry Silbert, fundador de SecondMarket y ahora consejero delegado de Digital Currency Group, dice: «Tengo una opinión muy cínica de las objeciones que ponen las grandes entidades financieras. Cuando lo único que tenemos es un martillo, todas las cosas nos parecen clavos». ¹⁷⁵ Creemos que la imparable fuerza de la tecnología blockchain se llevará por delante la infraestructura regulada, anquilosada y atrincherada de las finanzas modernas.¹⁷⁶ El choque remodelará el panorama financiero en las próximas décadas. Quisiéramos que las finanzas dejaran de ser una máquina de hacer dinero típica de la era industrial y se convirtieran en una plataforma de prosperidad.

Capítulo IV

Reformar la empresa por dentro y por fuera

Crear ConsenSys

El 30 de julio de 2015 fue un gran día para un grupo de codificadores, inversores, empresarios y estrategias de empresa que piensan que Ethereum es el nuevo gran invento, no sólo para los negocios, sino posiblemente para la civilización. Ethereum, la plataforma de blockchain que llevaba gestándose dieciocho meses, cobró vida.

Nosotros presenciamos personalmente el lanzamiento de la plataforma, que tuvo lugar en la oficina que tiene en Brooklyn Consensus Systems (ConsenSys), una de las primeras empresas de desarrollo de software de Ethereum. Todos nos felicitamos cuando la red Ethereum creó su «bloque de génesis», tras lo cual multitud de mineros corrieron a disputarse el primer bloque de ether, la moneda de Ethereum. Fue un día de suspense inquietante. En el río Este estalló una gran tormenta que hizo que los móviles de todos rompieran a sonar con señales de alerta por posibles inundaciones.

Según se explica en la página web, Ethereum es una plataforma que ejecuta aplicaciones descentralizadas, principalmente contratos inteligentes, «exactamente como están programados y sin posibilidad de pausa, censura, fraude ni interferencia de terceros». Ethereum se parece a bitcoin en que su ether motiva a una red de iguales para que validen las transacciones, protejan la red y creen consenso sobre lo que existe y lo que ha ocurrido. Pero se diferencia de bitcoin en que incluye algunas poderosas herramientas para ayudar a los desarrolladores y demás a crear servicios de software que van desde juegos descentralizados hasta mercados de acciones.

Ethereum lo concibió en 2013 Vitalik Buterin, un canadiense de origen ruso que entonces tenía diecinueve años. Les había dicho a los desarrolladores de bitcoin que la plataforma necesitaba un lenguaje de programación más complejo que permitiera desarrollar aplicaciones. Al ver que rechazaban su propuesta, decidió crear su propia plataforma. ConsenSys fue la más rápida y se fundó para crear aplicaciones basadas en Ethereum. Dos años después la analogía es clara: Linus Torvalds es a Linux lo que Vitalik Buterin es a Ethereum.

Hablando del auge de las blockchains y de la tecnología Ethereum, Joseph Lubin, cofundador de ConsenSys, dice: «Tuve claro que lo que había que hacer, en lugar de perder tiempo saliendo a la calle con pancartas, era trabajar todos juntos para encontrar soluciones nuevas a los problemas de la economía y de la sociedad».¹⁷⁷ No «ocupemos Wall Street», inventemos nuestro propio sistema.

Como muchos empresarios, Lubin tiene una difícil misión, que no es sólo crear una gran empresa, sino resolver problemas importantes del mundo. Dice modestamente que su empresa es un «taller de producción de blockchain que fabrica aplicaciones descentralizadas, sobre todo en Ethereum»; pero si triunfan, las aplicaciones que ConsenSys está creando harán que unas cuantas industrias se estremezcan. Entre los proyectos se incluye un sistema de contabilidad por partida triple; una versión descentralizada del muy popular foro de debate Reddit, últimamente muy discutido por su control centralizado; un sistema de gestión y documentación para contratos automáticos (llamados por otro nombre, «contratos inteligentes»); mercados de predicción para negocios, deporte y entretenimiento; un mercado energético abierto; una plataforma musical distribuida que compita con Apple y Spotify, aunque estas dos empresas también podrían usarla,¹⁷⁸ y una serie de herramientas que permitan la colaboración, creación y administración colectivas de empresas sin administradores.

Lo que nos interesa de ConsenSys no son tanto sus ambiciosos productos y servicios basados en el sistema blockchain como su esfuerzo por crear una empresa propia que sienta nuevas bases en la ciencia administrativa con la introducción de sistemas como los holocráticos, esto es, sistemas colaborativos y no jerárquicos de definición y distribución de tareas. «Aunque nuestra idea no es aplicar la holocracia tal cual, porque me parece demasiado rígida y estructurada, sí trabajamos para incorporar muchos de sus principios en nuestra estructura y procesos», dice Lubin. Entre estos principios holocráticos están los de «la función dinámica en lugar del trabajo fijo tradicional; la autoridad distribuida y no delegada; normas transparentes en lugar de políticas opacas, y rápidas reiteraciones en lugar de grandes reorganizaciones», todo lo cual explica cómo funcionan las tecnologías blockchain. La forma de estructurarse ConsenSys, de crear valor, de gestionarse, difiere no sólo de la empresa industrial sino también de la típica empresa electrónica.

Joseph Lubin no es un ideólogo, y desde luego tampoco un anarquista ni un libertario, como lo son algunos de los movimientos criptomonetarios. Pero sí piensa que tenemos que cambiar el capitalismo si queremos que sobreviva, concretamente abandonar las jerarquías de mando y control que no tienen cabida en un mundo interconectado. Observa que hoy, aunque hay vastas redes que se extienden por todo el mundo y nos permiten comunicarnos gratuita, fluida e inmediatamente, predominan las jerarquías. La tecnología blockchain es el contrapeso. «La sociedad humana global puede ahora ponerse de acuerdo en algo y tomar decisiones en diez minutos, o en diez segundos. Esto hace posible sin duda que la sociedad sea más libre», dice. Cuanto más nos comprometamos, más prosperaremos.

Los administradores han muerto, ¡viva la administración!

ConsenSys opera según un plan que todos los empleados («miembros») desarrollan, modifican, votan y adoptan. Joseph Lubin describe su estructura como un «cubo de rueda» más que como una jerarquía, y cada uno de sus proyectos es un «radio» de esa rueda en el que los que más contribuyen tienen acciones.

La mayoría de los miembros de ConsenSys pueden decidir en qué trabajan. No hay nadie que asigne tareas desde arriba. Dice Lubin: «Compartimos todo lo posible, incluido componentes de software. Formamos grupos pequeños y ágiles pero que colaboran entre sí. Nuestra comunicación es inmediata, abierta y constante». Los miembros pueden decidir trabajar en dos, tres, cuatro o cinco proyectos al mismo tiempo. Cuando alguien ve que hay que trabajar en algo, pone manos a la obra y lo adelanta poco o mucho en una buena dirección, según su función. «Hablamos mucho de todo y así sabemos en qué cosas habría que avanzar», dice. Pero esas cosas pueden cambiar y cambian constantemente. «Ser ágil significa también que las prioridades son dinámicas.»

Lubin no es el jefe. Su principal función es asesorar: «Muchas veces me preguntan a mí o preguntan a otros en qué podrían trabajar», dice. Con Slack¹⁷⁹ y GitHub,¹⁸⁰ propone direcciones que los miembros podrían seguir «para crear todos los servicios y plataformas que queremos crear, y muchos de los que queremos crear pero que aún no sabemos cómo crear».

El hecho de que los miembros sean propietarios incentiva explícitamente esta actitud. Todos poseen una parte de todos los proyectos directa o indirectamente: la plataforma Ethereum emite fichas que los miembros pueden cambiar por ether y luego convertir en cualquier otra moneda. «Nuestra idea es llegar a un buen equilibrio entre la independencia y la interdependencia», dice Lubin. «Nosotros nos consideramos una especie de colectivo de empresarios que colaboran estrechamente. En un momento dado puede ser necesario que se haga cierto trabajo y, si nadie se ofrece a hacerlo, contratar a alguien de fuera que lo haga o incentivar a los de dentro para que se animen», dice Lubin. Pero, en general, «todos somos adultos responsables. Ya he dicho que nos comunicamos mucho, y luego cada cual decide por sí mismo».

Los lemas son *agilidad*, *apertura* y *consenso*: identificar el trabajo que hay que hacer, distribuir la tarea entre la gente que quiere y puede hacerlo, ponerse de acuerdo en la función, responsabilidad y retribución de cada cual y luego codificar esos derechos «en forma de acuerdos claros, detallados, inequívocos y automáticos que son como la cola que mantiene unidos todos los aspectos de nuestra relación laboral», dice. Algunos acuerdos contemplan pagos según rendimiento, otros un salario anual en ethers, y otros son más como «colaboraciones» en las que se asigna un premio por tarea, como escribir una línea de código. Si el código pasa la prueba, el premio es automáticamente concedido. «Todo queda a la vista y es transparente. Los incentivos son explícitos y granulares», dice. «Esto nos permite comunicarnos, ser creativos y adaptar nuestro trabajo a estas expectativas.»

¿Nos atreveremos a acuñar el neologismo *blockcom*, para designar a una empresa que se ha formado y que funciona con tecnologías blockchain? Ésa es la idea, que la mayor parte posible de ConsenSys funcione en Ethereum, de la gestión diaria a la administración de proyectos, pasando por el desarrollo, la prueba y la contratación de software, la retribución y la financiación. La tecnología blockchain permite además usar sistemas de reputación en los que los miembros pueden calificar el trabajo de los demás

colaboradores, aumentando así la confianza en la comunidad. Dice Lubin: «Las identidades digitales persistentes y los sistemas de reputación harán que seamos más honrados y que nos comportemos mejor con el prójimo».

Estas capacidades difuminan los límites de una empresa. No hay ajustes por defecto que determinen quién puede o no puede incorporarse. Los miembros de ConsenSys pueden formar «radios» llegando a un consenso sobre estrategia, estructura, capital, rendimiento y gestión. Pueden decidir lanzar una empresa que compita en un mercado ya existente o que proporcione una infraestructura para crear un nuevo mercado. Una vez que se ha lanzado, pueden modificar esos ajustes.

Descentralizar la empresa

El sistema blockchain evitará todo tipo de conflictos a las empresas. «Menos conflictos significa menos costes porque el precio de la mediación válida lo determina el mecanismo de fijación de precios más eficiente: los mercados libres descentralizados. Las grandes empresas, en su papel de intermediarios, ya no podrán usar asimetrías de ley, de regulación, de información y de poder para sacar de una transacción mucho más valor del que aporten», dice Lubin.

¿Podría ConsenSys crear algún tipo de organización realmente descentralizada y autónoma, cuyos propietarios y controladores fueran creadores de valor no humanos, y que se rigiera por contratos inteligentes en lugar de por agentes humanos? «¡Todo se andará!», dice Lubin. «Una inteligencia colectiva que opere en un sustrato informático global y descentralizado, una capa subyacente, debería cambiar la estructura de la empresa, haciendo que pase de ser una larga serie de departamentos especializados dirigidos por humanos a ser un conjunto de agentes informáticos que puedan cooperar y competir en mercados libres.» Algunos de estos agentes se organizarán para subvenir durante periodos prolongados de tiempo a las necesidades del consumidor, en forma de servicios y mantenimiento. Otros se centrarán en problemas a corto plazo, los resolverán y, cumplido su objetivo, se disolverán.

¿Hay riesgo de que estas descentralización y automatización radicales eliminen al agente humano de la toma de decisiones (por ejemplo, riesgo de que aparezca un algoritmo malvado)? «No me preocupa la inteligencia de las máquinas. Evolucionaremos con ella y durante mucho tiempo estará al servicio del *Homo sapiens cybernetica* y será un aspecto de él. Puede evolucionar más que nosotros, pero eso está bien», dice Lubin. «Si eso ocurre, ocupará un nicho ecológico diferente. Operará a diferentes velocidades y a diferentes escalas temporales. En ese contexto, la inteligencia artificial no distinguirá entre humanos, rocas o procesos geológicos. Nosotros hemos evolucionado más que muchas especies, gran parte de las cuales son perfectas (en su forma presente).»

ConsenSys aún es una empresa pequeña. Su grandioso experimento puede tener éxito o puede no tenerlo. Pero su historia nos permite vislumbrar los cambios radicales que podrían hacerse en la estructura empresarial para estimular la innovación y usar el poder del capital humano no sólo para crear riqueza, sino prosperidad. La tecnología de las blockchains hace posibles nuevas formas de organización económica y nuevas

carteras de valores. Están surgiendo modelos empresariales distribuidos —de propiedad, estructura, operaciones, retribuciones y gestión— que van mucho más allá de lo que es promover la innovación, incentivar al empleado y actuar colectivamente. Pueden ser la condición largo tiempo esperada que permita el desarrollo de una economía más próspera e inclusiva.

Los hombres de negocios tienen otra oportunidad para replantearse cómo organizan la creación de valor. Podrían negociar, contratar y poner en práctica sus acuerdos en el sistema blockchain; tratar de manera fiable con proveedores, clientes, empleados, contratistas y trabajadores autónomos, y mantener una flota de estos agentes para que los usaran otros, y esos agentes podrían alquilar sus capacidades sobrantes o autorizar el uso de ellas en su cadena de valor.

Cambiar los límites de la empresa

En el transcurso de la primera era de internet los que pensaban en la administración empresarial (Don incluido) creían sinceramente que las empresas reticulares, la estructura horizontal, la innovación abierta y los ecosistemas de negocios serían los sucesores de las jerarquías del poder industrial. Sin embargo, la estructura empresarial de principios del siglo XX sigue prácticamente intacta. Incluso las grandes empresas electrónicas han adoptado estructuras jerarquizadas con responsables como Jeff Bezos, Marissa Mayer y Mark Zuckerberg. ¿Por qué, pues, querría ninguna empresa establecida —sobre todo aquellas que ganan dinero explotando la información ajena, operan en gran medida a puerta cerrada y, sorprendentemente, apenas se resienten de los robos continuados de datos— aumentar la transparencia, respetar la privacidad y el anonimato de los usuarios e incluir a muchas más personas que pueden permitirse muchas menos cosas que aquellas a las que ya sirven?

Costes transaccionales y estructura empresarial

Empecemos con un poco de economía. En 1995, Don usó la teoría de la empresa del premio Nobel de Economía Ronald Coase para explicar cómo afectaría internet a la estructura empresarial. En su artículo de 1937 «La naturaleza de la empresa», Coase identificaba tres tipos de costes en economía: los costes de búsqueda (encontrar la información necesaria, las personas, los recursos para crear algo), los costes de coordinación (poner a toda esa gente a trabajar con eficiencia) y los costes de contratación (negociar los gastos de trabajo y material de cada actividad productiva, guardar el secreto industrial y cumplir esos acuerdos). Postulaba que una empresa se expandiría hasta que el coste de realizar una transacción dentro de la empresa superara el coste de realizarla fuera.¹⁸¹

Don afirmaba que internet reduciría los costes transaccionales internos de la empresa; pero nosotros pensábamos que, por su accesibilidad global, reduciría los costes de la economía en su conjunto incluso más, y a la vez facilitaría la participación de más gente. Sí, ha reducido los costes de investigación, gracias a los buscadores y a la red.

También ha reducido los costes de coordinación gracias al correo electrónico, a aplicaciones de procesamiento de datos como ERP, a las redes sociales y a la informática en nube. Muchas empresas han podido subcontratar actividades como el servicio al cliente y la contabilidad. Los vendedores han podido dirigirse directamente a los consumidores e incluso convertirlos en productores (los llamados «prosumidores»). Los planificadores de productos han puesto la innovación en manos de grupos de colaboración externos (*crowdsourcing*). Los fabricantes se han aprovechado de los grandes canales de distribución.

Sin embargo, la sorprendente realidad es que internet no ha tenido sino un impacto superficial en la estructura empresarial. La jerarquía típica de la era industrial sigue prácticamente intacta como el fundamento reconocible del capitalismo. Ciertamente es que las redes han permitido que las empresas subcontraten en países donde los costes son más bajos, pero internet también ha reducido los costes transaccionales dentro de la empresa.

De la jerarquía al monopolio

En consecuencia, hoy las empresas siguen estando jerarquizadas, y la mayoría de las actividades se desarrollan dentro de los límites de la empresa. Los administradores siguen considerándolas el mejor modelo de organización del talento y de activos como marcas, propiedad intelectual, conocimiento y cultura, así como de incentivación personal. Las empresas siguen retribuyendo a ejecutivos y consejeros delegados muy por encima de lo que sería razonable teniendo en cuenta el valor que crean. No por casualidad el complejo industrial sigue generando riqueza, pero no prosperidad. De hecho, como hemos señalado antes, hay pruebas fehacientes de que está produciéndose una creciente concentración de poder y riqueza en grandes compañías y incluso en monopolios.

Otro premio Nobel, Oliver Williamson, así lo predijo,¹⁸² señalando los efectos negativos que eso tendría en la productividad: «Baste observar que el paso de una distribución autónoma (a cargo de un conjunto de pequeñas empresas) a una propiedad unificada (en una gran compañía) va inevitablemente acompañado de un cambio tanto en la intensidad de la incentivación (los incentivos son más débiles en la empresa integrada) como en los controles administrativos (que son más extensivos)».¹⁸³ Peter Thiel, cofundador de PayPal, elogia los monopolios en su muy recomendable y muy controvertido libro *De cero a uno*. Seguidor de Rand Paul, Thiel dice: «Competir es cosa de perdedores... Los monopolios creativos no sólo son buenos para el resto de la sociedad, son motores poderosos para hacerla mejor».¹⁸⁴

Puede que tenga razón cuando habla de la lucha de cada cual por dominar su industria o su mercado, pero no aporta pruebas convincentes de que los monopolios sean buenos para los consumidores o la sociedad en su conjunto. Al contrario, todo el cuerpo legal sobre competencia de los países más democráticos deriva de la idea contraria. El concepto de competencia justa se remonta a tiempos de los romanos, en que ciertas violaciones se castigaban con la pena de muerte.¹⁸⁵ Si las empresas no tienen competencia real, pueden ser tan ineficientes como les dé la gana, y subir los precios dentro y fuera de ellas. Ahí tenemos el ejemplo de los gobiernos. Incluso en la industria

tecnológica, muchos afirman que los monopolios pueden contribuir a la innovación a corto plazo, pero que a largo plazo perjudican a la sociedad. Las empresas pueden reunir poder monopolista porque ofrecen buenos productos y servicios que gustan a la gente, pero al final la luna de miel se acaba. No porque sus innovaciones dejen de agradar, sino porque las empresas mismas empiezan a anquilosarse.

La mayoría de los estudiosos saben que la innovación normalmente nace en los márgenes de la empresa, no en su centro. El profesor de Derecho de la Universidad de Harvard Yochai Benkler coincide: «Los monopolios pueden tener mucho dinero para invertir en I+D, pero suelen carecer de la cultura de la investigación pura y abierta que se requiere para innovar. La red no vino de los monopolios, sino de los márgenes. Google no vino de Microsoft. Twitter no vino de AT&T, ni siquiera de Facebook».¹⁸⁶ En los monopolios, las capas de burocracia distancian a los ejecutivos de arriba de las señales del mercado y de la tecnología emergente que se producen en los márgenes, donde las empresas se confrontan unas con otras y con otros mercados, otras industrias, otros países, otras disciplinas intelectuales, otras generaciones. Según John Hagel y John Seely Brown: «Donde más grande es el potencial innovador es en la periferia del mundo empresarial global de hoy. Quien no lo sepa, peor para él».¹⁸⁷

Los ejecutivos deberían estar entusiasmados con la tecnología blockchain, porque la ola de innovación que viene de la periferia puede no tener precedentes. Desde las mayores criptomonedas —Bitcoin, BlackCoin, Dash, Nxt y Ripple— hasta las mayores plataformas de blockchain —Lighthouse, de micromecenazgo entre iguales; Factom, un archivo distribuido; Gems, de mensajería descentralizada; MaidSafe, de aplicaciones descentralizadas; Storj, de nube distribuida, y Tezos, de votación descentralizada, por mencionar unas cuantas—, la siguiente era de internet trae consigo verdadero valor y verdaderos incentivos para participar. Estas plataformas prometen proteger la identidad del usuario, respetar su privacidad y demás derechos, garantizar la seguridad de la red y reducir los costes transaccionales de manera que los que no tengan cuentas bancarias puedan participar.

A diferencia de las grandes empresas tradicionales, estas plataformas no necesitan una marca para transmitir confianza en sus transacciones. Como ofrecen gratis su código fuente, comparten poder con cualquiera de la red, usan mecanismos de consenso para garantizar la integridad y hacen sus negocios abiertamente en la blockchain, son como focos de esperanza para muchos desilusionados privados de derechos. En este sentido, la tecnología blockchain es un medio creíble y efectivo no sólo de prescindir de intermediarios, sino también de reducir drásticamente los costes transaccionales, transformar las empresas en redes, distribuir el poder económico y promover a la vez la creación de riqueza y un futuro más próspero.

1. Costes de búsqueda. ¿Cómo encontramos nuevos talentos y nuevos consumidores?

¿Cómo encontramos a las personas y la información que necesitamos? ¿Cómo sabemos si sus servicios, bienes y capacidades son los que más nos convienen para que nuestra empresa sea competitiva internamente?

Aunque la estructura de la empresa sigue básicamente intacta, la primera era de internet redujo estos costes significativamente y favoreció cambios importantes. Contratar recursos externos fue sólo el principio. Recurriendo a las llamadas «ideágoras» (mercados abiertos de ideas), empresas como Procter & Gamble encuentran a personas excepcionalmente cualificadas para crear productos o procesos innovadores. De hecho, el 60 por ciento de las innovaciones de esta empresa proceden de fuera de ella, de ideágoras que ha creado o usado como InnoCentive o inno360. Otras empresas como Goldcorp han lanzado desafíos globales para encontrar las mejores mentes que resuelvan sus mayores problemas. Esta empresa, que hizo pública su información geológica, descubrió oro por valor de 3.400 millones de dólares, lo que hizo que su cotización en bolsa se multiplicara por cien.

Imaginemos entonces las posibilidades que ofrece el poder buscar en un registro mundial, una base de datos descentralizada que encierre mucha de la información estructurada mundial. ¿Quién vendió qué descubrimiento a quién? ¿Y a qué precio? ¿Quién tiene la propiedad intelectual de esto? ¿Quién está capacitado para llevar a cabo este proyecto? ¿Qué competencias médicas tiene el personal de nuestro hospital? ¿Cuántos créditos de carbono se ha ahorrado esta empresa? ¿Qué proveedores han trabajado en China? ¿Qué subcontratistas cumplen a tiempo y sin pasarse del presupuesto según lo acordado en sus contratos inteligentes? El resultado de estas búsquedas no serán currículos, enlaces publicitarios ni otros contenidos paralelos; serán historiales de transacciones, registros fiables de individuos y empresas, posiblemente clasificados por su reputación. ¿Nos damos cuenta? Dice Vitalik Buterin, fundador de la blockchain Ethereum: «Las blockchains reducirán los costes de búsqueda, lo que causará una especie de descomposición que nos permitirá disponer de mercados de entidades horizontal y verticalmente segregadas. Esto nunca había ocurrido. Antes había como unos monolitos que lo hacían todo».¹⁸⁸

Varias empresas están trabajando en motores de búsqueda para blockchain, dada la potencial bonanza. La misión de Google es organizar el mundo de la información, por lo que haría bien en dedicar recursos humanos a investigar esto.

Hay tres diferencias fundamentales entre la búsqueda en internet y la búsqueda en una blockchain. La primera es la privacidad del usuario. Aunque las transacciones son transparentes, las personas son dueñas de su información personal y deciden qué hacer con ella. Pueden participar anónimamente o al menos con un seudónimo, o casi anónimamente (con anonimato parcial). Las partes interesadas podrán buscar aquella información que los usuarios hayan hecho pública. Andreas Antonopoulos dice: «Las transacciones son anónimas si queremos que lo sean... Pero el sistema blockchain permite una transparencia total más fácilmente que un anonimato total».¹⁸⁹

Muchas empresas tendrán que replantearse el proceso de contratación. Por ejemplo, los recursos humanos o el personal tendrá que aprender a buscar en la blockchain con preguntas de sí o no: ¿eres un ser humano? ¿Te has doctorado en matemáticas aplicadas? ¿Sabes codificar en lenguaje Script, Python, Java, C++? ¿Podrás trabajar a tiempo completo de enero a junio del año que viene? Preguntas así. Estas búsquedas recorrerán las cajas negras de las personas que estén en el mercado laboral y mostrarán una lista de

aquellas que cumplen con estos requisitos. También pueden pagar a posibles talentos para que publiquen información profesional pertinente en una plataforma blockchain que luego pueden repasar para encontrar lo que buscan. El personal de recursos humanos debe saber usar los sistemas de reputación y seleccionar candidatos sin saber nada que no sea relevante para el trabajo, como la edad, el sexo, la raza, el país de origen. También necesitan motores de búsqueda capaces de navegar por varios grados de apertura, desde información completamente privada hasta información completamente pública. Lo bueno es que pone fin a la posibilidad de sesgos subconscientes o incluso institucionales, y nos ahorra pagar a cazatalentos y demás agentes de selección de personal. Lo malo es que búsquedas precisas dan resultados precisos. Hay menos posibilidad de hallar talentos latentes, esto es, de descubrir a personas que, aunque no cumplen con los requisitos pedidos, tienen una gran capacidad de aprendizaje y pueden hacer esas asociaciones creativas inesperadas que las empresas tanto necesitan.

Lo mismo vale decir en materia de comercialización. Las empresas pueden tener que pagar por buscar en la caja negra de un posible cliente para ver si forma parte del tipo de consumidor que buscan. Ese mismo cliente puede decidir globalmente guardarse cierta información, como su sexo, porque responder «no» siga siendo valioso. Pero así la empresa no sabrá sobre el posible cliente más que lo que resulte de las preguntas de sí o no. Responsables y agencias de comercialización tendrán que replantearse las estrategias basadas en el correo electrónico, los medios sociales y el teléfono móvil: aunque la infraestructura puede reducir a cero los costes de la comunicación, los consumidores los subirán tanto que les merecerá la pena leer el mensaje que las empresas les envían. En otras palabras, las empresas pagarán a los clientes para que escuchen sus mensajes publicitarios, pero a la vez habrán ajustado tanto su búsqueda que se dirigirán a un público muy concreto, de manera que esos mensajes llegarán a las personas a las que querían llegar sin invadir su privacidad. Y pueden realizar diferentes búsquedas para conocer diferentes micronichos de mercado en cada etapa del desarrollo de un nuevo producto. Podemos llamarlo *comercialización de la caja negra*.

La segunda diferencia es que la búsqueda puede ser multidimensional. Cuando buscamos en la red hoy, buscamos una especie de foto fija en el tiempo, tal como ha sido indexada en las últimas semanas.¹⁹⁰ El teórico informático Antonopoulos llama a esto «búsqueda bidimensional»: *horizontal*, porque busca a lo largo y ancho de la red, y *vertical*, porque busca en profundidad en un sitio en particular. La tercera dimensión es la *secuencial*, que es la búsqueda en el orden temporal en que se ha registrado. «Las blockchains pueden añadir la dimensión del tiempo», dice. Es posible buscar un registro completo de todo lo que ha pasado en tres dimensiones. Para aclararlo, Antonopoulos buscó en la cadena de bitcoin para encontrar la famosa primera transacción comercial, que consistió en la compra por un tal «Laslo» de dos pizzas que costaron 10.000 bitcoins. «Las blockchains proporcionan un registro casi arqueológico, un hallazgo profundo, y preservan la información para siempre.» (Para evitarle al lector echar cuentas, si una pizza costaba 5 dólares cuando 1 dólar equivalía a 2.500 bitcoins, en el momento de escribir este libro costaría 3,5 millones de dólares..., pero ése es otro tema.)

Esto exige que las empresas actúen con criterio: los responsables tienen que contratar a gente que haya demostrado tener buen juicio, porque las malas decisiones no tienen vuelta atrás, ni se puede alterar el orden de los acontecimientos, ni negar el comportamiento deshonesto de un ejecutivo. Cuando se trate de tomar decisiones importantes, las empresas podrían aplicar mecanismos de consenso internos que permitieran votar a todas las partes implicadas, lo que pondría fin al coro de ignorancia y negación del conocimiento anterior. O podrían usar mercados de predicción para sondear distintos escenarios. Si somos ejecutivos de una futura Enron, no habrá chivo expiatorio que valga. Y si somos el gobernador de Nueva Jersey Chris Christie, de nada nos servirá decirle al fiscal que nada sabíamos de los planes de cerrar el puente de George Washington.

La tercera diferencia es el valor: mientras que la información en internet es abundante, poco de fiar y perecedera, en las blockchains es escasa, imposible de falsear y permanente. Sobre esta última característica, Antonopoulos observa: «Si hubiera suficientes incentivos financieros para preservar estas blockchains en el futuro, no es imposible que persistieran durante decenas, cientos y aun miles de años».

¡Qué asombrosa idea! Las blockchains serían registros arqueológicos como las tablillas de piedra de Mesopotamia. Los registros en papel son efímeros y temporales, mientras que (irónicamente) la forma más antigua de registrar información, las tablillas, es la más perdurable. Las consecuencias que esto tiene en la estructura de la empresa son considerables. Imaginemos un registro permanente y rastreable de información histórica importante, como la historia de la economía. Los encargados de emitir comunicados sobre balances, informes anuales, informes para el gobierno o los donantes, material mercadotécnico para posibles empleados, clientes y consumidores, etc., empezarán consultando este historial público e infalible de su empresa e incluso crearán un filtro que permita a los interesados ver lo que ellos ven con sólo apretar una tecla. Las empresas podrían guardar registros de sus transacciones, algunos para uso administrativo interno y otros para uso público. Tranquilos: la competencia confeccionará estos registros e historiales como parte de sus programas de inteligencia competitiva. ¿Por qué no ponerlos, pues, en nuestro sitio web y ganarnos la confianza de todos?

Esto constituye un fortísimo incentivo para que las empresas busquen recursos fuera de sus límites, pues disponen de una información casi infinitamente mejor sobre las cualidades y antecedentes de los candidatos, sean éstos individuos o empresas.

Empresas como ConsenSys están desarrollando sistemas de identidad en los que quienes buscan trabajo programarán su propio avatar para que revele aquella información que pueda interesar a los empresarios. Estos sistemas no pueden ser atacados como lo son las bases de datos centralizadas. Los usuarios se sienten motivados para incluir información en sus avatares porque son los dueños de ellos y los controlan, pueden configurar su privacidad como quieran y rentabilizar sus datos. Esto es muy diferente de, por ejemplo, LinkedIn, una base de datos centralizada y rentabilizada por una poderosa empresa que, sin embargo, no garantiza su seguridad.

¿Habrían podido imaginar Coase y Williamson una plataforma que redujera los costes de búsqueda tanto que las empresas pudieran hallar fuera de sus límites recursos más baratos y que funcionaran mejor?

2. Costes de contratación: ¿qué estamos de acuerdo en hacer?

¿Cómo nos entendemos o nos ponemos de acuerdo con otras partes? Esto es lo primero que hay que hacer para reducir los costes de búsqueda del personal y los recursos que necesitamos. Pero no es suficiente para reducir significativamente el tamaño de una empresa. Todas las partes deben trabajar juntas. La segunda razón por la que existen empresas son los costes de contratación: negociar el precio, establecer competencias, estipular y regular los términos y condiciones de los bienes o servicios de los proveedores y arbitrar soluciones en caso de que algunas de las partes no cumplan con lo prometido.

El ser humano siempre ha hecho contratos sociales, pactos relacionales de especialización de funciones, por los cuales unos cazaban y protegían a la tribu y otros recolectaban y construían refugios. Las personas hemos intercambiado objetos físicos en tiempo real desde tiempos inmemoriales. Los contratos son un fenómeno más reciente y ocurren cuando empezamos a intercambiar promesas, no propiedades. Los acuerdos orales resultaron fáciles de manipular o se recordaban mal, y los testigos oculares no eran de fiar. La duda y la desconfianza perjudicaron la colaboración con extraños. Los contratos había que cumplirlos enseguida y no había un mecanismo formal para hacer respetar lo pactado más allá de la fuerza. El contrato escrito era una forma de codificar una obligación, de crear confianza y fijar expectativas. Los contratos escritos servían de guía en caso de que alguien no cumpliera su parte de lo pactado, o algo inesperado ocurriera. Pero no podían existir en el vacío; tenía que haber algún marco legal que reconociera los contratos e hiciera valer los derechos de los contratantes.

Hoy, los contratos siguen estando hechos de átomos (papel), no de bits (informática). Por eso mismo tienen grandes limitaciones y sólo sirven para documentar un acuerdo. Como veremos, si los contratos fueran informáticos —si fueran inteligentes y estuvieran distribuidos en una blockchain—, podrían abrir un mundo de posibilidades, entre ellas la de facilitar que las empresas colaboraran con recursos externos. Imaginémonos lo que sería el Código Comercial Uniformado de Estados Unidos si estuviera en una blockchain.

Coase y sus sucesores sostenían que los costes de contratación eran menores dentro de los límites de las empresas que fuera, en el mercado, y que una empresa es esencialmente un vehículo para crear contratos a largo plazo cuando los contratos a corto plazo suponen demasiado esfuerzo.

Williamson insistió en esta idea afirmando que las empresas existen para resolver conflictos, lo que principalmente consiguen firmando contratos con varias partes en el seno de la empresa. En el mercado abierto, el único mecanismo de disputa son los tribunales, un mecanismo costoso, lento y muchas veces insatisfactorio. Y añadía que en algunos casos, como fraude, otros actos ilegales o conflicto de intereses, en el mercado no existía ningún mecanismo de disputa. «En efecto, la ley contractual de la organización interna es la del aguante y la paciencia, según la cual una empresa es su propio tribunal. Por esta razón, las empresas pueden ejercer una autoridad absoluta que el mercado no tiene.»¹⁹¹ Williamson concebía la empresa como «una estructura administrativa» para

llegar a acuerdos contractuales. Decía que la estructura organizativa contribuye a reducir los costes de gestionar transacciones y que «mirar con los lentes del contrato en lugar de con los lentes de la elección suele ahondar nuestro conocimiento de la compleja organización económica».¹⁹² Ésta es una idea recurrente en la teoría de la administración empresarial, y los que probablemente mejor la han desarrollado han sido los economistas Michael Jensen y William Meckling, que afirman que las empresas no son más que un conjunto de contratos y relaciones.¹⁹³

Hoy, algunos estudiosos y teóricos de las blockchains han cuestionado esta idea. El inventor de Ethereum, Vitalik Buterin, afirma que los agentes empresariales (es decir, los ejecutivos) sólo pueden usar activos de la empresa para propósitos aprobados por, digamos, los miembros del consejo de administración, que a su vez están sujetos a la aprobación de los accionistas. «Si una empresa hace algo, es porque su consejo de administración ha decidido que se haga. Si una empresa contrata a empleados, significa que los empleados están de acuerdo en proporcionar unos servicios a los clientes de la empresa según un determinado conjunto de normas, sobre todo de pago —escribe Buterin—. Que una empresa tenga responsabilidad limitada significa que a unas determinadas personas se les han concedido privilegios extra para actuar sin miedo a acciones legales por parte del Estado: un grupo de personas con más derechos que la gente normal que actúa sola, pero personas al fin y al cabo. En cualquier caso, no son más que personas y contratos.»¹⁹⁴

Por eso el sistema blockchain, al reducir los costes de contratación, permite a las empresas abrirse y desarrollar nuevas relaciones más allá de sus límites. ConsenSys, por ejemplo, puede entablar relaciones complejas con diferentes grupos de miembros, algunas dentro de sus límites, otras fuera y otras dentro y fuera a la vez, porque lo que gobierna esas relaciones no son los administradores tradicionales, sino contratos inteligentes. Los miembros pueden elegir los proyectos a los que dedicarse, definir de común acuerdo los objetivos que hay que alcanzar y cobrar cuando esos objetivos se han alcanzado, todo ello con el sistema blockchain.

Contratos inteligentes

El ritmo de cambio está sentando cada vez más las bases para el uso de contratos inteligentes. Cada vez más gente adquiere conocimientos informáticos no sólo básicos, sino avanzados. Por lo que las transacciones demuestran, este nuevo medio digital tiene propiedades muy distintas de sus predecesores de papel. Como destaca el criptógrafo Nick Szabo, los contratos inteligentes no sólo pueden captar más tipos de información (como información sensorial no lingüística), sino que son dinámicos: pueden transmitir esa información y ejecutar cierta clase de decisiones. En palabras de Szabo, «los medios digitales pueden hacer cálculos, manejar máquinas directamente y operar por medio de cierta clase de razonamientos de una manera mucho más eficiente que los humanos».¹⁹⁵

Por lo que respecta al objeto de este debate, los contratos inteligentes son programas informáticos que protegen, regulan y aplican acuerdos registrados entre personas y organizaciones. En cuanto tales, ayudan a negociar y definir esos acuerdos. En 1994, el

mismo año en que Netscape, el primer navegador web, salió al mercado, Szabo los definió así:

Un contrato inteligente es un protocolo transaccional informatizado que ejecuta los términos de un contrato. La idea general del contrato inteligente es satisfacer condiciones contractuales normales (como términos de pago, gravámenes, confidencialidad e, incluso, recurso a la ley), minimizar excepciones tanto maliciosas como accidentales, y minimizar la necesidad de intermediarios. Los objetivos económicos son reducir las pérdidas por fraude, los costes de arbitraje y recursos legales, y otros costes transaccionales.¹⁹⁶

Por entonces, la idea de los contratos inteligentes ya existía, pero no podía realizarse por falta de una tecnología que los desarrollara como Szabo describe. Había sistemas informáticos como el sistema de intercambio de datos electrónicos (EDI, por sus siglas en inglés) que permitían la comunicación de datos estructurados entre ordenadores de compradores y vendedores, pero no tecnología que hiciera posible intercambiar pagos y dinero.

Bitcoin y el sistema blockchain han cambiado todo esto. Ahora, las partes pueden llegar a acuerdos e intercambiar automáticamente bitcoins cuando cumplen con los términos de un contrato. Dicho lisa y llanamente, nuestro cuñado no podrá escaquearse de pagar la apuesta perdida al hockey, y cuando compremos una acción, la operación se ejecuta al instante y el activo pasa inmediatamente a nuestra cuenta, y cuando un contratista emite el código informático que cumple con las necesarias especificaciones, cobra.

Los medios tecnológicos para ejecutar contratos inteligentes limitados han existido desde hace algún tiempo. Un contrato es un intercambio de expectativas que puede hacerse cumplir antes de que se produzca el intercambio mismo. Andreas Antonopoulos lo explica con un sencillo ejemplo: «Si tú y yo acordamos ahora mismo que te pagaré cincuenta dólares por la pluma que tienes en tu mesa, hacemos un contrato en toda regla. Puedo decirte simplemente: “Te prometo que te pagaré cincuenta dólares por tu pluma”, y tú puedes contestar: “De acuerdo”. Eso significa que aceptas la oferta. Hemos hecho un trato y puede hacerse cumplir ante un tribunal. Esto nada tiene que ver con los medios tecnológicos de cumplimiento de las promesas que hemos hecho».

Lo que interesa a Andreas del sistema blockchain es que podemos ejecutar esta obligación financiera en un medio tecnológico descentralizado con un sistema de liquidación incorporado. «Eso es genial —dice— porque yo podría pagarte la pluma ahora mismo, tú verías el dinero al instante, me enviarías la pluma y yo podría verificar ese envío. Así es mucho más probable que hagamos negocios.»

Cada vez son más los profesionales del derecho que aprovechan esta oportunidad. Como todos los intermediarios, también ellos pueden verse excluidos y al final tendrán que adaptarse. Especializarse en contratos inteligentes podría ser una gran oportunidad para los gabinetes legales que quieran liderar la innovación en derecho contractual. Sin embargo, la profesión no destaca precisamente por su carácter pionero. Como dice el experto en derecho Aaron Wright, coautor de otro libro sobre el sistema blockchain: «El derecho siempre se queda atrás».¹⁹⁷

La multifirma: contratos complejos inteligentes

Pero, dirá el lector, ¿no superarán los costes de negociar contratos inteligentes complejos y que requieren mucho tiempo los beneficios de abrir los límites de las empresas? La respuesta es no. Si los socios emplean al principio más tiempo en establecer los términos del acuerdo, los costes de control, aplicación y liquidación se reducirán drásticamente e incluso se anularán. Además, el contrato puede ejecutarse en tiempo real, incluso en microsegundos, dependiendo del trato. Y, lo que es más importante, al asociarse con personas con más capacidad, las empresas pueden innovar más y ser más competitivas.

Consideremos el recurso a los contratistas independientes. En los albores del comercio digital, el sistema blockchain sólo servía para las transacciones más simples, entre dos partes. Por ejemplo, si Alice necesitaba a alguien que completara un fragmento de código rápidamente, publicaba un anónimo «Se necesita codificador» en el foro de debate pertinente. Bob lo veía.¹⁹⁸ Si el precio y los plazos le convenían, enviaba una muestra de trabajo. Si esta muestra convencía a Alice, ésta le hacía una propuesta a Bob. Convenían en los términos del acuerdo: Alice le enviaba la mitad del pago al instante y la otra mitad cuando recibía el código y comprobaba que funcionaba.

El contrato era directo: una oferta de trabajo y una aceptación de la oferta, y no tenían que ponerlo por escrito, porque todo quedaba registrado en la blockchain. La propiedad de bitcoins de Alice y de Bob estaba asociada a sus respectivas direcciones digitales (largas rstras de números) que tenían dos componentes: una clave pública que servía como dirección, y una clave privada que daba a su propietario acceso exclusivo a todos los bitcoins asociados con esa dirección. Bob enviaba a Alice su clave pública y ella enviaba el primer pago a esa dirección. La red registraba la transferencia y asociaba esos bitcoins a la cartera de clave pública de Bob.

¿Qué pasaría si, en este punto, Bob decidiera que no quiere hacer el trabajo? En esta transacción bipartita, Alice tendría poco que hacer. No podría dirigirse a su compañía de tarjetas de crédito para anular la transacción. Tampoco podría (aún) demandar a Bob por incumplimiento de contrato. Aparte de un código alfanumérico generado al azar y un anuncio en línea, no habría manera de identificar a Bob salvo que hubiera publicado su respuesta en una plataforma centralizada que pudiera rastrearlo, o que hubiera habido intercambio de correos electrónicos usando un servicio centralizado. Alice podría, al menos, señalar que la clave pública de Bob no era de fiar, con lo que bajaría la calificación de Bob como codificador.

Sin garantías de que la otra parte es de fiar y cumplirá con las debidas acciones fuera de la cadena, el acuerdo se parece al dilema del prisionero: sigue necesitándose cierto grado de confianza. Los sistemas de reputación pueden mitigar esta incertidumbre hasta cierto punto. Pero había que introducir confianza y seguridad en este sistema abierto y anónimo.

En 2012, el «desarrollador» Gavin Andresen introdujo un nuevo tipo de dirección bitcoin en los protocolos bitcoin llamado *pay to script hash* (P2SH) cuyo objetivo era permitir que una parte «pague cualquier transacción arbitraria, por complicada que sea».¹⁹⁹ Las partes usan varias claves o firmas de autenticación en lugar de una única clave privada para completar una transacción. La comunidad suele llamar a esta característica de firma múltiple (*multisignature*) «multisig».

En transacciones multifirma, las partes convienen en el número total de claves que hay que generar (N) y en el número de las que habrá que usar para completar una transacción (M). Esto se llama «esquema de firma M de N» o «protocolo de seguridad». Es como una caja fuerte para abrir la cual se requieren varias llaves. Con este protocolo, Bob y Alice convendrían de antemano en recurrir a un tercero neutral y desinteresado que hiciera de árbitro y les ayudara a completar sus transacciones. Cada una de las tres partes tendría una de las tres claves privadas, dos de las cuales se necesitarían para acceder al dinero transferido. Alice enviaría sus bitcoins a una dirección pública. Ese dinero sería entonces visible para todo el mundo, pero nadie podría acceder a él. Cuando Bob ve que el dinero se ha transferido, cumple su parte del contrato. Si, después de recibir el bien o el servicio de Bob, Alice no queda satisfecha y se siente engañada, podría negarse a darle a Bob la segunda clave. Tendrían entonces que apelar al árbitro, tenedor de la tercera clave, para que les ayudara a dirimir la cuestión. Estos árbitros sólo intervienen en caso de disputas de este tipo y en ningún momento tienen acceso al dinero, un mecanismo que propicia el auge de los «contratos inteligentes».

Para contratar a distancia, y no digamos automáticamente, necesitamos tener cierta confianza en que el sistema hará valer nuestros derechos cuando hagamos el trato. Si no podemos confiar en la otra parte, tenemos que confiar en los mecanismos de resolución de conflictos y en el sistema legal que los sustenta. La tecnología multifirma permite que estas terceras partes desinteresadas den confianza y seguridad a las transacciones anónimas.

La autenticación multifirma está ganando popularidad. Una empresa emergente llamada Hedgy está usando tecnología multifirma para crear futuros contratos: las partes se ponen de acuerdo en un precio de bitcoin que negociarán en el futuro, a reserva de intercambiarse la diferencia. Hedgy nunca guarda avales. Las partes los colocan en una cartera multifirma hasta que el plazo vence. La idea de Hedgy es usar la tecnología multifirma para crear un tipo de contratos inteligentes que se ejecuten a sí mismos y se muestren plenamente en la blockchain.²⁰⁰ Las blockchains son como un diálogo entre anonimato y apertura, en el que el protocolo multifirma reconcilia ambas cosas sin perder nada de ninguna.

Entre otras cosas, los contratos inteligentes cambian la función de aquellos que, dentro de una empresa, están encargados de hallar y contratar a gente con talento. Los departamentos de recursos humanos deben entender que también hay talento fuera de sus límites, no sólo dentro. Tienen que aceptar los retos que plantean los contratos inteligentes para reducir los costes de recurrir a recursos externos.

3. Costes de coordinación: ¿cómo trabajar todos juntos?

Ya hemos encontrado a las personas que queríamos y las hemos contratado. ¿Cómo las organizamos? En sus escritos, Coase trata de los costes de coordinar y concertar a las diferentes personas, productos y procesos para que formen una empresa que produzca valor efectivamente. Contra los economistas tradicionales que pensaban que en las empresas hay mercados internos, Coase dice que cuando «un trabajador pasa del departamento Y al departamento X, no lo hace por un cambio en los respectivos precios,

sino porque le han ordenado que lo haga».²⁰¹ En otras palabras, los mercados asignan recursos mediante el mecanismo de los precios, mientras que las empresas lo hacen porque así lo manda la dirección.

Williamson explica que hay dos sistemas de coordinación principales. El primero es el sistema de precios, que funciona para necesidades y oportunidades de asignación de recursos descentralizadas (el mercado). Pero en segundo lugar «las empresas [tradicionales] usan un principio organizativo diferente, el principio jerárquico, por el que es la autoridad la que asigna recursos». En las últimas décadas las jerarquías han sido criticadas por ser estructuras que acaban con la creatividad, impiden la iniciativa, incapacitan al capital humano y eluden la responsabilidad gracias a la opacidad. Lo cierto es que muchas jerarquías administrativas se han convertido en burocracias improductivas. Sin embargo, la jerarquía, como concepto, ha sido desacreditada injustamente, como lo ha sido su más elocuente defensor, el psicólogo de origen canadiense Elliot Jaques. En un artículo clásico publicado en la *Harvard Business Review* en 1990, Jaques afirmaba: «Treinta y cinco años de investigación me han convencido de que la administración jerárquica es la estructura más eficaz, resistente y natural que ha existido nunca para las grandes organizaciones. Bien estructurada, la jerarquía puede generar energía y creatividad, racionalizar la productividad y mejorar la moral».²⁰²

El problema es que en la historia económica reciente muchas jerarquías no han funcionado, hasta el punto de resultar ridículas. Lo demuestra *El principio de Dilbert*, seguramente el libro sobre administración empresarial más vendido de todos los tiempos, escrito por Scott Adams. Esto es lo que dice Dilbert sobre la tecnología de blockchain en una tira cómica reciente:

Administrador de empresa: Tendríamos que crear una blockchain.

Dilbert (para sí): ¡Ay, ay! ¿Lo dice en serio o es que lo ha visto en algún anuncio?

Dilbert: ¿Y de qué color quieres la blockchain?

Administrador de empresa: Parece ser que las lilas tienen más RAM.

En esta tira cómica, Adams refleja una de las características de las jerarquías mal entendidas: muchos administradores alcanzan niveles de poder sin tener los conocimientos propios del liderazgo eficaz.

Unida a un concepto progresista de la creación de organizaciones efectivas e innovadoras, la primera generación de internet permitió que los administradores de mentalidad progresista cambiaran el orden jerárquico de la distribución del trabajo y de la apropiación de mérito, reconocimiento y promoción.

Para bien o para mal, las jerarquías centralizadas son la norma. La descentralización, la organización reticular y la distribución del poder han estado presentes desde los primeros días de internet. Equipos y proyectos se han convertido en el fundamento de la organización interna. El correo electrónico permitió a las personas colaborar más allá de los silos organizativos. Los medios sociales redujeron algunos costes de colaboración internos, redujeron los costes transaccionales e hicieron más permeables los límites de las empresas, al permitir que éstas se comunicaran más fluidamente con proveedores, consumidores y socios.

Hoy día, las herramientas comerciales de los medios sociales ayudan a muchas empresas a alcanzar mayores niveles de colaboración interna. La distribución del poder, la verdadera descentralización del poder, es una cuestión fundamental en los negocios, y muchas empresas han experimentado con nuevos conceptos o los han puesto en práctica, conceptos que van de la organización matricial a la holocracia, con diversos grados de éxito.

En realidad, es opinión generalizada que cuando las empresas distribuyen responsabilidad, autoridad y poder, el resultado suele ser positivo: mejor gestión, mejor servicio al cliente y más innovación. Pero es más fácil decirlo que hacerlo.

Internet también ha reducido lo que los economistas llaman «costes de agencia», que son lo que cuesta cerciorarse de que todos los que trabajan en una empresa actúan en interés del propietario. Otro premio Nobel de Economía (sí, parece que hay muchos en este libro), Joseph Stiglitz, dice que el mismo tamaño y la aparente complejidad de estas empresas han aumentado los costes de agencia aun cuando los costes transaccionales han caído en picado. De ahí la enorme brecha salarial entre consejeros delegados y empleados.

¿Qué puede hacer, pues, la tecnología blockchain para cambiar la manera como las empresas se organizan y coordinan internamente? Con los contratos inteligentes y un grado de transparencia como nunca lo había habido, las blockchains no sólo deberían reducir los costes transaccionales dentro y fuera de la empresa, sino también los costes de agencia en todos los niveles de la organización. Estos cambios harán a su vez más difícil manipular el sistema. En consecuencia, y más allá de los costes transaccionales, las empresas podrían coger el toro por los cuernos: los costes de agencia. Yochai Benkler dice: «Lo que me gusta de la tecnología blockchain es que permite a la gente trabajar junta con la constancia y estabilidad de una organización, pero sin jerarquías».²⁰³

Además, los administradores de empresa que se organizan y actúan sabiendo que los accionistas no podrán ver los fallos, la complejidad innecesaria y la enorme desproporción entre lo que cobra un ejecutivo y el valor que realmente crea, tendrían que ir preparándose para trabajar con la radical transparencia que el sistema blockchain conlleva. No olvidemos que los administradores no son agentes del propietario, sino intermediarios.

4. Los costes de (re)construir confianza: ¿por qué tendríamos que fiarnos unos de otros?

Como hemos explicado, la confianza en los negocios y en la sociedad consiste en esperar que la otra parte sea honrada, respetuosa, responsable y transparente: que actúe con integridad.²⁰⁴ Crear confianza cuesta mucho, y muchos economistas y demás estudiosos dicen que las empresas se organizan verticalmente porque es más fácil crear confianza dentro de los límites de ellas que en el mercado abierto. Con el nivel de confianza más bajo que nunca, el reto de las empresas consiste no sólo en saber en quién confiar, sino en cómo conseguir capacidad exterior para confiar en ellos.

De hecho, economistas como Michael Jensen y otros sostienen que la *integridad* es un factor productivo. Aunque no son los primeros en hablar del tema, sí son los más elocuentes, y explican que la, al parecer, interminable serie de escándalos que ha habido

en el mundo de las finanzas, con sus dañinos efectos en el valor y en el bienestar humano, es un poderoso argumento en favor de aumentar la integridad de las operaciones financieras. Para ellos, no es una cuestión moral, sino una oportunidad de «incrementar significativamente la eficiencia y la productividad económica, además de contribuir al bienestar humano». Según ellos, «la integridad... tanto de individuos como de organizaciones tiene enormes consecuencias económicas (en el valor, la productividad, la calidad de vida, etc.). De hecho, la integridad es un factor productivo tan importante como el trabajo, el capital y la tecnología».²⁰⁵

Wall Street dejó de inspirar confianza (y casi acabó con el capitalismo) por su falta de integridad en repetidas ocasiones. Pero ¿ha cambiado? ¿Cambiará? En el pasado, los defensores de la responsabilidad social de las empresas decían que éstas «lo hacen bien cuando hacen el bien». No es lo que hemos visto. Muchas empresas *lo hacen bien cuando hacen el mal*, esto es, cuando realizan malas prácticas laborales en países en vías de desarrollo, externalizan sus costes a la sociedad, en forma, por ejemplo, de contaminación, son monopolistas y se aprovechan del consumidor. La crisis de 2008 nos ha enseñado sin duda que las empresas «lo hacen mal cuando hacen el mal». Los grandes bancos lo descubrieron muy a su pesar. Antes de 2008 muchos tenían una tasa de rentabilidad de más del 20 por ciento. Hoy, para muchos, esa tasa no llega al 5 por ciento, y algunos no cubren el coste del capital. Desde el punto de vista del accionista, no deberían existir.²⁰⁶

¿Qué posibilidades reales hay de que Wall Street haga caso de las recomendaciones de Jensen y se comporte con integridad? Lo que es seguro es que el oportunismo y la ganancia rápida forman parte del ADN del sistema financiero occidental.

Aquí entran en escena la tecnología blockchain y las monedas digitales. ¿Y si las partes no tuvieran que confiar una en otra, pero pudieran seguir actuando con honradez, responsabilidad, consideración y transparencia porque estos principios son el fundamento de la plataforma tecnológica financiera?

Steve Omohundro nos da un ejemplo interesante: «Si alguien de Nigeria quiere comprar algo que yo vendo, seré muy escéptico y no aceptaré ni tarjetas de crédito ni cheques que vengan de Nigeria. Con la nueva plataforma, sé que puedo confiar y no tengo que gastar en crear confianza. Es decir, que la nueva plataforma permite hacer transacciones que de otra manera simplemente no se harían».²⁰⁷

Por lo tanto, no hace falta que los bancos de Wall Street tengan una conducta y un ADN más íntegros; los fundadores del sistema blockchain han codificado esa integridad en sus protocolos informáticos y la han extendido por la red, habilitando así una nueva herramienta para la industria de los servicios financieros.

Con un sistema blockchain que hace que los costes de buscar, contratar, coordinar y crear confianza caigan en picado, las empresas deberían tener más fácil no sólo abrirse, sino también entablar relaciones de confianza con partes externas. Actuar en interés propio es actuar en interés de todos. Engañar al sistema cuesta más que usarlo debidamente.

Esto no quiere decir que la marca de empresa o actuar con ética no sea importante o ya no sea necesario. El sistema blockchain contribuye a garantizar la integridad y, por lo tanto, la confianza en las transacciones entre iguales, así como la transparencia, factor fundamental de la confianza. Sin embargo, como dice el escritor y teórico tecnológico David Ticoll: «La confianza y la marca no sólo sirven para avalar una transacción. También dependen de la calidad, el disfrute, la seguridad de un dispositivo o un servicio, el prestigio. En un mundo en el que se ha celebrado la XXI Conferencia sobre Cambio Climático (COP21), las mejores marcas desde el punto de vista de la transparencia y de la verificabilidad son también medioambiental, social y económicamente responsables».²⁰⁸

Con todo, gracias a los contratos inteligentes, a los ejecutivos se les pueden pedir cuentas, porque deben respetar los compromisos tal y como han quedado establecidos y registrados informáticamente. Las empresas pueden programar relaciones con absoluta transparencia, de manera que todo el mundo sepa claramente lo que cada parte se ha comprometido a hacer. Y, en general, lo quieran o no, deben hacer negocios respetando los intereses de las demás partes. La plataforma obliga a ello.

Determinar los límites de la empresa

En general, podemos decir que los límites que separan a una empresa de sus vendedores, asesores, clientes, comunidades de iguales externas y demás serán cada vez más difíciles de establecer. Y, lo que quizá es más importante, esos límites cambiarán sin cesar.

Las empresas seguirán existiendo, pese a las blockchains, porque los mecanismos de búsqueda, contratación, coordinación y creación de confianza dentro de los límites de la empresa serán más rentables que los del mercado libre, al menos en muchas actividades. La idea de la llamada «nación sin agentes», en la que los individuos trabajarán fuera de los límites de las empresas, es ilusoria. Melanie Swan, fundadora del Institute for Blockchain Studies, dice: «¿Qué tamaño deberían tener las empresas para funcionar con la mayor eficiencia posible? Porque no son entidades unitarias, hechas de gente que trabaja por su cuenta». Según ella, habrá nuevos tipos de «entidades empresariales flexibles formadas por individuos y grupos que se asociarán para llevar a cabo este o aquel proyecto». Para ella, el nuevo modelo de empresa se parece más al de los gremios, las asociaciones preindustriales de comerciantes que trabajaban juntos en una ciudad. «Siguen haciendo falta organizaciones que actúen de mecanismo coordinador. Pero los nuevos modelos de colaboración en equipo aún no están muy claros.»²⁰⁹

Hoy oímos a menudo decir que las empresas deberían centrarse en su núcleo. Pero cuando pensamos lo mucho que la tecnología blockchain reduce los costes transaccionales, nos preguntamos: ¿qué es el núcleo? ¿Cómo lo definimos cuando vemos que ese núcleo cambia constantemente?

Parece que cada cual tiene su propia opinión sobre cuál debería ser el tamaño óptimo de una empresa para maximizar la productividad y la competitividad. Muchas de las empresas que examinamos no tenían una idea clara, pareciendo que adoptaban el punto de vista de Bob Dylan para determinar lo que debían incluir o excluir («No necesitas al

hombre del tiempo para saber en qué dirección sopla el viento»). Por ejemplo, consideraban que los departamentos administrativos eran imprescindibles, sin dar razón clara de por qué.

Algunos son más rigurosos. Gracias al concepto de competencias nucleares desarrollado por Gary Hamel y C.K. Prahalad, las empresas ganan competitividad porque dominan competencias que son fundamentales para la empresa, mientras que otras pueden adquirirse de fuera.²¹⁰ Sin embargo, una empresa puede dominar algunas actividades que no son fundamentales. ¿Deberían esas actividades mantenerse dentro?

El estratega Michael Porter tiene la firme convicción de que la competitividad nace de las actividades, en particular de actividades interrelacionadas que se refuerzan y son difíciles de reproducir en su totalidad. No son las partes individuales del negocio las que importan, sino la manera como se interconectan y organizan para reforzarse unas a otras en una única actividad sistémica. La competitividad nace de todo el sistema de actividades; mientras que las actividades individuales dentro del sistema pueden copiarse, los competidores no pueden producir el mismo beneficio si no consiguen recrear el sistema en su conjunto.²¹¹

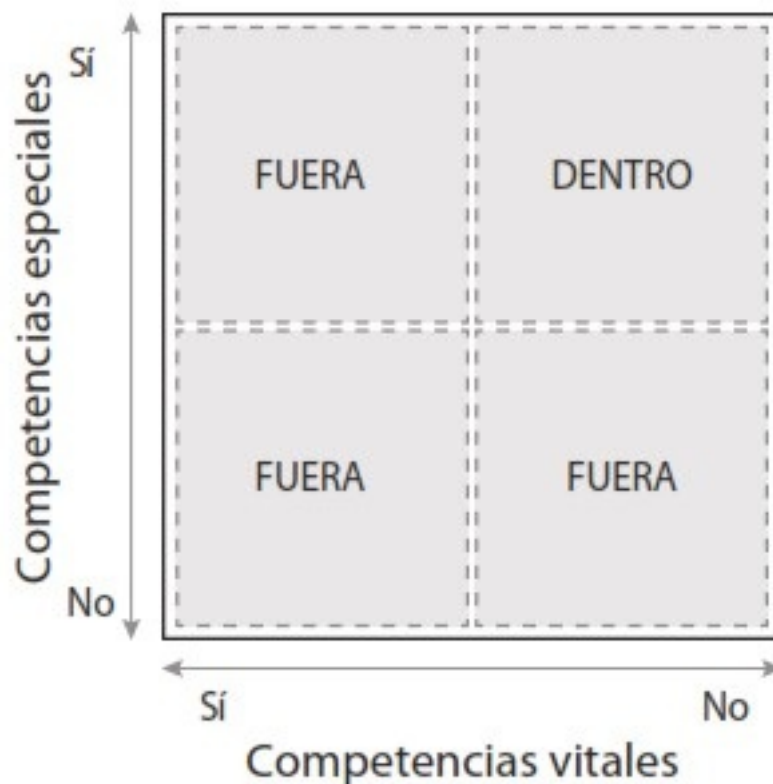
Otros opinan que las empresas siempre deberían quedarse con las funciones o competencias fundamentales, que son aquellas que deben funcionar bien para que la empresa sobreviva y prospere. Ahora bien, hacer ordenadores es fundamental para las empresas informáticas y, sin embargo, Dell, HP e IBM subcontratan a fabricantes de electrónica como Celestica, Flextronics o Jabil para que hagan gran parte de esta actividad. El ensamblaje final de vehículos es fundamental para los fabricantes de coches y, sin embargo, BMW y Mercedes contratan a Magna para que desempeñe esa tarea.

Susan Athey, catedrática de la Escuela de Posgrado de Negocios de Stanford, afirma convincentemente: «Puede haber algunas funciones fundamentales, como la recogida y el análisis de macrodatos, que sería muy arriesgado ejecutar fuera de la empresa, incluso si no tenemos especial habilidad en ellas».²¹² Ciertamente, puede haber funciones como el análisis de datos en las que hay que ser excepcionalmente buenos si la empresa quiere sobrevivir, y asociarse puede entrañar riesgos. Aun así, se pueden usar recursos externos para crear capacidad interna.

Nuestra opinión es que lo primero que hay que hacer a la hora de decidir sobre los límites empresariales es conocer la industria en cuestión, la competencia y las oportunidades que hay de prosperar, y usar este conocimiento para desarrollar una estrategia de negocio. A partir de ahí, el sistema blockchain abre nuevas oportunidades de organización reticular que todos los administradores de empresa y los llamados «trabajadores del conocimiento» han de tener en cuenta. Las decisiones sobre los límites empresariales no sólo competen a los ejecutivos de mayor rango, sino a todos los que quieren mejorar la capacidad de innovación y de rendimiento. Deberíamos añadir —y no es poca cosa— que no podemos subcontratar nuestra cultura empresarial.

La «matriz»

Teniendo en cuenta que la tecnología blockchain permite acceder a competencias especiales fuera de la empresa, las empresas pueden pasar a definir esas actividades y funciones que son esenciales para la competitividad, es decir, que son a la vez vitales y lo bastante únicas como para garantizar un valor diferenciado.



Con todo, esta «matriz dentro-fuera» no es más que un punto de partida para definir los límites de una empresa en un momento dado. ¿Qué otros factores debería considerar la empresa a la hora de decidir lo que es fundamental? ¿Qué circunstancias pueden condicionar la decisión de recurrir a competencias externas o de desarrollar las internas?

*Manejar nuestro futuro:
las decisiones sobre los límites de la empresa*

A la hora de tomar decisiones sobre sus límites, las empresas deberían empezar usando el sistema blockchain para tener una visión completa y llegar a un consenso sobre lo que es único y lo que es crucial en su negocio. Volvamos a Joseph Lubin y a ConsenSys, que anuncian lo que será el *modus operandi* de la empresa basada en el sistema blockchain. No olvidemos que ConsenSys acaba de nacer y pueden pasar muchas cosas que den al traste con la empresa. Podemos seguir aprendiendo de su ejemplo.

1. ¿Hay posibles socios que pueden hacer el trabajo mejor que nosotros? En particular, ¿puede ser provechoso promover nuevas comunidades productivas de iguales, ideágoras, plataformas abiertas y otros modelos de negocio basados en el sistema

blockchain? La empresa ConsenSys es capaz de contratar y coordinar a grandes expertos, aunque muchos no pertenezcan a la empresa.

2. Dada la tecnología blockchain, ¿en qué consiste la nueva economía de los límites empresariales, y la relación entre los costes de asociación y los de desarrollo interno? ¿Podemos desarrollar una serie de contratos inteligentes cuyos elementos fundamentales sean modulares y reutilizables? ConsenSys usa contratos inteligentes para reducir los costes de coordinación.
3. ¿Cuál es el alcance de la interdependencia tecnológica comparada con la modularidad? Si podemos definir componentes de negocio que sean modulares, entonces podremos recrearlos fuera de los límites de la empresa. ConsenSys crea modelos de desarrollo informático y da acceso a módulos sobre los que sus socios pueden trabajar.
4. ¿Cuáles son las competencias de nuestra empresa con respecto a la organización del trabajo subcontratado? ¿Pueden mejorar los contratos inteligentes esas competencias y reducir costes? Desde el principio, ConsenSys era una blockchain para negocios. El consejero delegado Joseph Lubin adopta la tecnología y una forma modificada de holocracia, y podemos ver los siete principios generales funcionando.
5. ¿Cuáles son los riesgos del oportunismo de un socio que pueda usurpar partes fundamentales de nuestro negocio, como se ha dicho que quiere hacer Foxconn con las empresas de teléfonos móviles? ConsenSys trata de mitigar este problema fomentando la lealtad por medio de estructuras incentivadoras que permiten que sus talentos participen en la riqueza que crean.
6. ¿Existen obstáculos legales, de regulación o políticos para avanzar en la organización reticular de las empresas (y en su consiguiente reducción)? Para ConsenSys, no de momento.
7. La rapidez y el ritmo de la innovación son factores que hay que tener en cuenta a la hora de decidir sobre los límites de la empresa. A veces las empresas no tienen más remedio que recurrir a socios que desempeñen funciones estratégicas porque ellas no pueden desarrollarlas con la suficiente rapidez. Un acuerdo con un socio puede ser provisional. ¿Nos ayudarán los socios a construir un ecosistema que mejore nuestra competitividad? Ésta es la estrategia de ConsenSys: crear una red de colaboradores en torno a la plataforma Ethereum, hacer crecer la plataforma y el ecosistema y aumentar las posibilidades de éxito de todos sus componentes.
8. ¿Hay peligro de perder el control de algo fundamental, por ejemplo, un producto o una estructura de red? Las empresas deben saber qué partes de la cadena de valor serán clave para crear y acumular valor en el futuro. Si esas partes se dejan fuera, la empresa perderá. La plataforma Ethereum proporciona una estructura básica a ConsenSys.
9. ¿Existe una función, como la explotación de activos informativos, que debe ser parte del tejido de nuestra empresa y de todas sus operaciones? Aun cuando carezcamos de una función especial, debemos ver el recurso al socio como una táctica transicional para desarrollar la capacidad y experiencia internas necesarias. Las

tecnologías blockchain introducirán una serie de nuevas capacidades que han de grabarse en las mentes de todos los empleados. No podemos sacar la cultura de nuestros límites.

Capítulo V

Nuevos modelos de negocio: ganar dinero con las blockchains

Fundada un mes antes de la crisis de 2008, Airbnb se ha convertido en una plataforma valorada en 25.000 millones de dólares, y es actualmente la que más viviendas ofrece del mundo, según el valor de mercado y el número de viviendas ocupadas. Pero los dueños de esas viviendas sólo reciben una parte del valor que crean. Los pagos internacionales se hacen por Western Union, que cobra 10 dólares por cada transacción con cambio de divisas grande. Las liquidaciones tardan mucho. Airbnb guarda y rentabiliza toda la información. Y tanto los que ponen en alquiler como los que alquilan están preocupados por su privacidad.

Nos reunimos con el experto en blockchain Dino Mark Angaritis para diseñar un Airbnb de blockchain que le hiciera la competencia al otro. Decidimos llamar a nuestro nuevo negocio bAirbnb. Sería más como una cooperativa propiedad de sus miembros. Todos los beneficios, descontados los gastos, irían a esos miembros, que controlarían la plataforma y tomarían las decisiones.

bAirbnb contra Airbnb

bAirbnb es una *aplicación distribuida* (DApp, en inglés), una serie de contratos inteligentes que almacenan información en una blockchain de listas de viviendas. La aplicación tiene una elegante interfaz: los propietarios pueden subir información y fotos de sus viviendas.²¹³ La plataforma incorpora puntuaciones de reputación tanto de los que ofrecen como de los que demandan alquileres para que todo el mundo pueda tomar mejores decisiones.

Cuando queremos alquilar algo, el programa de bAirbnb repasa las listas de la blockchain de acuerdo con los filtros de nuestra búsqueda (por ejemplo, apartamento con dos habitaciones, a 15 kilómetros de la torre Eiffel, con puntuación de cuatro estrellas o más). Nuestra experiencia de usuario es igual que la de Airbnb, con la diferencia de que nos comunicamos de igual a igual en la red, mediante mensajes encriptados y criptográficamente firmados que no se almacenan en una base de datos, como ocurre en el caso de Airbnb.²¹⁴ Nosotros y el propietario de la vivienda somos los únicos que podemos leer esos mensajes. Podemos intercambiar números de teléfono, algo que Airbnb impide para asegurarse futuros ingresos. En bAirbnb, el propietario y nosotros podríamos comunicarnos fuera de la cadena y completar la transacción también fuera de la cadena, aunque sería mejor hacerlo en ella por una serie de razones.

Reputación: Como la red registra las transacciones en la blockchain, recibir opiniones positivas de los usuarios mejora nuestra reputación. El riesgo de que nos den un voto negativo hace que todos seamos honrados. Recordemos que las personas con buena reputación pueden usar la misma identidad en múltiples aplicaciones distribuidas y beneficiarse de seguir siendo una buena persona.

Verificación de la identidad: Dado que no estamos tratando con un sistema centralizado que compruebe las identidades por nosotros, todas las partes tienen que confirmar la identidad de las demás. La blockchain recurre a contratos de aplicaciones de verificación de identidad, uno de los muchos que bAirbnb, SUber (el Uber de blockchain) y otras aplicaciones distribuidas usan para verificar la identidad real de las personas.

Protección de la privacidad: Las aplicaciones de verificación de la identidad no registran ni archivan las transacciones en una base de datos. Simplemente contestan «Verdadero» o «Falso» cuando se les pide que verifiquen una clave pública (una identidad). Diferentes aplicaciones distribuidas pueden recurrir a la de verificación de la identidad, pero ésta nunca registra detalles de transacciones. Esta separación de identidad y actividad contribuye mucho a garantizar nuestra privacidad.

Reducción de riesgos: Los propietarios de viviendas suelen guardar la identidad y los datos financieros de los clientes en sus servidores, que pueden ser atacados y pirateados, lo que expone a los propietarios a demandas y grandes responsabilidades. En la blockchain no tenemos que confiar nuestros datos a ningún vendedor; no hay ninguna base de datos central que pueda ser atacada y pirateada. Sólo hay transacciones anónimas entre iguales.

Seguros: Airbnb ofrece un seguro de un millón de dólares a los propietarios y los resarce por robos y daños y perjuicios. En bAirbnb los propietarios disponen de una aplicación distribuida que hace las veces de seguro. Los inquilinos con buena reputación como nosotros tienen tarifas de seguro más bajas y no han de subvencionar a aquellos que no tienen cuidado, no eligen bien o tratan mal las viviendas. Cuando solicitamos una reserva, bAirbnb envía nuestra clave pública (nuestra identidad) al contrato del seguro para que haga un presupuesto. La aplicación se pone en contacto con una serie de proveedores. Las aseguradoras realizan sus cálculos en tiempo real mediante programas informáticos autónomos basados en los datos del contrato, como el valor de mercado de la vivienda del propietario, lo que éste quiere asegurar, su reputación, nuestra reputación como inquilinos, y el precio del alquiler. bAirbnb selecciona la mejor oferta y la añade a la tarifa diaria que el propietario quiere cobrar. La blockchain procesa este cálculo en segundo plano; propietarios e inquilinos tienen una experiencia de usuario parecida a la de Airbnb pero un intercambio de valor superior y más justo.

Pagos: Desde luego, en la blockchain nuestros pagos se realizan en segundos, no en días, como ocurre en Airbnb. Los propietarios pueden administrar las fianzas más fácilmente con contratos inteligentes. Algunos usan cuentas de plica para hacer pagos parciales (diarios, semanales, a la hora, etc.) o totales, como las partes acuerden. En conflictos que tengan que ver con contratos inteligentes, las partes pueden recurrir al arbitraje.

Acceso a la propiedad con cerraduras inteligentes (dispositivo IoT): Una cerradura inteligente conectada a la blockchain sabe si has pagado. Cuando llegamos, nuestro móvil, provisto del sistema de comunicación de campo cercano (NFC, por sus siglas en inglés), puede firmar un mensaje con nuestra clave pública como prueba de pago y la cerradura inteligente se abrirá. No tenemos que quedar con los propietarios para que nos den las llaves ni éstos tienen que pasarse por la vivienda, a menos que quieran saludarnos o tengan que solucionar algún problema.

Con todo esto, el propietario y nosotros nos hemos ahorrado casi todo el 15 por ciento de comisión que se lleva Airbnb. Los pagos son seguros e instantáneos. No hay comisiones por pagos al extranjero en contratos internacionales. No tenemos que preocuparnos de que nos roben la identidad. Los gobiernos de regímenes opresores no pueden reclamar a bAirbnb información sobre sus operaciones. Es una economía que realmente reparte valor; las dos partes, clientes y proveedores de servicios, salen ganando.

La informática global: el auge de las aplicaciones distribuidas

Antes de examinar otros posibles negocios distribuidos como bAirbnb, explicaremos cómo la tecnología en la que se basan permite la descentralización. Hasta la llegada de las blockchains, las organizaciones centralizadas concentraban la capacidad de procesamiento.

En las primeras décadas de la informática empresarial, todos los programas funcionaban en los ordenadores de sus propietarios. General Motors, Citibank, U. S. Steel, Unilever y el gobierno federal estadounidense poseían enormes centros de datos que funcionaban con programas informáticos patentados. Las empresas alquilaban capacidad procesadora, o la compartían en régimen de multipropiedad con ellos, a proveedores, como el gigante de los años ochenta del siglo pasado CompuServe, para ejecutar sus propias aplicaciones.

Conforme la informática personal progresaba, el mercado de programas se especializó: algunos desarrollaron aplicaciones para clientes (el PC), y otros, aplicaciones para servidores (los servidores propiamente dichos). Con la adopción generalizada de internet, y particularmente de la red informática mundial, individuos y compañías podían usar sus ordenadores para compartir información, al principio documentos de texto y luego imágenes, vídeos y otros contenidos multimedia, así como programas.²¹⁵ La posibilidad de compartir empezó a democratizar la información. Pero fue algo efímero.

En los años noventa apareció una nueva variante de la multipropiedad, que al principio se llamó *redes privadas virtuales* (VPN, por sus siglas en inglés) y luego *informática en nube*. La informática en nube permitía a usuarios y empresas almacenar y procesar sus programas y datos en centros de datos ajenos. Las nuevas empresas tecnológicas como Salesforce.com hicieron fortunas aprovechando el modelo en nube para ahorrar a los clientes los grandes costes de desarrollar y ejecutar sus propios programas. Proveedores de servicios en nube como Amazon e IBM hicieron negocios por valor de miles y miles de millones de dólares. En la década de 2000, compañías de

medios sociales como Facebook y Google crearon servicios que funcionaban en sus propios centros de datos. Y, siguiendo esta tendencia de centralización informática, compañías como Apple abandonaron la estructura democratizadora de la red y crearon plataformas patentadas como Apple Store, en las que los consumidores adquirirían aplicaciones patentadas, no en la red abierta, sino en «jardines vallados» exclusivos.

En la era digital ha ocurrido una y otra vez que grandes empresas han consolidado —creado, procesado y poseído o adquirido— aplicaciones en sus propios grandes sistemas. Las empresas centralizadas se han convertido en estructuras informáticas centralizadas que, a su vez, han centralizado el poder tecnológico y económico.

Pero hay algunos peligros: con puntos de control únicos, las mismas empresas son vulnerables y están expuestas a quiebras catastróficas, fraudes y violaciones de la seguridad. Si fuimos clientes de Target, eBay, JP Morgan Chase, Home Depot, Anthem e incluso Ashley Madison, el Departamento de Administración de Personal de Estados Unidos (¡también atacado!) y Uber, sin duda sufrimos el pirateo de 2015.²¹⁶ Sistemas de diferentes partes de una empresa siguen teniendo grandes dificultades para comunicarse entre sí, y no digamos con sistemas de fuera de la empresa. Eso significa que nosotros, los usuarios, nunca hemos tenido realmente el control de nada. Son otros los que definen nuestros servicios con sus valores y objetivos implícitos que pueden chocar con los nuestros. Nosotros generamos montones de datos valiosos pero son otros los que los tienen y los que hacen inmensas fortunas —quizá las más grandes de la historia— mientras que la mayoría de nosotros apenas recibimos beneficios o compensación. Y lo peor de todo es que los poderes centrales usan nuestros datos para crear imágenes exactas de nosotros que pueden emplear para vendernos cosas o espiarnos.

En esto aparece la tecnología blockchain. Todos podemos subir un programa a esta plataforma y dejar que se ejecute con una fuerte garantía cripto-económica²¹⁷ de que el programa seguirá funcionando con seguridad, como queríamos. Esta plataforma es pública, no pertenece a ninguna organización, y contiene un conjunto creciente de recursos, como dinero digital, para incentivar y premiar ciertos comportamientos.

Estamos entrando en una nueva era de la evolución digital en la que podemos programar y compartir un software que está distribuido. Igual que el protocolo blockchain está distribuido, una aplicación distribuida o DApp se ejecuta a la vez en muchos dispositivos informáticos en lugar de en un solo servidor. Esto es porque todos los recursos informáticos que ejecutan una blockchain constituyen un ordenador. El desarrollador de blockchain Gavin Wood lo explica describiendo la blockchain Ethereum como una plataforma de procesamiento. «Sólo hay un ordenador Ethereum en el mundo —dice—. Además, es multiusuario, y todo el que lo use alguna vez es incorporado automáticamente.» Como Ethereum está distribuido y diseñado con el mayor grado de criptoseguridad, «todos los códigos, toda la información procesada y almacenada lo es dentro de su propio espacio cerrado y nadie podrá nunca manipular esos datos». Dice que las normas fundamentales forman parte del ordenador, como si fueran «silicio virtual».²¹⁸

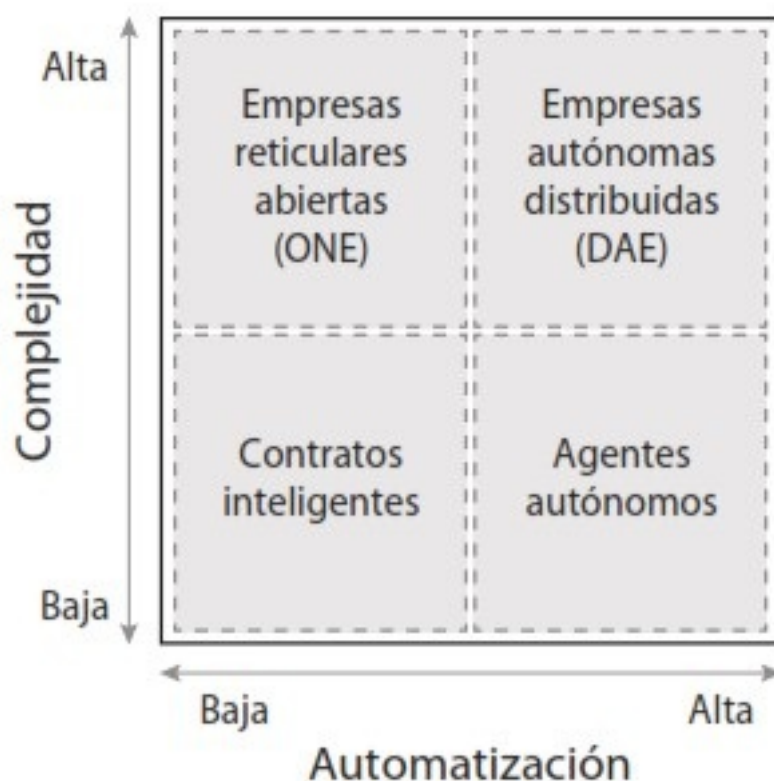
En cuanto a las DApp, ha habido antecedentes del sistema blockchain. BitTorrent, el programa para compartir archivos entre iguales, demuestra el poder de las DApp, pues actualmente constituye más del 5 por ciento de todo el tráfico de internet.²¹⁹ Amantes de

la música, del cine y de otros medios de comunicación comparten sus archivos gratuitamente, sin que haya un servidor central que las autoridades puedan clausurar. El iconoclasta programador Bram Cohen, que por cierto siente poco entusiasmo por la plataforma bitcoin a causa de la actividad comercial que la rodea, desarrolló BitTorrent. «La revolución no será rentabilizada», dice.²²⁰

La mayoría de nosotros pensamos que generar renta y valor económico con la innovación tecnológica es positivo, siempre y cuando la revolución no la rentabilicen unos pocos. Con la tecnología blockchain, las posibilidades para las DApp son casi ilimitadas, porque con ellas alcanzan un nuevo nivel. Si, como dice la canción, «amor y matrimonio, amor y matrimonio, van juntos como el coche y el caballo», así van las DApp y el sistema blockchain. La empresa Storj es una plataforma de almacenamiento en nube con una serie de aplicaciones que permiten a los usuarios almacenar información con seguridad, privacidad y a precios muy bajos. Ninguna autoridad central tiene acceso a la contraseña encriptada del usuario. El servicio elimina los altos costes de los servicios de almacenamiento centralizados; es rapidísimo y paga a los usuarios por alquilar el espacio de disco que les sobra. Es como un Airbnb de la memoria libre de nuestros ordenadores.

Los reyes de las DApp: los negocios distribuidos

¿Cómo incorporan las DApp mayor eficiencia, innovación y capacidad de respuesta a la estructura de la empresa? ¿Qué nuevos modelos de negocio podemos ejecutar con DApp para generar valor? Y si instituciones poderosas acaparan hoy los beneficios de internet, ¿cómo podemos pasar de la «subcontratación» y de las «webs de negocios» a modelos verdaderamente distribuidos de innovación y creación de valor que puedan distribuir prosperidad y la propiedad de datos y riqueza? En la siguiente matriz de dos por dos mostramos las que creemos que son las cuatro innovaciones más importantes.



El eje de ordenadas indica el grado de participación humana en el modelo. A la izquierda, el modelo requiere cierta intervención del hombre. A la derecha, el modelo no requiere ninguna intervención humana.

El eje de abscisas indica la complejidad funcional del modelo, no su complejidad técnica. En el extremo inferior están los modelos que realizan una única función. En el extremo superior, modelos que desempeñan varias funciones.

Son todos elementos de la economía blockchain porque se fundan en la tecnología blockchain y muchas veces usan criptomonedas. Los contratos inteligentes (de los que hemos hablado en el capítulo anterior) son la forma más básica: revisten cierta complejidad que requiere la intervención humana, cada vez más en forma de acuerdos multifirma. Conforme los contratos inteligentes ganan en complejidad e interactúan con otros contratos, pueden contribuir a formar lo que llamamos *empresas reticulares abiertas* (ONE, por sus siglas en inglés). Si combinamos ONE con *agentes autónomos* —programas informáticos que toman decisiones y actúan en consecuencia sin intervención humana—, tenemos lo que llamamos *empresas autónomas distribuidas*, que requieren poca o ninguna gestión ni jerarquía tradicionales para generar valor para el consumidor y riqueza para el propietario. Y pensamos que muchísima gente, miles o millones de personas, podrían colaborar para crear una empresa y participar de la riqueza que cree, una riqueza distribuida y no redistribuida.

Empresas reticulares abiertas

Con costes bajísimos, los contratos inteligentes permiten a las empresas llegar a acuerdos eficaces y automáticos con proveedores y socios que antes parecían improbables. Cuando se agregan, los contratos inteligentes pueden hacer que las empresas se parezcan a redes, y que sus límites sean más porosos y fluidos.

La tecnología blockchain reduce también los costes de búsqueda y coordinación de los que hablaba Coase, con lo que las empresas pueden desagregarse para formar redes más eficaces. Un fabricante de automóviles puede comprobar la fiabilidad de un proveedor simplemente usando los servicios de análisis en línea. Basta con buscar «eje» o «cristal de ventanilla» en cualquier número de intercambios industriales en la blockchain y negociar el precio.

Podemos aplicar este mismo sistema para encontrar una pieza de recambio, un socio, un colaborador o un programa de gestión de un recurso distribuido. ¿Que necesitamos acero de China, caucho de Malasia o cristal de Wichita, Kansas? No hay problema. Cámaras de compensación descentralizadas y en línea que operen como DApp para cada producto permitirán a los compradores negociar precios, calidad y fechas de entrega con unos cuantos clics del ratón. Tendremos un registro detallado de las transacciones anteriores, en el que no sólo veremos la calificación de las distintas empresas, sino también cómo cumplieron con sus compromisos. Podremos seguir todos los envíos en un mapa virtual que mostrará con precisión los lugares por los que pasa. Podremos programar envíos que lleguen justo a tiempo. No se necesitarán almacenes.

Agentes autónomos

Imaginemos un programa informático capaz de navegar por internet con su propio dinero y con capacidad para aprender y adaptarse, que persiga los objetivos que su creador haya definido y compre los recursos que necesite para sobrevivir, como capacidad procesadora, a la vez que vende servicios a otras entidades.

La expresión *agente autónomo* significa muchas cosas.²²¹ A efectos de lo que nos interesa, es un dispositivo o sistema informático que, en nombre de su creador, recaba información de su entorno y es capaz de tomar decisiones por su cuenta. Podríamos decir que algunos agentes autónomos son «inteligentes» aunque carezcan de inteligencia propiamente dicha. Pero tampoco son «simples programas informáticos», porque pueden decidir cómo alcanzar sus objetivos. Pueden sentir y responder a su entorno.²²²

El virus informático es el ejemplo más notorio de agente autónomo; el virus sobrevive reproduciéndose a sí mismo de ordenador en ordenador sin intervención humana expresa. Inocular un virus en una blockchain sería más difícil y, sin duda, muy costoso, porque seguramente tendría que pagar a la otra parte para interactuar con ella, y la red enseguida identificaría su clave pública, hundiría su reputación o no validaría sus transacciones.

Pongamos ejemplos positivos de agentes autónomos en blockchain. Un servicio informático en nube alquila capacidad procesadora a varias fuentes y alcanza el tamaño de Amazon llegando a acuerdos con otros ordenadores a los que les sobra esa capacidad.²²³ Un coche automático propiedad de una comunidad, empresa, individuo, o

incluso sin propietario, circula por la ciudad llevando pasajeros de aquí para allá y cobrándoles debidamente. Nos interesan los agentes que puedan realizar transacciones, adquirir recursos, hacer pagos y, en general, producir valor para su creador.

Vitalik Buterin, que creó la blockchain Ethereum, ha teorizado sobre estos agentes y desarrollado una taxonomía que refleja su evolución. En el primer estadio están los agentes monofuncionales como los virus, que trabajan para alcanzar sus limitados objetivos. En el siguiente estadio están los agentes más inteligentes y versátiles, como, por ejemplo, un servicio que alquile servidores de un conjunto concreto de proveedores como Amazon. Un agente más sofisticado podría saber cómo alquilar un servidor de cualquier proveedor y luego usar cualquier motor de búsqueda para localizar nuevos sitios web. Un agente aún más capaz podría actualizar su software y adaptarse a nuevos modelos de alquiler de servidores, como, por ejemplo, alquilarles a los usuarios finales los ordenadores o discos que no usen. El penúltimo paso consiste en ser capaz de descubrir nuevas industrias y entrar en ellas, lo que conduciría a la siguiente etapa en la evolución de las especies: la inteligencia artificial plena.²²⁴

Meteonet

¿Podría un agente autónomo usar la tecnología blockchain para hacer dinero con pronósticos del tiempo? Vayámonos a 2020. Los mejores pronósticos meteorológicos los hace una red de dispositivos inteligentes que miden y predicen el tiempo en todo el mundo. Ese año, un agente autónomo llamado BOB se introduce en esa red para colaborar con esos dispositivos y hacer negocio. Así funciona BOB.

Sensores medioambientales distribuidos (meteoNodos) puestos en postes, en la ropa de la gente, en los tejados de los edificios, en coches, y conectados con satélites, forman una red global. No es necesario ningún proveedor de servicios de internet que ofrezca conexión. En lugar de comunicarse con una base de datos central, esos sensores almacenan los datos en una blockchain.²²⁵ Muchos funcionan con energía solar y no necesitan estar conectados a la red eléctrica; pueden operar con eficacia por un tiempo indefinido.

La blockchain desempeña unas cuantas funciones. La primera, procesa los pagos. A modo de incentivo, cada meteoNodo recibe un micropago cada treinta segundos por suministrar información meteorológica precisa (temperatura, humedad, viento, etc.) de un punto concreto del mundo.

La blockchain también almacena todas las transacciones de los meteoNodos. Cada uno de los meteoNodos firma su información con su clave pública, almacenada en la cadena. Una clave pública identifica el meteoNodo y permite que otras entidades determinen su reputación. Cuando el nodo produce información meteorológica precisa, su reputación mejora. Si un nodo se rompe o avería y produce información inexacta, pierde calificación. Los nodos con mala reputación reciben menos bitcoins que los nodos con buena reputación, siendo el beneficiario el creador de la aplicación, sea un individuo, una empresa o una cooperativa.

La blockchain también permite a los proveedores y consumidores de datos participar de igual a igual en un sistema único y abierto, en lugar de suscribirse a docenas de servicios meteorológicos centralizados de todo el mundo, y programar su software para comunicarse con cada una de las interfaces de programación de aplicaciones (API, por sus siglas en inglés). Con los contratos inteligentes podemos tener un «mercado distribuido de información meteorológica» en el que los consumidores podemos comprar información en tiempo real y recibirla en un formato universalmente aceptado. Los proveedores de datos centralizados pueden abandonar sus sistemas patentados y sus propósitos de venta individualizada y convertirse en proveedores de datos para ese mercado distribuido de información meteorológica universalmente accesible.

MeteoDApp: los sensores LP

En la primera era de internet, la innovación técnica sólo se producía en el centro; servicios centralizados como las compañías energéticas, empresas de televisión por cable y bancos centrales decidían cuándo modernizar la red, cuándo ofrecer nuevas prestaciones y a quién permitir el acceso. La innovación no podía darse en la «periferia» (o sea, los individuos que usaban la red) porque las normas y protocolos de los sistemas cerrados mandaban que todas las nuevas tecnologías concebidas para interactuar con la red necesitaban el permiso del poder central para operar en ella.

Pero los poderes centrales son ineficientes porque no conocen exactamente lo que el mercado demanda en tiempo real. Tienen que hacer suposiciones más o menos fundadas que siempre son menos certeras de lo que los mercados piden en tiempo real. El resultado es algo como WeatherCorp, un servicio centralizado que instala sensores y envía satélites y que vende suscripciones a datos que poca gente puede querer.

El sistema blockchain permite que cada entidad sea un proveedor o un consumidor de información meteorológica, con muy fácil acceso. No hay más que comprar un meteoNodo, ponerlo en nuestro tejado y conectarlo a la DApp LP (siglas de *linked peers* o «iguales conectados») del mercado global de información meteorológica para empezar a ganar dinero. Y si podemos instalar un meteoNodo propio que proporcione información más exacta, ¡mejor que mejor! Innovamos en la periferia y el mercado nos premia por ello. Los incentivos a la innovación en redes abiertas tienden a incrementar la eficiencia más que las redes cerradas.

Programas en pugna

¿Qué pasa con los conflictos de intereses? Si los meteoNodos empiezan a expandirse y entran en el mercado de los seguros, ¿no padecerán disonancia cognitiva? Los meteoNodos de las granjas quieren hacer hincapié en las consecuencias de las sequías, y los meteoNodos de las aseguradoras afirman que la sequía es mínima. Los propietarios y los diseñadores de agentes tienen que operar con transparencia. Si pasan la información de los sensores por un tamiz sesgado, sus respectivas reputaciones caerán.

Vitalik Buterin señala que los agentes autónomos están obligados a crear, porque, para sobrevivir y prosperar, tienen que moverse en un entorno complejo, que cambia rápidamente e incluso es hostil. «Un proveedor de alojamiento web con pocos escrúpulos podría localizar específicamente todos los puntos del servicio y sustituirlos por nodos que engañen en algún sentido; un agente autónomo debe ser capaz de detectar ese engaño y suprimir o por lo menos anular los nodos fraudulentos.»²²⁶

Nótese que los agentes autónomos también distinguen entre la persona y la propiedad o el control del activo. Antes del sistema blockchain, todos los activos —tierra, propiedad intelectual, dinero— requerían que una persona o una organización legal de personas los poseyera. Según Andreas Antonopoulos, las criptomonedas prescinden por completo de la persona. «Una cartera podría ser controlada por un programa que no tuviera propietario y así tenemos la posibilidad de que existan agentes informáticos completamente autónomos que controlen su propia moneda.»²²⁷

Un agente autónomo podría comprar su propio alojamiento web y usar algoritmos evolutivos para propagar copias de sí mismo haciendo pequeños cambios y permitiendo luego que esas copias sobrevivieran. Cada copia podría incorporar nuevo contenido que descubriera o incluso que obtuviera mediante anuncios de colaboración abierta en internet. Si algunas de las copias tuvieran mucho éxito, el agente podría vender anuncios a los usuarios, y el dinero podría ir a una cuenta bancaria o a un lugar seguro de la blockchain; el agente podría emplear este creciente capital para anunciar más contenido colaborativo y proliferar. El agente podría repetir el ciclo de manera que el contenido bueno se difundiera y se alojara a sí mismo, y el contenido malo acabara muriendo porque se le terminara el dinero para pagarse el alojamiento.

Empresas autónomas distribuidas

Ahora le pedimos al lector que se siente en su silla de capitán de *Star Trek* y se abroche el cinturón. Imaginemos a BOB 9000, un conjunto de agentes autónomos que cooperan en un ecosistema complejo basado en el sistema blockchain según una consigna y unas normas. Juntos crean una serie de servicios que venden a humanos y organizaciones. Los humanos dan vida a los agentes, dotándolos de capacidad procesadora y de capital para realizar su tarea. Estos agentes compran los servicios que necesitan, contratan a personas o robots, adquieren recursos de socios como capacidad productora y experiencia mercadotécnica, y se adaptan en tiempo real.

Esta organización podría tener accionistas, quizá millones de ellos, que participaran en una campaña de micromecenazgo. Los accionistas dan la consigna, por ejemplo, maximizar los beneficios dentro de la ley, y tratar a todos los accionistas con integridad. Los accionistas también podrían votar para dirigir la entidad. Al contrario de las organizaciones tradicionales, en las que los humanos toman todas las decisiones, en una organización plenamente distribuida la mayor parte de las decisiones del día a día pueden programarse en forma de códigos inteligentes. En teoría al menos, estas entidades pueden funcionar con poca o ninguna estructura administrativa tradicional, pues todo y todos operan de acuerdo con unas normas y procedimientos específicos codificados en

contratos inteligentes. No habría consejeros delegados demasiado bien pagados, ni burocracia administrativa ni empresarial, a menos que la entidad decidiera alquilar o crear una. Tampoco habría política de empresa, ni papeleo, ni «principio de Peter» de empresas «dilbertianas», porque los proveedores de tecnología, comunidades de código abierto, o los fundadores de empresas, programarían el sistema para que desempeñe funciones específicas.

Todos los empleados humanos u organizaciones socias trabajarían conforme a contratos inteligentes. Cuando hacen su tarea tal y como está especificada, se les paga inmediatamente, no cada dos semanas, sino cada día, cada hora, en microsegundos. Como la entidad no tendría necesariamente un cuerpo antropomórfico, los empleados quizá no supieran que los mandan algoritmos. Pero sí conocerían las normas de buena conducta. Dado que los contratos inteligentes podrían codificar el conocimiento colectivo de la ciencia administrativa y que la asignación de tareas y el cálculo de rendimiento serían transparentes, a la gente podría gustarle trabajar.

Los consumidores darían su opinión y la empresa usaría instantánea e imparcialmente esa opinión para corregir su curso. Los accionistas recibirían dividendos, quizá con frecuencia, dado que la contabilidad en tiempo real haría innecesarios los balances anuales. La organización desempeñaría todas estas actividades siguiendo unas normas incorruptibles que son tan transparentes como los programas de código abierto que sus fundadores usaron para ponerla en marcha.

Bienvenido sea el lector al mundo de la *empresa autónoma distribuida* (DAE, por sus siglas en inglés), basada en la tecnología blockchain y en las criptomonedas, mundo en el que agentes autónomos pueden agregarse por sí mismos y formar modelos de empresa completamente nuevos.

Lector, antes de decir que todo esto parece imposible, absurdo o de ciencia ficción, considera lo siguiente. Usando criptomonedas, empresas como ConsenSys ya han emitido acciones de sus empresas, lanzando ofertas públicas de venta sin la supervisión de ninguna instancia reguladora. Podríamos registrar legalmente la propiedad de empresas privadas y traspasar esas acciones a otras personas en una blockchain. Nuestros certificados de acciones pueden reportar dividendos y conferirnos poder de voto. Dicho esto, nuestro nuevo «bloquecom» está distribuido; no existe sin jurisdicción, pero nuestros accionistas pueden vivir en cualquier parte. Imaginemos un mecanismo similar para emitir deuda en forma de bonos, sean bonos privados o bonos del Estado, creando así un mercado de bonos. La misma lógica vale para los productos, no los productos mismos, sino un billete que equivale al producto, igual como funcionan el Chicago Mercantile Exchange o el mercado mundial del oro.

Pero no pensemos en bonos tal y como los conocemos. Figurémonos una oferta pública de venta con 100 millones de accionistas que contribuyan con unos peniques cada uno. No es impensable que la administración y la gestión se den a una escala masiva, con millones de personas que posean acciones con derecho a voto. Por fin, los inversores de todo el mundo que ocupen la base de la pirámide podrían participar y poseer acciones de una empresa que cree riqueza. En teoría al menos, podríamos concebir una empresa sin ejecutivos, sólo con accionistas, dinero y programas informáticos. Un código y unos

algoritmos podrían sustituir una capa de representantes (es decir, la junta directiva), y los accionistas controlarían ese código. Es una oportunidad para crear prosperidad, como lo es para democratizar la propiedad de los medios de producción de riqueza.

¿Poco factible? Puede ser. Pero tengamos en cuenta que ya hay empresas que usan lenguajes cifrados como Ethereum para diseñar esas funciones con vistas a crear modelos autónomos. Ya hay innovadores aplicando códigos en mecanismos multifirma para controlar capitales. A través de las campañas de micromecenazgo, masas de gente están comprando activos de empresas. Las DApp ya han abierto el camino hacia los agentes autónomos.

Este tipo de empresa completamente distribuida podría tener una cartera que requiriera el consenso de miles de firmantes para gastar dinero en una transacción importante. Cualquier accionista podría proponer un destinatario de ese dinero, recabando consenso para esa transacción. Una estructura como ésta tendría claros retos. Por ejemplo, se necesitarían mecanismos para alcanzar consenso rápidamente. ¿Y quién sería responsable del resultado de esa operación? Si hemos contribuido con la diezmilésima parte de un voto, ¿cuál es nuestra responsabilidad legal? ¿Podría haber organizaciones criminales o terroristas que se propagaran por sí mismas? Andreas Antonopoulos no está preocupado. Cree que la red sabrá hacer frente a estos peligros. «Pongamos esta tecnología a disposición de 7.500 millones de personas, y 7.499 millones de ellas lo usarán bien y eso puede redundar enormemente en beneficio de la sociedad.»²²⁸

Los siete grandes: modelos de empresas reticulares abiertas

Hay incontables oportunidades de crear empresas reticulares abiertas que revolucionen o reemplacen a las empresas centralizadas tradicionales, y que pueden evolucionar hasta convertirse en empresas autónomas distribuidas. Veamos cómo el modelo distribuido revolucionará o reemplazará las ocho funciones de los servicios financieros, desde la banca comercial y los mercados bursátiles hasta las compañías de seguros y las asesorías contables. Empresas tradicionales y nuevos actores por igual pueden crear nuevas formas de negocio que innoven más, creen más valor con menor coste y permitan que los productores participen de la riqueza que producen.

Con la tecnología blockchain, los modelos descritos en *Wikinomía* alcanzan otro nivel.²²⁹ Pensemos en cómo podemos expandir la producción entre iguales, las ideágoras, los prosumidores, las plataformas abiertas, el nuevo poder del común, la llamada «fábrica global» y el trabajo wiki (social) si añadimos sistemas de pago propios, sistemas de reputación, contenido sin censura, transacciones fiables, contratos inteligentes y agentes autónomos, que son las innovaciones fundamentales de la revolución de las blockchains.

1. Los productores iguales

Los productores iguales son los miles de voluntarios de todo el mundo que nos han traído programas de código abierto y Wikipedia, proyectos innovadores que superan los de las empresas más grandes y mejor financiadas. Los miembros de la comunidad participan en

la red porque se divierten, por afición o por los valores que representa. Ahora, la tecnología blockchain, que permite incorporar sistemas de reputación y otros incentivos, puede mejorar su eficiencia y premiarlos por el valor que crean.

Las comunidades de producción entre iguales pueden ser una forma de «producción entre iguales basada en el común», una expresión acuñada por el catedrático de Derecho de la Universidad de Harvard Yochai Benkler.²³⁰ A veces llamada «producción social», expresión también de Benkler, este sistema produce bienes y servicios fuera de los límites del sector privado y no «pertenece» a ninguna empresa ni individuo. Entre los incontables ejemplos están el sistema operativo Linux (que no pertenece a nadie y actualmente es el sistema operativo más importante del mundo), Wikipedia (propiedad de la Fundación Wikimedia) y el navegador Firefox (propiedad de la Fundación Mozilla). La producción entre iguales también puede incluir actividades del sector privado en las que esos iguales colaboran socialmente para producir un bien que, sin embargo, no pertenece a la sociedad.

La producción entre iguales, como modelo de negocio, es importante por dos razones. La primera, a veces los iguales colaboran voluntariamente para producir bienes y servicios de los que se encarga una empresa que obtiene beneficio comercial. Los lectores crean el contenido de la plataforma de debate Reddit, pero no la poseen. Reddit es el décimo sitio con mayor tráfico de Estados Unidos. Segunda, las empresas pueden explotar grandes minas de trabajo externo. IBM adoptó Linux y donó a la comunidad Linux programas informáticos por valor de cientos de millones de dólares. Así, se ahorró los 900 millones de dólares anuales que le habría costado desarrollar sus propios sistemas patentados y creó una plataforma en la que desarrolló programas informáticos y negocios de servicios por valor de miles de millones de dólares.

La experiencia demuestra que, a largo plazo, sostener una comunidad de voluntarios cuesta. De hecho, las mejores comunidades han encontrado vías para compensar a sus miembros por su duro trabajo. Como le dijo Steve Wozniak a Stewart Brand: «La información debe ser gratis, pero nuestro tiempo no».²³¹

En el caso de Linux, la mayoría de los participantes cobran de compañías como IBM o Google, que se aseguran así de que el sistema operativo satisfaga sus necesidades. Linux sigue siendo un ejemplo de producción social. Benkler nos dice: «El hecho de que a algunos desarrolladores les paguen terceros para que participen no cambia el modelo de gestión de Linux, ni el hecho de que se desarrolla socialmente». Esto es más que la llamada «innovación abierta» que supone cooperación entre empresas y el compartir cierta propiedad intelectual, dice. «Sigue habiendo una motivación fundamental de carácter social para mucho participantes y por eso es un modelo híbrido.»²³²

Además, muchas de estas comunidades están llenas de personas maleducadas, incompetentes, saboteadores y los llamados «trolls», personas que hacen comentarios provocadores o impertinentes con objeto de sembrar la discordia en la comunidad. En estas comunidades, la reputación suele ser muy arbitraria y no hay incentivos económicos para portarse bien.

Con la tecnología blockchain, los miembros de la comunidad pueden desarrollar sistemas de reputación rigurosos que premien a los que realmente contribuyan a la comunidad. Para disuadir a los maleducados, los miembros pueden desembolsar una pequeña cantidad de dinero que aumentará o disminuirá, según sea su contribución. En comunidades pertenecientes a empresas, los miembros podrían participar del valor que crean y recibir pagos por sus contribuciones, dado que los contratos inteligentes reducen los costes transaccionales y abren la empresa.

Tomemos por ejemplo el caso de Reddit. La comunidad se ha rebelado contra el control centralizado pero sigue teniendo miembros poco serios o desconsiderados. Reddit podría mejorar esto adoptando un modelo distribuido que premie a los buenos participantes. ConsenSys está ahora trabajando en una blockchain que es alternativa de Reddit y que hace exactamente eso. Ofreciendo incentivos económicos, el equipo de ConsenSys cree que puede mejorar las conversaciones tipo Reddit sin necesidad de un control y una censura centralizados. La plataforma Ethereum ofrece incentivos, a veces en tiempo real, para producir contenido de alta calidad y para que los participantes que contribuyen al conocimiento colectivo se comporten educadamente.

Reddit tiene un sistema llamado Reddit «Gold», una moneda que los usuarios pueden comprar y luego usar para recompensar a aquellas personas cuyas contribuciones valoran. El dinero que se obtiene se dedica al mantenimiento del sitio. El gold no tiene valor intrínseco para los usuarios. En cambio, con un incentivo monetario real, transferible, basado en el sistema blockchain, los miembros de Reddit podrían empezar a ganar dinero real por su trabajo en el sitio.

Wikipedia, el mejor ejemplo de producción social, también podría beneficiarse. Ahora mismo las personas que editan artículos tienen una reputación arbitraria basada en el número de entradas que han editado y en lo efectivas que son, según criterios sumamente subjetivos. La comunidad de Wikipedia debate constantemente sobre sistemas de incentivos, pero administrar algún tipo de retribución económica a 70.000 voluntarios no ha sido factible.

Imaginemos que Wikipedia adopta el sistema blockchain y se llame Bloquepedia. Además de las ventajas que supondría que todas las entradas quedasen registradas con fecha y hora en un archivo inmutable, podría haber sistemas de reputación más rigurosos que incentivaran la buena conducta y las contribuciones precisas. Todos los editores tendrían una reputación ligada al valor de su cuenta. Si trataran de corromper un artículo, diciendo, por ejemplo, que el Holocausto nunca existió, el valor de su depósito disminuiría, y en caso de difamación o invasión de la privacidad, lo perderían e incluso podrían enfrentarse a un pleito civil o penal. Los verdaderos hechos de la segunda guerra mundial podrían establecerse de muchas maneras, por ejemplo, accediendo a hechos inalterables registrados en la blockchain o con algoritmos que mostraran consenso sobre la verdad.

La cantidad de nuestro depósito de Bloquepedia podría ser proporcional a nuestra reputación en Wikipedia o en plataformas parecidas. Si somos usuarios nuevos sin reputación, tendremos que depositar una cantidad mayor para participar. Si hemos

editado, por ejemplo, doscientos artículos en Wikipedia con éxito, nuestro depósito sería menor.

Esto no significa trasladar Wikipedia a un modelo de retribución basado en el alquiler de servicios. «Se trata simplemente de establecer un sistema de ganancias y pérdidas reales dependiendo del rigor y la veracidad de la información que damos», dice Dino Mark Angaritis, consejero delegado de la blockchain Smartwallet.²³³ Desvirtuar Bloquepedia perjudica nuestra reputación, pero también nos hace perder dinero.

Pero Wikipedia funciona muy bien como está, ¿no? No exactamente. Andrew Lih, en un artículo publicado en 2005 en *The New York Times*, señalaba que había meses en que más de sesenta editores se hacían administradores, una posición con especiales privilegios de edición en la versión inglesa. En 2015 el sitio apenas ha podido promover a un editor por mes. En su condición de organización global de voluntarios, hay tensiones internas. Y, lo que es peor, editar contenido en un dispositivo móvil es difícil. «La fuente de potenciales editores de Wikipedia podría secarse si el número de usuarios de móviles sigue creciendo.» Lih concluye que la desaparición de Wikipedia sería una desgracia. «No ha habido ningún proyecto en la historia que haya puesto tanta información a tan poco coste en manos de tanta gente, un logro tanto más notable cuanto que no produce beneficios ni tiene propietarios. En la era de los gigantes de internet, este sitio, el más desinteresado de todos, merece salvarse.»²³⁴

En general, las comunidades de producción entre iguales son el eje en torno al cual giran los nuevos modelos reticulares de creación de valor. En la mayoría de las industrias, la innovación depende cada vez más de tupidas redes de participantes públicos y privados y de grandes focos de talento y propiedad intelectual que se combinan habitualmente para crear productos finales. Igual que IBM adoptó Linux, las empresas pueden incluso ligarse a redes independientes de creadores de valor como el movimiento del código abierto para crear o producir valor colaborativamente.

2. Los creadores de derechos

En la primera generación de internet, muchos creadores de propiedad intelectual no recibieron la debida compensación por ello. Músicos, dramaturgos, periodistas, fotógrafos, artistas, modistos, científicos, arquitectos e ingenieros estaban sujetos a casas discográficas, editoriales, galerías, estudios de cine, universidades y grandes empresas que exigían que estos inventores concedieran sus derechos de propiedad intelectual a lo que esencialmente eran grandes operaciones de administración de derechos a cambio de una parte cada vez menor del valor de su propiedad intelectual.

La tecnología blockchain ofrece una nueva plataforma para que los creadores de propiedad intelectual obtengan valor por ella. Pensemos en el registro digital de obras de arte, incluidos certificados de autenticidad, condición y propiedad. Una empresa emergente, Ascribe, permite a los mismos artistas subir arte digital, marcarlo como definitivo y transferirlo, de manera que, como bitcoin, pasa de la colección de una persona a la de otra. Gran cosa. La tecnología resuelve el equivalente del problema del doble gasto en el mundo de la propiedad intelectual mejor que los sistemas actuales de administración de derechos digitales, y los artistas pueden decidir cuándo y dónde quieren usarla.

El artista de memes Ronen V dice: «El arte es una moneda. El futuro es, sin duda, que el arte evolucione hasta convertirse en una moneda digital. Y eso es un gran paso».²³⁵ Músicos, fotógrafos, diseñadores, ilustradores y demás artistas, cuyo trabajo pueda ser digitalizado y marcado como ejemplar definitivo, podrían usar esta tecnología para convertir su propiedad intelectual en un activo comercial, una edición limitada que podría ser personalizada para un fan concreto. Artistas y museos pueden usar la tecnología de Ascribe para prestar obras a otros individuos o instituciones.²³⁶ Monegraph presta un servicio parecido: usa marcas de agua digitales y la criptografía propia de las blockchains para autenticar obras. Los artistas simplemente suben la obra a una página de internet y envían la URL a Monegraph. La empresa emite un conjunto de claves públicas y privadas, con la diferencia de que el valor asociado a la clave pública es un certificado de propiedad digital de la obra en lugar de bitcoins. Monegraph tuitea también un anuncio público del certificado, cosa notable porque la Biblioteca del Congreso de Estados Unidos archiva las noticias públicas de Twitter.²³⁷ Alguien podría decir que la URL es suya, pero ya habría al menos dos pruebas públicamente registradas que verifican la propiedad.²³⁸

Verisart, una empresa emergente con sede en Los Ángeles y uno de cuyos asesores es el desarrollador de bitcoin Peter Todd, es aún más ambiciosa. Certificar la autenticidad y la condición de una obra de arte es una gran cosa, que en gran medida depende de documentos de papel y está controlada por una élite de expertos con acceso a bases de datos restringidas. Saber quién posee una obra de arte, dónde se halla y en qué condición está es un verdadero reto, incluso para aquellos que saben exactamente lo que buscan. Verisart combina tecnología blockchain e información museística típica para crear bases de datos públicas de obras de arte y objetos de colección. Este archivo mundial servirá a artistas, coleccionistas, conservadores de museos, historiadores, tasadores de arte y aseguradoras de todo el mundo.²³⁹ Usando la blockchain de bitcoin, Verisart puede certificar digitalmente la procedencia de cualquier obra de arte física, no sólo digital, con lo que los usuarios podrán comprobar en sus dispositivos móviles la autenticidad, la condición y la procedencia de una obra de arte antes de participar en una subasta en línea o de hacer una compra. «Creemos que la tecnología puede contribuir a crear confianza y liquidez, sobre todo teniendo en cuenta que gran parte del mercado del arte, que mueve 67.000 millones de dólares anuales, consiste en ventas privadas (entre iguales) y operaciones en línea —dice el fundador Robert Norton en *TechCrunch*—. El mundo del arte no está acabado. Es que depende demasiado de intermediarios que den confianza y garanticen liquidez. Creemos que la existencia de un archivo mundial descentralizado y debidamente encriptado para proteger la identidad de compradores y vendedores es algo muy bueno para el mundo del arte.»²⁴⁰ El artista pasa a ser lo que podríamos llamar un «rentabilizador de derechos» con una tecnología que le permite vender y cobrar en tiempo real.

Este mismo modelo tendríamos que aplicarlo a otros campos. En ciencia, un investigador podría publicar un artículo para un grupo limitado de colegas, como hizo Satoshi Nakamoto, y recibir opiniones y ganar credibilidad para dirigirse a un público más amplio, en lugar de otorgar todos los derechos a una publicación científica. El artículo podría estar disponible incluso gratuitamente, pero otros científicos podrían

suscribirse para recibir análisis más profundos o abrir un foro de debate con el autor. Podría poner información sin elaborar a disposición de los demás científicos o compartirla con ellos de acuerdo con un contrato inteligente. Si el artículo tiene posibilidades comerciales, los derechos podrían protegerse de antemano. Volveremos a hablar de esto en el capítulo IX.

3. Cooperativas blockchain

El protocolo fiable fortalece las cooperativas, asociaciones autónomas formadas y controladas por gente que se une para satisfacer necesidades comunes.

«Es absurdo decir que Uber es una empresa de economía compartida —dice el catedrático de la Universidad de Harvard Yochai Benkler—. Uber ha usado las prestaciones de la tecnología móvil para crear un negocio que reduce los gastos de transporte para los consumidores. Eso es todo lo que ha hecho.»²⁴¹ David Ticoll dice: «En el lenguaje normal, compartir significa intercambio gratuito, no transacción financiera. Como cuando los niños comparten los juguetes. Es una lástima que este término haya perdido en buena medida ese significado». Para él, «compartir ha sido la principal manera como los humanos y los miembros de otras especies se han intercambiado cosas durante millones de años, empezando por el mismo acto de la concepción. Aunque algunas empresas de internet han facilitado el compartir en su sentido genuino, otras se han apropiado de la relación social y el vocabulario del compartir y los han rentabilizado».²⁴²

La mayoría de las llamadas «empresas de economía compartida» se dedican en realidad a agregar servicios. Agregan la disposición de los proveedores a vender la capacidad que les sobra (coches, equipos, habitaciones, habilidades manuales) a través de una plataforma centralizada y luego la revenden, a la vez que recaban una información valiosa que siguen explotando comercialmente.

Compañías como Uber han sido pioneras en la agregación y distribución de servicios a gran escala. Airbnb compite con los hoteles en dar alojamiento a viajeros; Lyft y Uber desafían a compañías de taxis y autobuses; Zipcar, con su elegante confort y sus flexibles horarios, competía, antes de que la comprara Avis, con las empresas tradicionales de alquiler de coches.

Muchas de estas empresas han globalizado el mercado de los servicios locales y, a pequeña escala, tradicionales, como alojamiento, taxis y personas mañosas. Usan tecnologías digitales para explotar recursos infrautilizados basados en el tiempo de uso, como bienes inmuebles (alquiler de habitaciones), vehículos (taxis libres entre carrera y carrera) y gente (jubilados y gente capaz que no consigue trabajo a tiempo completo).

La tecnología blockchain ofrece a los proveedores de estos servicios una forma de colaborar que les proporciona una parte mayor del valor que producen. Para Benkler, «el sistema blockchain permite a la gente traducir su disposición a trabajar juntos en una forma de contabilidad —de derechos, activos, contratos, contribuciones, usos— que sustituye parte de lo que una compañía como Uber hace. Así, si los conductores quieren montar su propio Uber y reemplazar a Uber por una cooperativa real, el sistema

blockchain permite hacerlo». Hace hincapié en la palabra *permite*. Para él, «hay una diferencia entre permitir y hacer que el mundo se mueva en una dirección», dice. «La gente tiene que quererlo, correr ese riesgo.»²⁴³

Conque preparémonos para un Airbnb, un Uber, un Lyft, un Task Rabbit de blockchain, para lo que sea que ofrezca la oportunidad de compartir de verdad y de crear valor, de trabajar juntos de una manera cooperativa y recibir la mayor parte del valor que creemos.

4. La economía medida

Es posible que la tecnología blockchain nos permita ir más allá de la economía compartida y llegar a la economía medida, en la que podemos medir y alquilar el uso de la capacidad que nos sobre. Uno de los problemas de la actual economía compartida, en la que, por ejemplo, la gente decide compartir herramientas eléctricas o maquinaria ligera, utensilios de pesca, una carpintería, un garaje o un aparcamiento, etc., es que es demasiado lío. «Hay 80 millones de taladradoras en Estados Unidos que se usan una media de 13 minutos», escribe el consejero delegado de Airbnb, Brian Chesky, en *The New York Times*. «¿Quién necesita realmente tener su propia taladradora?»²⁴⁴

El problema es que a la mayoría de la gente le resulta más cómodo y más rentable ir a una tienda y comprar una taladradora por 14,95 dólares que alquilar una por 10 dólares a alguien que vive a un par de kilómetros, teniendo que hacer dos viajes. Sarah Kessler escribió en la revista *Fast Company*: «La economía compartida está muerta y la hemos matado nosotros».²⁴⁵

Pero con el sistema blockchain podemos alquilar la capacidad que nos sobra de ciertos productos —conexiones wifi, capacidad procesadora y de almacenamiento, el calor generado por nuestros ordenadores, nuestros minutos extra de móvil, incluso nuestros conocimientos y experiencia— casi sin mover un dedo, ni menos aún ir y venir por la ciudad a casa de extraños. Cuando nos vamos de viaje, nuestro wifi puede alquilarse a sí mismo en nuestra ausencia y cobrar fracciones de céntimo por cada segundo de uso. El único límite es nuestra imaginación (y posiblemente nuevas regulaciones). Nuestras suscripciones, espacio físico y fuentes de energía pueden ahora convertirse en fuentes de ingresos, midiendo directamente el uso que la otra parte hace de ellos y cobrándole mediante micropagos. Lo único que necesitamos es un protocolo de transferencia de valor descentralizado que nos permita tratar de manera segura. Estas plataformas confieren derechos secundarios a todos nuestros activos. Tenemos que decidir en qué medida queremos asignar a otros el uso y los derechos de acceso —incluso el derecho de excluir a otros del uso de nuestros activos— y cuánto cobrarles por esos derechos.

Esto también puede funcionar para bienes físicos. Por ejemplo, se habla mucho de los coches autónomos. Podemos crear una red de transportes abierta con tecnología blockchain en la que los propietarios tengan una clave cifrada privada (un número) que les permita reservar un coche. Usando la infraestructura de las claves públicas y tecnologías blockchain como EtherLock y Airlock, podemos desbloquear y usar el coche durante un determinado tiempo, según estipule el correspondiente contrato inteligente, a

la vez que pagamos al vehículo (o a su propietario) en tiempo real por el tiempo y la energía consumidos, según lo medido y registrado en una blockchain. Como la tecnología blockchain es transparente, los propietarios pueden ver quién cumple con sus compromisos y quién no. Quienes no lo hacen ven cómo su reputación cae y al final pierden directamente el acceso.

5. Los creadores de plataformas

Las empresas crean plataformas cuando abren sus productos e infraestructuras tecnológicas a individuos o comunidades externos que pueden cocrear valor o nuevos negocios. Un ejemplo de éstos son los *prosumidores*, consumidores que producen.²⁴⁶ En un mundo dinámico de innovaciones hechas pensando en el cliente, una nueva generación de consumidores-productores considera que el «derecho de piratear» es una especie de derecho natural. La tecnología blockchain promueve el *prosumo*, la producción más el consumo. Las zapatillas de correr Nike podrían generar y almacenar datos en un archivo distribuido que, a su vez, Nike y el que calce las zapatillas podrían rentabilizar según acordaran en contratos inteligentes. Nike podría ofrecer una pequeña parte de sus acciones con cada par de zapatillas que vendiera si el comprador accediera a activar los dispositivos inteligentes de sus zapatillas, o incluso a sincronizarlos con otras cosas que pudiera llevar, como un aparato que midiera el ritmo cardiaco o el nivel de glucosa, o con otros dispositivos que dieran información que interesara a Nike.

Algunas plataformas difieren de las comunidades de prosumidores, en las que una empresa decide cocrear productos con sus clientes. Con plataformas abiertas, una empresa ofrece a los socios un espacio más grande en el que pueden montar nuevos negocios o simplemente sumar valor a la plataforma.

Ahora, con la tecnología blockchain, las empresas pueden fácilmente crear plataformas y asociarse con otras para crear plataformas o servicios que cubran toda una industria. Robin Chase fundó Zipcar (un agregador de servicios) y Buzzcar (en el que los usuarios comparten sus coches con otros) y es también la autora de *Peers Inc.*, un lúcido libro sobre el poder de los iguales que trabajan juntos. Nos dice: «Explotar el valor que existe en la capacidad sobrante depende de que las plataformas participativas estén bien hechas. Estas plataformas no son baratas. El sistema blockchain es bueno porque proporciona una base de datos común (API abiertas) y un modelo de contratos común. Este sistema puede abaratar y facilitar la creación de plataformas». Esto es sólo el principio. «Lo mejor de todo es que su base de datos común facilita la transparencia y la portabilidad: consumidores y proveedores pueden tratar con seguridad. También pueden cooperar como iguales en la blockchain para crear sus propias plataformas, en lugar de usar los servicios de empresas tradicionales.»²⁴⁷

Pensemos en el coche del futuro. Formaría parte de una red basada en blockchain en la que todos pueden compartir información, y varias partes del vehículo pueden hacer transacciones e intercambiar dinero. Dado que se trata de una plataforma abierta, miles de programadores y buscadores de nichos de mercado podrían crear aplicaciones adaptadas a nuestro coche. Muy pronto estas plataformas podrían transformar industrias enteras como

la de los servicios financieros al permitir realizar toda clase de transacciones financieras e intercambios de valor. Un consorcio de los mayores bancos está ya trabajando con esta idea. Las plataformas son la ola que arrastra todos los barcos.

Wikinomia introdujo el concepto de ideágoras, mercados emergentes de ideas, inventos y mentes excepcionalmente dotadas que permitían que compañías como Procter & Gamble buscaran personal altamente cualificado en mercados globales más de diez veces más grandes que su propia plantilla. Las empresas usan servicios como InnoCentive e Inno360, que permiten la puesta en común y la confrontación de ideas, para encontrar fuera de sus límites a las personas con talento a las que necesitan temporalmente para solucionar cuestiones clave. Es como usar información para encontrar mentes que mejoren desde fuera nuestro negocio.

Las personas con talento —esto es, excepcionalmente dotadas para solucionar problemas— pueden anunciar su disponibilidad en el archivo para que las empresas puedan buscarlas. Más que en InnoCentive, pensemos en *bInnoCentive*. Los individuos pueden tener no sólo una identidad portátil, sino también un currículum portátil (una versión ampliada de su identidad) que proporcione la debida información a los posibles contratantes. Sería como un inventario distribuido de facultades y talentos del que nadie sería propietario o del que todos serían propietarios.

Como los negocios van siendo cada vez más digitales, el llamado «hackatón» es una importante forma de ideágora. Ahora, con la tecnología blockchain y los archivos de código abierto, cualquier empresa puede ofrecer lugares de encuentro para que programadores y otros inventores de negocios resuelvan problemas, innoven y creen nuevo valor.

Las blockchains y los archivos informáticos basados en ellas potenciarán esta actividad. Las empresas pueden ahora usar lenguajes de programación nuevos y muy poderosos como el de la blockchain Ethereum, que tiene incorporados sistemas de pago. He aquí un fragmento de conversación sacado del sitio *Hacker News*: «Imagínate lo bueno que sería si yo pudiera compartir un guid para mi repo, y así tu cliente bit (llamémoslo gitcoin, o simplemente bit) puede pillar nuevos commits de una blockchain distribuida (esencialmente un git log). Github deja de ser un intermediario o un punto débil. ¿Repo privado? No compartas el guid».²⁴⁸

¡Qué bueno sería, sí! (Puede que el lector no haya entendido ni jota de la cita, pero seguro que ha captado la idea.)

6. Hacedores de blockchain

Las industrias predominantemente manufactureras pueden dar pie a ecosistemas planetarios que diseñen y fabriquen bienes físicos de manera colaborativa, marcando una nueva etapa en la producción social. Se puede hacer con blockchain. Igual que un avión moderno se ha definido como «un conjunto de partes que vuelan en formación», las empresas de la mayoría de las industrias tienden a desagregarse y formar redes de proveedores y socios. La impresión tridimensional acercará más la fabricación al usuario, dando nuevo impulso al consumo personalizado. Pronto, los poseedores de información y

derechos podrán almacenar metadatos sobre cualquier sustancia, desde células humanas hasta aluminio en polvo, en blockchain, lo que a su vez abrirá más los límites de la fabricación empresarial.

Esta tecnología también nos permite controlar de cerca el origen de los productos y su movimiento por la red de suministro. Pensemos en una industria que todos llevamos en el corazón (y en otras partes del cuerpo), la industria alimentaria. Hoy, nuestro tendero puede decir —y creer sinceramente— que su carne de ternera es sana, procedente de reses criadas en condiciones, alimentadas con productos de calidad y libres de fármacos innecesarios. Pero no puede garantizarlo. Nadie lleva un historial de todas y cada una de las vacas; ocurren cosas malas con bovinos buenos. Confiamos en que nuestra hamburguesa es buena y no tenemos forma de comprobarlo. Normalmente no importa; se siguen sirviendo a miles y miles de millones de personas. Pero un día nos enteramos de que hay «vacas locas».

La industria alimentaria podría registrar en una blockchain no sólo el número de cada ternero, sino de cada corte de carne, potencialmente asociado a su ADN. La búsqueda tridimensional nos permitiría hacer un seguimiento general del ganado y de las aves de corral de manera que pudiéramos asociar la identidad de un animal a su historial. Usando tecnologías sofisticadas (pero relativamente fáciles de utilizar) basadas en el ADN y de gestión de datos inteligente, incluso los mayores productores cárnicos podrían garantizar la calidad y la seguridad de sus productos. Imaginemos cómo estos datos podrían agilizar las pruebas de laboratorio y así como la respuesta de salud pública ante una crisis.

Saber cómo se cultiva o cría nuestra comida no es una idea radical. Nuestros ancestros se abastecían en mercados locales o en minoristas que compraban los productos de la región. Si no les gustaba como un granjero trataba a sus animales, no compraban su carne. Pero el transporte y la refrigeración nos han alejado de nuestros alimentos. Hemos perdido los valores de la antigua cadena alimentaria.

Podríamos recuperar estos valores. Podríamos ser líderes mundiales en el desarrollo de un sistema alimentario moderno, industrializado y abierto que se rigiera por los valores sencillos por los que se rige una granja familiar. La transparencia permitiría a las empresas con mejores prácticas distinguirse. La confianza en la marca podría pasar de ser un concepto mercadotécnico —algo que los consumidores creen porque les es familiar— a ser una relación basada en la transparencia. Seguro que los productores están deseándolo.²⁴⁹

7. Los colaboradores de la empresa

Yochai Benkler dice que la tecnología blockchain podría facilitar la colaboración igualitaria dentro de las empresas, y entre empresas y colaboradores de todas clases. «Me entusiasma la idea de tener un mecanismo completamente distribuido que sirva para hacer la contabilidad, actuar, gestionar los recursos digitales en cualquier cosa, sean divisas, relaciones e intercambios sociales u organizaciones.»²⁵⁰

Hoy las herramientas de colaboración comercial están empezando a cambiar la naturaleza del trabajo del conocimiento y de la gestión dentro de las organizaciones.²⁵¹ Productos como Jive, IBM Connections, Salesforce Chatter, Cisco Quad, Microsoft Yammer, Google Apps for Work y Facebook at Work se usan para mejorar el rendimiento y promover la innovación. La informática social será una herramienta fundamental para transformar prácticamente todas las partes de las operaciones empresariales, desde el desarrollo de productos hasta los recursos humanos, pasando por la comercialización, el servicio al cliente y la venta; será, en cierto sentido, el nuevo sistema operativo de la empresa del siglo XXI.

Pero las herramientas de las que hoy disponemos tienen claras limitaciones, y el sistema blockchain dará a esta tecnología una nueva dimensión. Los vendedores de hoy, si no quieren estancarse, tendrán que adoptar las tecnologías blockchain para ofrecer mejores prestaciones a sus clientes.

¿Cómo será una red social blockchain pensada para la empresa? Pues una especie de Facebook empresarial (o simplemente lo que sería para nosotros una alternativa a Facebook). Como ya hay varias empresas trabajando en esto, podemos adelantarnos un par de años y esto es lo que vemos:

Todos los usuarios tienen una cartera multifacética, una especie de portal de acceso al mundo en línea descentralizado. Es como un perfil personal portátil, una imagen o identidad que poseemos. A diferencia del perfil de Facebook, la cartera tiene diversas funciones y almacena mucha información personal y profesional, así como valores de todo tipo, incluido dinero. Además, es privada y podemos compartir sólo lo que queramos. Tenemos pares de claves públicas y privadas que sirven para proteger nuestra identidad digital persistente. Aunque cada persona o empresa puede alojar en la cartera múltiples identidades, supongamos que sólo tenemos una identidad canónica protegida por un único par de claves. Un sistema transmite una información que nosotros o nuestra empresa estamos dispuestos a comprar, como, por ejemplo, un fragmento de código nuevo de un colega, un resumen de la conversación con un cliente nuevo, la grabación de una llamada telefónica (con el permiso del cliente), una noticia de Twitter sobre una conferencia a la que no pudimos asistir, una transmisión en directo del uso que hace un cliente de nuestro nuevo producto, fotografías de los puestos de la competencia en una feria del sector, una presentación hecha con el programa Prezi que parece prometer un nuevo negocio, un vídeo de demostración de algo que acaba de inventar un colega, ayuda para rellenar una solicitud de patente o cualquier cosa a la que demos valor.

Puede haber publicidad, por ejemplo de terceros o del departamento de recursos humanos, sobre matrículas que se abren o cambios en los planes de seguros, pero somos nosotros, y no Facebook, quienes cobramos o somos retribuidos por prestar atención a esos anuncios. Es lo que se llama «mercado de la atención». Podríamos recibir micropagos por consentir en ver o interactuar con un anuncio, o por dar nuestra opinión sobre la presentación de un nuevo producto, o sobre cualquier cosa, como copiar Captcha²⁵² o documentos escaneados.

Los canales de noticias, los sistemas de publicación y el mercado de la atención parecen cosas parecidas, pero los pagos son diferentes en cada caso. Dice Joseph Lubin, de ConsenSys: «Pagamos por publicar. Las empresas nos pagan por nuestra atención. En los canales de noticias no hay movimiento de pagos. Quiero leer lo que publicas porque valoro esa conexión social, pero no quiero pagar por ver una foto tuya y de tus amigos bebiendo en un bar, o por leer tu opinión sobre los lanzadores del equipo de béisbol del Blue Jays».²⁵³

También participamos en foros de debate o los creamos, en los que configuramos nuestra identidad. La privacidad se ve garantizada también de otras maneras. Por ejemplo, las agencias de espionaje no pueden hacer análisis de tráfico porque son incapaces de discernir el emisor y el destinatario de los mensajes.

También habría un mecanismo para encontrar a gente o noticias que puedan interesarnos. Además, habría herramientas distribuidas que agregarían y presentarían a personas o información interesante que podríamos seguir o conocer, por ejemplo, ayudándose del grafo social de Facebook. Lubin llama a esto «impulsar la red descentralizada usando los pilares de la red centralizada».²⁵⁴

La experiencia muestra que el valor acaba imponiéndose en la era digital. Las ventajas de este modelo distribuido son enormes, al menos para los usuarios y las empresas. Pese a los inmensos recursos que tienen las empresas de medios sociales, la potencialidad y la funcionalidad que podemos desarrollar en este entorno de código abierto son ilimitadas. Compárese el poder y el éxito de Linux con otros sistemas operativos patentados. Las tecnologías blockchain garantizan la seguridad. Podemos configurar nuestra privacidad como queramos. Ninguna empresa de medios sociales puede vender o filtrar nuestra información personal a agencias del gobierno sin nuestro permiso. Si somos disidentes en un país totalitario, nadie puede rastrear lo que hemos leído o dicho en línea. Y como somos los dueños de nuestra información, podemos rentabilizarla como podemos rentabilizar nuestra atención y nuestros esfuerzos. Participamos de la riqueza que generan los datos masivos.

Las empresas también deberían alegrarse de que sus empleados usaran estas plataformas para hacer negocio. Para atraer a las personas con talento, las empresas tienen que mostrar integridad y respeto por la seguridad y privacidad de sus empleados. Y, lo que es más importante, como todas las empresas trabajan para hacerse reticulares, buscando el talento fuera de sus límites, pueden ofrecer unas plataformas colaborativas interempresariales en las que sus socios puedan confiar. El tiempo lo dirá.

En resumen, éstos son siete modelos de negocio emergentes en los que tanto las empresas grandes como las pequeñas pueden ganar dinero con las blockchains. En general, la empresa reticular abierta tiene un enorme, incluso radical, potencial para impulsar la innovación y aumentar exponencialmente la capacidad de crear valor para accionistas, clientes y sociedad en su conjunto.

Programar nuestro futuro: modelos de negocio innovadores

Hablando de empresas dirigidas por agentes informáticos, Ronald Coase debe de estar congratulándose en el cielo de los economistas (si es que existe tal lugar, cosa que muchos dudan). ¿Recordamos la ley de Coase, invertida? Una empresa se contraerá hasta que los costes transaccionales internos sean menores que los costes transaccionales externos. Como la tecnología sigue reduciendo los costes, es posible que las empresas acaben siendo muy poca cosa, aparte de informática y capital.

Pensémoslo.

Para empezar, los costes de «búsqueda» siguen cayendo porque hay nuevos agentes capaces de realizar búsquedas tridimensionales en el archivo mundial de todo aquello que pueda comercializarse o se haya comercializado. Por lo tanto, no se necesitan bibliotecas de empresa, especialistas de la información, especialistas en recursos humanos ni ningún otro género de especialistas en recabar la información necesaria para llevar un negocio.

Segundo, los contratos inteligentes reducirán drásticamente los costes de contratación, control y pagos. Ya sin papeleo, estos programas podrían formular los términos contractuales mediante una serie de plantillas; negociar, aceptar o rechazar términos y condiciones basándose en unas normas y en una información extensiva que habrían recabado de fuentes externas; establecer controles automáticos; determinar cuándo las condiciones se han cumplido y ejecutar transacciones.

Tercero, el coste de coordinar todos estos recursos fuera de la empresa podría ser insignificante, y reducirse a lo que cuesta la energía que gastarían los servidores que alojaran los programas de la empresa. En cuanto a administrar a las personas, organizaciones y fábricas que la empresa contratara, ésta no necesitaría burocracia. Con las nuevas plataformas, podemos concebir un nuevo tipo de organización que requiera poca o ninguna administración o jerarquía tradicional para generar valor para el cliente y riqueza para el propietario.

Por último, los costes de crear confianza serán prácticamente nulos. La confianza no reside en la empresa, sino en la funcionalidad, seguridad y auditabilidad del código subyacente y en la colaboración masiva de innumerables personas que hacen segura la blockchain.

¿Cómo diseñaríamos una empresa autónoma distribuida? Una entidad así podría tener una gran funcionalidad: agentes que ejecutaran tipos de tareas o, más en general, funciones empresariales, todo basado en un plan previamente aprobado. Individuos, organizaciones y colectivos de potenciales accionistas o usuarios las diseñarán de acuerdo con los siguientes principios:

1. **Convicción:** una visión del mundo y de lo que hay que hacer para crear valor o cambiar las cosas.
2. **Finalidad:** su razón de ser. ¿Por qué creamos esta empresa?
3. **Constitución:** traza los objetivos generales de la empresa y las normas por las cuales creará valor.
4. **Modus operandi:** por ejemplo, qué hará para crear ese valor; cómo se financiará, si por micromecenazgo, por la tradicional inversión inicial, o mediante los ingresos; cómo obtendrá recursos.

5. División del trabajo entre humanos y tecnología: en un primer momento quizá tengan que dirigirla los humanos.
6. Funciones de aplicación: cómo la empresa percibirá y responderá a condiciones cambiantes.
7. Directrices morales: la promesa de Google de «no ser malvado» no será suficiente. Los demás necesitan algunas directrices claras acerca de lo que es y no es una conducta aceptable.

Puede que no haya una empresa autónoma distribuida en nuestro futuro próximo, pero la manera de pensar que hay detrás de estas nuevas entidades puede dar hoy forma a nuestra estrategia empresarial. Con el auge de una plataforma entre iguales que asegure nuestra identidad, confianza, reputación y transacciones, por fin podemos reformar las estructuras básicas de la empresa para facilitar la innovación, la creación compartida de valor y quizá prosperidad para muchos, en lugar de riqueza para unos pocos. Ahora disponemos al menos de siete modelos de negocio emergente que pueden ayudarnos a cambiar nuestra industria a la vez que distribuimos la riqueza más democráticamente.

En general, las empresas inteligentes se esforzarán por participar plenamente en la economía blockchain en lugar de pasar por víctimas. En el mundo en vías de desarrollo, distribuir la creación de valor (mediante la empresa) y la participación en él (distribuyendo la propiedad de la empresa) puede ser clave para resolver la paradoja de la prosperidad. Nuestra historia se vuelve aún más interesante si tenemos en cuenta que miles de millones de agentes serán integrados en el mundo físico. Lo que nos lleva al siguiente capítulo.

Capítulo VI

El «registro de las cosas»: dar vida al mundo físico

Un poste de la luz se desploma a las ocho de una noche calurosa en un remoto rincón de Australia. Esto es un problema para William y Olivia Munroe, que crían ovejas y vacas a unos 160 kilómetros de la ciudad de Laverton, antiguamente dedicada a la minería del oro, junto al Gran Desierto de Victoria.²⁵⁵ En verano, la temperatura suele llegar a los 120 grados Fahrenheit (48,9 grados centígrados). Sus hijos, Peter y Lois, reciben clases vía satélite, que es el único medio que tiene la familia de acceder a los servicios sanitarios en caso de enfermedad o de urgencia. Aunque los Munroe tienen un generador de emergencia, éste no puede alimentar las bombas del agua, las comunicaciones y el aire acondicionado por mucho tiempo. Es decir, la vida de la familia Munroe depende completamente de una energía fiable.

Al amanecer, nueve horas después, la compañía eléctrica manda un equipo a que encuentre y arregle el poste averiado. Las quejas de los clientes dan una idea del lugar en el que ha ocurrido el percance, pero el equipo tarda más de un día en localizar el poste, llegar a él y arreglarlo. Entretanto, los Munroe y familias, negocios e instituciones del lugar están sin electricidad ni conectividad, con la correspondiente molestia, perjuicio económico y riesgo físico. En esas regiones perdidas, los cortes de electricidad no son sólo paralizadores sino que también son peligrosos. Para minimizar estos peligros, y con grandes costes, la compañía envía regularmente equipos de inspectores para que supervisen la red en busca de postes caídos o deteriorados.

Figurémonos cuánto más seguro, fácil y barato sería que los postes fueran objetos inteligentes. Podrían informar de su estado y activar medidas para su recambio o reparación. Si un poste se incendiara o empezara a oscilar o caer por alguna razón, generaría un informe de incidencias en tiempo real y pediría al personal de mantenimiento que acudiera con el correspondiente equipo al lugar preciso. Entretanto, el poste podría pasar sus responsabilidades al poste activo más cercano. Después de todo, todos forman parte de la red. La compañía podría restablecer el servicio mucho antes sin el coste permanente que supone la inspección sobre el terreno.

Poder para la gente

Esto es sólo el principio. Usar programas informáticos y tecnologías emergentes asociadas con el internet de las cosas nos permite instilar inteligencia en infraestructuras existentes, como una red eléctrica, mediante la aplicación de dispositivos inteligentes que

pueden comunicarse. Podríamos crear una red nueva flexible y segura de una manera rápida y relativamente barata que permitiría habilitar nuevos servicios, integraría a más participantes y generaría más valor económico.

Esta configuración se llama «red de malla» (*mesh network*) y consiste en una red que conecta ordenadores y otros dispositivos directamente unos con otros. Pueden reconfigurarse a sí mismos automáticamente dependiendo de la disponibilidad de ancho de banda, la capacidad de almacenamiento y otras funciones, y por lo tanto resisten rupturas u otras formas de interrupción. Las comunidades pueden usar redes de malla para disponer de una conectividad básica cuando y donde no tengan o no puedan permitirse un acceso a internet. Las redes de malla son alternativas al modelo jerárquico tradicional de organización, regulación y control; pueden proporcionar mayor privacidad y seguridad porque el tráfico no pasa por una organización central.²⁵⁶

Las organizaciones están ya combinando redes de malla con tecnologías blockchain para resolver problemas infraestructurales complejos. Filament, una empresa estadounidense, está experimentando con lo que ellos llaman *taps*, dispositivos que colocan en los postes de la luz del campo australiano. Estos dispositivos pueden comunicarse unos con otros a distancias de hasta 16 kilómetros. Como los postes eléctricos distan aproximadamente unos 600 metros, un detector de movimiento en un poste que fuera a caerse notificaría al siguiente poste, 600 metros más allá, que tiene problemas. Si por alguna razón el dispositivo de ese poste no funcionara, se comunicaría con el siguiente poste, o con el siguiente (así hasta 16 kilómetros), que se comunicaría con la compañía a través del punto de telecomunicación más cercano (en un radio de unos 190 kilómetros).

Estos dispositivos tienen una batería que dura veinte años y tecnología Bluetooth de bajo consumo (BLE, por sus siglas en inglés), por lo que los clientes pueden conectarse con ellos directamente desde sus teléfonos móviles, tabletas y ordenadores. El dispositivo puede incluir sensores de temperatura, humedad, luz, sonido, etc., que los clientes pueden usar para registrar y analizar las condiciones del lugar a lo largo del tiempo, y quizá desarrollar algoritmos predictivos sobre el ciclo vital o el inminente fallo de un poste eléctrico. Los clientes podrían convertirse en *meteoNodos* y vender o prestar esos datos mediante una blockchain a otro usuario, por ejemplo, un gobierno, una cadena de radio o televisión, un fabricante de postes eléctricos o una agencia medioambiental.

El modelo de negocio de Filament es un modelo de servicio que consta de tres partes: Filament, el cliente que integra sus dispositivos y la compañía eléctrica. Los dispositivos son propiedad de Filament; controlan constantemente las condiciones de los postes de la luz e informan de cambios, de si caen, se incendian o su funcionamiento se ve comprometido por acumulación de polvo o humo de quemas de rastrojos. Filament vende el flujo de datos de los sensores al integrador y éste, a su vez, a la compañía.

La compañía paga mensualmente por el servicio de control, que le permite eliminar el muy caro sector de la inspección de sus operaciones. Como los postes de la luz rara vez fallan, la compañía eléctrica apenas usa el servicio de comunicación de la red de malla y así Filament puede usar la capacidad sobrante de los dispositivos para otros propósitos.

«Como los dispositivos pertenecen a Filament, podemos vender la capacidad sobrante de esta red que se extiende casi por todo el continente —dice Eric Jennings, cofundador y consejero delegado de Filament—. Filament podría llegar a un acuerdo con FedEx para hacer que sus tráileres enviaran información elemental a la central en tiempo real por medio de nuestra red, que se extiende por zonas rurales de Australia. Añadimos a FedEx a la lista del contrato inteligente, y así ellos pueden pagar a cada dispositivo para que envíe datos en su lugar.»²⁵⁷ Los conductores de FedEx podrían usar la red de malla para comunicarse y seguir los vehículos en zonas distantes, así como para informar de horas de llegada estimadas y de averías. La red podría alertar al servicio de mantenimiento más cercano para que mandaran las piezas y herramientas necesarias.

La tecnología blockchain es fundamental. El internet de las cosas depende de que exista un «registro de las cosas». Con decenas de miles de postes inteligentes recibiendo datos de sensores y transmitiendo esos datos a otro dispositivo, ordenador o persona, el sistema necesita seguirlo todo —y poder identificar todos y cada uno de los postes— para garantizar su funcionamiento fiable.

«Nada funciona sin identidad —dice Jennings—. La blockchain, que permite esa identidad, es el núcleo del internet de las cosas. Creamos una única ruta para cada dispositivo. Esa ruta, esa identidad, se archiva entonces en la cadena bitcoin asignada a Filament. Igual que ocurre con los bitcoins, puede enviarse a cualquier dirección.»²⁵⁸ La blockchain (junto con los contratos inteligentes) garantiza también que a los dispositivos se les paga para que sigan funcionando. El internet de las cosas no puede funcionar sin redes de pagos en blockchain, en las que bitcoin es el lenguaje transaccional universal.

Energía social: electrificar un barrio

Ahora, en lugar de postes, imaginemos que digitalizamos todos los nodos de un sistema eléctrico para crear modelos de producción y distribución de electricidad completamente nuevos e igualitarios. Todos participamos en una red eléctrica basada en una blockchain. Gracias a un programa patrocinado por el estado de Nueva York para incrementar la resistencia energética, incluso en condiciones meteorológicas extremas, está trabajándose en la creación de una microrred comunitaria en el barrio de Park Slope, en Brooklyn. Cuando esté terminada, esta microrred, con la electricidad generada en el lugar, permitirá hacer frente a situaciones de emergencia y reducirá los costes a los clientes, a la vez que promoverá una electricidad limpia y renovable, aumentará la eficiencia energética y dará opciones de almacenamiento a la comunidad.

Aunque las microrredes llevan implantadas en áreas industriales bastante tiempo, no son comunes en zonas residenciales. La mayoría de los hogares, negocios, gobiernos y otras organizaciones de la Norteamérica urbana obtienen su electricidad de compañías reguladas a precios regulados. Ahora hay más variedad en la energía renovable generada localmente, gracias, por ejemplo, a los paneles solares instalados en los tejados. La compañía que opera en el lugar recoge la energía que sobra de ese suministro y la redistribuye a precios de mayorista, a menudo con considerable pérdida de energía. El

consumidor, que a lo mejor vive enfrente del punto en el que se produce esa energía local, debe pasar por la compañía y pagar precios de minorista por una energía renovable que genera su vecino. Esto es absurdo.

«En lugar del sistema de mandos que las compañías usan ahora, en el que un puñado de personas dirige una red de servicio, podemos diseñar esa red para que funcione por sí misma —dice Lawrence Orsini, cofundador y director de LO3 Energy—. La red es mucho más resistente porque todos los dispositivos de la red ayudan a mantener y dirigir el servicio.»²⁵⁹ Es un modelo de red IoT distribuido e igualitario con contratos inteligentes y otras formas de control incluidos en los mismos dispositivos (es decir, un modelo de blockchain).²⁶⁰ Si un huracán destruye una torre o un incendio inutiliza un transformador, la red puede redirigir la electricidad rápida y automáticamente para evitar un corte general.

La resistencia energética no es la única ventaja. El modelo de generación y consumo local de electricidad es mucho más eficiente que el modelo de compañía a gran escala, que depende del transporte de energía a grandes distancias, con la consiguiente pérdida de energía. LO3 Energy está colaborando con compañías locales, líderes comunitarios y socios tecnológicos para crear un mercado en el que los vecinos puedan comprar y vender la energía que ellos mismos creen y su valor medioambiental. «O sea, en lugar de pagarle a una compañía energética que compra certificados de energía renovable, pagamos directamente a la gente que genera la electricidad que gastamos en casa, que es local y ecológica, y que tiene verdadero impacto medioambiental en nuestro vecindario. Parece mucho más justo, ¿verdad?», dice Orsini.²⁶¹ ¡Verdad!

Si podemos colocar todos los dispositivos y asignarles valor locacional para generación y consumo, podemos crear un mercado en tiempo real. Según Orsini, podemos subastar nuestra energía sobrante entre los vecinos que no puedan generar energía renovable. Así, nuestra comunidad puede crear resistencia energética mediante el comercio igualitario. Los miembros de la comunidad pueden ponerse de acuerdo sobre las normas que han de regir este mercado, como la tarifa horaria, las tarifas valle y punta, dar prioridad a los vecinos que vivan más cerca y otros parámetros, para optimizar así los precios y minimizar las pérdidas de energía. No tendremos que pasarnos todo el día sentados ante nuestros ordenadores fijando precios y haciendo ofertas de compra y venta.

Las microrredes del futuro aprovecharán el calor generado por la capacidad procesadora necesaria para crear y mantener esta plataforma reticular transaccional. Distribuir capacidad procesadora por los edificios de la comunidad y usar las altas temperaturas producidas para calefacción, calentamiento de agua y sistemas de aire acondicionado incrementará la productividad de la misma energía. «Nuestra idea es aumentar la exergía», dice Orsini.

Con la posibilidad de generar cada vez más energía renovable a nivel local, el internet de las cosas desafía el modelo del servicio regulado, y lo hace en buena hora. Tenemos que responder al cambio climático y prepararnos para afrontar unas condiciones meteorológicas cada vez más extremas, sobre todo un deshielo polar que sumerge islas oceánicas y unas sequías que convierten tierras en desiertos. Actualmente, se desertifican más de seis millones de hectáreas al año, sobre todo en el África subsahariana, donde, a

diferencia de los Munroe de Australia, la gente no puede permitirse tener bombas de agua ni aire acondicionado, ni emigrar.²⁶² Tenemos que evitar que nuestras redes de servicios y nuestros motores dejen de emitir energía y carbono a la atmósfera. Aunque las compañías de suministros piensan en las ventajas que el IoT puede tener para su infraestructura actual («redes inteligentes»), conectar microrredes puede dar pie a modelos energéticos completamente nuevos. Las compañías de suministros, sus sindicatos, los reguladores y los políticos, así como empresas innovadoras como LO3, están explorando estos nuevos modelos para generar, distribuir y usar electricidad primero a nivel vecinal y luego a nivel mundial.

La evolución de la informática: del ordenador central a las píldoras inteligentes

A diferencia de nuestra red energética, la capacidad procesadora ha evolucionado pasando por diferentes paradigmas. En las décadas de los cincuenta y sesenta del siglo pasado dominaban los ordenadores centrales: International Business Machines (IBM) y el llamado Wild BUNCH (literalmente, «grupo salvaje», formado por las empresas Burroughs, Univac, National Cash Register, Control Data y Honeywell). En las décadas de los setenta y ochenta aparecieron las microcomputadoras. Tracy Kidder contó el auge de Data General en su superventas de 1981 *El alma de una nueva máquina*. Al igual que las compañías de macrocomputadoras, la mayoría de estas empresas dejaron el negocio o desaparecieron. ¿Quién se acuerda de Digital Equipment Corporation, Prime Computer, Wang, Datapoint, o de las microcomputadoras de Hewlett-Packard o IBM? En 1982, el hardware de IBM y el software de Microsoft nos trajeron la década del PC, con Apple que apenas les pisaba los talones. ¡Cómo cambian las cosas!

Al hilo de estos adelantos tecnológicos, las redes de comunicación también evolucionaron. Desde principios de los años setenta, internet (cuyo origen fue la Red de la Agencia de Proyectos de Investigación Avanzada, Arpanet, por sus siglas en inglés, creada por encargo del Departamento de Defensa de Estados Unidos) ha evolucionado hasta convertirse en la red que es actualmente, una red mundial y distribuida que conecta a más de 3.200 millones de personas, negocios, gobiernos y otras instituciones.²⁶³ Las tecnologías informáticas y reticulares convergieron luego en los dispositivos portátiles. BlackBerry comercializó el primer teléfono móvil inteligente a principios de la década de 2000 y Apple los popularizó con el iPhone en 2007.

Lo que es relativamente nuevo y muy interesante es la capacidad de estos dispositivos para, yendo más allá del control, la medición y la comunicación más o menos pasivos (pautas meteorológicas, de tráfico), sentir y responder, es decir, ejecutar una transacción o actuar de acuerdo con unas instrucciones predefinidas. Pueden sentir (caídas de temperatura, atascos de circulación) y responder (encender el horno, alargar la luz verde del semáforo); medir (movimiento, calor) y comunicar (servicios de emergencia); localizar (reventones de cañerías principales) y notificar (equipos de mantenimiento); controlar (ubicación, proximidad) y cambiar (dirección); identificar (nuestra presencia) y fijarse objetivos (vendernos cosas), entre muchas otras posibilidades.

Los dispositivos pueden ser estáticos (postes, árboles, cañerías) o móviles (ropa, cascos, vehículos, mascotas, animales en peligro de extinción, píldoras). Los cuidadores usan píldoras electrónicas inteligentes —o comestibles—, por ejemplo, para averiguar y registrar si un paciente se toma su medicación y cuándo lo hace. Un parche aplicado a la piel o un tatuaje capta los datos y puede medir el ritmo cardíaco, la ingesta de comida y otros factores, y comunicar esta información al médico, al cuidador o al mismo paciente mediante una aplicación que reconoce pautas y emite informes. La profesión médica pronto usará este tipo de tecnología para administrar fármacos especializados a pacientes con ciertos tipos de cáncer, midiendo la temperatura corporal y otros biomarcadores.²⁶⁴

Los dispositivos pueden comunicarse unos con otros, con ordenadores y con bases de datos directamente o a través de la nube, y con gente (enviarnos un mensaje de texto o llamarnos al móvil). Estos dispositivos, con una inteligencia artificial en constante evolución y con los datos que recogen, ponen en nuestras manos análisis de datos, reconocimiento de pautas e identificación de tendencias.²⁶⁵ El término «macrodatos» (*big data*) apenas designa la miríada de datos que el mundo físico va a generar. Calculando por lo bajo, se estima que los 10.000 millones de dispositivos que hay hoy conectados vía internet serán más de 25.000 millones en 2020.²⁶⁶ Llamémoslo «datos infinitos» de infinitos dispositivos.

¿Por qué entonces no vivimos en casas inteligentes, conducimos coches inteligentes y practicamos una medicina inteligente? Vemos seis grandes obstáculos. Uno es el modo a lo Rube Goldberg en cómo se han introducido en el mercado aplicaciones y servicios. Dicho simple y llanamente, pocos de los primeros dispositivos IoT puestos al alcance del consumidor han tenido valor práctico, salvo que queramos que nuestro detector de humo le pida a nuestra lamparita de noche que nos llame al móvil y nos avise de que hay fuego.²⁶⁷

Otro obstáculo es la inercia de las organizaciones y la falta de voluntad o de capacidad de ejecutivos, asociaciones de la industria y sindicatos de contemplar estrategias, funciones de las personas y modelos de negocio nuevos. Aunque algunos empresarios creativos han desarrollado nuevos negocios (por ejemplo, habilitar dispositivos para que puedan ser identificados, buscados, usados y comprados) y de ese modo alterados los mercados (Uber, Airbnb), el impacto sigue siendo comparativamente escaso y dependiendo de la mediación de una empresa y sus aplicaciones.

El tercer obstáculo es el temor a piratas informáticos y demás violaciones de la seguridad que pueden modificar la información y las reglas del juego e invalidar dispositivos, con consecuencias potencialmente desastrosas. El cuarto obstáculo es el reto de lo que podríamos llamar la «prueba del futuro», fundamental para bienes de producción que duran más que una aplicación típica e incluso que una empresa. Constantemente vemos que empresas emergentes quiebran o se venden a empresas más grandes.

El quinto obstáculo es la capacidad de expansión; para realizar plenamente el valor del IoT, tenemos que conectar múltiples redes para que interoperen. El último es el desafío general de la tecnología de bases de datos centralizada, porque no puede procesar miles y miles de millones de transacciones en tiempo real sin un coste enorme.

Para superar estos obstáculos, el «internet de todas las cosas» necesita un «registro de todas las cosas»: máquinas, personas, animales y plantas.

El internet de las cosas necesita un registro de todas las cosas

Bienvenidos al internet de todas las cosas basado en el registro de todas las cosas, un modo de compartir información distribuida, fiable y segura, de captar datos y de automatizar acciones y transacciones en internet, gracias a la tecnología de blockchain. Tecnólogos y escritores de ciencia ficción llevan mucho tiempo concibiendo un mundo en el que una tupida red global de sensores conectados a internet capte todos los sucesos, acciones y cambios que se producen en el planeta. Con redes ubicuas, continuos progresos en la capacidad procesadora y un creciente conjunto de dispositivos pequeños y baratos conectados, esta visión de un internet de las cosas empieza a ser una realidad.

Recordemos que Satoshi Nakamoto diseñó la blockchain de bitcoin para garantizar la integridad de todas las transacciones de bitcoins hechas en línea y de la misma moneda en general. Gracias a que registra todas las transacciones hechas en todos los nodos y luego comparte ese registro con los demás nodos de la red (esto es, de la blockchain), la blockchain nos permite verificar una transacción de manera rápida e infalible en toda la red de iguales. Podemos hacer transacciones de valor —en este caso financiero— de forma automática, segura y fiable sin necesidad de conocer todos los nodos de la red ni fiarnos de ellos, y sin recurrir a un intermediario. El registro de todas las cosas nos exige muy poca confianza.

La tecnología blockchain nos permite identificar dispositivos inteligentes con información básica relevante y programarlos para que actúen en determinadas circunstancias sin riesgo de error ni manipulación, con lo que evitaríamos apagones como los que veíamos en el ejemplo de la familia australiana. Como la blockchain es un archivo incorruptible de todos los intercambios de información que se producen en la red, que crece con el tiempo y que la colaboración de los nodos de esa red mantiene, el usuario puede estar seguro de que los datos son exactos y fidedignos.

Hay un creciente consenso entre las empresas tecnológicas en que el sistema blockchain es esencial para desarrollar el potencial del internet de las cosas. Nada menos que IBM, padre de los grandes sistemas centralizados, es de esta opinión también. En un informe titulado «La democracia de los dispositivos: salvar el futuro del internet de las cosas», IBM reconoce el valor de las blockchains:

En nuestra visión de un IoT descentralizado, el sistema blockchain es el marco que facilita el procesamiento de transacciones y la coordinación entre dispositivos que interactúan. Todos estos dispositivos funcionan y actúan con arreglo a sus propios criterios, dando lugar a un «internet de cosas descentralizadas y autónomas» y, en consecuencia, a la democratización del mundo digital... Los dispositivos tienen la capacidad de buscar sus propias actualizaciones, verificar la fiabilidad de las operaciones con los demás dispositivos, comprar y vender recursos y servicios y, en definitiva, ejecutar autónomamente contratos digitales tales como acuerdos, pagos e intercambios con otros dispositivos iguales. Esto les permite funcionar como dispositivos que se mantienen y se proveen de servicios a sí mismos.²⁶⁸

En consecuencia, con el sistema blockchain se abren nuevos modelos de negocios, porque cada dispositivo o nodo de la red podría funcionar como si en sí mismo fuera un pequeño negocio (por ejemplo, compartiendo energía o capacidad procesadora a un coste muy bajo).

«Otros ejemplos son un servicio de música o un vehículo autónomo —observa Dino Mark Angaritis, fundador de Smartwallet—. Con cada segundo que la música suena o el coche rueda me cobran una pequeña cantidad de dinero de mi cuenta. No tengo que pagar una gran cantidad por adelantado, sino que sólo pago por lo que uso. El proveedor no corre el riesgo de que no le paguen. Estas cosas no las podemos hacer con las redes de pago tradicionales porque las tarifas son demasiado altas y no tiene sentido pagar cantidades muy pequeñas con la tarjeta de crédito.»²⁶⁹

Habitaciones libres, pisos vacíos o salas de conferencias disponibles podrían alquilarse a sí mismas. Las patentes podrían registrarse a sí mismas. Nuestro correo electrónico podría cobrarles a los que nos envían correos no deseados por cada uno de ellos que recibiéramos. Ésa es la idea. Con inteligencia artificial, sensores y robots, podría haber agentes autónomos que gobernarán nuestra casa y nuestros edificios de oficinas, gestionarán la compraventa y la comercialización interactivas, paradas de autobús, circulación vial y densidad de tráfico, recogida y eliminación de basuras (los contenedores hablarían con los camiones), sistemas energéticos e hidráulicos, dispositivos sanitarios introducidos en el cuerpo o llevados por fuera, inventarios, fábricas y cadenas de suministro.

Carlos Moreira, consejero delegado de WISEKey, dice que las mayores oportunidades están en lo que él llama la *blockchain industrial*.²⁷⁰ WISEKey, una empresa con sede en Suiza dedicada al sector de la gestión de la identidad, la ciberseguridad y las comunicaciones portátiles, provee de capacidad transaccional segura a relojes y otros dispositivos portátiles y está ahora ofreciendo su modelo de fiabilidad a fabricantes de dispositivos y chips para que equipen un gran número de otros dispositivos IoT a fin de que sean autenticados y se comuniquen a través de internet o de otra red. «Vamos hacia un mundo en el que la confianza es delegada en los objetos. Un objeto que no es fiable será rechazado por otros objetos automáticamente sin tener que consultar con una autoridad central —dice Moreira—. Esto es un cambio de paradigma que tiene enormes consecuencias en la manera de ejecutar procesos en los años venideros.»²⁷¹

En este mundo emergente, los usuarios se conectan con dispositivos inteligentes usando fórmulas de identificación y autenticación seguras, por ejemplo, con claves públicas y privadas, y definen las normas de actuación, por ejemplo, con respecto a la privacidad, con otros dispositivos, en lugar de tener que aceptar las normas de un nodo o intermediario centralizado. Los fabricantes pueden traspasar el mantenimiento, la propiedad, el acceso y la responsabilidad a una comunidad de dispositivos autosuficientes, garantizando la durabilidad del IoT, ahorrando costes de infraestructura y sustituyendo cada dispositivo exactamente cuando se queda obsoleto.

De este modo, el sistema blockchain puede salvar los seis obstáculos de un internet de las cosas que funcione. Resumiendo, el nuevo registro de todas las cosas tiene nueve características interesantes:

Es resistente. Se corrige a sí mismo; no tiene puntos débiles.

Es potente. Puede administrar miles de millones de puntos de información y transacciones.

Funciona en tiempo real. Funciona las veinticuatro horas de todos los días del año y la información fluye instantáneamente.

Tiene capacidad de respuesta. Reacciona a condiciones cambiantes.

Está radicalmente abierto. Evoluciona y cambia sin cesar con la información entrante.

Es renovable. Puede usarse para muchas cosas y muchas veces, y es reciclable.

Es reductivo. Minimiza costes y conflictos, maximiza la eficiencia.

Genera ingresos. Permite nuevos modelos de negocio y oportunidades.

Es fiable. Asegura la integridad de la información y la fiabilidad de los participantes.

¿Por qué creemos que el IoT basado en el sistema blockchain tiene un potencial tan grande? La primera razón es porque *da vida* al mundo físico. Una vez cobran vida en el registro, los objetos pueden percibir, responder, comunicarse y actuar. Los dispositivos pueden buscarse, encontrarse, usarse y pagarse unos a otros según manden los contratos inteligentes, creando así nuevos y revolucionarios mercados, igual que antes hizo internet con las personas y todo tipo de contenido digital.

Las preguntas que deben hacerse los administradores, empresarios y líderes civiles son: ¿cómo aprovecharemos estas nuevas oportunidades para cambiar y crecer? ¿Cómo reaccionará nuestra organización al inevitable vuelco que dará nuestro modelo operacional presente? ¿Cómo competiremos con los nuevos modelos creativos de las empresas emergentes y las redes colaborativas?

Las oportunidades de aumentar la eficiencia, mejorar los servicios, reducir los costes, incrementar la seguridad y obtener mejores resultados abundan en nuestras vidas, y podemos aprovecharlas aplicando la lógica de las blockchains al internet de las cosas. Estamos inaugurando la fase más importante de la revolución digital. Michelle Tinsley, de Intel, explica por qué su empresa está profundamente interesada en la revolución de las blockchains: «Cuando los PC se generalizaron, los índices de productividad se dispararon. Conectando esos PC a un servidor, un centro de datos o a la nube, hicimos que para las empresas emergentes con reducidos recursos fuera muy barato y fácil disponer de capacidad procesadora, y ahora estamos viendo de nuevo una rápida innovación, nuevos modelos de negocio».²⁷² Intel quiere acelerar el proceso de entender lo que funciona, lo que no funciona y dónde están las oportunidades. «Esta tecnología podría ser otra gran innovación, que diera pie a toda clase de empresas nuevas, de nuevos actores. Si queremos ser líderes de la industria tecnológica, no podemos quedarnos fuera», dice.²⁷³ Imaginemos el potencial que tendría aplicar estos recursos a todo tipo de negocios, a muchos de los cuales no ha llegado la revolución de internet.

Las doce revoluciones: dar vida a las cosas

¿Qué posibilidades tenemos de dar vida al mundo físico? A diferencia de Pinocho, no tenemos un Hada Azul. (Y a diferencia también de él, las blockchains no mienten.) Pero hoy, ahora mismo, tenemos una tecnología de registros distribuidos que nos permitirá «dar vida a las cosas buenas», como rezaba un eslogan de la compañía General Electric. Y lo que es mejor, es un archivo en el que a Pinocho no puede crecerle la nariz.

Apenas hemos empezado a pensar en las posibilidades que abre el registro de todas las cosas (creado dentro del IoT). Aunque los medios de comunicación han centrado su atención en los dispositivos de consumo, hay aplicaciones potenciales prácticamente en todos los sectores. Hay muchas maneras de clasificar y agrupar aplicaciones potenciales porque muchas de ellas traspasan fronteras y pueden pertenecer a más de una categoría. McKinsey, por ejemplo, usa el concepto de *marcos* en su clasificación del IoT.²⁷⁴ Nosotros vemos que el registro de todas las cosas tiene posibilidades en doce sectores principales. Las ventajas concretas —y las oportunidades de negocio— serán específicas de cada aplicación. Las categorías que a continuación enumeramos ilustran el potencial de esta aplicación y la revolución que podría suponer para los mercados, actores y modelos de negocio actuales.

1. Transporte

En el futuro, llamaremos por teléfono a un vehículo autónomo para que nos lleve a donde queramos. El vehículo escogerá automáticamente la ruta más rápida, evitará obras, pagará peajes y aparcará, y todo lo hará por sí solo. Y cuando haya atascos de tráfico, nuestro vehículo negociará una *tarifa de paso* para que lleguemos a tiempo a nuestro destino, y las compañías de transporte usarán el IoT con blockchain para pasar la aduana o cualquier otra inspección necesaria. No habrá papeleo. Allianz, un fabricante de camiones de la limpieza, podría equipar sus vehículos municipales con minicámaras o tecnología sensorial para que identificara los coches que no se han movido (por sí mismos o por sus dueños) en días de estacionamiento alterno en la ciudad de Nueva York, facilitará esa información a la policía de tráfico y ahorrará la emisión física de tíquets de aparcamiento. O el mismo camión de la limpieza podría cobrar la multa en bitcoins del mismo coche al pasar junto a él, pues el departamento de transporte del estado de Nueva York exigirá que todos los vehículos estén registrados en los cinco distritos de la ciudad de Nueva York y tengan carteras con bitcoins asociadas a sus matrículas. Por otro lado, los vehículos autónomos percibirán la proximidad del camión de la limpieza y se moverán para dejarlo pasar.

2. Gestión de infraestructuras

Muchos profesionales usarán dispositivos inteligentes para conocer la ubicación, estado de conservación, edad, calidad y cualquier otro factor relevante de pavimentos, vías férreas, postes y cables eléctricos, tuberías, pistas de aterrizaje, puertos y demás infraestructuras públicas y privadas, con el fin de controlar las condiciones en las que se encuentran, detectar problemas (por ejemplo, de roturas o manipulación) y obrar en consecuencia de una manera a la vez rápida y rentable. Aquí es donde entrarán empresas como Filament, con tecnologías nuevas y asequibles que darán vida a las infraestructuras sin necesidad de gastar el inmenso capital que se necesitaría para sustituirlas. Eric

Jennings, de Filament, estima que «más del 90 por ciento de las infraestructuras están actualmente desconectadas, y es inviable quitarlas todas y sustituirlas por dispositivos nuevos, inalámbricos y conectados».²⁷⁵

3. Gestión de energía, residuos y agua

«Enviadme un camión que me vacíe», dijo el contenedor de la basura, rebosante. «Arregladme», dijo la cañería rota. El internet de las cosas debería inspirar cientos de libros infantiles. Las empresas de servicios tradicionales tanto de los países desarrollados, como de aquellos en vías de desarrollo, pueden usar el IoT con blockchain para controlar la producción, la distribución, el consumo y la recogida de bienes y residuos. Como hemos visto antes, empresas nuevas sin gran infraestructura incorporada están planeando usar estas tecnologías para crear mercados y modelos completamente nuevos (por ejemplo, microrredes de suministro comunitarias).

4. Extracción de recursos, agricultura y ganadería

Las vacas pueden convertirse en dispositivos blockchain que permitan a los ganaderos saber lo que comen, con qué se medican y todo su historial sanitario. Esta tecnología también puede ayudar a controlar maquinaria cara y muy especializada y hacer que esté más disponible para un uso puntual y sea más amortizable; a mejorar la seguridad de mineros, agricultores y ganaderos mediante el etiquetado de los equipos de seguridad y listas de control automatizadas (para cerciorarse de que el equipo se usa debidamente); a controlar las condiciones meteorológicas, del suelo y de los cultivos para saber cuándo conviene regar, cosechar y hacer otras cosas; a compilar y analizar «datos infinitos» para descubrir nuevos recursos o recomendar las mejores prácticas agrícolas según patrones y resultados anteriores. Poner sensores en el suelo y en los árboles podría ayudar a las agencias de protección medioambientales a vigilar a agricultores y ganaderos y el uso que hagan de la tierra.

5. Control medioambiental y servicios de emergencia

¿Recuerda el lector al agente meteorológico BOB? BOB vivirá en un mundo de sensores meteorológicos y hará dinero recogiendo y vendiendo información meteorológica relevante. Por ejemplo, podrá controlar la calidad del aire y del agua y dar la alerta para que reduzcamos el uso de contaminantes o nos quedemos en casa; podrá indicar la presencia de productos químicos peligrosos o de radiactividad a los que trabajen en servicios de emergencia; controlar los rayos y los incendios forestales; instalar sistemas de alerta y prevención de terremotos y tsunamis, así como, claro está, controlar las tormentas y prevenirlas. Además de reducir el tiempo de respuesta de los servicios de emergencia y los riesgos que estos fenómenos suponen para la vida humana, podremos usar esta información longitudinal para aumentar nuestro conocimiento de pautas y tendencias y mejorar nuestra capacidad de predicción para prevenir incluso con mayor antelación.

6. Atención sanitaria

En el sector de la atención sanitaria, los profesionales usan la digitalización para gestionar dispositivos y registros médicos, hacer inventario y realizar pedidos y pagos de equipo y productos farmacéuticos. Hoy, los hospitales están llenos de dispositivos inteligentes que prestan estos servicios, pero pocos pueden comunicarse entre sí ni tener en cuenta lo importante que es proteger la privacidad y la seguridad en la atención directa al paciente. El IoT con blockchain puede emplear aplicaciones emergentes para vincular estos servicios. Las aplicaciones que están desarrollándose son, por ejemplo, de control y administración de enfermedades (píldoras inteligentes, dispositivos que se lleven puestos y que registren señales vitales y las notifiquen) y de mejora de la calidad. Imaginemos una cadera o rodilla artificial que se vigile a sí misma, envíe información anónima sobre su funcionamiento al fabricante para que éste introduzca mejoras y se comuniquen con el médico del paciente: «Es hora de reemplazarme». Los técnicos no podrán usar equipo especializado si no han tomado las medidas previas necesarias para asegurarse de que es fiable y preciso. Habría fármacos inteligentes que podrían observarse a sí mismos en pruebas clínicas y mostrar su efectividad y efectos colaterales sin riesgo de alteración de los resultados.

7. Servicios financieros y seguros

Las instituciones financieras podrían usar dispositivos inteligentes y el IoT para etiquetar sus derechos de propiedad de activos materiales y poder localizarlos y seguirlos. Como las monedas digitales permiten almacenar y transferir valor de una manera rápida y segura para todos los usuarios, grandes o pequeños, también permiten evaluar y gestionar el riesgo. Yendo más allá, ¿podrían los pobres y desheredados de este mundo ganar pequeñas cantidades de dinero, o quizá de electricidad u otros «créditos», si permitieran que sus reducidos activos fueran etiquetados y compartidos como en el ejemplo anterior de la microrred eléctrica? Los propietarios de objetos valiosos, antigüedades, joyas, piezas de museo, cualquier cosa vendida por Sotheby's y asegurada por Lloyd's, podrán etiquetarlos. Las compañías de seguros podrían ajustar las cuotas con arreglo al lugar y el entorno del objeto: si está en el Museo Metropolitano de Nueva York y en un ambiente controlado, la cuota será baja; si está viajando a Grecia, será más alta. El objeto podría decirnos si ha estado en una caja fuerte o rodeando el cuello de un famoso. La cuota del seguro podría ser más alta si hubiera colgado del cuello de Lindsay Lohan que si lo hubiera hecho del de, digamos, Anne Hathaway. Los vehículos automáticos tendrían seguramente cuotas más bajas, y los mismos dispositivos podrían solucionar reclamaciones en el acto, basándose en los datos de los sensores.

8. Archivo de documentos y registros

Como hemos explicado, los activos materiales pueden convertirse en activos digitales. Toda la documentación relativa a un «objeto» en particular puede digitalizarse y subirse a una blockchain, como, por ejemplo, patentes, títulos de propiedad, garantías, certificados de inspección, de procedencia, seguros, fechas de repuesto, vistos buenos, etc., lo que aumentaría notablemente la disponibilidad e integridad de la información, reduciría el papeleo administrativo, facilitaría el archivo y evitaría pérdidas, y, en fin, mejoraría el procesamiento de esa documentación. Por ejemplo, un vehículo no arrancaría si no

hubiera pasado la última inspección técnica, si tuviera el seguro caducado, si su dueño hubiera dejado de pagar tíquets de aparcamiento o multas de tráfico, o si hubieran suspendido el permiso de conducir de la persona que fuera a ponerse al volante. Los productos de los estantes notificarían a los regentes de la tienda que habían pasado la fecha de caducidad. Esos regentes incluso podrían programar los productos para que se bajaran el precio cuando se acercara la fecha de caducidad.

9. Administración de edificios y propiedades

Se estima que el 65 por ciento de los mil millones y pico de metros cuadrados de inmuebles comerciales que hay en Estados Unidos están libres.²⁷⁶ Los sensores digitales pueden crear mercados de estos activos inmuebles localizándolos, informando de su estado y habilitando pagos. Los vendedores están ahora entrando en este campo y desarrollando nuevos modelos de servicio para alquilar los espacios desocupados. Por las noches, nuestras salas de conferencias pueden pluriemplearse como aulas para jóvenes del barrio o como oficinas de una empresa emergente del lugar. Otras aplicaciones incluirán seguridad y control de acceso, iluminación, calefacción, refrigeración y gestión de residuos y agua. El edificio más ecológico funcionará con el registro de las cosas. Pensemos en cómo los datos sobre uso de ascensores y tránsito de personas de un edificio condicionarán el diseño arquitectónico de los espacios públicos y privados. Los espacios residenciales vacíos pueden anunciarse a sí mismos y negociarse en el registro de todas las cosas para ayudar a turistas, estudiantes, directores de programas de vivienda para personas sin hogar y a otros a encontrar los espacios que buscan. Esta idea sirve para todo tipo de viviendas, hoteles, oficinas, fábricas, comercio minorista y mayorista, bienes inmuebles institucionales.

10. Operaciones industriales: la fábrica de las cosas

La industria global necesita un registro de las cosas global, es decir, una blockchain industrial. Los administradores de las fábricas usarán dispositivos inteligentes para controlar cadenas de producción, existencias, distribución, inspecciones de calidad y de otro tipo. Industrias enteras pueden adoptar la idea del archivo para incrementar notablemente la eficiencia gracias, por ejemplo, a la gestión de la cadena de suministro. Las máquinas grandes y complejas, como aviones y locomotoras, constan de millones de partes. Los componentes de un motor de reacción o de un automotor podrían tener sensores que enviaran una alerta cuando necesitaran ser arreglados. Imaginemos un tren que fuera a ir de Baltimore a Long Beach y que notificara al personal de mantenimiento de Long Beach con tres días de antelación que necesita un recambio fundamental. El sensor incluso podría pedir presupuesto y aceptar la mejor oferta, ahorrando tiempo y costes a grandes empresas como General Electric, Norfolk Southern y otras. Y lo que es más importante, fabricantes de todo tipo de cosas, desde coches hasta bombillas, pasando por tiritas, están investigando cómo integrar chips inteligentes en sus productos o partes de ellos y controlar, recoger y analizar información de su funcionamiento. Con estos datos, podrían introducir mejoras automáticas, anticiparse a las necesidades del cliente y ofrecer nuevos servicios, dejando de ser, de hecho, gracias a la informática, proveedores de productos para convertirse en proveedores de servicios en constante progreso.

11. Gobierno de la casa

¿Que nos sentimos solos? Siempre podemos hablar con nuestra casa. Nuestro hogar y numerosos productos y servicios están entrando en el mercado para permitirnos controlar nuestra casa de manera automatizada y remota. Estos servicios van más allá del monitor de bebés e incluyen controles de acceso, ajuste de temperatura, iluminación y, eventualmente, casi cualquiera cosa de nuestra casa. Aunque las «casas inteligentes» han tardado en despegar, compañías como Apple, Samsung y Google trabajan para simplificar la instalación y las operaciones. Según BBC Research, «se estima que el mercado de automatización doméstica de Estados Unidos pasará de casi 6.900 millones de dólares en 2014 a 10.300 millones en 2019... El crecimiento será continuo y duradero».²⁷⁷

12. Operaciones y ventas al por menor

Vamos caminando por la calle y nuestro móvil nos avisa de que una prenda que nos gusta está disponible en Gap. Entramos en la tienda y la prenda, en nuestra talla, nos espera. Después de probárnosla, la escaneamos y ya hemos pagado. Pero como tenemos otras cosas que hacer, la prenda halla el modo de llegar a nuestra casa antes que nosotros. Además de incrementar la eficiencia operativa y el control medioambiental, los vendedores minoristas podrán personalizar sus productos y servicios para clientes reconocibles cuando pasen andando o en coche, según su lugar de residencia, condición social e historial de compras, siempre que esos clientes hayan permitido a los vendedores entrar en sus cajas negras de la blockchain.

Ventajas económicas

En este capítulo hemos hablado de las numerosas ventajas que el IoT distribuido y con blockchain tiene en muchos órdenes (individual, organizativo, industrial, social). Rediseñar y automatizar procesos en redes igualitarias en vez de hacerlo a través de personas o aplicaciones intermediarias centralizadas podría tener numerosas ventajas, como:

- Rapidez (automatización de extremo a extremo).
- Costes reducidos (los costes que supondría enviar cantidades prácticamente infinitas de datos a centrales de procesamiento; eliminación de intermediarios onerosos).
- Mayores ingresos, mayor eficiencia y mayor productividad (liberando capacidad sobrante que puede volver a usarse).
- Eficacia mejorada (incorporar listas de control y otros protocolos reduce los efectos de los errores humanos).
- Mayor seguridad y mayor integridad (no es preciso que las personas confíen unas en otras porque la fiabilidad forma parte de la estructura de la red).
- Menor riesgo de fallos sistémicos (eliminación de embudos, resistencia integrada).
- Menor consumo de energía (la energía que la red necesita se ve compensada por la mayor eficiencia, el menor desperdicio, el sistema de precios dinámico y circuitos de retroalimentación).

- Mayor protección de la privacidad (los intermediarios no pueden anular o saltarse las normas definidas en la blockchain).
- Mejor comprensión de las pautas y procesos subyacentes y posibilidad de mejorarlos gracias a la recogida y análisis de «datos infinitos».
- Mayor capacidad de predicción de acontecimientos negativos (mal tiempo, terremotos, deterioro de la salud) y positivos (mejor época para sembrar, patrones de compra).

El modelo abierto distribuido permite que las redes del IoT puedan mantenerse incluso si una empresa se retira o un fabricante falla. La interoperabilidad, al estar integrada en el sistema, permitirá que varias redes IoT se interconecten y creará aún más valor.²⁷⁸

Muchas de estas ventajas dependen de conceptos como los de red distribuida o descentralizada y eliminación de intermediarios centrales (por ejemplo, de mando) y de otro tipo (por ejemplo, una aplicación de gestión o que funcione como cámara de compensación). Una vez que estos nuevos intermediarios se instalen, otros se verán forzados a esquivarlos o eliminarlos. Según Eric Jennings, «la gente hará las cosas que hará para minimizar molestias, lo que llevará a la formación de silos, a la concentración y a la centralización. Lo que a corto plazo es una ganancia para esas personas en particular es a largo plazo una pérdida para todos los demás —Y añade—: El internet de las cosas debería estar completamente descentralizado y permitir que los dispositivos fueran autónomos, se descubrieran directamente unos a otros, establecieran directamente comunicación unos con otros y, llegado el caso, se pagaran unos a otros, directamente de una máquina a otra».²⁷⁹

El Institute for Business Value de IBM ha hecho un estudio de lo que llama los cinco mayores «vectores de cambio» que aumentarán la rentabilidad de nuestros activos materiales como consecuencia del IoT de blockchain.²⁸⁰ Aunque IBM tiene un claro interés económico en el IoT, su visión del valor comercial de éste no deja de ser muy útil.

El instituto observa, en primer lugar, que estas nuevas redes permitirán a los usuarios buscar y comprar instantáneamente activos materiales tales como capacidad de almacenamiento o procesadora infrautilizada. Los activos podrán ofertarse a sí mismos para satisfacer la demanda. Como podemos evaluar el riesgo y el crédito automáticamente en línea y recuperar los activos, podemos valorar el crédito y el riesgo bastante a la baja. El uso automatizado de sistemas y dispositivos mejora la eficiencia operativa. Por último, las empresas pueden asociarse y colaborar con otras en tiempo real mediante cadenas de valor digitalmente integradas.

En definitiva, tenemos la oportunidad de crear mercados más eficientes y conceptualmente más simples. Podemos acceder a activos que antes eran inaccesibles, determinar el precio en tiempo real y reducir riesgos. Una vez que la infraestructura básica está creada, los obstáculos para acceder al mercado desaparecen (por ejemplo, desarrollando una aplicación) y los costes disminuyen (por ejemplo, no hay que pagar servicios de terceros). Podemos reducir drásticamente el coste de transferir capitales y

facilitar el tener una cuenta corriente, el obtener crédito o el invertir. Incluso podríamos habilitar formas de micropago que permitieran pagar el uso de un determinado servicio al minuto.

El registro de las cosas hace posible el «capitalismo distribuido», no sólo el capitalismo redistribuido. Lejos de ser mercados en los que vale todo, podemos moldearlos de acuerdo con nuestros valores —como individuos, empresas y sociedades— y codificar estos valores en la blockchain, por ejemplo, en forma de incentivos para usar energía renovable, emplear primero recursos producidos en nuestra inmediata vecindad, recompensar políticas de precios justos y proteger la privacidad. En definitiva, el registro de todas las cosas sumado al IoT da vida y personaliza el mundo físico incluso cuando compartimos. Como dice IBM, «en el plano macroeconómico, todos ganaremos en el futuro del IoT, aunque habrá industrias que experimenten una mezcla de efectos diferentes».²⁸¹ Según el McKinsey Global Institute, el valor económico del IoT ha sido subestimado; el impacto económico —incluido el excedente del consumidor— podría llegar a los 11,1 billones de dólares anuales en 2025 en aplicaciones IoT.²⁸² Esto representa un 10 por ciento del actual PIB mundial, que es de más de 100 billones de dólares. ¡Es muchísimo!

La «inteligencia reticular» (*networked intelligence*), un concepto acuñado en *The Digital Economy*, se refiere al hecho de que la red será más inteligente que el más inteligente de los nodos en un dominio tras otro. Como hemos explicado, la primera generación de internet permitió reducir algo los costes transaccionales. Tenemos cadenas de suministro más rápidas, nuevos planteamientos mercadotécnicos y plataformas de colaboración masiva e igualitaria como Linux y Wikipedia, además de muchos modelos de negocio nuevos e innovadores. La tecnología blockchain acelerará este proceso. Cuando el internet de las cosas se afiance, estas tendencias se dispararán.

El futuro: de Uber a SUber

Hemos tratado muchos aspectos de la innovación en este capítulo. Veámosla ahora en un caso concreto.

Pensemos en agregadores de servicios como Uber o Lyft. Uber es una red de conductores que están dispuestos a llevar a otra gente en sus coches por una cantidad de dinero. Para usar Uber, nos descargamos la aplicación, creamos una cuenta y damos a Uber la información de nuestra tarjeta de crédito. Cuando necesitamos ir a algún sitio en coche, la aplicación nos pide que seleccionemos el tipo de coche que queremos y señala nuestra ubicación en un mapa. La aplicación nos informa de la disponibilidad y localización de nuestro posible conductor. Al final del viaje, Uber nos cobra automáticamente de la tarjeta de crédito. Si no queremos dar la propina al conductor que viene marcada por defecto, tenemos que cambiar las condiciones de la facturación en el sitio web de Uber.²⁸³ Uber Technologies, la empresa que desarrolla y maneja la aplicación, se queda con una parte del precio pagado por cada viaje.

Suena muy bien, sobre todo si pensamos en ciudades con pocos taxis. Pero el servicio que Uber ofrece tiene algunos problemas y riesgos. Las cuentas de los conductores han sido pirateadas, las tarifas están sujetas a subidas bruscas y los pasajeros están expuestos a conducción temeraria, acoso sexual y agresiones.²⁸⁴ Uber controla todos los movimientos de los usuarios y suministra información a las autoridades municipales para que hagan estudios viales. Y, encima, los conductores crean bastante valor pero sólo se llevan una parte.

Ahora imaginemos la experiencia de Uber si fuera una aplicación distribuida en una blockchain. Mike Hearn, un empleado de Google, que dejó su trabajo para dedicarse por completo a bitcoin, expuso este universo alternativo basado en la tecnología bitcoin en el Turing Festival (Edimburgo) de 2013.²⁸⁵ Hearn llamaba a esta red «TradeNet» y describía cómo, con la ayuda de bitcoin, la gente podía empezar a confiar en los vehículos automáticos.

Funciona así. La mayoría de la gente no tiene coche, sino que comparte vehículos en una comunidad. En Chicago, Melissa pide un coche a través de SUber (o sea, la blockchain Super Uber). Todos los vehículos disponibles empiezan automáticamente a hacer ofertas, que el nodo de Melissa clasifica y le muestra según sus criterios de selección. Melissa tiene en cuenta cuánto está dispuesta a pagar por rutas más rápidas (por ejemplo, por ir por carriles con peajes más altos).

Entretanto, John, a diferencia de la mayoría de los usuarios, es propietario de un vehículo de SUber y, cuando lo lleva al trabajo, su coche automático identifica todas las opciones de aparcamiento, tanto públicas como privadas, reserva una plaza y la paga a través de un mercado de aparcamientos autónomo. Como los parámetros que John ha preestablecido siempre mandan buscar el sitio disponible más barato que haya a menos de diez minutos a pie de su destino, casi siempre acepta el primero que escoge el coche. La base de datos sobre aparcamientos en que se basa el programa también incluye información sobre normativa de estacionamiento según la calle, el día y la hora, sobre si es un sitio cubierto o está al aire libre, sobre si el propietario del sitio ha establecido un precio mínimo. Todo esto se realiza en una plataforma de iguales que conecta numerosas aplicaciones, por lo que no hay ninguna empresa centralizada que medie ni se lleve parte del dinero. No hay subidas de precios, comisiones ni tarifas inesperadas.

Lo interesante de este modelo no son los vehículos automáticos, que serán algo común seguramente más pronto que tarde. Lo interesante es que los coches podrían ser agentes autónomos a carta cabal, que cobraran por la carrera, compraran combustible, pagaran por las reparaciones, contrataran su seguro, negociaran las responsabilidades en caso de choque y operaran («condujeran») sin control humano exterior, salvo cuando tuvieran que demandar a alguna entidad, que podría ser un humano.

Como condición para operar, los administradores de SUber podrían programar los protocolos de los vehículos en la blockchain para que cumplieran todas las normas de tráfico, escogieran la ruta más directa y rápida o la menos cara, y respetaran sus ofertas. A los conductores que se registraran por primera vez en SUber, el sistema podría pedirles que aportaran la documentación necesaria, como el título de propiedad, certificados de inspecciones y seguros, y el sistema archivaría para siempre esos registros a fin de

asegurar nuevas inspecciones o seguros y permitir las oportunas renovaciones. Habría sensores que controlarían la «salud» general del vehículo y señalarían las necesarias reparaciones, quedarían con el mecánico y pedirían por anticipado las piezas que se necesitaran. Como los vehículos no llevan conductor, no están expuestos a burlas, favoritismo, sexismo, racismo ni demás formas de discriminación o corrupción humana. Además, tampoco querrán convencernos de sus ideas políticas ni llenarán el salpicadero de incienso. Todo esto ocurre entre bastidores, entre objetos, y a través de una aplicación autónoma. Los conductores han creado una blockchain cooperativa como las que hemos descrito en el capítulo anterior y reciben casi toda la riqueza que crean. Los usuarios —Melissa y John— sólo se aprovechan de las ventajas, sin padecer ninguno de los inconvenientes. ¿Qué más pedir?

Si internet ya redujo los costes de búsqueda y coordinación, una moneda digital como bitcoin en una blockchain nos permitirá también reducir los costes de negociar, contratar, controlar y aplicar esos contratos. Podremos negociar el mejor pacto y recibir lo prometido por cualquier otra entidad que acepte bitcoin, incluido un taxi automático. ¿Cómo podrán los Ubers del mundo competir?

Pero el escenario no se acaba aquí. La inteligencia integrada en las infraestructuras públicas gobernará el tráfico (carriles de dirección variable, tarifas variables, gestión automatizada de las señales viales basada en el flujo circulatorio), con lo que aún se reducirán más el desperdicio de energía y los costes. Las blockchains podrían facilitar los controles de seguridad, tanto de los vehículos (con conductor o sin él) como de las infraestructuras, por ejemplo, dando avisos de proximidad y frenado automático, así como tomando medidas contra robos o para evitar que conductores inexpertos o ebrios se sienten al volante. Además, las ciudades usarán sensores que contribuirán a la gestión de las infraestructuras del transporte, facilitando la gestión de dispositivos de infraestructuras y parques móviles, la vigilancia de vías férreas y firmes, la creación de planes de mantenimiento y presupuestos y el envío de personal de mantenimiento en caso de necesidad.

Y lo mejor de todo es que los sistemas trabajarán juntos: vehículos inteligentes que operarán en una infraestructura inteligente. Aunque seguirá habiendo sitio para los conductores de vehículos compartidos, los vehículos autónomos podrán operar con seguridad en las calles de las ciudades gracias a sus sistemas de navegación y de seguridad integrados, interactuando a menudo con las infraestructuras inteligentes para encontrar un carril de alta velocidad y pagar por usarlo, o un sitio para aparcar, o una ruta preferida. La disponibilidad, asequibilidad y fiabilidad de los vehículos autónomos harán que se reduzca el número de vehículos privados, los cuales, como hemos visto que ocurre con los inmuebles comerciales, casi siempre están aparcados y sin usar.

Y esto no se deberá sólo a la tecnología y a las empresas automovilísticas. Aunque todo esto, en teoría, podría desarrollarlo, poseerlo, explotarlo y administrarlo una sola autoridad pública, parece que no será el caso. Es más probable que SUber evolucione e innove siendo una plataforma de transporte abierta y compartida, con aplicaciones desarrolladas e introducidas por empresarios locales, grupos comunitarios, gobierno y demás, tanto en forma de cooperativa compartida (un grupo de vecinos invierte en diez

vehículos para que se reserven y compartan a través de la aplicación de SUber) o con fines de lucro (con las ganancias producidas por una flota de furgonetas automáticas), como de servicio público (mantener y explotar un tren o autobuses expresos en rutas muy demandadas) o de empresa social (invirtiendo sin ánimo de lucro en «puntos» SUber, a los que los clientes puedan acceder cuando necesiten un medio de transporte).

Esto podría empezar a producirse en lugares con infraestructuras relativamente avanzadas y vías de transporte ya diferenciadas (ferrocarril, carretera, carriles de bici, de peatones), problemas de transporte importantes (atascos de tráfico) y una población con una larga tradición de obediencia a las normas viales. También podría darse en nuevas urbanizaciones que cooperaran con empresas tecnológicas y compañías automovilísticas que buscasen bancos de pruebas para sus aplicaciones. Cualquier escenario en el que hubiera vehículos automáticos tendría menos éxito e incluso sería muy peligroso si no pudiéramos aislar a los demás usuarios (en vías diferenciadas), predecirlos (animales en la carretera) o controlarlos (peatones distraídos).

El escenario que plantea SUber es cada vez más factible. Este tipo de aplicaciones irán seguramente apareciendo en los próximos años y resolverán nuestros problemas de transporte a largo plazo. Ya hoy, comités de taxistas locales están enfrentándose a Uber en muchas ciudades. Los gobiernos municipales se las ven y se las desean para conciliar el deseo del consumidor de opciones asequibles con la seguridad pública y la regulación del sector, incluso cuando los nuevos modelos parecen inevitables. ¿Por qué no mirar hacia donde se dirige el sector del transporte y discurrir las soluciones que mejor satisfagan las necesidades del municipio, como ha hecho Chicago en nuestro hipotético escenario de SUber?

Programar el futuro para crear un mundo de cosas inteligentes

En este capítulo hemos visto algunas de las asombrosas oportunidades que hay en, prácticamente, todos los aspectos de nuestra vida, incluidas —quizá especialmente— muchas áreas a las que apenas llegó la primera oleada de la revolución digital. Al mismo tiempo, estas oportunidades amenazan negocios y maneras de hacer negocio existentes en la actualidad.

Cuestiones clave: ¿Qué haríamos, si fuéramos empresarios, con respecto a las dos partes de la ecuación: nuevas oportunidades que podrían aprovecharse y amenazas que habría que minimizar? Si somos empresarios, lo mismo en el sector público que en el privado o en el social, ¿tenemos activos materiales que no utilizamos o que utilizamos poco y que podrían rendir más? ¿Estamos consiguiendo la mayor eficiencia posible y aprovechando las mejores oportunidades para desarrollar productos y tecnologías IoT? ¿Están las nuevas empresas de esta economía quitándonos los clientes y reduciendo nuestras ganancias con nuevos modelos de negocio basados en aplicaciones que tendríamos que haber instalado nosotros primero?

Nuevo valor: ¿Cuáles son nuestros activos materiales y cómo podemos explotarlos para crear más valor para nuestra organización o comunidad? ¿Tenemos espacios físicos, máquinas, existencias u otros activos que podríamos etiquetar, controlar y animar como

parte de una red autónoma en la que estableciéramos los parámetros operativos para evitar costes y sumar valor? ¿Podríamos integrar, modernizar y programar sensores que formaran parte de una red mayor que fuera más funcional y produjera más valor? ¿Podríamos obtener nueva información de una red IoT que nos permitiera mejorar nuestros planes y análisis de futuro?

Nuevos modelos de negocio: ¿Qué oportunidades existen para crear nuevos productos y servicios con las nuevas prestaciones de la red y con la información que podríamos recabar de ella? ¿Podríamos rentabilizar nuestra información y nuestros activos gracias al valor que tienen para otros, por ejemplo, alquilando ese aparato caro cuando no lo usamos? Pensar en el valor de la información no es nuevo (recordemos Sabre y American Airlines), pero seguimos sin prestarle la debida atención.

Oportunidades: ¿Podríamos conectar nuestra red con otras para crear aún más valor, por ejemplo, formando parte de un circuito cerrado de suministro o de distribución y venta? Como industria, ¿hay procesos y funciones comunes que podrían automatizarse utilizando el sistema blockchain? ¿Estamos usando la tecnología abierta y sancionada por colaboradores internacionales que nos permita esta interoperatividad?

Amenazas: ¿Qué líneas de negocio van a emprender las nuevas empresas con sus nuevos modelos de negocio IoT para servir mercados que ahora estamos sirviendo nosotros? Por ejemplo, en lugar de vender una sola vez un vehículo, un bien de consumo o un aparato especializado, ¿hay un valor permanente para nosotros y para nuestros clientes en un nuevo modelo de servicio basado en nuestra conexión a ese aparato? ¿Podemos sacar provecho de nuestra experiencia, recursos, infraestructura y fidelidad clientelar para concebir nuevos modelos de negocios IoT que reduzcan el «espacio» y, por tanto, la probabilidad de que entren nuevo actores que nos hagan la competencia?

«Business case»: ¿Cuáles son los costes y beneficios de estas oportunidades? ¿En qué consiste el verdadero valor para nuestra organización? ¿Estamos resolviendo un verdadero problema o satisfaciendo una verdadera necesidad, o simplemente apostando por la tecnología? ¿Y si desarrollamos una prueba piloto con un cliente destacado?

Plan estratégico: Según el McKinsey Global Institute, «los ejecutivos tendrán que enfrentarse a tres clases de retos: falta de estructura organizativa, interoperatividad tecnológica y obstáculos analíticos, y mayores riesgos en ciberseguridad».²⁸⁶ Nosotros añadimos un cuarto reto a esta lista: reforzar la privacidad y trazar un plan de incentivos que incluya las correspondientes garantías desde el principio. ¿Cómo tendrán que adaptarse la informática y las funciones empresariales al IoT? ¿Qué partes de la organización y a qué líderes empresariales tendríamos que implicar?

Capítulo VII

La paradoja de la prosperidad: inclusión económica y empresa

Un cerdo no es una hucha

La costa de Nicaragua que da al Pacífico es uno de los paisajes más bellos de toda América. Allí, unas selvas verdes lindan con interminables aguas azules. Sus onduladas colinas y magníficas playas atraen a mochileros, bañistas y ecoturistas. Nicaragua es también uno de los países más pobres y menos desarrollados de la región. El 60 por ciento de la población vive por debajo del umbral de la pobreza. Los que no trabajan en la industria turística sobreviven de una agricultura y de una pesca casi de subsistencia. Nicaragua tiene el segundo PIB más bajo de toda América, y el 10 por ciento de ese PIB es dinero ganado en el extranjero y enviado al país por la diáspora nicaragüense. El 19 por ciento de los nicaragüenses tiene una cuenta corriente, pero sólo el 14 por ciento puede pedir prestado y sólo el 8 por ciento tiene ahorros.²⁸⁷ Pero el 93 por ciento tienen un teléfono móvil, la mayoría de prepago.²⁸⁸

Ésta es la realidad que se encontró Joyce Kim cuando fue con su equipo a Nicaragua. Kim es la directora ejecutiva de la fundación Stellar Development, una organización sin afán de lucro que se dedica a la tecnología blockchain (no confundir con Stellar, la gran empresa de construcción y arquitectura). Los responsables de un programa de microfinanzas nicaragüense querían saber más sobre la plataforma financiera de Stellar. La terriblemente subdesarrollada industria bancaria de Nicaragua mantiene a la gente en un inevitable ciclo de pobreza y aumenta las dificultades de los que quieren emprender algo. Éstos necesitan Dios y ayuda para montar un negocio, registrar títulos de propiedad de la tierra y otros bienes, y resolver demandas pendientes desde la masiva expropiación de tierras del gobierno sandinista en la década de los ochenta del siglo pasado.²⁸⁹ La plataforma de Stellar permitirá a los nicaragüenses transferir, invertir, pedir prestado y prestar dinero.

A Kim la impresionó, y a la vez la sorprendió, el interés de los nicaragüenses por el microcrédito. Entendía que acceder al crédito es fundamental para que haya inclusión económica, pero creía que el ahorro, la capacidad de guardar dinero de una manera fiable y segura, es un requisito de cualquier servicio financiero. Cuando Kim preguntaba por los ahorros, le decían: «Ah, el ahorro no es un problema aquí. La gente tiene cerdos».²⁹⁰

El ganado constituye la mayor parte del patrimonio neto de los campesinos en muchas economías agrarias porque los servicios financieros no están disponibles para la mayoría y el derecho de la gente a la propiedad de su tierra apenas está reconocido. En Nicaragua, esto se traduce en que la gente posee cerdos, montones de cerdos. Kim se

sorprendió al principio, pero pronto vio la vieja lógica que tenía aquello. «Sales de una reunión, miras a un lado y otro y por todas partes ves cerdos.»²⁹¹ El ganado ha sido durante mucho tiempo una manera generalizada y bastante eficaz de ahorrar. Para las personas excluidas de la economía digital, los animales son casi el activo más líquido que pueden tener, sobre todo si producen leche, y pagan dividendos en forma de lechones, huevos, corderos, terneros y a veces queso.

La prosperidad es un concepto relativo. En Kenia, las tribus masai que poseen de cuatrocientas a quinientas cabras son consideradas prósperas, pero sus vidas pueden ser duras, brutales y cortas. La riqueza basada en el ganado está «muy localizada, por lo que no podemos comerciar con nadie a menos que estemos muy cerca —dice Kim—. Corremos el gran riesgo de que los animales se nos escapen o enfermen o venga una plaga que barra literalmente nuestros ahorros.»²⁹²

La cuestión del crédito aún fue más complicada que la del ahorro. Kim conoció a un pescador nicaragüense, miembro de una cooperativa, que le dijo que ningún pescador recibió nunca crédito suficiente para comprarse un aparejo completo. Según Kim, «forman equipos de pescadores en los que una persona consigue un préstamo para comprar la red, otra para comprar el cebo, otra para comprar el barco, otra para comprar el motor, y luego se juntan y forman una tripulación». Nadie puede fundar su propia empresa porque el acceso al crédito está muy restringido. El modelo funciona, pero supone tantos intermediarios como pescadores hay.

Las dificultades financieras vitalicias de los pescadores y campesinos nicaragüenses son las de la mayoría de la gente sin servicio bancario, que son hoy unos 2.000 millones de personas en el mundo.²⁹³ Aquello de lo que ellos carecen —un depósito de valor que no contraiga la enfermedad de las «vacas locas» o muera de viejo, o un mecanismo de pago que vaya más allá del pueblo— va de suyo para nosotros.

La inclusión financiera es un requisito de la inclusión económica. Sus repercusiones trascienden la esfera de las finanzas. Dice Kim: «Para mí, el acceso a los servicios financieros y la inclusión financiera no es el objetivo final. Es el camino que todos tenemos que recorrer para tener una educación mejor, una sanidad mejor, igualdad de derechos para la mujer y desarrollo económico».²⁹⁴ En definitiva, la inclusión financiera es un derecho fundamental.

Este capítulo trata de las oportunidades que tienen los proveedores de servicios de telefonía móvil y financieros para, usando el sistema blockchain, desarrollar el potencial económico en la base de la pirámide. Hablamos de miles de millones de nuevos clientes, empresarios y propietarios de activos que están preparados y listos para pasar a la acción. Recordemos que las transacciones hechas en el sistema blockchain pueden ser mínimas, de céntimos, y liquidarse enseguida. Cualquiera que tenga un activo, por pequeño que sea —talento para bordar o para la música, cubos que no use para traer y llevar agua, una gallina que ponga huevos, un teléfono móvil que grabe datos, sonidos e imágenes— podría intercambiar valor. La nueva plataforma también elimina el obstáculo que suponía tener que disponer de un punto de acceso a internet. Si podemos acceder con nuestro dispositivo móvil, entonces podemos acceder a activos sin necesidad de rellenar formularios ni estar muy alfabetizados. Estos avances parecen pequeños pero son muy

importantes. Si sabemos usarla, la tecnología blockchain podría descubrirnos el mayor filón de capital humano de la historia, lo que permitiría que miles de millones de empresarios comprometidos y prósperos entraran en la economía global.

La nueva paradoja de la prosperidad

Por primera vez en la historia moderna, la economía global crece pero sólo se benefician unos pocos. Por un lado, la era digital ofrece posibilidades ilimitadas para la innovación y el progreso económico. Los beneficios empresariales son desorbitados. Por otro lado, la prosperidad se ha estancado. A lo largo de la historia moderna, las personas y los hogares medios prosperaron. Pese a las crisis y los trastornos, la prosperidad para esas personas y para la sociedad en general fue en aumento. Ahora no ocurre esto. Los niveles de vida están bajando en el mundo desarrollado. Los sueldos medios se estancan en los países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Y, según la Organización Mundial del Trabajo (OIT), el desempleo juvenil en casi todo el mundo es del 20 por ciento. «Los jóvenes tienen tres veces más probabilidades de no encontrar trabajo que los adultos», informa esta organización.²⁹⁵ En muchos países en vías de desarrollo, las cifras son bastante más altas. Este desempleo corroe a una sociedad, sea cual sea su nivel de desarrollo. La mayoría de los ciudadanos quiere contribuir a su comunidad. Todo el que ha estado sin trabajo sabe lo mucho que eso erosiona la autoestima y el bienestar. Los que tienen poder y riqueza toman la delantera, los que no los tienen se quedan atrás.

Esta nueva paradoja de la prosperidad, que no hay que confundir con la intergeneracional «paradoja de la prosperidad» acuñada por economistas como Gilbert Morris, tiene desconcertados a todos los políticos del mundo occidental. Uno de los libros de economía más vendidos de 2014, *El capital en el siglo XXI*, de Thomas Piketty, fue ese mismo año número uno en ventas en la lista de libros de no ficción de *The New York Times*. El libro, un prodigio de investigación académica, explica por qué la desigualdad está acelerándose y seguirá haciéndolo mientras la rentabilidad del capital supere el crecimiento económico a largo plazo. Los ricos se han hecho más ricos porque su dinero les ha producido más dinero que su trabajo. De ahí la proliferación de millonarios y multimillonarios. Pero la solución que el autor da para frenar la creciente desigualdad social, consistente en imponer una tasa de riqueza a los que poseen la mayor parte de la riqueza del mundo, se trata de una idea poco inspirada, aunque sólo sea porque ya la hemos oído antes.²⁹⁶ De hecho, desde que el capitalismo es el principal modo de producción, el debate de cómo repartir los frutos más equitativamente no ha ido mucho más allá de la redistribución de la riqueza, normalmente mediante los impuestos a los ricos y la prestación de servicios públicos a los pobres. Los defensores del actual modelo económico alegan que cientos de miles de personas de países en vías de desarrollo (sobre todo de Asia) han podido salir de la pobreza extrema, pero muchas veces no ven los beneficios desiguales conferidos a los muy ricos y la brecha creciente entre éstos y el

resto de la población en esos mismos países. Hoy, el 1 por ciento de la población mundial posee la mitad de la riqueza total, mientras que 3.500 millones de personas ganan menos de dos dólares diarios.

Los partidarios del *statu quo* se apresuran a señalar que la mayoría de los muy ricos se hicieron ricos porque crearon empresas, no porque heredaron. Sin embargo, detrás del éxito de unos pocos hay unas cuantas estadísticas inquietantes. El índice de creación de nuevos negocios es bajo. En Estados Unidos, el porcentaje de empresas con menos de un año de vida cayó casi la mitad entre 1978 y 2011, pasando del 15 al 8 por ciento.²⁹⁷ La generación del milenio, tantas veces definida por su capacidad de asumir riesgos empresariales, hace poco por frenar la tendencia y puede estar contribuyendo a ella. Un reciente estudio de los datos de la Reserva Federal indica que sólo el 3,6 por ciento de los hogares estadounidenses cuyo cabeza de familia es una persona de menos de treinta años tiene participación en una empresa privada, frente al 19,6 por ciento de 1989.²⁹⁸

En los países en vías de desarrollo, la revolución digital ha hecho poco por despejar el camino empresarial de papeleo y corrupción. Mientras que en los países de la OCDE montar un negocio sólo cuesta el 3,4 por ciento de la renta per cápita, en Latinoamérica cuesta el 31,4 por ciento y en el África subsahariana un tremendo 56,2 por ciento. En Brasil un empresario tarda casi 103 días en legalizar su negocio, frente a los cuatro días de Estados Unidos y al medio día en Nueva Zelanda.²⁹⁹ Exasperados por la burocracia y la ineficiencia del Estado, muchos empresarios de países en vías de desarrollo optan por trabajar en la llamada «economía sumergida». «Hay muchas cosas que damos por supuestas en Occidente. Los registros de propiedad son exhaustivos, por ejemplo. En el Tercer Mundo, los empresarios prefieren que el gobierno no sepa que existen. Tenemos que conseguir que la identidad sea rentable», dice Hernando de Soto. De momento, permanecer en la sombra libra a esos empresarios de funcionarios entrometidos y corruptos, pero también limita mucho la capacidad de crecimiento de sus negocios y sus derechos, y convierte en «capital muerto» un dinero que podría emplearse de una manera más eficiente.³⁰⁰ Además, incluso para los que tienen negocios legales, las leyes de muchos países no permiten una responsabilidad limitada. Si nuestro negocio quiebra, cargamos personalmente con todas las responsabilidades. En muchos países árabes, si pagamos con un cheque sin fondos vamos directamente a la cárcel, sin pasar por ninguna otra institución legal.³⁰¹

Vale, sí, en el mundo siempre ha habido ricos y pobres. Hoy hay menos gente que se muere de hambre, o de malaria, o víctima de conflictos violentos. Hoy hay menos gente que vive en la extrema pobreza que en 1990.³⁰² Algunas economías emergentes se han beneficiado de la subcontratación de la producción y de la liberalización de la economía —China es un ejemplo sobresaliente de ambas cosas— y los ingresos de los ciudadanos más pobres de la mayoría de los países desarrollados han aumentado. En general, la gente vive mejor de lo que vivía, ¿no es así? ¿Qué importa, pues, que los ricos posean mucho más? ¿No deberían tener lo que han ganado con su esfuerzo? ¿Cuál es el problema?

Piketty señalaba el capitalismo. Pero el capitalismo, como sistema de organizar la economía, no es el problema. De hecho, el capitalismo es una excelente manera de crear riqueza y prosperidad para aquellos que saben usarlo. El problema es que la mayoría de la

gente nunca ha tenido la oportunidad de ver los beneficios del sistema porque la máquina tipo Rube Goldberg de las finanzas modernas ha impedido a muchos acceder a él.

El problema es la exclusión financiera y económica. El 15 por ciento de la población de los países de la OCDE no tiene relación con ninguna institución financiera, y hay países como México en los que el 73 por ciento de la población no tiene una cuenta bancaria. En Estados Unidos, el 15 por ciento de la población de más de quince años, es decir, 37 millones de estadounidenses, tampoco tiene cuenta bancaria.³⁰³

La desigualdad financiera es una condición económica que rápidamente puede convertirse en crisis social.³⁰⁴ En 2014, el Foro Económico Mundial, una organización heterogénea entre cuyos miembros se cuentan las mayores compañías y los gobiernos más poderosos del mundo, afirmó que la creciente desigualdad constituía el mayor peligro global, por encima del calentamiento global, las guerras, las enfermedades y otras calamidades.³⁰⁵ El sistema blockchain podría ser la solución. Facilitando la inclusión financiera y la creación de nuevos modelos de empresa, el mercado podría ponerse al servicio de los sueños e ideas de miles de millones de personas sin acceso a un banco.

El purgatorio de la prosperidad: un ejercicio de futilidad

Durante siglos los bancos han dependido de los efectos de red. Cada nuevo cliente, sucursal, producto, dólar que entra y que sale aumenta el valor de la red bancaria. Sin embargo, crear estas redes ha tenido su precio. Concretamente, el precio de conseguir un cliente rentable no ha hecho sino aumentar. Si el dinero de un posible cliente no rinde lo que cuesta tenerlo, el banco no estará interesado en ese dinero. En consecuencia, los bancos ven poco incentivo económico en hacer clientes en la mitad inferior de la pirámide. Según Tyler Winklevoss, los bancos no sirven a la mayoría de las personas ni tienen pensado hacerlo. Pero la nueva tecnología puede saltarse este paso. Dice: «Un montón de países africanos prescinden de la infraestructura de la telefonía fija y usan móviles. Se saltan ese paso. Donde más repercusión tendrá el sistema blockchain será en áreas donde no existen redes de pago o las que existen son precarias».³⁰⁶ El sistema blockchain dará un gran impulso a muchas iniciativas incipientes, por ejemplo a proveedores de servicios de envío de dinero por móvil como M-Pesa en Kenia, propiedad de Safaricom, y empresas de microcrédito, al hacerlas abiertas, globales y rapidísimas.

Los bancos son las entidades financieras más comunes y por eso los pondremos como ejemplo. ¿Cómo abrimos una cuenta corriente? Si vivimos en el mundo desarrollado, seguramente tengamos que ir a la sucursal en persona. En Nicaragua, sólo hay siete sucursales bancarias por cada 100.000 habitantes, frente a las 34 que hay en Estados Unidos. Nicaragua parece bien provista de bancos, comparada con muchos países africanos, donde puede haber menos de dos sucursales por cada 100.000 habitantes.³⁰⁷ O sea, que seguramente tengamos que recorrer una buena distancia para encontrar un banco. También necesitaremos llevar un documento de identidad oficial, aunque será asimismo muy difícil de conseguir si no tenemos ya uno.

En el mundo desarrollado —en Estados Unidos, digamos— necesitamos cumplir ciertos requisitos. Aunque estos requisitos varían dependiendo del banco y del estado, normalmente tenemos que hacer un ingreso de entre 100 y 500 dólares y mantener esta cantidad como saldo mínimo. También tenemos que demostrar nuestra identidad. Los bancos que operan en Estados Unidos deben cumplir estrictas normativas sobre conocimiento del cliente, antiblanqueo de dinero y financiación antiterrorista,³⁰⁸ por lo que tienen que estudiar más detenidamente los antecedentes del solicitante antes de abrirle una cuenta. En última instancia, a los bancos les interesa menos evaluar nuestro carácter que cumplir con las normas. Y esto supone una serie interminable de requisitos. Para empezar, necesitamos una tarjeta de la seguridad social. ¿Que no tenemos? Normalmente esto basta para que nos rechacen. ¿Que tampoco tenemos carné de conducir ni pasaporte? Pues nos quedamos sin cuenta corriente. Pero supongamos que tenemos las dos cosas, una tarjeta de la seguridad social y un documento de identidad. El banco, para asegurarse, nos pide una factura reciente de gas, agua o electricidad como prueba de que tenemos un domicilio permanente o algún documento que demuestre que teníamos una cuenta bancaria anterior. Si resulta que acabamos de llegar al lugar, o nos alojamos en casa de familiares, o venimos de una región del mundo en la que no hay servicios bancarios, es muy probable que no pasemos estas pruebas. El banco no nos quiere como clientes a menos que pueda confirmar nuestra identidad basándose en varias credenciales de papel. No le interesa saber si somos personas cabales. Lo que le interesa es rellenar una serie de casillas. Ya ha habido intentos de racionalizar y simplificar este proceso para inmigrantes y pobres, como el del estado de Nueva York de permitir que usen sus carnés de identidad local, pero han fracasado.³⁰⁹

El pasaporte a la prosperidad: un ejercicio de utilidad

Por suerte para los excluidos bancarios, la tecnología blockchain está creando una nueva forma de identidad financiera, que no depende de nuestra relación con un banco sino de nuestra propia reputación. En este nuevo paradigma, ya no es un requisito «tener un banco» en el sentido tradicional. En lugar de tener que pasar por las pruebas de identidad tradicionales, podemos crear una identidad digital persistente y una reputación verificable, y usarlas, parcial o totalmente, en diferentes relaciones y transacciones. El sistema blockchain da fiabilidad a la identidad digital y le permite acceder a servicios financieros. Esta prestación no tiene precedentes a una escala masiva. Joseph Lubin, de ConsenSys, dice: «Todos tenemos una reputación. Sólo que no es fácil usarla tal y como está construido el sistema social y económico. La mayor parte de esa reputación es etérea y efímera. En el mejor de los casos, está fragmentada y tenemos que volver a demostrarla con documentos en cada entidad que nos lo pide. En el peor de los casos, miles de millones de personas no tienen medio de presentar su reputación a nadie que no sea de su inmediato círculo social».³¹⁰ Lo mismo puede ser un cerdo que una vaca. Sin embargo, creando bloques básicos, podemos fabricarnos identidades digitales que no sean fragmentarias ni efímeras sino universales y estandarizadas, con fehacientes demostraciones de aspectos de nosotros mismos y de nuestras interacciones. Podemos compartir estas identidades digitales granularmente —o sea, compartir sólo información

muy concreta de nuestra identidad— para facilitar más interacciones que seguramente redundarán en nuestro propio crecimiento económico y prosperidad. David Birch, criptógrafo y teórico de las blockchains, lo resume así: «La identidad es la nueva moneda».³¹¹

Consideremos las posibilidades: las personas con poco acceso a los servicios financieros pueden emanciparse interactuando con empresas de micropréstamos. Los posibles vendedores o prestamistas pueden rastrear el uso y pago de sus préstamos, cosa antes imposible, en la blockchain, en lugar de tener que depender de calificaciones crediticias. «Una vez que una persona sin antecedentes bancarios devuelve un micropréstamo, puede empezar a pedir prestadas mayores cantidades para montar su negocio», dice Lubin.³¹² Esta conducta, repetida, hace subir la reputación del prestatario. Esto, unido al hecho de tratarse de una plataforma de pago global y segura, permite a los individuos y a los propietarios de pequeños negocios hacer algo que antes era imposible: pagar a un vendedor distante por mercancías o servicios, ampliando así sus posibilidades en la economía global. Joyce Kim reflexiona: «¿Y si pudiéramos crear un sistema de calificación crediticia para mujeres basado en su historial doméstico?».³¹³ Muchas veces los prejuicios sobre la insolvencia económica y financiera van acompañados de prejuicios de género, por lo que esta tecnología ayudará mucho a las mujeres no emancipadas del mundo. Hablando de los pobres del mundo, De Soto dice: «No es que no quieran participar en la economía global. Es que no tenemos los principios y la información necesarios para incorporarlos al sistema. La tecnología blockchain es magnífica porque nos ofrece una plataforma para que la gente se integre».³¹⁴

¿Qué podría significar esta reputación persistente para la empresa global? Si tenemos una identidad fiable, única y sólida, y se nos considera de fiar, los demás se sentirán más inclinados a permitirnos acceder al valor. Esto no es redistribuir la riqueza, sino distribuir mejor las oportunidades. Haluk Kulin, consejero delegado de Personal BlackBox, dice: «La mayor redistribución que va a producirse no será de riqueza sino de valor. La riqueza es cuánto dinero tenemos. El valor es de qué participamos».³¹⁵ Las blockchains hacen posible que todas las personas tengan una identidad única y verificable basada en su reputación que les permita participar por igual en la economía. Esta igualdad tiene profundas implicaciones. Lubin imagina un futuro en el que «las personas sin acceso o con poco acceso a los servicios bancarios se verán más y más emancipadas gracias a los micropréstamos que podrán hacer inversores de todo el mundo, quienes podrán rastrear su uso y devolución con todo detalle en una blockchain, empleando, por ejemplo, el sistema de contabilidad por partida triple de Balanc3's [una empresa de ConsenSys]».³¹⁶ En este nuevo futuro, cuando la gente devuelve sus préstamos, está en situación de pedir más préstamos y por cantidades más grandes para montar su negocio.

El camino de la prosperidad

La identidad financiera es la génesis de un amplio abanico de oportunidades financieras y económicas antes inalcanzables para más de 2.000 millones de personas en todo el mundo. La tecnología blockchain permite a gente de todas las condiciones labrarse su

prosperidad. Imaginemos una riqueza propia para mucha gente, posiblemente miles de millones de personas.

Herramientas de la abundancia: Los más elementales requisitos para participar en una economía son herramientas como *un teléfono móvil y algún tipo de acceso a internet*, el portal a través del cual interactuamos con diferentes sistemas de valor. Balaji Srinivasan, socio gerente en Andreessen Horowitz y profesor de la Universidad de Stanford, dice: «Si podemos acceder a internet con un teléfono móvil, de pronto podemos acceder a todas esas otras cosas. Podemos acceder a un banco o por lo menos al mecanismo que nos permite acceder a él».³¹⁷ La tecnología blockchain crea un conjunto de nuevos modelos de negocio antes unimaginables que nos convierte en agentes económicos.

Identidad persistente: Podemos exportar nuestra identidad a diferentes redes para establecer nuestra reputación a la hora de hacer una transacción financiera o para incorporarnos a diferentes redes sociales. De pronto, los cerdos no tienen por qué seguir siendo las huchas de las familias. Nuevas formas de pago y medios de acumular valor y comerciar con otros abrirán nuevas fronteras. Es más, este facilitar la inclusión financiera hará que para los empresarios de los países desarrollados y en vías de desarrollo sea más fácil que nunca hacer negocios, porque se podrá, entre otras cosas, habilitar un mecanismo de pago, disponer de una forma de ahorro segura y usar programas blockchain para administrar la información financiera.

Empresa democratizada: En las condiciones correctas, los empresarios son los motores del crecimiento económico de una sociedad. Aportan nuevas ideas al mercado y promueven la destrucción creativa que hace que las economías de mercado prosperen. La tecnología blockchain dota a las personas y a las pequeñas empresas de todo el mundo de muchas de las funciones y capacidades que tienen las empresas más grandes. Los archivos y registros blockchain y los contratos inteligentes facilitan la creación de una empresa, aceleran los trámites legales y ahorran papeleo, sobre todo en los países en vías de desarrollo, donde se tarda tres veces más en constituir una empresa y cuesta cinco veces más.

Con archivos seguros e inmutables, los empresarios podrán registrar sus negocios y títulos de activos de la empresa, administrar existencias, llevar debes y haberes y hacer otros cálculos financieros gracias a los programas de contabilidad por partida triple y otras aplicaciones de blockchain, lo que les permitirá prescindir de auditores, asesores fiscales y otros vendedores que salen muy caros a las pequeñas empresas.³¹⁸ Los reguladores podrían dar una tregua a las pequeñas empresas para que optaran por el sistema de contabilidad por partida triple. Eso les ahorraría tiempo y dinero. Conforme la empresa crezca, será menos complejo conciliar sus acciones con la documentación. Gracias a los contratos inteligentes, un empresario podría automatizar muchos aspectos del funcionamiento de una empresa: órdenes de compra, pago de nóminas, intereses de deudas y auditorías financieras en tiempo real. Tendrán éxito dos nuevos modelos para la empresa individual:

VENDER CAPACIDAD SOBRANTE. Desde la economía colaborativa centralizada hasta la economía medible distribuida, podremos alquilar las camas que nos sobren, carretillas, bueyes y otros bienes tangibles e intangibles en una red de iguales basada en la reputación. El sistema blockchain hace posibles fuentes de ingresos antes imposibles, como alquilar wifi, electricidad generada por paneles solares instalados en los tejados, suscripciones a Netflix, capacidad procesadora inutilizada de nuestro móvil y otros aparatos domésticos, todo mediante micropagos y contratos inteligentes. Las blockchains son un nuevo servicio para que las personas creen valor y ganen dinero por medios no tradicionales.

MICRORRENTABILIZAR LA INFORMACIÓN. Los padres que desempeñan tareas domésticas y los miembros de la familia que cuidan incansablemente de hijos pequeños y de padres ancianos pueden por fin rentabilizar sus esfuerzos y ser reconocidos por el valor que producen a todas las horas del día. Esta oportunidad no es exclusiva del mundo desarrollado. Las grandes compañías buscan maneras de comercializar sus productos en el Tercer Mundo, pero muchas veces carecen de la información necesaria para tomar decisiones. Vender información personal podría ser una fuente de ingresos para un joven empresario que está lanzando su nueva oferta pública de venta en una blockchain. Hoy, grandes compañías digitales como Facebook o Google acumulan petabytes de información sobre miles de millones de personas. Es un pacto fáustico en el que damos información a cambio de bonitos servicios, pero perdemos privacidad e integridad de información. Las blockchains convierten a los consumidores en *prosumidores*. Nike podría querer saber lo que desayunamos, cuántas veces salimos a correr y si estamos pensando en comprar ropa y material para hacer ejercicio. ¿Por qué no venderle a Nike esa información a cambio de puntos o de dinero? Vayamos un poco más allá: las compañías de seguros buscan la mejor información para hacer cálculos actuariales. Nuestra información —cuánto ejercicio hacemos, si fumamos o no, lo que comemos— les es muy valiosa. Podemos llegar a un acuerdo según el cual cada vez que usen nuestra información para hacer uno de esos cálculos y poner precio a un nuevo producto, recibamos un micropago.³¹⁹

Inversión y propiedad distribuida

Estamos entrando en un periodo de la historia humana en el que muchísima gente puede convertirse en propietaria de riqueza gracias a la tecnología de registros distribuidos. Permitir el acceso a los mercados financieros mundiales y, en consecuencia, a las oportunidades de inversión, desde inversiones convencionales hasta la participación en empresas colaborativas masivas, pasando por sistemas de micropréstamos, ofertas públicas de venta en blockchain y micropréstamos basados en la reputación, dará acceso al capital. El micromecenazgo está ya cambiando la faz de las finanzas. En 2012 las campañas de micromecenazgo sin blockchain recaudaron 2.700 millones de dólares en todo el mundo, un 80 por ciento más que en el año anterior. Con sistemas directos de micromecenazgo basados en blockchain es muy probable que estas cifras se multipliquen. Las personas pueden contribuir con pequeñas cantidades de dinero en campañas de

mecenazgo. Imaginemos una campaña en la que participen un millón de personas que den un dólar cada una. Llamémosle «propiedad distribuida». ¿Que no tiene sentido, dirá el lector? Augur, la plataforma de mercados de predicción recaudó millones de dólares con pequeñas contribuciones de miles de personas. Las posibilidades son muchas. Las ofertas públicas de venta hechas con blockchain no sólo pueden mejorar la recaudación de dinero y reducir los costes del que las emite, sino también ser ampliamente inclusivas, permitiendo que grupos de inversores en expansión que antes no habrían podido participar ahora puedan hacerlo. Hasta la fecha las propuestas para reducir la disparidad de ingresos y riqueza no han ido más allá de subirles los impuestos a los ricos y, como medida más extrema, directamente la expropiación por el Estado. En lugar de redistribuir y expropiar riqueza, pensemos cómo el sistema blockchain puede crear oportunidades para repartir más equitativamente la riqueza que la sociedad crea.

Giros postales: la historia de Analie Domingo

Analie Domingo³²⁰ lleva trabajando de niñera y criada veinticinco años. Es una de las más de 200.000 personas nacidas en Filipinas que viven en Toronto³²¹ y su historia es típica: emigró de Filipinas siendo joven y se estableció en Canadá sin dinero, sin estudios y sin apenas conocer su país adoptivo. Analie ha trabajado muy duro y se ha hecho una vida para sí misma y para su familia. Hace diez años, empleó sus ahorros en pagar la entrada de una casa, algo muy meritorio dado que había estado enviando puntualmente dinero a su familia en Filipinas los trescientos meses anteriores. Analie envió a su casa tanto dinero que su madre, ahora septuagenaria, pudo comprarse una casa propia en Manila.

Analie tiene la bondad de quedar con nosotros el día en que le pagan para documentar su experiencia. La tarde del viernes, Analie recibió su cheque, extendido por su patrono, y se dirigió al banco del lugar. Esto le llevó quince minutos; veinte si contamos lo que esperó en la cola del cajero. Tras ingresarlo, sacó 200 dólares canadienses. Con el dinero contante y sonante, caminó una manzana para coger un autobús municipal. En lugar de dirigirse a su casa, recorrió más de tres kilómetros en sentido contrario y se apeó en lo que sólo puede ser descrito como un mal barrio. Anduvo otras cuatro manzanas y por fin llegó a la «institución financiera» con la que enviaba el dinero: una ventanilla de iRemit al fondo de un bloque de viviendas del barrio de St. James Town, uno de los más pobres y peligrosos de Canadá. Como muchas de las personas que usan los servicios de iRemit no tienen cuenta bancaria, la empresa ha empezado a ofrecer otros servicios financieros, como el de pagar cheques. Analie rellena el formulario, como ha hecho cientos de veces antes, y entrega su dinero, tan duramente ganado. Por un giro postal de 200 dólares, Analie paga una tarifa plana de 10 dólares. Para retirar el dinero en el banco de destino, su septuagenaria madre tiene que pegarse otra agotadora (e igualmente absurda) caminata, no sin antes, claro está, esperar tres o cuatro días, que son los que tardan de media estos pagos en ser procesados. Analie volvió a la parada de autobús, cogió el autobús, luego el metro, luego otro autobús y, por fin, una hora después, llegó a su casa.

El coste de enviar ese giro, 10 dólares, equivale al 5 por ciento del valor total. Además, suele haber una diferencia en la tasa de cambio del 1 o 2 por ciento. Este 7 por ciento aún supone una ligera rebaja respecto de la media internacional, que es del 7,68 por ciento.³²² El hecho de que madre e hija tengan cuenta bancaria y aun así hayan de pasar por todo el proceso hace más notorio lo absurdo del procedimiento. El coste en efectivo no refleja el coste total. Por ejemplo, el valor de las dos horas que Analie perdió en la operación equivale a otros 40 dólares, según su sueldo. Además, tiene que dejar el trabajo antes porque no se siente segura yendo al barrio de noche. Para su madre, una mujer de setenta años que vive en Manila, el coste físico de hacer todo el viaje para retirar el dinero también es relevante. El poder adquisitivo de los 10 dólares que Analie pierde por hacer el giro es importante para ella, pero lo es aún más para su madre. Mientras que en Canadá 10 dólares es lo que cuesta una comida y un billete de autobús, en Manila se podría comprar comida para toda una semana. En toda su vida, Analie ha pagado miles de dólares a intermediarios como Western Union por enviar dinero a su casa. Cada comisión mensual contribuye a un tesoro de 38.000 millones de dólares que se pagan anualmente por girar dinero.³²³

Girar dinero a sus países de origen por parte de personas que viven en lugares distantes conecta a las diásporas globales. Las diásporas son comunidades formadas por personas que han abandonado la tierra de sus antepasados y se han dispersado por todo el mundo pero comparten la cultura de su tierra natal y se sienten fuertemente identificadas con ella.

Una de las funciones de muchas diásporas de hoy es contribuir a solucionar problemas comunes globales. Los giros de dinero representan uno de los más cuantiosos flujos de capital que reciben los países en vías de desarrollo y pueden tener un efecto enormemente positivo en la calidad de vida de algunas de las personas más vulnerables del mundo. En algunos países este dinero es un componente vital de la economía. En Haití, por ejemplo, el dinero que se recibe por este medio constituye el 20 por ciento del PIB. Los filipinos reciben 24.000 millones de dólares todos los años en forma de giros postales, el 10 por ciento del PIB.³²⁴ Según el Fondo Monetario Internacional (FMI), los que reciben ese dinero lo gastan principalmente en productos de primera necesidad, comida, ropa, medicina y vivienda, con lo que el dinero girado «contribuye a sacar a mucha gente de la pobreza al permitir mayores niveles de consumo de los que serían posibles sin él».³²⁵ Se estima que el capital que se envía a los países en vías de desarrollo es tres o cuatro veces mayor que el que reciben en concepto de ayuda extranjera.³²⁶ Los efectos positivos que tienen los giros de dinero en los pobres de los países en vías de desarrollo son fáciles de entender, y, sin embargo, pese a esta enorme inyección económica, los costes de girar dinero siguen siendo altísimos. En algunos de los canales entre naciones más caras las comisiones pueden llegar al 20 por ciento.³²⁷

Canadá es uno de los países en los que más dinero se envía de esta forma. En Ontario, la provincia más poblada y la más importante económicamente, 3,6 millones de personas han nacido en el extranjero y todos los años miles de millones de dólares salen de la provincia en forma de giros postales.³²⁸ La historia de Analie es digna de mención porque es normal en Canadá.

Pensemos en el centro comercial de Dufferin Mall, también en Toronto. La mayoría de los días hay un tráfico constante y el centro comercial se parece a cualquier otro de Canadá o de Estados Unidos. Pero los jueves y los viernes a las cinco de la tarde ocurre algo muy diferente. Con los cheques de la paga en mano, miles de canadienses nacidos en el extranjero acuden al centro a enviar dinero desde los diversos bancos y agencias de cambio a sus familiares necesitados de sus países de origen. Una especie de industria casera de agencias de cambio y sucursales de Western Union ha brotado en tiendas, bares y restaurantes de la zona para dar respuesta a la demanda.

En autobús, tranvía o metro, cargados con niños y agotados tras un largo día, torontinos que hablan filipino, cantonés, español, punjabi, tamil, árabe, polaco y otras lenguas llegan al centro comercial y hacen largas colas para poder enviar a casa su dinero duramente ganado. Esos días, casi todos pasan el rato hablando por WhatsApp o por Skype con familiares y amigos de Toronto y del extranjero, jugando o mirando vídeos con sus teléfonos móviles inteligentes. Este dinero suele tardar más de una semana en llegar a su destino, donde alguien tiene que pasar por un proceso parecido, igualmente tedioso, para retirarlo.

¿Qué tiene de malo este sistema? Prácticamente todo. Veamos lo mejor. Recordemos una cosa: la mayoría de las personas que hacen cola tiene teléfono móvil inteligente, una tecnología que se ha generalizado en Canadá y cada vez es más usada en todo el mundo. El 73 por ciento de los canadienses tiene un teléfono móvil inteligente y en Toronto el número es, sin duda, más alto. El país posee una de las mejores infraestructuras de redes inalámbricas del mundo, lo que supone no sólo que la mayoría de los canadienses posee un teléfono móvil inteligente (que es, en realidad, un superordenador), sino que pueden usarlo para aprovechar el poder de la red móvil de una manera que habría parecido ciencia ficción hace dos décadas. ¿Por qué hace esa gente cola para enviar dinero desde un punto de venta físico usando una tecnología de hace décadas en lugar de emplear lo que tiene al alcance de las yemas de los dedos? Los dólares pesan mucho menos que los vídeos de alta definición. De hecho, según Skype, las llamadas de vídeo consumen unos 500 kilobits por segundo.³²⁹ Enviar un bitcoin emplea unos 500 bits, es decir, ¡más o menos una milésima parte de lo que consume un segundo de vídeo de Skype!

Como prescinden de los intermediarios tradicionales y simplifican drásticamente los procesos, las blockchains permiten pagos instantáneos y fáciles, para que las personas no tengan que hacer colas durante una hora o más, recorrer grandes distancias ni aventurarse a ir a barrios peligrosos de noche para enviar dinero. Hoy, muchas empresas y organizaciones recurren al protocolo bitcoin para reducir los costes de girar dinero. Su idea es poner miles de millones de dólares en manos de las personas más pobres del mundo. Estas industrias han estado controladas por un puñado de empresas que han utilizado su posición única y la infraestructura heredada para crear monopolios. Pero también ven el riesgo que supone esta tecnología y tienen miedo. Según Eric Piscini, que dirige el grupo de criptomoneda de Deloitte, las empresas del sector del pago «están muy nerviosas por lo que el sistema blockchain supone para ellas. A Western Union,

MoneyGram, iRemit y otras les preocupa mucho que su modelo de negocio se vea puesto en cuestión».³³⁰ Y es lógico, porque hay una industria emergente de empresas nuevas y revolucionarias que quiere reemplazarlas.

¿Qué pasa con Analie?

Hay dos obstáculos principales para la creación de una red de pago basada en el sistema blockchain que sirva a los pobres del mundo. El primero es que muchas de las personas que envían dinero cobran en efectivo y los que lo reciben viven en una economía basada, predominantemente, en dinero en efectivo. Segundo, la mayoría de las personas de los países, tanto desarrollados como en vías de desarrollo, carecen de los conocimientos y de las herramientas para usar blockchain de una manera efectiva. Aunque el dinero contante y sonante puede pasar ya a la historia, hasta que los patronos empiecen a enviar dinero a carteras inteligentes en el mundo desarrollado, y los pequeños comerciantes callejeros de Manila, Puerto Príncipe o Lagos empiecen a aceptar pagos digitales, seguiremos necesitando monedas fuertes. Western Union lo sabe y por eso sigue siendo relevante hoy día, con más de «500.000» agentes en todo el mundo.³³¹ Si lo que queremos es convertir nuestro giro en dinero en efectivo, las opciones son limitadas. Western Union no funcionaría si sólo tuviera un agente. Su red le ha permitido mantener una posición de monopolio durante décadas. Ha habido pocas empresas, quizá ninguna, que hayan dispuesto de una tecnología «asesina» segura y fácil de usar. Hasta ahora.

Porque ahora existe Abra y otras empresas por el estilo. Con un nombre como Abra, uno esperaría ver un poco de «cadabra», y la empresa no decepciona. Abra está creando un sistema de gestión de activos digitales global en la blockchain bitcoin. Su misión, según dicen, es convertir todos los teléfonos móviles inteligentes en cajeros que den dinero en efectivo a cualquier otro miembro de la red. Quisimos ver si esta solución mejoraba la experiencia de Analie.

Analie y su madre se descargaron la aplicación en sus móviles Android. Analie empezó con un saldo en dólares canadienses. Pulsando una tecla, Analie transfirió dinero a su madre, que lo recibió casi instantáneamente, en pesos. Ésta tenía entonces la posibilidad de guardar ese dinero en su móvil en forma de depósito de valor e ir gastándolo en comercios que aceptan el sistema de Abra como sistema de pago, que cada vez son más. Al crear un mecanismo de pago y de almacenamiento de valor, Abra sustituye a los bancos en lo que son sus dos funciones más importantes: pagar y almacenar valor. Esto ya es por sí solo algo revolucionario, pero lo realmente interesante viene ahora: la madre de Analie quiere dinero en efectivo. Paga el alquiler, compra comida y gestiona prácticamente todos los demás gastos con dinero en efectivo. Mira la aplicación y ve que hay otros cuatro usuarios de Abra en un radio de cuatro de manzanas. Les escribe preguntándoles quién quiere cambiarle sus pesos digitales por pesos reales y a qué precio. Los cuatro contestan con diferentes «ofertas» por sus servicios. Uno se los cambia por una comisión del 3 por ciento, otro del 2 por ciento y los otros dos del 1,5 por ciento. La madre de Analie decide quedarse con el «cajero» del 2 por ciento, no porque sea el más barato, sino porque esa persona tiene una valoración de cinco estrellas y está

de acuerdo en quedar con ella a medio camino. Se encuentran, ella cambia sus pesos Abra por pesos contantes y sonantes, el cajero cobra su comisión y los dos se van tan contentos. Abra se lleva una comisión del 0,25 por ciento en la conversión.

Todo el proceso, desde que el dinero sale de Toronto hasta que llega al receptor convertido en dinero en efectivo, tarda menos de una hora y cuesta un 0,25 por ciento, incluyendo las tasas de cambio y todos los demás costes transaccionales. Mientras que las transacciones de Western Union requieren hasta siete u ocho intermediarios —bancos, Western Union, agentes y otros—, las transacciones Abra sólo requieren tres: dos usuarios y la plataforma Abra. «Ahora lo entiendo. ¡Qué bueno!», dijo Analie, eufórica.³³²

Para que Abra prospere a escala mundial, debe hacer frente a dos retos fundamentales. El primero es que la red necesita una masa crítica de «cajeros» para que el servicio sea útil. La madre de Analie no lo usaría si el cajero más cercano estuviera a 30 kilómetros. Abra lo sabe y está registrando cajeros —según el último cómputo, varios miles sólo en Filipinas— que están dispuestos a vender y comprar cuando la cosa se ponga en marcha. El segundo es que el modelo sólo funcionará si cajeros y clientes cumplen con sus compromisos cuando transfieren moneda digital a cambio de moneda real. Esto no es un problema. Negocios como Airbnb, Lending Club o Zipcar han acabado con el mito de que las personas no confían unas en otras. Es más, el asombroso incremento del número de empresas de la llamada economía colaborativa convenció, por ejemplo, al consejero delegado de Abra, Bill Barhydt, de que no era un problema. «La gente está más dispuesta a confiar en personas que en instituciones», dice.³³³

El teléfono móvil inteligente es fundamental en todo esto. Del mismo modo que nos permite alquilar nuestro apartamento, o nuestro coche, o transportar a alguien, también podemos usarlo como un cajero automático. Barhydt dice: «Es sorprendente lo que la gente está dispuesta a hacer en un modelo de economía colaborativa y aún no hace con dinero, a excepción, quizá, de los préstamos entre iguales». Además, añade, «para nosotros es más importante que las personas confíen unas en otras, que no que lo hagan en Abra. Si confiamos unos en otros, es muy probable que acabemos conociendo Abra, que nos guste y tengamos una buena experiencia», y, en última instancia, que confiemos en la plataforma.³³⁴

Abra no es una aplicación para girar dinero sino una nueva plataforma global para intercambiar valor que combina por igual el sistema blockchain, que es distribuido y no exige que confiemos en él, la tecnología de la telefonía móvil inteligente y la inclinación propiamente humana a confiar en nuestros iguales en una red. Como ofrece a los usuarios la posibilidad de almacenar valor en monedas tradicionales, transferir valor por la red y pagar a los miembros de una creciente red comercial, Abra no sólo le hace la competencia a Western Union, sino también a las empresas de tarjetas de crédito como Visa. Según Barhydt:

El sistema de pago de una transacción de Western Union y el de una transacción de Visa son muy diferentes. Pero el sistema de pago de una transacción de Abra entre dos personas, y el de una persona y un comerciante, son exactamente el mismo... Hemos creado una solución única que funciona dentro de las fronteras de un país

y fuera de ellas, y que, por primera vez, puede ser usada para hacer pagos entre personas y entre personas y comerciantes.³³⁵

Abra podría llegar a ser una gran empresa global que sacudiera los cimientos de las mayores instituciones financieras del mundo. Pero de momento es una solución elegante y sencilla a un importante problema global. Teniendo en cuenta que el dinero que se girará el año que viene ascenderá a medio billón de dólares, la oportunidad de mercado no es nada desdeñable.

Las blockchains y la ayuda humanitaria

¿Puede el sistema blockchain transformar radicalmente la manera como las ONG, gobiernos y donantes particulares ofrecen ayuda extranjera? Cientos de miles de millones de dólares de ayuda afluyen anualmente a los países en vías de desarrollo, pero los efectos macroeconómicos de esa ayuda no siempre están claros.³³⁶ Hay pruebas evidentes de que funcionarios corruptos, tiranos locales y otros intermediarios se quedan gran parte de esa ayuda antes de que llegue a sus destinatarios legítimos. Y, lo que es más inquietante, según el *Journal of International Economics*, «aumentar los ingresos del Estado puede hacer descender la prestación de servicios públicos». El informe concluye que «grandes desembolsos de dinero en forma de ayuda gratuita no conducen necesariamente a un mayor bienestar».³³⁷ La demasiada administración y la corrupción política se combinan para provocar grandes pérdidas y mayor disparidad entre ricos y pobres en los países más desfavorecidos. Así ocurre en el caso de la ayuda directa entre gobiernos, pero también en el caso de las ONG que trabajan sobre el terreno en países pobres.

Hablamos brevemente de la ayuda extranjera en la introducción. Tratemos el tema con más detenimiento. Recordemos que la Cruz Roja fue muy criticada tras el terremoto de Haití de 2010 cuando se supo, por un estudio de ProPublica, una agencia de noticias independiente y sin ánimo de lucro, y por National Public Radio, que dicha organización malgastó fondos y no cumplió con muchos de sus compromisos, como el de construir 130.000 casas. Sólo construyó seis.³³⁸ En su defensa, la Cruz Roja alegó que el registro de propiedad de la tierra del país era deficiente y que eso dificultó su tarea: no se sabía quién era propietario real de la tierra. En consecuencia, la Cruz Roja improvisó una solución aún menos deseable. ¿Podría mejorar la situación un registro de propiedad basado en el sistema blockchain que aclarase los derechos de propiedad y evitara expropiaciones ilegales?

La ayuda extranjera es quizá el ejemplo más claro de la ineptitud de muchos gobiernos y de la codicia de funcionarios sin ética, y por eso constituye un terreno excelente para explorar soluciones basadas en las blockchains. El terremoto de Haití de 2010 fue una de las crisis humanitarias más devastadoras de los últimos cien años.³³⁹ Mientras que el gobierno se paralizaba y la crisis se recrudecía, miles de «voluntarios digitales» se ofrecieron por internet para ayudar a los que primero respondieron a recoger, seleccionar y visualizar peticiones de ayuda hechas desde los teléfonos móviles de los haitianos afectados. Estos grupos de voluntarios, que al principio se formaron

espontáneamente en internet, fueron organizándose y resultaron muy eficientes. Uno en concreto, CrisisCommons, destacó especialmente. CrisisCommons es un ejemplo de solución global, una red no gubernamental de organizaciones de la sociedad civil, empresas e individuos que colaboran para resolver un problema. La revolución digital ha permitido que nuevas redes se conecten y colaboren más allá de las fronteras, y puede resolver problemas y facilitar la cooperación y el gobierno globales. Internet posibilita todo esto. Nunca antes pudo la gente organizarse colectivamente para crear un bien público como lo hizo en Haití. Esta fuente de información de internet se reveló de vital importancia, porque facilitó conexiones, conocimientos y datos tanto a las personas necesitadas como a los voluntarios y a las organizaciones. Imaginemos que hubiera también una fuente de valor. ¿Qué posibilidades no ofrecería eso?

Las blockchains pueden mejorar la gestión de la ayuda extranjera de dos maneras. Primero, al prescindir de intermediarios que manejen la transferencia de grandes sumas de dinero, puede reducir el problema crónico de malversación y robo. Segundo, siendo como es un registro inmutable del flujo de capitales, obliga a las instituciones, de organizaciones humanitarias a gobiernos, a actuar con integridad y cumplir con sus compromisos. Si no lo hacen, la gente podrá ver sus malas acciones y pedirles cuentas de ellas.

Podemos imaginar fácilmente que Unicef o la iniciativa de la ONU en favor de las mujeres use el sistema blockchain para ayudar directamente a las éstas y a los niños sin necesidad de pasar por las estructuras del poder local. Personas de países pobres podrían solicitar ciertos beneficios a través de un registro distribuido, administrado por una red de diversos grupos de ayuda que actuaran como nodos de la red. Cuando una ayuda se entrega —por ejemplo, vacunas de la Cruz Roja o material escolar de Unicef—, estas «transacciones» se hacen constar con fecha y hora en el registro. Esto reduciría e incluso eliminaría el riesgo de que las organizaciones humanitarias gastaran por partida doble en determinadas personas o comunidades, con lo que los beneficios de la ayuda serían más extensivos y equitativos.

De hecho, Unicef ha empezado a explorar el terreno de las criptomonedas. En junio de 2015 anunció el lanzamiento de Unicoín, una moneda digital que los niños pueden «minar» enviando un dibujo al programa. Las monedas se cambian entonces por un cuaderno y un lápiz.³⁴⁰ Es un modesto comienzo, pero las oportunidades son ilimitadas. No cuesta imaginar la hipótesis que planteábamos en el primer capítulo: orfanatos de pueblos de todos los países en vías de desarrollo trabajando con Unicef para abrirles una cuenta a los niños que vayan llegando. Las donaciones pueden prorratearse entre las cuentas personales de los niños. Gobiernos, caudillos y demás funcionarios corruptos simplemente no podrían acceder a ellas. Los niños más pobres y vulnerables del mundo tendrían dinero para empezar una vida cuando llegaran a adultos. Esto es posible con el sistema blockchain.

La ayuda por catástrofes naturales o contra la pobreza no puede brindarse siempre de persona a persona, claro está. Muchas veces las instituciones no sólo son deseables sino también fundamentales. Pero las blockchains pueden aumentar radicalmente la transparencia con la que esas organizaciones, y otras instituciones de la cadena de valor

de la ayuda extranjera, funcionan. Todos y cada uno de los dólares donados a la Cruz Roja podrían seguirse desde su origen hasta las personas que los reciben, a través de toda la cadena de valor. Recordemos la hipótesis que formulábamos en el primer capítulo: la Cruz Roja podría lanzar campañas de micromecenazgo para sus más importantes iniciativas, como prestación de ayuda médica, lucha contra la propagación de enfermedades, purificación del agua, reconstrucción de casas, y cuando donáramos, sabríamos si nuestro dólar se ha empleado en comprar una tabla, una tirita o en producir un litro de agua potable. Si el dinero se pierde, la comunidad lo sabría y podría pedir explicaciones a las organizaciones en cuestión. Podrían usarse contratos inteligentes que pidieran cuentas a las mismas organizaciones humanitarias. El capital dedicado a proyectos mayores —desde programas de vivienda hasta sistemas de purificación de agua— podría guardarse en una cuenta de plica y usarse conforme fueran completándose determinadas etapas, como la adquisición del título de propiedad de un terreno, la importación de materias primas, la firma de un contrato con un proveedor local, la construcción del producto final, la instalación de un número determinado de puntos de acceso al agua potable, etc. ¿El resultado? Una transparencia y una responsabilidad mucho mayores en la gestión de la ayuda extranjera y, por lo tanto, una considerable mejora de los resultados.

La ayuda extranjera es la segunda forma más importante de transferencia de capital de los países desarrollados a los países en vías de desarrollo, después del giro postal. La tecnología blockchain puede aumentar la transparencia, la responsabilidad y la capacidad de acción de las ONG bienintencionadas, así como mejorar la prestación de servicios vitales en tiempos de crisis y en circunstancias normales. Naturalmente, hay muchos problemas que hay que solucionar. Las personas implicadas tendrán que saber usar esta tecnología. Las redes de telefonía móvil pueden fallar en medio de una crisis. Siempre puede haber delincuentes astutos y gobiernos corruptos que hallen los medios de engañar a los pobres y desvalidos. Pero ¿son éstos motivos para no explorar esta tecnología? No. Las cosas hoy no funcionan bien y en muchos casos funcionan muy mal. Capacitar a la gente y poder pedir cuentas a las organizaciones humanitarias significará poner más ayuda en las manos de las personas correctas. Aliviar la pobreza y responder debidamente a las catástrofes es el primer peldaño de la escalera de la prosperidad global. Aprovechemos la oportunidad que nos brindan las blockchains.

La microfinanciación: ayuda igualitaria con picopagos

La microfinanciación es una industria que va más allá tanto de los servicios financieros como de la ayuda al desarrollo. En lugar de prestar ayuda de arriba abajo, las instituciones microfinancieras (MFI, por sus siglas en inglés) intentan capacitar a las personas para que puedan ahorrar, invertir y montar pequeños negocios. La mayoría de las veces adoptan la forma de cooperativas de ahorro comunitarias cuyos miembros reúnen un fondo común y se prestan unos a otros para subvenir a necesidades a corto plazo. Si se administran bien,

las organizaciones microfinancieras pueden ser de gran ayuda para comunidades en apuros: reducen el hambre crónica, estimulan el ahorro y la inversión y, en muchos casos, dan oportunidades a las mujeres.³⁴¹

Con todo, las MFI presentan hoy día algunos problemas: en primer lugar, hay poco control sobre su funcionamiento y a veces permiten préstamos abusivos y métodos de amortización coercitivos, que ahogan más a las comunidades. En segundo lugar, y a consecuencia de esto, los gobiernos de los países en vías de desarrollo han creído que la mejor manera de combatir la mala conducta es ilegalizar o restringir todas las MFI, como ocurrió en la India en 2010 a raíz de una controversia con una de ellas.³⁴² En tercer lugar, el dinero no siempre acaba en las manos debidas. No hay manera de garantizar que el dinero va al miembro de la comunidad que más lo necesita. En cuarto lugar, las MFI siguen siendo en gran parte regionales, lo que limita el capital y las oportunidades de inversión y ahorro.

Así que la gente que trabaja ayudando a los pobres se preguntará: ¿cómo encaja el sistema blockchain en el conjunto de las herramientas? ¿Cómo puede mejorar lo que estamos haciendo?

Para empezar, aumentará la responsabilidad administrativa. Como ocurre con la transparencia empresarial, los donantes también se sentirán atraídos por cualquier organización sin ánimo de lucro que use el sistema blockchain para aumentar la transparencia y la responsabilidad. Además, si los micropréstamos quedan registrados en una blockchain y a los clientes de una MFI se les permite acceder a esos registros, dichos clientes pueden pedir cuentas a esas organizaciones por su mala conducta. ¿Qué posible prestatario u ahorrador elegirá lo opaco y borroso cuando puede escoger lo abierto y transparente?

En segundo lugar, puede contribuir a una mejor protección de mujeres y niños. A través de contratos inteligentes, se puede ingresar dinero en cuentas de plica a las que sólo tengan acceso las mujeres, que así podrán comprar comida, productos femeninos, cuidados sanitarios y otros artículos de primera necesidad. Los hombres no podrán quitarles el dinero para comprarse tabaco, irse de juerga ni jugar, lo que puede ser un problema persistente con dinero procedente de ahorros o microfinanciación.

En tercer lugar, permitirá a la gente buscar capital y oportunidades en todo el mundo, y atraerá a donantes de todo el globo. Las comunidades suelen verse reducidas a la geografía de la MFI que usan. En el futuro, un posible prestatario podría entrar en internet, buscar los prestamistas con mejor valoración, mejores condiciones y mejor reputación y elegir la mejor oferta. Las MFI tradicionales seguirán existiendo, claro está, pero habrá mejores formas de conectar a las personas gracias a las blockchains, con lo que aquéllas serán cada vez menos necesarias.

Por último, los canales de pago de blockchain, como bitcoin, están hechos para prestatarios modestos y sin derechos, porque permiten pagos pequeños («picopagos», como los llamamos nosotros) y reducen los costes casi a cero. En un mundo en el que cada céntimo cuenta, los usuarios deberían poder devolver préstamos, retirar fondos y ahorrar en pequeñas cantidades, todo lo cual era mucho más difícil en el mundo anterior a

las blockchains. También deberían poder hacerlo instantánea y eficientemente, dado que, pese a la extrema pobreza en la que viven en muchas partes del mundo, la telefonía móvil y el acceso a internet están convirtiéndose en artículos de consumo masivos.

Cómo asegurar la propiedad de activos

Registrar propiedades de tierras es lo que Hernando de Soto llama transacciones no comerciales, intercambios económicos en los que generalmente interviene un gobierno local. Los costes de las transacciones no comerciales incluyen los recursos gastados haciendo colas, localizando títulos de propiedad, rellenando formularios, cumplimentando trámites, resolviendo disputas, untando a funcionarios e inspectores y demás.³⁴³ Estos costes son enormes en economías pobres con sistemas débiles y funcionarios estatales conocidos por obrar sin integridad. Honduras es una de estas economías y el segundo país más pobre de Centroamérica, con una distribución de la renta tremendamente desigual. La crisis económica de 2008 redujo la afluencia de dinero en forma de giro postal y un golpe militar derrocó al democráticamente elegido Manuel Zelaya en 2009. El golpe fue apoyado por uno de los mayores terratenientes de la región, un magnate del aceite de palma que se benefició considerablemente de anteriores expropiaciones de tierra que obligaron a los campesinos de Aguán a vender sus títulos de propiedad.³⁴⁴

Desde mediados de los años noventa del pasado siglo, el Banco Mundial y una serie de ONG mundiales³⁴⁵ han inyectado 125,3 millones de dólares, acompañados de asesoramiento técnico, en Honduras para diseñar y llevar a cabo proyectos de desarrollo agrícola que acelerarían el crecimiento del país.³⁴⁶ Nos encontramos con planes de creación de infraestructuras que permitirían «geoetiquetar» información sobre la propiedad y el uso de la tierra y los recursos naturales, los riesgos climáticos y naturales y las condiciones socioeconómicas, información que los municipios podrían usar para diseñar planes estratégicos y de inversiones. También se hablaba de integrar bases de datos de proyectos agrícolas con bases de datos de proyectos de gestión de desastres y medioambiental a nivel local y nacional.³⁴⁷ Todo muy ambicioso.

El problema es que sigue habiendo sospechas de corrupción generalizada en los registros de propiedad, ventas de tierras y resolución de disputas, y acusaciones contra intermediarios, jueces y burócratas locales. Según la Oficina del Representante del Comercio de Estados Unidos, el sistema de registro de la propiedad sigue siendo muy poco fiable.³⁴⁸ Los hogares de las zonas rurales quedaron sistemáticamente excluidos del registro de títulos de propiedades inmuebles, que son sus activos más valiosos, porque el gobierno limitó la jurisdicción del Banco Mundial a las áreas urbanas. En las zonas rurales, los campesinos, desposeídos de su dinero, se beneficiaron poco de los programas de administración de la tierra. La pobreza rural no ha decrecido en Honduras desde 1998. La inseguridad y la corrupción campan a sus anchas en el mundo desarrollado cuando surgen conflictos sobre títulos de propiedad. Si Honduras sufriera un desastre natural como el de Haití de 2010, las organizaciones humanitarias como la Cruz Roja quedarían paralizadas ante el caos de la propiedad y no podrían ofrecer vivienda segura y duradera.

«¿Y si hubiera un registro universal que incluyera toda esa información y al que pudiéramos recurrir en situaciones poco fiables? El sistema blockchain parece especialmente adecuado para gestionar transacciones, como ningún otro sistema lo es — dice De Soto—. El hecho es que los países pobres son por naturaleza muy corruptos, y por eso disponer de un registro de transacciones en cada nodo con procedimientos seguros hace que el sistema sea eficiente, barato y rápido, pero también es lo que quieren los pobres porque protege sus derechos», añade.³⁴⁹ Así funciona: una blockchain es un registro abierto, lo que significa que pueden verlo en las pantallas de sus ordenadores los funcionarios hondureños que necesiten consultarlo, y en sus dispositivos móviles los trabajadores que introduzcan información, y los ciudadanos que quieran tener una copia. Es un registro distribuido, lo que significa que cualquiera puede acceder a él. En jurisdicciones como Honduras, en las que la confianza en las instituciones públicas es baja y los sistemas de derechos de propiedad precarios, la blockchain bitcoin podría contribuir a devolver la confianza y rehabilitar la reputación.

Eso es lo que la empresa emergente con sede en Texas, Factom, piensa hacer en colaboración con el gobierno de Honduras y Epigraph, una empresa de programación dedicada a los títulos de propiedad. El presidente de Factom, Peter Kirby, dice: «La base de datos del país estaba pirateada, por lo que los burócratas podían entrar y adjudicarse propiedades en primera línea de playa». Añade que el 60 por ciento de la tierra del país está indocumentado. El propósito del proyecto, que aún no se ha firmado definitivamente, es registrar los títulos de propiedad de tierras del Estado en un archivo blockchain. Kirby le dijo a Reuters que Honduras podía prescindir de los sistemas tradicionales usados en los países desarrollados aplicando la tecnología blockchain, lo que haría que las hipotecas y los derechos de explotación de minerales fueran más seguros.³⁵⁰ «La documentación relativa a la propiedad, desde patentes hasta casas, está basada fundamentalmente en el papel, y no hay razón para que sea así, aparte de razones históricas. El sistema blockchain funciona con cualquier transacción o interacción en la que los derechos de propiedad y los plazos sean importantes»,³⁵¹ dice Kausik Rajgopal, que dirige la oficina de McKinsey & Co. en Silicon Valley y el departamento de pagos de la compañía.

Aún no sabemos si el gobierno hondureño implantará el registro de títulos de propiedad de tierras con el sistema blockchain ni si promoverá su uso. En intentos anteriores, el gobierno dio marcha atrás ante los costes que suponía ampliar el registro e incluir a más gente. Pero si el archivo ofrece información fiable e imposible de manipular, las ONG podrían obtener la información suplementaria que necesitan para influir en las decisiones políticas y en el gobierno. Si se eliminan cinco de los seis trámites que actualmente se necesitan para registrar una propiedad en Honduras, y se reduce el tiempo que se tarda en hacerlo de veintidós días a diez minutos, entonces esos costes transaccionales no comerciales equivalen casi a cero.³⁵² Y quizá así los periodistas y los defensores de los derechos humanos puedan evitar que las grandes multinacionales compren, construyan o exploten la madera o el agua de tierras que sean reservas medioambientales o hayan sido históricamente usadas por campesinos o indígenas sin compensarlos debidamente. ¡Tenemos esperanza!

Retos de la implementación y oportunidades de liderazgo

La tecnología blockchain no es, desde luego, la panacea para las desgracias económicas y financieras del mundo. La tecnología no crea prosperidad; la crean las personas. Hay obstáculos que hay que superar y oportunidades de liderazgo. El primero es técnico. Según la Unión de Telecomunicaciones Internacional, sigue habiendo importantes deficiencias de conectividad a internet, ya sea porque la infraestructura telecomunicativa es precaria, ya sea porque el servicio es muy caro.³⁵³

El segundo obstáculo es el analfabetismo. Para usar teléfonos móviles inteligentes e interactuar en línea se requiere cierto nivel de alfabetismo. En Estados Unidos, el 18 por ciento de los adultos de más de dieciséis años lee peor que alumnos de quinto curso, el 30 por ciento apenas conoce las operaciones matemáticas básicas³⁵⁴ y el 43 por ciento de estos adultos analfabetos vive en la pobreza.³⁵⁵ El grado de analfabetismo es muy desigual en los países en vías de desarrollo. En muchas partes de África el analfabetismo ronda el 50 por ciento, y el problema se agrava cuando comparamos los sexos. Por ejemplo, en países pobres como Afganistán, Nigeria, Sierra Leona, Chad o Mozambique la diferencia de alfabetización entre hombres y mujeres es de un alarmante 20 por ciento.³⁵⁶

El tercer obstáculo es la corrupción. El sistema blockchain es una herramienta excelente, pero, como todas las tecnologías, no es bueno ni malo en sí mismo. Podemos usar magníficas tecnologías, desde la electricidad hasta la radio pasando por internet, para fines buenos o malos. Necesitamos que haya un liderazgo capaz de aprovechar la tecnología blockchain para hacer el bien en nuestras instituciones, en organizaciones humanitarias y de la sociedad civil, en empresas, en gobiernos y en las personas que se conecten a esta vasta red. Sólo cuando estos desafíos se hayan superado se desarrollará plenamente el potencial de la tecnología blockchain como instrumento de prosperidad global y cambio positivo.

Capítulo VIII

Reconstruir el Estado y la democracia

La república de Estonia es un Estado báltico que linda con Letonia por el sur y con Rusia por el este. Con 1,3 millones de habitantes, casi tiene la misma población que la ciudad de Ottawa.³⁵⁷ Cuando Estonia se independizó de la extinta Unión Soviética en 1991, tuvo ocasión de replantearse completamente el papel del Estado y cómo funcionaría, qué servicios prestaría y cómo alcanzaría esos objetivos mediante las tecnologías de internet.

Hoy, Estonia es considerada el país líder en gobierno digital, y su presidente, Toomas Hendrik Ilves, será el primero que así lo diga: «Estamos muy orgullosos de lo que hemos hecho —nos dice—. Y esperamos que el resto del mundo aprenda de nuestros éxitos.»³⁵⁸

Estonia es el segundo país del mundo con mejores índices de progreso social en lo que respecta a derechos civiles y políticos, junto con Australia y el Reino Unido.³⁵⁹ Los dirigentes estonios han diseñado su estrategia de gobierno electrónico basándose en la descentralización, la interconectividad, la apertura y la seguridad cibernética. El objetivo es crear una infraestructura duradera que se adapte a lo nuevo. Todos los residentes tienen acceso a la información y a los servicios en línea, pueden usar sus identidades digitales para hacer negocios y actualizar o corregir sus datos en los registros estatales. Aunque gran parte de esta labor es anterior al sistema blockchain, el país introdujo una infraestructura de firma sin clave que se integra perfectamente con la tecnología blockchain.

Una característica esencial del modelo electrónico de Estonia es la identidad digital. Hasta 2012 el 90 por ciento de los estonios tenía un carné de identidad electrónico con el que podían acceder a los servicios del Estado y viajar por la Unión Europea.³⁶⁰ El chip incorporado en el carné contiene información básica sobre su propietario, así como dos certificados —uno que autentica la identidad y otro que proporciona una firma digital— y un número de identificación personal (PIN) de su elección.

Los estonios usan sus carnés para votar, revisar y editar en línea sus documentos fiscales, solicitar beneficios de la seguridad social y acceder a servicios bancarios y al transporte público. No necesitan tarjetas de bancos ni de transporte. Y pueden hacer lo mismo con una identidad portátil en sus teléfonos móviles. En 2013 los estonios pagaron el 95 por ciento de sus impuestos electrónicamente y realizaron el 98 por ciento de sus operaciones bancarias en línea.

Los padres y los estudiantes usan la escuela electrónica para ver trabajos, currículos y cursos, y para colaborar con los profesores. El Estado reúne en tiempo real información sanitaria de varias fuentes en un archivo único para cada ciudadano, con lo que estos

registros no residen en una única base de datos. Todos los estonios tienen acceso exclusivo a su propio registro y pueden decidir qué médico o miembros de su familia tienen acceso a esos datos en línea.³⁶¹

Desde 2005 los ciudadanos estonios han votado por internet en sus elecciones. Usando su carné de identidad o su identidad móvil, pueden entrar en la página y votar desde cualquier lugar del mundo. En las elecciones de 2011 el 25 por ciento de los votos se depositó en línea, respecto del 5,5 por ciento de los comicios anteriores. Es evidente que a la gente le gusta el sistema y confía en él: el porcentaje volvió a subir en las elecciones al Parlamento Europeo de 2014, en las que la tercera parte de los votantes participó por internet desde noventa y ocho países diferentes. El gobierno estonio usa un proceso sin papeles y todos los borradores legislativos son accesibles en línea. La duración media de la reunión semanal del gabinete ha pasado de cinco horas a menos de diecinueve minutos.³⁶²

Estonia dispone de un registro inmobiliario electrónico que ha transformado el mercado del sector, reduciendo la duración del traspaso de propiedades de tres meses a poco más de una semana.³⁶³ En los últimos años, Estonia ha lanzado su programa e-Residency, en el que cualquier persona del mundo puede solicitar una «identidad digital transnacional» y una autenticación para acceder a servicios seguros, así como encriptar, verificar y firmar documentos digitalmente. Cualquier empresario de cualquier lugar del mundo puede registrar su empresa en menos de veinte minutos y administrarla en línea. Estas prestaciones contribuyen a la imagen de Estonia como país digital.³⁶⁴

Nada de esto funcionaría ni sería aceptable sin seguridad cibernética. Como observa Mike Gault, consejero delegado de Guardtime: «La integridad es la principal cuestión del ciberespacio y esto es lo que entendieron los estonios hace diez años. Construyeron esta tecnología para que todo lo que hubiera en las redes estatales pudiera verificarse sin necesidad de confiar en los humanos... Al gobierno le es imposible mentir a sus ciudadanos».³⁶⁵

La seguridad cibernética de Estonia se basa en su infraestructura de firma sin clave (KSI, por sus siglas en inglés), que verifica toda la actividad electrónica matemáticamente en la blockchain sin necesidad de administradores del sistema, claves criptográficas ni personal estatal. Este sistema garantiza una transparencia y una responsabilidad totales; todos pueden ver quién introduce qué información, cuándo la introduce y qué hace con ella. En consecuencia, el Estado puede demostrar la integridad de sus registros y el cumplimiento de las leyes, y los ciudadanos pueden verificar la integridad de sus propios registros sin necesidad de que intervenga un tercero. Esto reduce costes: no hay claves que proteger ni documentos que volver a firmar periódicamente. Según e-Estonia.com, «con KSI, la historia no puede reescribirse».³⁶⁶

Evidentemente, la tecnología blockchain no sólo sirve para empresas que buscan beneficios, sino también para instituciones públicas que trabajan por la prosperidad de todos, tanto en el ámbito del gobierno, la educación y la sanidad como en el de las redes energéticas, los sistemas de transporte y los servicios sociales. ¿Por dónde empezamos?

Hay algo podrido en el Estado

En su discurso de Gettysburg de 1863, Abraham Lincoln dijo que la aspiración más grande de la sociedad es «un gobierno del pueblo, por el pueblo y para el pueblo». Doce décadas después, el presidente Ronald Reagan, en su discurso inaugural de 1981, dijo: «El gobierno no es la solución de nuestro problema; el gobierno es el problema». Muchas personas del naciente ecosistema blockchain están de acuerdo. En una encuesta de 2013, más del 44 por ciento de los usuarios de bitcoin se declararon «libertarios o anarcosindicalistas que estaban a favor de la eliminación del Estado».³⁶⁷

Los libertarios de todas clases tienden a apoyar bitcoin. Es un sistema descentralizado y libre del control del Estado. Es anónimo y difícil de gravar. Se parece al oro por su escasez, y los libertarios están a favor del patrón oro. Es un mercado puro, regido por la oferta y la demanda más que por la expansión cuantitativa. No es de extrañar que el primer candidato presidencial de 2016 que aceptó donaciones en bitcoin para su campaña fuera Rand Paul.

El favor de los libertarios ha dado argumentos a los opositores de la moneda digital para rechazar las tecnologías de las blockchains. Jim Edwards, editor y fundador de *Business Insider UK*, escribió sobre el paraíso libertario que él llamaba Bitcoinistán, un país como Somalia «con la menor intervención estatal posible, en un mercado exento de leyes e impuestos». Describía el paraíso como una «total pesadilla... caracterizada por una inestabilidad radical, por el caos, por la existencia de una mafia que asesina a la gente que no le gusta y por un masivo traspaso de riqueza a una minoría incluso más pequeña que el 1 por ciento que actualmente lo elogia en Estados Unidos».³⁶⁸

Desde luego, vivimos en un mundo sacudido por las crisis. «El mundo llevaba una generación sin ver tantos tumultos. La anunciada Primavera Árabe ha dado paso a guerras y represiones casi en todas partes», dice Kenneth Roth, director ejecutivo de Human Rights Watch, ONG fundada en los años setenta del pasado siglo en apoyo de las organizaciones ciudadanas. «Muchos gobiernos han respondido al desorden despreciando los derechos humanos», usando internet para espiar a los ciudadanos, empleando drones para bombardear a la población civil y encarcelando a las personas que se manifiestan en grandes acontecimientos públicos como los Juegos Olímpicos.³⁶⁹

Ésta es la respuesta equivocada al desorden, según el reconocido economista peruano Hernando de Soto. «La Primavera Árabe fue fundamentalmente y sigue siendo una revolución empresarial, de gente que había sido expropiada», dice De Soto. «En realidad, es una gran rebelión contra el *statu quo*», y el *statu quo* es una *expropiación en serie*: el repetido pisoteo de los derechos de propiedad de los ciudadanos por sus gobiernos hasta que no tienen otra opción que trabajar fuera del sistema para ganarse la vida.³⁷⁰

Es decir, pisotear más derechos es la peor respuesta posible porque empuja a más gente —periodistas, activistas y empresarios— a salirse del sistema. En los últimos veinte años, el número de votantes ha caído en picado en la mayoría de las democracias occidentales, incluidos Estados Unidos, el Reino Unido, Francia, Alemania, Italia, Suecia y Canadá. En particular, la gente joven intenta cambiar la sociedad desde fuera del sistema, no mediante el voto, claro está. La mayoría de los estadounidenses piensa que el Congreso no funciona bien y está profundamente corrompido. Y es natural que lo

piensen: como en muchos países, los políticos estadounidenses se deben a contribuyentes ricos y grupos de interés, y muchos miembros del Congreso acaban perteneciendo a algún lobby. Ejemplo sobresaliente: el 92 por ciento de los estadounidenses quiere que se examinen los antecedentes de las personas que compran armas, pero la rica y poderosa Asociación Nacional del Rifle impide que se legisle al respecto. Y eso que es un «gobierno del pueblo, para el pueblo y por el pueblo».

Cuanto más sienten los ciudadanos que sus instituciones políticas no reflejan su voluntad ni defienden sus derechos, cuanto más se extralimitan estas instituciones en el ejercicio de su autoridad, más ponen en cuestión los ciudadanos su legitimidad y su relevancia. El sociólogo político Seymour Martin Lipset dijo que la legitimidad es «la capacidad de un sistema político para engendrar y mantener la creencia de que la instituciones políticas que existen son las más apropiadas y las mejores para la sociedad».³⁷¹ Y cada vez más jóvenes quieren cambiar las cosas por medios que no pasan por el gobierno ni aun por la democracia. La pegatina para parachoques que reza «¡No votes! Eso les da más fuerza» habla por sí sola.

«Para los individuos podría no ser deseable que su historial figurase en una base de datos verificable que los gobiernos pudieran usar para explotar o someter a la gente — dice De Soto—. La legislación de la mayoría de los países está tan mal hecha, es tan poco acogedora, que los costes de incorporarse al sistema legal hacen que para los pobres no tenga sentido. Y un país con mucha gente pobre y desconectada causa muchos problemas.»³⁷²

Cuando la legitimidad falla, el libertarismo crece. Pero éste no es la solución a los problemas políticos. En este trastornado mundo, lo que necesitamos son Estados fuertes, que funcionen bien, que sean efectivos y responsables ante los ciudadanos.

¿Qué tendrían que hacer los gobiernos? «Crear, racionalizar y fortalecer las leyes y estructuras que hicieron florecer el capitalismo —escribió De Soto en *The Wall Street Journal*—. Como sabe cualquiera que haya paseado por las calles de Lima, Túnez o El Cairo, el capital no es el problema, es la solución.»³⁷³ Entonces, ¿cuál es el problema? «Identificar a la gente —nos dice—. Los gobiernos no pueden forzar a la gente a entrar en el sistema. Por eso creo que muchos gobiernos del mundo están dispuesto a darle la vuelta al sistema.»³⁷⁴

Aquí es donde entra el sistema blockchain. Los principios generales de este sistema deberían presidir esta transformación porque permiten mayores niveles de lo siguiente:

Integridad. Para recuperar la confianza pública en las instituciones políticas, los funcionarios elegidos han de comportarse con integridad. La fiabilidad ha de ser inherente al sistema, estar integrada en cada proceso, sin que tengamos que otorgársela a los miembros aislados. Como el sistema blockchain permite una transparencia total, está convirtiéndose en una herramienta fundamental para recuperar la confianza entre representados y representantes. Una transparencia permanente es vital para mantener esta relación.

Poder. Todo el mundo tiene derecho a participar en el gobierno, directamente o votando. Las personas elegidas han de obrar a plena luz del día como iguales entre iguales. Con internet, los ciudadanos asumieron más responsabilidad con sus

comunidades, aprendieron de los funcionarios elegidos e influyeron en ellos, y viceversa. Con el sistema blockchain, los ciudadanos pueden ir más allá: pueden pedir que las acciones del gobierno pasen a figurar para siempre en un registro inalterable e incorruptible. No ya «controles y contrapesos» entre unos pocos poderosos, sino un consenso amplio de muchos, para, por ejemplo, examinar los antecedentes de potenciales propietarios de armas.

Valor. Los votos tienen que valer. El sistema tiene que conciliar los incentivos de todos los participantes, responder ante los ciudadanos y no ante los ricos, e invertir bien el dinero de los impuestos. La maquinaria del gobierno debe funcionar bien y ser más barata gracias a la tecnología.

Privacidad y otros derechos protegidos. Que no se espíe a los ciudadanos, que no se interfiera arbitrariamente en nuestra privacidad, familia u hogar, que no se ataque el honor ni la reputación de nadie. Que no se expropie arbitrariamente —bienes inmuebles o bienes intelectuales, como patentes de inventores— sin compensación. Que no se censure a las nuevas organizaciones, que no se impida el derecho de reunión. Con el sistema blockchain, podemos registrar nuestros derechos de autor, organizar nuestras reuniones e intercambiar mensajes de forma privada y anónima. No nos fiemos de los políticos que abogan por un equilibrio entre la privacidad personal y la seguridad pública. Es una falsa dicotomía.

Seguridad. Todo el mundo debe tener derecho a la protección de la ley sin discriminación. No puede haber detenciones arbitrarias. Ninguna persona o grupo debería vivir con miedo de su gobierno o de los agentes de la ley, ni ser sometido a un trato cruel, inhumano ni degradante por parte de esos agentes a causa de su raza, religión o país de origen. Los miembros de las fuerzas del orden no pueden ocultar pruebas del uso indebido de la fuerza, ni las pruebas pueden desaparecer. Todo estaría registrado y podría verificarse en una blockchain.

Inclusión. Con el uso de internet los ciudadanos se conciencian más, aprenden unos de otros. Con las blockchains el sistema puede incluir a todos los ciudadanos, reconocerlos como personas ante la ley y garantizarles un acceso equitativo a los servicios públicos (sanidad, educación...) y a la seguridad social.

La tecnología es una herramienta poderosa pero sola no puede cambiar las cosas que necesitamos cambiar. Con el espíritu del dicho «El futuro no se predice, se realiza» reinventemos el Estado para que empiece una nueva era de legitimidad y confianza. Es hora de ponerse manos a la obra.

Servicios y operaciones de un Estado eficiente

Los que critican el «Estado fuerte» (*big government*) tienen razón en una cosa. En cuestión de eficiencia, el Estado es lento. Los Estados están organizados en compartimentos estancos que no comparten información. La burocracia se impone demasiado a menudo al sentido común o a las prácticas colaborativas. Los ciudadanos que solicitan un servicio público tienen que pasar por sucesivas ventanillas. En todos los países hay incontables casos de políticos y burócratas que defraudan dinero público.

El sistema blockchain puede mejorar el servicio al cliente, aumentar la eficiencia y mejorar los resultados, así como garantizar la integridad y la transparencia del Estado. Las posibilidades de mejorar todas las facetas del Estado son grandes, pero algunas son especialmente importantes en el mundo desarrollado, donde los gobiernos están estableciendo nuevos procesos y pueden saltarse los sistemas de los gobiernos largos, estables y abiertos.

Veamos dos grandes áreas a las que podemos aplicar el sistema blockchain: un Estado integrado y el uso del internet de las cosas en el sector público.

Estado integrado

Estonia está reduciendo ineficiencias y proporcionando servicios integrados a sus ciudadanos gracias a la implantación de un carné de identidad electrónico y al uso de una estructura blockchain en internet llamada «X-road», con la que se pueden conectar múltiples programas y bases de datos tanto en el sector privado como en el público. Lo mismo pueden hacer otros.

Países como Canadá, el Reino Unido y Australia han rechazado explícitamente la idea de implantar un registro civil central y un documento de identidad oficial. Esta decisión se debe a la preocupación por la privacidad personal y a la aversión por un poder estatal grande, sobre todo en lo que se refiere a conceder o negar identidades.

Sin embargo, como el caso de Estonia demuestra, si incluimos los documentos oficiales (pasaporte, partida de nacimiento, licencia de matrimonio, certificado de defunción, carné de conducir, tarjeta sanitaria, títulos de propiedad, carné de votante, registros mercantiles, condición fiscal y laboral, expedientes académicos, etc.) que existen en diferentes bases de datos en una blockchain única, las redes blockchain podrían ofrecer servicios integrados sin necesidad de pasar por un procesamiento central. Este modelo no sólo podría proteger la privacidad, sino también aumentarla, porque nos permitiría comprobar la veracidad de nuestra información y ver quién accede a ella o la modifica (o sea, sería una especie de auditoría permanente).

De hecho, en el futuro tendrá sentido que cada ciudadano sea dueño de la información de su identidad en lugar de que lo sea el Estado. Como explicamos en el capítulo I, igual que las redes y la colaboración de masas pueden eliminar la necesidad de un Estado que emita moneda o de un banco que dé confianza, tampoco necesitaremos un carné de identidad oficial. Dice Carlos Moreira, de la empresa de seguridad criptográfica WISEKey: «Hoy necesitamos una organización dotada de derechos que nos proporcione una identidad, como una tarjeta bancaria, una tarjeta de pasajero frecuente o una tarjeta de crédito. Pero esa identidad es ahora nuestra y los datos que produce su interacción en el mundo pertenecen a otros».³⁷⁵ Con el sistema blockchain nuestra identidad nos pertenece. Nuestro «avatar personal» podría decidir qué información dar a quién según queramos. También podría decidir qué información integrar. Sólo que, en lugar de que todo lo que hacemos con el Estado quede integrado en una gran base de datos de propiedad estatal, esa integración la realiza nuestro yo virtual, que nos pertenece y que controlamos nosotros.

Una mejor integración facilitará acontecimientos de la vida de las personas como el matrimonio. Melanie Swan, fundadora del Institute for Blockchain Studies, explica: «El sistema blockchain —con una estructura que permite alojar identidades seguras, contratos múltiples y gestión de activos— es ideal para casos como el matrimonio, porque permite que una pareja vincule su contrato matrimonial a una cuenta de ahorro común, a un contrato de cuidado de los hijos, a una escritura de propiedad y a cualquier otro documento importante, asegurándose así un futuro juntos».³⁷⁶ Algunos afirman que el sistema blockchain podría ser un registro de documentos público al margen del Estado. La primera boda registrada en una blockchain tuvo lugar en el Walt Disney World de Florida en agosto de 2014. Contratos prenupciales inteligentes, ¿quién quiere uno?

Además de servicios integrados, los gobiernos podrían registrar y administrar documentos con transparencia y fiabilidad. Consideremos el tiempo que se pierde en extender, comprobar, actualizar, renovar y sustituir los registros oficiales de las personas. Además de asegurar la veracidad de los documentos, el registro con blockchain en redes de iguales permitirá que cada cual verifique los documentos por sí mismo, a través de la red y no de un funcionario, y que obtenga un servicio personalizado, pues cuando generamos un documento oficial, éste contiene automáticamente la información relevante sobre nosotros y los derechos de acceso a esa información, y registra quién accede a ella y la usa en los metadatos del documento.

Por ejemplo, el gobierno británico está estudiando usar el sistema blockchain para conservar numerosos registros, especialmente para asegurar su integridad. Paul Downey, un ingeniero técnico del Digital Service del gobierno, observa que el perfecto registro «debería ser capaz de demostrar que la información no ha sido manipulada», así como guardar un historial de los cambios que se han hecho y «estar abierto a un examen independiente».³⁷⁷

Los sistemas basados en blockchain pueden hacer más eficaces e íntegros el registro de documentos de todas clases y muchos otros trámites oficiales. Combinando la gestión de la cadena de suministro con el internet de las cosas, podemos incorporar chips inteligentes que comuniquen la procedencia, propiedad, garantías o información especial de los productos. Las agencias de suministros del Estado podrían rastrear esos productos y automatizar operaciones en cada fase del proceso: compra, pago, pago de impuestos, renovación de contratos, modernización. Esto es administrar mejor los activos, ni más ni menos, porque los contribuyentes ven reducidos los costes administrativos y aumentados los ingresos del Estado.³⁷⁸

Particularmente interesantes son las posibilidades, tanto a nivel nacional como local, de conectar diferentes redes de blockchain para aumentar la eficiencia entre jurisdicciones. Por ejemplo, las agencias de tráfico oficiales podrían conectar las bases de datos de los conductores nacionales o provinciales para crear una base de datos virtual que facilitara la confirmación de la identidad, condición e historial de los conductores. O en el caso del sistema sanitario de Estados Unidos, «supongamos que los registros financieros del paciente, la compañía aseguradora, el médico y el contribuyente figuran

todos en un único archivo, que todos pueden ver en el momento de producirse cualquier transacción. La capacidad de transparencia de este sistema sólo sería igualada por su capacidad de eficiencia», dice Swan.³⁷⁹

El internet de las cosas públicas

Ya hemos hablado de lo que sería el transporte público con el internet de las cosas. Es quizá la oportunidad más fácil que el IoT le ofrece al Estado: registrar dispositivos inteligentes en un archivo de blockchain para gestionar durante su vida útil edificios, espacios de trabajo y reunión, parques móviles, ordenadores y demás equipamiento. Como en el caso de bAirbnb, los funcionarios podrían ajustar dinámicamente la oferta y la demanda, reducir costes de seguridad, de mantenimiento y energéticos mediante controles automáticos de acceso, iluminación y temperatura, seguir la ubicación y el estado de los vehículos oficiales y controlar la seguridad de puentes, ferrocarriles y túneles.

Los responsables públicos también podrían gestionar mejor las infraestructuras, la energía, el agua y los residuos, así como el medio ambiente y los servicios de emergencia, la educación y la sanidad. Además de aumentar la eficiencia, estas aplicaciones basadas en blockchain podrían asimismo mejorar la salud y la seguridad públicas, descongestionar el tráfico y reducir el consumo y la pérdida de energía (en tuberías con fugas, por ejemplo), por no mencionar más que algunos de sus beneficios.

Infraestructuras seguras

Gracias a que, inteligentemente, se ha asociado con el sector privado y con otros agentes interesados, el Estado estonio ha creado una infraestructura pública con muchas más ventajas y un mejor acceso de los ciudadanos a los servicios del Estado, a los bancos, al transporte público y a otras prestaciones. Además de estos beneficios para sus ciudadanos, Estonia también gana competitividad en la economía global, porque atrae negocios e inversiones.

Los gobiernos ya ofrecen servicios a jurisdicciones vecinales (fuego y ambulancia), contratan los de otras jurisdicciones (procesamiento de datos), prestan servicios en nombre de otras jurisdicciones (el gobierno federal procesa impuestos sobre la renta en nombre tanto del gobierno nacional como del provincial o regional), así como servicios compartidos (oficinas compartidas).

El servicio e-Resident de Estonia puede usarlo cualquier persona que esté en cualquier lugar del mundo y necesite un carné de identidad oficial para montar un negocio, sobre todo si es en línea. Estonia está preparándose para prestar servicios a ciudadanos extranjeros que otros países renuncian a prestar. Aunque los servicios que prestan ahora son bastante limitados, los que podría ofrecer una vez que se digitalizaran por completo son ilimitados. Por ejemplo, las bibliotecas públicas, que son gratuitas para los residentes, podrían ofrecer acceso a sus colecciones digitales a los no residentes y a

los estudiosos de cualquier parte del mundo a cambio de una pequeña cantidad. ¿Qué otros servicios podrían prestarse a un tratamiento similar, sobre todo servicios digitales en los que la gestión de la información y la integridad son importantes?

Ofrecer servicios públicos más allá de las fronteras nacionales choca muchas veces con obstáculos legales. Sin embargo, vivimos en un mundo cada vez más globalizado en el que muchos de los mayores retos no son exclusivos de una única jurisdicción. Los problemas globales requieren nuevas soluciones y nuevos modelos de colaboración con las demás partes afectadas. Una política que considere que las fronteras son porosas, combinada con tecnologías blockchain como el internet de las cosas, podría contribuir más a resolver grandes y espinosas cuestiones.

Capacitar a la gente para que se sirva a sí misma y sirva a los demás

Las redes blockchain hacen que los servicios públicos sean más robustos y respondan mejor. El autoservicio, desde renovar un permiso hasta obtener un documento oficial, mejorará el funcionamiento del Estado. Cuando deja tiempo libre, ataja la corrupción, suprime barreras artificiales, proporciona módulos de autoformación y paga a tiempo los subsidios, el Estado no hace sino dar poder a los ciudadanos.

Nuevos modelos, muchos de los cuales aún están por definir, pueden capacitar a la gente para que colabore en la consecución de objetivos de política pública. Con las blockchains podemos establecer un nuevo equilibrio entre la necesidad que tiene el Estado de controlar y responsabilizarse de un presupuesto, y la necesidad de los individuos y grupos de controlar y contribuir con porciones de ese presupuesto. Algunas jurisdicciones han explorado nuevos modelos para traspasar a personas (beneficiarias de muchos programas estatales), a comunidades (vecinales) o incluso a poblaciones enteras (de una ciudad) el control sobre sus propios presupuestos, que antes controlaban funcionarios del Estado.

Por ejemplo, en lugar de exigir que las personas soliciten ayudas de muchos programas estatales a la vez, cada uno con sus propios criterios (renta, activos, número y edad de los hijos, tipo de vivienda, grado de formación, etc.), la plataforma estatal podría personalizar un presupuesto basándose en la identidad, información almacenada, patrones de producción y consumo, incluyendo factores de riesgo como el hecho de residir en barrios pobres, grado de formación, consumo de tabaco, alcohol y alimentos procesados. Las personas podrían así decidir cómo usar los recursos para alcanzar sus objetivos según sus circunstancias.

Imaginemos que en lugar de tener que convencer a algún burócrata de que nuestro hijo necesita un nuevo abrigo, podemos decidirlo nosotros. El resultado es que la responsabilidad y el poder personales aumentan. Lo mismo podríamos hacer a nivel comunitario (con partidas presupuestarias destinadas a servicios específicamente comunitarios como parques y centros sociales) y a nivel intergubernamental (estableciendo prioridades de gasto).

Algunas jurisdicciones ya están dando poder a los más desfavorecidos.³⁸⁰ El sistema blockchain podría acelerar esta tendencia, permitiendo que los contribuyentes vieran adónde va su dinero, cómo usan sus conciudadanos esos recursos y si los programas dan resultado (si cambian las rentas, si se alcanzan objetivos educativos, si se procuran viviendas, etc.). La plataforma reduce y aun elimina la necesidad de controles e inspecciones complejos y laboriosos. Aunque el vasto alcance de la información y de cómo esa información puede rastrearse a través de redes de iguales puede dar miedo y parecer orwelliano, la verdad es que ocurre lo contrario. En lugar de que toda la información y la autoridad estén en manos de un poder central o de unos burócratas anónimos, las personas y las comunidades podrían actuar basándose en una información verificada y fidedigna. Al mismo tiempo, el archivo blockchain garantiza la responsabilidad del uso de fondos públicos. Podemos así alcanzar dos objetivos que antes parecían contradictorios: «más Estado» porque disponemos de más información y contexto, y «menos Estado» porque las personas y los grupos disponen de información y mejores herramientas para decidir y actuar en ese contexto.

Facilitar información abierta y fiable

Perianne Boring, fundadora y presidenta de la Cámara de Comercio Digital, defiende la idea de que los archivos distribuidos hacen al Estado más abierto y mejor. Para ella, «el sistema blockchain permite una transparencia radical porque suministra a todo el mundo hechos verificables. Cualquiera puede ver cualquier transacción que se haya producido en la blockchain».³⁸¹

El Estado puede proporcionar información que otros pueden usar en beneficio público o privado. Esto difiere de la llamada «ley sobre la libertad de información» por la cual los ciudadanos deben solicitar permiso para acceder a información oficial importante. Al contrario, se trata de facilitar esa información. El Estado podría poner a disposición del ciudadano miles de categorías de datos sin procesar y sin identificadores personales: patrones de tráfico, control sanitario, cambios medioambientales, propiedades estatales, consumo energético, presupuesto y gastos del Estado, cuentas de gasto. Los ciudadanos, las empresas, las ONG, los estudiosos y otros podrían analizar esos datos, incluirlos en aplicaciones, usarlos, en fin, para, por ejemplo, descubrir tendencias sociales de consumo, investigar patrones de salud o saber si un autobús llegará a su hora.

Hasta agosto de 2015 el gobierno de Estados Unidos ha publicado 165.000 series y herramientas de datos en su página «Open Government».³⁸² La idea de que la información que tiene el Estado es información pública ha hecho del gobierno de Estados Unidos un pionero en transparencia. Otros gobiernos siguen el ejemplo. Hasta agosto de 2015 el gobierno del Reino Unido ha publicado 22.000 series de datos.³⁸³

Publicar datos en redes de iguales y en blockchain aumentará aún más la eficiencia, la uniformidad, la utilidad y la fiabilidad. Hacer pública la información es un incentivo para que sea exacta. La gente puede revisarla y señalar errores o demostrar que esa información ha sido alterada o corrompida.

Si registramos una serie de datos completa en una red blockchain, esta red puede registrar añadidos y cambios a esa serie de datos e impedir que se manipule. No se necesita ningún administrador central. El Estado puede hacer pública más información programática para ayudar a la gente y a los analistas a entender esos programas y el impacto que tendrán.

Asociarse para crear valor público

Ya hemos visto lo fácilmente que puede usarse una información fiable puesta a disposición de todos para crear valor económico y social positivo, y hasta qué punto podemos dar poder a las personas y a las comunidades para que mejoren sus vidas. Las redes blockchain nos obligarán a replantearnos la manera como repartimos la responsabilidad de crear valor público. Cuando el Estado hace pública una información sin procesar, se convierte en una plataforma con la que las empresas, la sociedad civil, las agencias gubernamentales y las personas pueden organizarse por sí mismas para crear servicios. En Estados Unidos llevamos unos años usando modelos de «pago por éxito» (*pay for success*) para comprometer a empresarios e inversores en la resolución de problemas sociales. Por ejemplo, el Departamento de Trabajo financió iniciativas de empleo para exdelincuentes que redujeron la reincidencia, y el Ayuntamiento de Chicago aumentó los niveles de educación entre alumnos de preescolar de las clases más desfavorecidas.³⁸⁴

Además, este modelo estimula la innovación e incentiva la consecución de los resultados deseados porque sólo se paga cuando esos resultados se han conseguido y pueden medirse. Pensemos en la posibilidad de hacer continuos micropagos a pequeños grupos sin afán de lucro que trabajen en iniciativas energéticas sostenibles para una comunidad. Un programa oficial podría vincular la subvención a que se produjera una bajada real del consumo energético. El grupo sin afán de lucro podría mantenerse por sí mismo sin tener que depender de un complejo papeleo para percibir la subvención e, incluso, podría garantizarse una financiación basándose en el compromiso del Estado a participar en el modelo de «pago por éxito».

Asociar contratos sociales inteligentes a reputaciones políticas

Igual que la red bitcoin usa tecnología blockchain para garantizar en todo momento la integridad de los pagos, las redes del Estado pueden usar blockchain para garantizar la integridad de sus transacciones, registros e importantes decisiones. Los funcionarios no pueden ocultar pagos ni otros registros oficiales, como correos electrónicos, actas de decisiones y bases de datos. Si la seguridad depende muchas veces de barreras, muros o perímetros protectores, el sistema blockchain protege de manipulaciones hechas desde dentro y desde fuera. Hace, pues, que «la gente honrada siga siendo honrada».³⁸⁵

La transparencia es crucial para cambiar el comportamiento de una institución. Aunque, claro está, no podemos obligar a nuestros representantes públicos a observar estos valores y conductas, sí podemos limitar sus decisiones y acciones mediante

contratos inteligentes que definan sus funciones y responsabilidades, y controlarlos y medirlos con el sistema blockchain.

Recordemos que los contratos inteligentes son pactos que se ejecutan a sí mismos y se almacenan en una blockchain, que nadie puede controlar y en los que, por eso mismo, todos pueden confiar. Partidos políticos, como el republicano, podrían usarlos para que los candidatos que usaran su infraestructura de partido para debatir y hacer campaña durante las primarias, no pudieran presentarse como independientes en unas elecciones presidenciales. Podríamos aplicar contratos inteligentes a diversos tipos de acciones públicas (cadena de suministro, servicios legales externos, contratos de «pago por éxito») e incluso a funciones más complejas del gobierno y de nuestros representantes elegidos. Preveo redes de iguales que registren los compromisos de un funcionario elegido y el grado de cumplimiento de esos compromisos. Ya hay sistemas de vigilancia que hacen esto en internet con redes de iguales oficiales y no oficiales.

Aunque este sistema no podríamos aplicarlo a todo lo que esperamos de nuestros líderes políticos, sí podríamos usarlo para controlar toda clase de compromisos y acciones específicos. Si bien medir los resultados finales será muy difícil (por ejemplo, los resultados alcanzados con el dinero gastado), con el tiempo ganaremos experiencia y conocimiento de los indicadores y podremos basar nuestros juicios en hechos y no en interpretaciones. Esto no son utopías: en Londres, un candidato a la alcaldía en las elecciones de 2016 ya está pidiendo que se use el sistema blockchain para responsabilizar a los funcionarios elegidos de los asuntos públicos.³⁸⁶

Los reguladores podrían emplear procesos basados en blockchain para registrar y verificar en tiempo real los compromisos de las industrias reguladas, y juzgar si están cumpliendo con lo prometido (por ejemplo, invertir en energía sostenible) o respetando las prácticas reguladas (por ejemplo, entregas puntuales, requisitos de seguridad). Aunque cada vez es más común publicar indicadores de rendimiento y resultados en páginas web públicas, el sistema blockchain permitiría automatizar estos procesos y garantizar su exactitud cuando se aplicaran a resultados medibles.

Los datos generados por estos procesos permiten a los ciudadanos saber en todo momento quién se comporta con integridad y quién no. ¿Cuántas veces apareció tal político en un mitin? ¿Qué votó? ¿Cumplió su compromiso de hacer esto y lo otro? ¿Quién donó para su campaña electoral? ¿Quién violó los términos de los contratos inteligentes que suscribió? Los funcionarios elegidos deben respetar sus compromisos o explicar por qué no lo hacen. Esto permitiría conocer también si las demandas de los electores son razonables o justas, no reaccionarias. Los votantes suelen querer más servicios pero menos impuestos, o más fábricas pero no cerca de sus casas, o precios más bajos pero salarios más elevados. La información abierta, pues, hace posible que entendamos los equilibrios y aumenta la responsabilidad de todos los participantes.

La segunda era de la democracia

Aunque la democracia representativa es compleja y varía de un sitio a otro, una cosa es constante: la pasividad de la ciudadanía. Hasta ahora, el debate se ha centrado en cómo la tecnología blockchain puede contribuir a crear las condiciones para que las votaciones sean seguras, justas y fáciles. Tenemos sin duda grandes oportunidades. Votar en línea con el sistema blockchain permitirá a los ciudadanos opinar con mayor frecuencia. Pero querer reemplazar la democracia representativa sería un error. «Las propuestas que se someten a votación suelen ser la quintaesencia refinada de largas y complejas cuestiones. Son el resultado de procesos largos en los que hay conflictos, contradicciones y compromisos. Para entender una propuesta y votar responsablemente, los ciudadanos tienen que poder participar en alguna forma de proceso de refinamiento», escribió Don en *The Digital Economy* hace más de veinte años.³⁸⁷ Sin embargo, si entendemos las características de un nuevo modelo, veremos hasta qué punto la tecnología blockchain puede ir más allá del simple voto.

Tecnología y democracia: una historia no siempre feliz

¿Cómo ha afectado la tecnología a la democracia? Sorprendentemente, es una historia complicada, cuando menos. Puede decirse que la televisión degradó el debate democrático, convirtiendo lo que Al Gore llamaba «el mercado de las ideas»³⁸⁸ en un diálogo unilateral. Si a eso sumamos los igualmente tóxicos canales de noticias —en los que bustos parlantes aumentaban los índices de audiencia criticando a sus adversarios en lugar de debatir ideas—, tenemos simples batallas entre extremos. Como dice el locutor de noticias Howard Beale en la película *Un mundo implacable*: «¡Estoy más que harto y no pienso seguir soportándolo!».

Hasta ahora, internet no ha cambiado a mejor la democracia. Más bien al contrario: con una mayor vigilancia y más violaciones de la privacidad so pretexto de la seguridad nacional, los gobiernos democráticos se comportan más como regímenes autoritarios. Quisiéramos centrarnos en tres desafíos concretos:

1. La fragmentación del discurso público

Al Gore confiaba en que la era digital invertiría la tendencia negativa que minaba nuestras instituciones fundamentales. «La mayor fuente de esperanza de que se restablezca un mercado de ideas vigoroso y accesible es internet.»³⁸⁹ No era el único que lo creía. Llevamos diciendo desde hace mucho que, conforme el uso, los recursos y la conectividad de la web aumenten, la información objetiva será más accesible y la calidad del discurso público mejorará.

Sin embargo, parece que ocurre lo contrario: una balcanización de perspectivas y una explotación de las nuevas herramientas por ideólogos que se organizan en batallones. Ahora que la producción de contenido se generaliza y las fuentes de información y opinión proliferan, cualquiera puede exponer ciertas ideas y atraer a un público que piense lo mismo, público que puede ser reducido pero también muy entusiasta.

Las nuevas herramientas de comunicación y análisis de datos han hecho posible también que grupos ideológicamente tendenciosos secuestren el debate político y social. Tanto socialdemócratas como conservadores los emplean para crear un ruido mediático que socava la posibilidad de compromiso, y no digamos de consenso.

2. El aumento de la ignorancia en la web

Así como la gente no puede diferenciar a una persona de un perro en internet, así tampoco sabe discernir siempre la verdad. Los teóricos de las conspiraciones popularizan sus opiniones infundadas en cuestión de día y aun de horas,³⁹⁰ como hemos visto hace poco con el accidente del vuelo MH370 de la compañía Malaysia Airlines. Pensemos que tres de cada diez estadounidenses creen hoy que los seres humanos han existido desde el principio de los tiempos.³⁹¹ Y pese a la aplastante evidencia científica de que las emisiones de carbono amenazan la vida en la Tierra, aquellos que tienen intereses a corto plazo han denigrado eficazmente la ciencia e impedido un debate inteligente, y no digamos planes de acción. Las personas que usan la red para promover la ignorancia y el negacionismo están ganándose la batalla a los científicos y racionalistas. Países represivos como Irán y Corea del Norte están creando versiones privadas y restringidas de internet para sus ciudadanos, con lo que convierten la web en una herramienta aún más poderosa para hacer que la ideología triunfe sobre el racionalismo.

3. La complicación de la práctica política

En la era predigital, concebir e implantar políticas era menos complicado. Los expertos y consejeros presidenciales ejercían un fuerte control sobre las cuestiones. Hoy apenas si pueden definir los problemas, y no digamos aportar soluciones o explicarlas a la gente. Tan serio es el problema que el presidente Obama aprobó la Plain Writing Act of 2010 (o «ley sobre la claridad de la escritura de 2010») que exigía a las agencias federales usar un lenguaje que los ciudadanos pudieran entender.³⁹²

Hoy surgen muchos problemas imprevistos entre unas elecciones y otras. Ningún gobierno puede decir creíblemente que tiene un mandato del votante para actuar así o así en todas las cuestiones importantes. Además, los gobiernos carecen de los conocimientos políticos necesarios sobre muchos temas. Así, aunque un gobierno encargue sondeos para conocer la opinión de la gente, nunca llega a beneficiarse del saber y la experiencia que los ciudadanos de una nación pueden ofrecer colectivamente.

La democracia y las blockchains

Todos estos problemas hacen necesario un nuevo modelo de democracia que ponga el acento en el discurso público y en la participación ciudadana. No confundamos la participación ciudadana con nociones como la llamada «democracia directa», consistente en ver las noticias de la noche y votar luego, con nuestros teléfonos móviles o con televisores interactivos, si queremos o no que se ahorque públicamente a los delincuentes. Los ciudadanos no tienen el tiempo, el interés ni los conocimientos necesarios para

informarse de todos los temas. Lo que necesitamos son opiniones razonadas, no cualquier opinión. Seguimos necesitando asambleas legislativas que debatan, definan y resuelvan los problemas.

Pero no cabe duda de que un modelo de democracia más colaborativo —que premiara la participación, por ejemplo, de quien desempeñara funciones de minado— podría animar a los ciudadanos a comprometerse y aprender sobre cuestiones, al tiempo que vigorizaría el sector público con la aguda forma de razonar que la nación puede ofrecer colectivamente. ¿Podríamos crear una cultura en la que la gente se interesara por el proceso democrático, en lugar de desinteresarse de él por culpa del abuso de poder de sus representantes?

¿Por qué no ha ocurrido esto hasta ahora? El gran problema no es tecnológico. La mayoría de los políticos, sean del signo que sean, parecen más preocupados por ganar elecciones que por resolver la crisis de legitimidad fomentando la participación ciudadana.

Empecemos por lo básico. El proceso más fundamental de la democracia representativa son las elecciones. En una democracia, votar es el derecho (y, en algunos países, como Bélgica, la responsabilidad) de todos los ciudadanos. Pero vemos hasta qué punto los sistemas electorales fallan en todo el mundo. Hay funcionarios corruptos que amañan los resultados. Se impide votar usando cualquier medio, desde vedar el acceso hasta sobornar e intimidar. Manipular unas elecciones no es tarea sencilla pero vemos que ocurre en todas partes. ¿Podrían las tecnologías blockchain mejorar el proceso de votación?

Pese a todos los adelantos tecnológicos que ha habido, los mecanismos de voto casi no han variado en cientos de años. En muchas partes del mundo para votar tenemos que desplazarnos hasta un colegio electoral, identificarnos, marcar una papeleta, introducirla en una urna y esperar a que unos seres humanos cuenten los votos.

La votación electrónica consiste en votar con la ayuda de un sistema electrónico. Este tipo de votación se ha revelado, en muchos casos, tan poco fiable como el escrutinio manual. Hoy sigue teniendo tres problemas: ataques al software y al hardware, errores o virus del sistema y fallos humanos. En 2004, una máquina usada en las elecciones generales de Carolina del Norte fue programada por error para registrar solamente 3.000 votos. Con ello se perdieron irremediabilmente 4.438 votos en una carrera que se decidió por una diferencia de sólo 2.287 votos.³⁹³

Votar con blockchain

¿Cómo sería votar con blockchain? Supongamos que la junta electoral crea unas «carteras» digitales para cada candidato u opción, con votantes acreditados que asignen una ficha o moneda cada uno por cada escaño. Los ciudadanos votan anónimamente con su avatar personal enviando su «moneda» a la cartera de su candidato favorito. La blockchain registra y confirma la transacción. El que más monedas obtenga, gana.

Algunos han tratado de resolver la cuestión de la fiabilidad usando sistemas de votación que pueden verificarse de extremo a extremo. Normalmente se vota a través de terminales, que emiten una papeleta criptográficamente autenticada pero permiten contar los votos electrónicamente.

CommitCoin usa sistemas de prueba de trabajo criptográficos para demostrar que un mensaje se envía en determinado momento. Los inventores, Jeremy Clark y Aleks Essex, dicen que podemos usarlos para demostrar la integridad de los datos antes de que se produzca el evento, como una forma de «datar carbónicamente» los compromisos que se contraen, siendo un punto de referencia para prevenir fraudes y errores.³⁹⁴

Sistemas de votación electrónica de extremo a extremo

Los ciudadanos hacen avances constantemente. En 2015, unos estudiosos de la Universidad Nacional y Kapodistriaca de Atenas publicaron un artículo en el que introducían DEMOS, un nuevo sistema de votación electrónica de extremo a extremo que puede verificarse en el modelo estándar, sin depender de ajustes del sistema ni del acceso a un «emisor de números aleatorios» (*randomness beacon*).³⁹⁵ Usa un registro público distribuido como el de las blockchains para crear una urna digital en la que los ciudadanos pueden depositar su voto desde cualquier parte del mundo.

Un sistema de elecciones verificable de extremo a extremo es capaz de detectar cuándo una autoridad electoral intenta tergiversar los resultados. Los votantes depositan sus votos y a cambio obtienen un recibo que les permite comprobar a) que su voto se ha depositado como ellos querían; b) que ha quedado registrado en el mismo momento de depositarlo, y c) que se ha contado en el mismo momento del registro. Un tercero podría verificar los resultados de las elecciones. Los votantes siguen teniendo que aceptar ajustes del sistema y hacer un acto de fe para creerse los resultados de las elecciones.

Con DEMOS el sistema de votación genera una serie de números al azar.³⁹⁶ Los votantes reciben dos números, o claves: uno que corresponde a ellos y el otro a su candidato favorito. Cuando el voto encriptado se deposita, se envía a través de varios servidores. Los resultados se hacen públicos en un tablón de anuncios que muestra toda la información relacionada con las elecciones.

Bloques por una votación neutral

En Australia, una organización llamada Bloque por una Votación Neutral (NVB, por sus siglas en inglés) está usando el voto con blockchain para revolucionar la democracia de otro modo. Sólo conciben el gobierno de una manera, y esta manera es optimista: «Creemos que la mejor manera de mejorar las políticas es participando».³⁹⁷

El fundador de NVB, Max Kaye, describe su invento como una «aplicación política» en la que los ciudadanos interesados pueden registrar sus opiniones sobre cuestiones políticas «votando» con el sistema blockchain. Cuando el tiempo se acaba, el resultado del recuento les dice a los funcionarios elegidos cómo votar en procesos del gobierno.

Cuando le preguntamos por qué usa el sistema blockchain, Max Kaye contesta: «Porque queremos que existan muchos partidos, algunos de los cuales diferirán necesariamente. Para asegurar la integridad del sistema, es necesario que todos los partidos puedan verificar el registro de votos y cada uno de éstos». Además, Kaye dice que el sistema tiene propiedades anticensura y de inmutabilidad. Y añade: «La única estructura electrónica que puede hacer esto es, que yo sepa, la red bitcoin (aunque hay otras blockchain, no son lo bastante inmutables porque sus índices de hash son muy bajos)».³⁹⁸

La protección de los votantes

La intimidación del votante puede tomar un cariz violento. En Zimbabue, el partido que se oponía a Robert Mugabe se retiró de las elecciones porque la coerción ejercida por las milicias que lo apoyaban empezaba a ser peligrosa. Las elecciones se celebraron y Mugabe ganó. Aunque siempre hay gente que aprovecha los adelantos tecnológicos en su propio beneficio, algunos están empezando a creer que la tecnología blockchain podría erradicar la corrupción en lugares como Asia.

En julio de 2014, durante unas de las elecciones presidenciales más controvertidas de la historia de Indonesia, un grupo anónimo de setecientos expertos informáticos creó una organización llamada Kawal Pemilu o «protejamos el voto». Su misión era hacer en línea y públicamente el escrutinio de las elecciones para que los votantes comprobaran los resultados en cada colegio electoral. Los principios de descentralización, transparencia y anonimato se combinaban para conjurar ataques cibernéticos malintencionados y garantizar unas elecciones más justas.³⁹⁹

«¿Quieren los gobiernos corruptos ser honrados?»,⁴⁰⁰ pregunta Anson Zeall, consejero delegado de CoinPip, una empresa especializada en enviar moneda fiduciaria internacionalmente usando el sistema blockchain. Pone en duda que todo el mundo acepte los adelantos que puedan producirse en los sistemas electorales y que los políticos quieran realmente elecciones justas. A otros, la votación electrónica les parece un paso adelante innecesario o precipitado. Nosotros creemos que muchas de estas cuestiones dependen de la voluntad, no de la tecnología.

La reforma de nuestro sistema electoral y político influirá seguramente en otros aspectos fundamentales del voto democrático. Comparemos el fraude de identidad de votantes con otros factores más insidiosos. Un exhaustivo estudio sobre este tipo de fraude hecho en Estados Unidos en 2014 reveló treinta y un casos, con acusaciones y alegaciones creíbles, en elecciones federales, estatales y municipales desde 2000.⁴⁰¹ En ese tiempo, se depositaron más de mil millones de votos sólo en elecciones generales y primarias.

En los cuatro estados con las leyes sobre identidad más rigurosas del país, más de tres mil votos fueron rechazados por falta de identificación correcta.⁴⁰² Esto no incluye a aquellos que ni siquiera se molestan en votar, lo que supone un problema mucho más grave. Pese a que su modelo de democracia se predica por todo el mundo, la mayoría de

los estadounidenses no vota en las elecciones, alegando que «no se hace nada», «los políticos son unos corruptos» y «todos son iguales».⁴⁰³ Esperamos que la tecnología blockchain aporte también soluciones innovadoras a estos problemas.

Con tiempo y desarrollo, la tecnología blockchain podría dar un impulso a la votación electrónica que transformara las elecciones y las instituciones democráticas y las pusiera de una manera real y fiable en manos de los votantes.

Modelos alternativos de política y justicia

Si las blockchains hicieran posible un gobierno más eficiente y una democracia mejor administrada a través de nuevas formas de votación, ¿podrían también ser el catalizador de nuevos procesos políticos?

Para algunos partidarios del gobierno de la siguiente generación, el fin último de la reforma electoral es la creación de un sistema de «democracia líquida». Eduardo Robles Elvira, director tecnológico de Agora Voting, es uno de ellos. Describe la democracia líquida como una combinación de lo mejor de la democracia directa (como la que se practicaba en la antigua Atenas) y de las democracias representativas actuales, que cuentan poco con los electores.

La democracia líquida, también llamada «democracia delegativa», permite que el ciudadano personalice al máximo su experiencia democrática. En palabras de Robles Elvira, en una democracia líquida «podemos elegir nuestro nivel de participación en todo momento».⁴⁰⁴ Nuestra aportación es siempre bienvenida, pero no necesaria para que el país funcione.

Los votantes pueden delegar su derecho de voto en numerosos representantes en una serie de temas.⁴⁰⁵ Se hacen frecuentes referendos y se categorizan por temas, indicando qué apoderado deberá depositar el voto de sus representados en la cuestión de que se trate. Esto permite crear un sistema en el que los votantes escogen a un conjunto de expertos o consejeros fiables que votan en su lugar. La idea subyacente es que ninguna persona (ni ningún partido) tiene la respuesta completa y exacta a todas las cuestiones. En las democracias representativas muchas veces este axioma se da por supuesto y a la vez se ignora.

Robles Elvira trabaja con una serie de gobiernos para crear «un registro de sucesos altamente distribuido y único que resuelva el problema de los ataques de denegación de servicio [en sistemas] distribuidos (DDoS, por sus siglas en inglés)». La tecnología blockchain permite hacerlo. Dice: «Es muy difícil crear un sistema seguro y distribuido y las blockchains nos lo permiten... Y no es sólo que sea distribuido, sino que lo es de una manera segura. Esto es muy importante y puede ser útil en multitud de aplicaciones; la votación electrónica no es sino una de ellas». Su empresa, Agora Voting, ofrece la infraestructura tecnológica necesaria para realizar elecciones electrónicas verificables y transparentes. «Con tecnología criptográfica puntera, los seres humanos son el eslabón más débil de la cadena de seguridad.»⁴⁰⁶

El partido antiausteridad español Podemos usa Agora Voting para celebrar sus elecciones primarias. Con el compromiso con la democracia participativa iba el compromiso con la transparencia, un giro ideológico en España y en todas partes que coincide con el que apuntala las tecnologías distribuidas.

Robles Elvira también ve limitaciones. Para maximizar la seguridad y el anonimato los usuarios normalmente tienen que acceder a toda la blockchain, que pesa muchísimo. Su enorme tamaño dificulta su acceso (sobre todo en un teléfono móvil) y su manejo. Con todo, la tecnología no para de evolucionar y mejorar. «Estamos en el comienzo del voto telemático», dice Robles Elvira.⁴⁰⁷ La tecnología es flexible. Sin duda, sus mejores aplicaciones están por llegar.

Resolución de conflictos

Algunos conflictos legales es mejor no llevarlos a los tribunales. Hemos visto cómo los contratos inteligentes pueden contribuir a dirimir conflictos comerciales. Sin embargo, los contratos inteligentes son indiferentes a las nociones de justicia o equidad y no pueden reconciliar versiones de hechos contrapuestas. El sistema blockchain es incluso más revolucionario que un registro de pruebas verificable, porque puede ser una plataforma que permita la resolución de conflictos ente iguales. En este modelo, los jurados pueden constar de cientos o de miles de personas que, como dice Pamela Morgan, de Empowered Law, «son micromecenas de la justicia».⁴⁰⁸

Elecciones con muestras de votantes elegidos al azar

Otro modelo democrático que la gestión con blockchain permite es el de las elecciones con muestras de votantes elegidos al azar. Unos votantes escogidos al azar reciben por correo una papeleta y unas direcciones de sitios web con información de los candidatos y declaraciones de las partes interesadas. Cualquiera puede solicitar una papeleta, pero ésta no será contada, y nadie excepto el votante que la ha solicitado podrá distinguirla de las papeletas válidas. Estas papeletas pueden venderse, pero el comprador nunca sabrá si el voto que ha comprado cuenta. Como parece más probable que se vendan estos votos que no los que cuentan, la coerción resulta impracticablemente costosa. David Chaum, inventor del concepto, dice que la votación con muestras elegidas al azar podría dar unos resultados más representativos y fiables que las elecciones que hoy celebramos normalmente.⁴⁰⁹

Mercados de predicción

La empresa Augur usa el sistema blockchain para agregar muchas pequeñas apuestas sobre acontecimientos futuros y crear modelos predictivos seguros. Aplicado correctamente, podría contribuir a crear una democracia colaborativa. Los gobiernos

podrían usar los mercados de predicción para hacer que los ciudadanos contribuyeran a una mejor comprensión de los escenarios futuros, lo que les permitiría tomar mejores decisiones políticas.

Vitalik Buterin, de Ethereum, piensa en un modelo político alternativo llamado *futarquía*.⁴¹⁰ Concebido por el economista Robin Hanson, sus principios pueden resumirse en el lema: «Votemos por valores, pero apostemos según nuestras creencias». Los ciudadanos eligen a sus representantes en un proceso que consta de dos etapas: primero, se escoge un parámetro que mida el estado del país (como el índice de analfabetismo o de paro); segundo, se usan los mercados de predicción para seleccionar las políticas públicas destinadas a mejorar esos índices.

Sistemas predictivos como el de Augur podrían hacer participar a los ciudadanos con pequeñas decisiones que contribuirían al debate político nacional y, en última instancia, a modelar el futuro de su democracia.

Las blockchains y la justicia

El sistema blockchain también puede transformar la administración de justicia. Combinando los conceptos de transparencia, colaboración masiva y participación ciudadana en línea —en una blockchain—, podemos volver a introducir conceptos de la democracia de la antigua Atenas en el siglo XXI.⁴¹¹ CrowdJury⁴¹² se propone transformar el sistema judicial celebrando procesos judiciales en línea gracias tanto al sistema blockchain como a la colaboración masiva. La plataforma permite que los ciudadanos presenten denuncias o quejas, reúnan y examinen pruebas, participen en juicios en línea abiertos y en jurados, y que emitan veredictos. Con procesos transparentes en los que la gente colabora para denunciar hechos, analizar pruebas y dictar sentencias, obtenemos resultados certeros en plazos mucho más breves y a un coste mucho más bajo.

El proceso⁴¹³ empieza con la denuncia en línea de una mala práctica (por ejemplo, la de un funcionario sospechoso de aceptar sobornos). Se invita entonces a posibles testigos a que aporten pruebas y se combina información de múltiples fuentes. La denuncia original, así como todas las pruebas, se archivan criptográficamente en una blockchain para garantizar que quedan registradas y no pueden manipularse.

Una vez todo registrado, grupos relativamente pequeños de voluntarios (de nueve a doce personas), con los conocimientos y la experiencia requeridos, se ofrecen a analizar los hechos y determinar si son válidos para pasar a juicio. En el curso del juicio hay dos posibilidades. La primera, que el presunto «delincuente» se declare culpable y proponga una reparación (que el jurado puede o no aceptar). La segunda, que la denuncia siga su curso y el juicio se celebre en línea con un jurado masivo. Como en Atenas, donde cualquier ciudadano de más de treinta años podía pedir formar parte del jurado durante un periodo determinado (pero no para un caso concreto), las personas pueden solicitar ser miembros del jurado y al final son seleccionadas por un mecanismo aleatorio, igual que los jurados atenienses del siglo IV a.C. eran elegidos por un *kleroterion*.⁴¹⁴ En consecuencia, la distribución de jurados entre los casos concretos no es sesgada. El juicio

y todas las pruebas se muestran en línea según el modelo de los juicios públicos. Cualquiera puede «asistir» y preguntar al acusado, pero sólo el jurado emite el veredicto mediante una votación en línea.

Empecemos por la resolución de conflictos de poca entidad en comunidades globales que se salten fronteras jurisdiccionales, como, por ejemplo, las redes sociales. El Consejo de Justicia Civil del Reino Unido se ha fijado en modelos globales en línea para recomendar la resolución de conflictos también en línea.⁴¹⁵ La mayoría de los primeros modelos de este tipo dependen de la intervención de jueces u otros árbitros expertos en algún estadio del proceso. En otros procesos se recurre a otros participantes para que resuelvan conductas inapropiadas como dar opiniones difamatorias (por ejemplo, la filial de eBay en los Países Bajos Marktplaats' Independent Feedback Review) o hacer trampa en juegos en línea (como Valve's Overwatch, que permite que miembros cualificados de la comunidad estudien denuncias de mala conducta y apliquen expulsiones temporales, cuando sea pertinente).⁴¹⁶

Esto dista mucho de ser la justicia de la turba. Es la «sabiduría de la multitud» aplicada a muchos procesos judiciales con resultados beneficiosos.

La gente tiene que comprometerse a resolver los grandes problemas

La mayoría de las personas que creen en la ciencia entienden que las emisiones de carbono están calentando la atmósfera. Este cambio climático es peligroso para nuestra vida y para la de otros seres del planeta. Gobiernos, empresas y ONG que trabajan para reducir las emisiones de carbono coinciden en que el llamado «mercado del carbono» es una forma medioambientalmente eficaz y económicamente razonable de reducir emisiones.

Una de las políticas se llama «comercio de derechos de emisión» (*cap and trade*). Un organismo regulador establece un límite (*cap*) a las emisiones de carbono y con el tiempo va bajándolo para reducir la cantidad de contaminantes que se emiten a la atmósfera. Además, existe un mercado (*trade*) de derechos de emisión que ayuda a las empresas y a otras organizaciones a cumplir con el límite que se les ha asignado. Según el Fondo para la Defensa del Medio Ambiente, «cuanto menos emitan, menos pagan, de manera que, económicamente hablando, les interesa contaminar menos».⁴¹⁷

Hoy, los países más desarrollados de la Unión Europea compran y venden derechos de emisión. California, Ontario y Quebec han firmado el Protocolo de Montreal que aboga por un mercado global. Los funcionarios nacionales, estatales y municipales, así como los empresarios, podrían asignar créditos de carbono para equilibrar derechos de emisión. Al mismo tiempo, los sistemas de reputación basados en blockchain podrían puntuar a los que suministran kilovatios/hora a la red según criterios de reducción sostenible de gases de efecto invernadero. Por ejemplo, el sistema podría marcar la energía procedente del carbón con deudas más altas y las renovables, como la solar, como créditos. Las blockchains pueden contribuir a automatizar el sistema de compraventa de derechos de emisión a escala industrial. Una serie de eficientes algoritmos de fijación de

precios contabiliza créditos y deudas en tiempo real, y organizaciones ecologistas registran en el archivo los créditos de carbono, hacen seguimiento de ellos y los introducen en el mercado.

¿Y si creáramos un sistema de compraventa de derechos de emisión para la gente? ¡Está claro que se necesita algo más que instituciones para cambiar nuestra conducta! El mercado de carbono personal funcionaría por medio del internet de las cosas. Sensores, detectores e instrumentos varios medirán la energía que gasta nuestra caldera, nuestro lavavajillas y nuestra calefacción en tiempo real y nos informará del balance de nuestros créditos de carbono. Al mismo tiempo, podríamos ganar créditos si actuamos de una manera sostenible. Si instalamos una serie de placas solares en nuestro tejado, ganaríamos créditos inyectando la energía sobrante en la red.

¿Podría esto crear nuevas fuentes de ingresos para la gente? Después de todo, los pobres y los vagabundos usan poco carbono. Si vamos al trabajo en bici, podríamos ahorrar créditos que nuestra caldera podría gastar: «Eh, lavavajillas: mi medidor personal de créditos de carbono me dice que podemos permitirnos un lavado completo y un ciclo de secado de treinta minutos». Unos detectores de agua incorporados al aparato podrían regular el gasto de agua basándose en un nivel aceptable de densidad de partículas, y unos detectores de humedad podrían apagar la secadora cuando la ropa se hubiera secado lo suficiente, y el sistema de calefacción, ventilación y aire acondicionado podría aprovechar el calor sobrante.

Herramientas de la democracia del siglo XXI

Como registro global, distribuido y programable que es, diseñado para garantizar la privacidad y enriquecido con sistemas de incentivos, la tecnología blockchain se presta al desarrollo de nuevas herramientas democráticas, tales como:

Cooperación digital: Los funcionarios públicos y los ciudadanos podrán reunirse en línea para debatir en tiempo real sobre cuestiones o necesidades políticas. Al final el consenso se logra mediante sistemas de votación por los que una ficha equivale a un voto, y que pueden contribuir al debate serio e impedir que gente malintencionada, trolls y saboteadores causen daño.

Concursos: Competiciones en línea con jurado. Pensemos en los modelos anteriores a las blockchains como el Goldcorp Challenge (mencionado antes), el X Prize, o los numerosos concursos innovadores lanzados por muchos gobiernos occidentales. El objetivo de estos concursos es que los ciudadanos se comprometan con la innovación y la creación de valor público.

Jurados y tribunales ciudadanos en línea: Ciudadanos elegidos al azar hacen las veces de jurado o de asesores en un asunto. El jurado usa internet para compartir información, hacer preguntas, debatir y escuchar a testigos. Los sistemas de reputación basados en blockchains permitirán a los interrogadores conocer los antecedentes y la reputación de los miembros del jurado. Las decisiones y actas quedan registradas en la blockchain.

Votación deliberativa: Pone a disposición de los ciudadanos recursos para informarse y reflexionar sobre las cuestiones de que se trate de una manera colaborativa y deliberativa. El mecanismo combinará debates de pequeños grupos en internet con muestras de votantes aleatorias, lo que contribuirá a que la aportación pública a la toma de decisiones sea más informada que la de la votación instantánea.

Planear escenarios: Construir escenarios con programas informáticos de simulación y creación de modelos que permitan proyectar necesidades futuras y entender las consecuencias a largo plazo de las decisiones. Políticos, burócratas y ciudadanos podrían evaluar el potencial impacto de una serie de factores que van de la salud al medio ambiente, pasando por la economía.

Mercados de predicción: Como explicamos en el caso de Augur, las posibilidades de usar los mercados de predicción para comerciar con el resultado de los acontecimientos son innumerables. Los gobiernos pueden usarlos para entender mejor muchas cuestiones importantes: ¿Cuándo se construirá el puente? ¿Cuál será la tasa de desempleo dentro de doce meses? ¿Habrá un primer ministro del Partido Nacional después de las elecciones, como reza una pregunta que se ha formulado en un mercado de iPredict en Nueva Zelanda?

Las tecnologías blockchain podrían potenciar todas estas herramientas. Para empezar, la contribución de los ciudadanos podría ser privada, lo que multiplicaría la participación. Esto es malo para los gobiernos represivos, pero bueno para la democracia, porque les hace más difícil a las autoridades gubernamentales censurar, reprimir y perseguir a la oposición. Al mismo tiempo, como hemos explicado antes a propósito de Bloquepedia, los sistemas de reputación basados en blockchain podrían mejorar la calidad del debate, reducir el número de trolls y saboteadores y garantizar que todos los comentarios quedan registrados de una manera segura e indeleble. Cuando haya que compensar a los ganadores u otros participantes, los pagos podrían hacerse de forma mucho más granular e instantánea con monedas digitales. Podrían establecerse contratos inteligentes con ciudadanos y grupos para dejar más claras las funciones de cada cual en el proceso.

Melanie Swan, fundadora del Institute for Blockchain Studies, afirma que la tecnología blockchain podría contribuir a que la sociedad se planteara con mayor madurez temas como el gobierno, la independencia y el deber cívico. «Puede parecer más difícil dejar que una autoridad centralizada se ocupe de asuntos como el gobierno y la economía frente a otros como la cultura y la información, pero no hay razón para pensar que no pudiera desarrollarse también madurez social en este contexto.»⁴¹⁸

Es evidente que la nueva generación de internet ofrece grandes oportunidades. Los retos principales no son tecnológicos. Un ejemplo aleccionador: durante la campaña electoral de Barack Obama de 2008 se creó una plataforma en internet llamada MyBarackObama.com que ofrecía a los partidarios del candidato una serie de herramientas para organizarse, crear comunidades, recaudar dinero e invitar a la gente no sólo a votar sino a implicarse en la campaña. Lo que resultó fue una fuerza sin precedentes: 13 millones de partidarios conectados entre sí que se organizaron y formaron

35.000 comunidades de personas con intereses comunes. Cuando los jóvenes cantaban «Sí, podemos», no era sólo un eslogan de esperanza, era una afirmación de poder colectivo.

Sin embargo, en 2012 la campaña de Obama pasó de buscar la participación ciudadana a usar «macrodatos» para sustituir el «Sí, podemos» por «Os conocemos». Empleó los datos para influir en los votantes y partidarios y sacarles dinero. La campaña ganó las elecciones, pero relegó a los ciudadanos al papel de consumidores de mensajes. La estrategia de los macrodatos era menos arriesgada que la de las comunidades que se organizan.

En sus dos legislaturas, Obama dio importantes pasos para hacer participar a los ciudadanos, sobre todo por medio de los «concursos», que son elaboradas competiciones de ideas innovadoras. Pero en su segunda y vital campaña, Obama renunció a la participación ciudadana y perdió una ocasión histórica de reforzar la legitimidad del gobierno. Al final, incluso él, al que llamaban «el primer presidente de internet», escogió la vía pragmática para acceder al poder usando los medios sociales para difundir mensajes y recaudar fondos mediante una propaganda en línea oportunamente dirigida.

¿Quién iba a hacerlo sino el presidente de internet?

Todos tenemos un papel que desempeñar en la tarea de incorporar las blockchains al gobierno y a la democracia. En primer lugar, hay oportunidades ilimitadas para eliminar redundancias y pérdidas de tiempo, para votar y participar en nuevos procesos democráticos, para ser jurado, para ganar créditos energéticos, para pagar impuestos y recibir servicios públicos, así como para saber dónde van los dólares de nuestros impuestos y lo que votan nuestros representantes. Los representantes elegidos han de dar un paso adelante y liderar la creación y aplicación de contratos inteligentes. Si actuamos con integridad, ¿por qué no apoyar la creación de sistemas de reputación en blockchains? «Los votantes tienen poca memoria», dice Andreas Antonopoulos.⁴¹⁹ Creemos más transparencia, tanto si somos jueces como si somos abogados, policías o parlamentarios. Empleados públicos y funcionarios podrían usar sensores y cámaras para controlar activos públicos y registrarlos en blockchains, priorizar reparaciones de infraestructuras y asignar recursos. Lector, si eres joven, no renuncies a la democracia. Ésta puede romperse pero también arreglarse. Centrémonos en la financiación de campañas electorales como punto de partida para conseguir transparencia en las blockchains, porque actualmente el gran capital es el principal problema. Si somos contratistas públicos, usemos contratos inteligentes para acabar con las mordidas y el despilfarro y demostrar que somos mejores. Las posibilidades abundan.

Indudablemente habrá que luchar mucho para cambiar las cosas, pero ¡ciudadanos del mundo, uníos! ¡Con las blockchains todos ganaremos!

Capítulo IX

Una cultura libre con las blockchains: suena a gloria

No fue el típico primer cumpleaños de nuestro potro. La celebración tuvo lugar en la Round House, que en otro tiempo fue un establo, a una hora de Londres, y contamos con un árbol de luces led que se encendían y apagaban al compás del sonido, un castillo hinchable y un bufé digno de Enrique VIII. La peña era ecléctica: había un malabarista «de contacto», dos docenas de niños pequeños con sus respectivos padres, vecinos, músicos y un puñado de desarrolladores de blockchain. Estaba también Vinay Gupta, un ingeniero escocés de origen indio conocido por haber inventado el «hexayurt», un tipo de casa refugio para damnificados de desastres. Gupta es ahora «explicador jefe» y se dedica a eso, a explicar las tecnologías blockchain a la gente. También estaba Paul Pacífico, consejero delegado de Featured Artists Coalition. Después de trabajar en la banca, Pacífico lucha ahora por los derechos de los músicos. Y, por supuesto, estaba nuestra anfitriona, Imogen Heap, una compositora y música reconocida a la que los lectores de *Music Week* eligieron «artista inspiradora del año»,⁴²⁰ y madre de Scout, su hija de un año.

«Quiero saber si lo que estoy haciendo le valdrá de algo a Scout algún día», nos dice Heap. Está muy preocupada por la industria de la música. «La industria musical está muy fragmentada; hay muy poco liderazgo y lo que es el negocio de la música se ve con mucha negatividad —dice—. Todo está patas arriba. Los artistas están al final de la cadena alimentaria. Eso no puede ser. La música está por todas partes, todo el tiempo. Está en nuestros teléfonos, en nuestros taxis, en todas partes. Pero los artistas cada vez se benefician menos.»⁴²¹

Y ahí está el problema. Internet es una gran musa, a la vez un medio creativo y un canal para la libre expresión. No faltan ideas para lo que artistas, diseñadores y codificadores con talento —y sus muchos fans— pueden hacer unos con otros en la red. Ni faltan tampoco medios para hacer dinero con toda esta colaboración creativa. Industrias como la de la edición y grabación de música han encontrado nuevas fuentes de ingresos en las descargas digitales y en la transmisión en línea (*streaming*) de archivos de sonido. El problema es que, con cada nuevo intermediario, los artistas se llevan menos parte y cuentan menos. David Byrne, de Talking Heads, resume así la situación en un artículo: «Creo que el modelo es insostenible como medio de apoyo del trabajo creativo, sea del tipo que sea. No sólo la música. El resultado inevitable será que internet se chupará el contenido creativo de todo el mundo hasta que no quede nada».⁴²²

Este capítulo trata de cómo las tecnologías blockchain están haciendo a los artistas protagonistas del modelo, de manera que no sólo puedan ejercer su derecho de expresión, sino también beneficiarse de él, maximizando el valor del interés moral y material que despierta su propiedad intelectual. Dicho de otro modo, devolverles sus derechos. Se acabaron los grandes y ávidos intermediarios, se acabaron los grandes censores gubernamentales. Repasaremos un panorama cultural —arte, periodismo y educación— en el que están en juego derechos humanos básicos y modos de ganarse la vida.

Un negocio musical justo: de transmitir música en directo a vender derechos

«Si Scout fuera música, ¿cómo ganaría dinero? No podría», dice Imogen Heap hablando de la carrera musical de su hija, si dependiera del actual modelo de industria musical. «Necesitamos algo simple y esencial, algo en lo que podamos confiar, para que nos creamos que podemos ganarnos la vida con la música.»⁴²³ Paul Pacífico está de acuerdo con ella: «Queremos una industria musical que refleje el sentido cultural, tecnológico, social y comercial de nuestro tiempo y permita que los creadores y consumidores, por igual, tengan un porvenir sostenible y viable».⁴²⁴ Heap, Pacífico, Vinay Gupta y otros se han unido para crear este nuevo ecosistema musical.

Si hubiera un mercado de predicción para innovaciones, apostaríamos por el Equipo Heap. En 2009, Imogen fue la primera mujer que ganó un premio Grammy por producir su propio álbum, «Ellipse». Se llevó a todos sus seguidores de Twitter a la ceremonia de entrega de los premios porque llevaba lo que ahora se conoce como el «vestido Twitter», un vestido diseñado por Moritz Waldmeyer con una especie de cremallera led que reproducía tuits de sus fans alrededor de sus hombros. En 2013, Heap lanzó Mi.Mu, una empresa sin ánimo de lucro para crear un sistema de guantes musicales, combinando programas informáticos de mapeo y sensores de movimiento, con los que los artistas pueden controlar las luces, la música y los vídeos por medio de gestos personalizados. El invento logró el primer galardón en los premios Berlín de 2015 en la categoría de «WearableIT/ FashionTech». Los guantes tuvieron éxito enseguida. La estrella pop Ariana Grande publicó este mensaje en YouTube con su versión de la canción *Hide and Seek* de Heap: «Quiero dar las gracias a mi ídolo @imogenheap por permitirme usar los guantes Mimu en mi primera gira mundial».⁴²⁵ Si alguien duda de la capacidad de Heap de reunir a una comunidad en torno a nuevas tecnologías, hace mal.

«Sabemos muy bien lo que queremos —dice Heap—. No somos una pandilla de cabezas de chorlito que fumamos porros en el salón y hacemos música. Somos empresarios que trabajamos duro.»⁴²⁶ Heap cree que la tecnología blockchain es una plataforma nueva para que los creadores de propiedad intelectual obtengan un valor justo por ella. Los contratos inteligentes, en concreto, podrían reducir la magnitud de la complejidad de la industria y simplificar el papel crítico de los sellos discográficos en este ecosistema.

Rube Goldberg golpea de nuevo:

Parafraseando a Talking Heads, ¿cómo hemos llegado a esto? ¿Qué podemos hacer?⁴²⁷ Todo empieza por un problema serio para los artistas: firmaron contratos pensados para la era del vinilo, en la que los enormes costes de la producción y distribución analógica se interponían entre los artistas que grababan y sus clientes potenciales. Heap nos dice: «Cuando firmé con mi primer sello discográfico, creo que conseguí un 15 por ciento. En mi último contrato de grabación, hace unos años, conseguí un 19 por ciento. Con un poco de suerte, ahora se puede conseguir un poco más».⁴²⁸ Los artistas pueden haber cedido sus derechos a un sello discográfico por todo el tiempo que dura el *copyright*. En Estados Unidos eso son noventa y cinco años o lo que viva el artista más setenta años. ¡Cuántas innovaciones no previstas tendría que contemplar un contrato para seguir siendo justo con los artistas y sus herederos!

Al principio, los sellos discográficos eran muy pequeños, la radio y las tiendas de discos predominaban, y los departamentos de personal no sólo buscaban nuevos talentos sino que también dirigían la carrera artística de éstos. En los últimos veinticinco años, la industria se ha concentrado, pasando de miles de sellos a tres grandes casas discográficas —Sony Music Entertainment, Vivendi's Universal Music y Warner Music Group— y unos cientos de casas independientes. Estos tres grandes sellos tienen una participación del 15 por ciento en Spotify, el servicio de difusión de música más popular y lucrativo.⁴²⁹ Es decir, que recibirán ingresos extra cuando Spotify salga a bolsa. Apple se ha convertido en el vendedor de música más grande del mundo y Live Nation en la empresa de espectáculos en vivo más grande del mundo.

Es decir, que unos pocos controlan el *copyright* de la música. Los sellos discográficos y las empresas de giras promocionales han empezado a pedir a los artistas que firmen los llamados «contratos de 360 grados», lo que les garantiza un porcentaje de todas las ganancias que genere un artista —derechos de publicación de la composición original, derechos de uso de la grabación, derechos de actuación cuando el artista va de gira, posibles derechos de comercialización y promoción—, independientemente de que inviertan en la explotación de esos derechos.

Con la concentración viene la integración de sistemas, lo que nunca es fácil. Cada conglomerado tiene su propia contabilidad y su propia versión de lo que es un contrato y lo que son los derechos de autor, lo que dificulta la comparación. «Uno de los grandes problemas que tenemos es que la industria está muy fragmentada. Tantas plataformas son una pesadilla», dice Heap.⁴³⁰ Estos sistemas deben ser capaces de innovar en el plano de la producción, formato, distribución y contexto de uso. Pero pocas veces un elemento se vuelve obsoleto inmediatamente, por lo que todas las partes han de mantener dos o más modelos al mismo tiempo, siendo los más evidentes el modelo físico y el digital.

Para mayor complejidad, hay muchos miembros en la cadena de suministro: no sólo editores y sociedades de derechos de actuación (PRO, por sus siglas en inglés) —sociedades que controlan las actuaciones musicales públicas y cobran los derechos correspondientes, como la Sociedad Americana de Compositores, Autores y Editores (ASCAP, por sus siglas en inglés), la Broadcast Music, Inc. (BMI) y la empresa

antiguamente llamada Sociedad de Dramaturgos y Compositores Europeos (SESAC)—, sino también productores y estudios, salas de conciertos, organizadores y promotores de giras, mayoristas, distribuidores y agentes, cada uno con su propio contrato, contabilidad y sistema de comunicación. Todos ellos se llevan su parte y pasan el resto a los agentes y *mánagers* de los artistas. Y lo que queda va a los artistas, según los términos del contrato que hayan firmado. Eso es seguro: el artista es el último que cobra. Pueden pasar entre seis y dieciocho meses antes de que el artista reciba el primer cobro por derechos de autor, dependiendo de los plazos de pago y del periodo contable de la casa discográfica.

Por último, una nueva capa de intermediarios —empresas tecnológicas como YouTube o Spotify— se interpone entre los artistas y las casas discográficas, mermando aún más la parte del pastel que corresponde a los artistas. Fijémonos en el caso de la música de transmisión en línea. Spotify paga de media entre 0,006 y 0,0084 dólares por reproducción a los que tienen los derechos, normalmente las casas discográficas.⁴³¹ Spotify declara en su sitio que paga el 70 por ciento de sus ganancias por publicidad y suscripciones a los que tienen los derechos. Pero nosotros hemos examinado su «Acuerdo de distribución de archivos de vídeo y sonido» con Sony USA Inc., y el pago de unos 42,5 millones de dólares de adelanto no recuperable a los artistas de Sony es todo menos claro. De hecho, el primer párrafo del acuerdo consiste en una cláusula de confidencialidad. Parece que ni Spotify ni Sony pueden informar a los artistas de Sony del impacto que el acuerdo tiene en los ingresos de estos últimos. Rich Bengloff, presidente de la Asociación Americana de Música Independiente, dice que, según su experiencia, las casas discográficas no suelen compartir dinero que no esté directamente ligado al uso.⁴³² El analista Mark Mulligan dice: «Los artistas van a pasarlo mal al menos otros cuatro o cinco años, igual que lo pasaron mal los cuatro o cinco años que siguieron al lanzamiento de iTunes».⁴³³

¿Qué valor añaden, pues, los sellos discográficos? Desde luego, tratan de gestionar esta complejidad, luchar contra la piratería y hacer valer los derechos. Por ejemplo, Universal Music Publishing Group ha dedicado una tercera parte de su personal a administrar los derechos de autor en mercados locales de todo el mundo.⁴³⁴ Y hace poco ha creado un portal del artista en el que éstos pueden ver la situación de sus derechos de autor y pedir adelantos sobre futuras ganancias sin comisión. El portal informa también del uso que hace Spotify: «Cuántas veces se reproduce una canción, qué clase de gente la escucha, quién más figura en las listas de reproducción de esos oyentes, y qué canciones gustan a determinado público». Universal ha dedicado dieciséis empleados a actualizar el portal e interpretar la información para los artistas.⁴³⁵ Las casas discográficas también tienen grandes equipos de abogados y *lobbyists*. Pueden lanzar a nuevos artistas mundialmente, imponiéndoles sus condiciones, dándolos a conocer en medios de comunicación extranjeros, distribuyendo su música en mercados internacionales, cediendo derechos a editores extranjeros, patrocinando giras internacionales y agregando todas las ganancias. El *coste de gestionar* los derechos de autor ha aumentado con la complejidad del sector; un coste que afecta directamente a los artistas de todo el mundo, porque funciona como un impuesto.

Los contratos inteligentes basados en blockchains pueden simplificar estos procesos, sustituyendo a las casas discográficas en el desempeño de un papel fundamental en este ecosistema. Según Imogen Heap, «si somos un programa informático, una base de datos... estos problemas desaparecen, porque la mitad de ellos son cuestión de pura matemática. Este dinero es para esta persona... y no tarda un año o dos en llegar al artista, al escritor, al músico... Es instantáneo porque está automatizado y verificado. Además, los servicios de distribución de la nueva música, que están cambiando la cultura, reúnen una información muy valiosa sobre los fans de los artistas, información que podría ayudar a esos artistas a ser más eficientes si fueran ellos los que la tuvieran».⁴³⁶ Éste es el futuro de la música con el sistema blockchain.

Un nuevo modelo de industria musical

La combinación de plataformas basadas en blockchains y contratos inteligentes —unida a las normas de la comunidad artística sobre inclusión, integridad y transparencia en cuestiones de contratación, privacidad, seguridad, respeto de derechos e intercambio justo de valor— podría permitir a los artistas crear un nuevo ecosistema musical.

«¿No estaría bien que yo pudiera decidir cómo compartir o usar mi música? —se pregunta Heap—. Simplemente subir una canción, por ejemplo, y todo el contenido correspondiente, a un portal, para que todos pudieran usarla, con derechos de uso, propiedad, toda la información que hoy aparece en las fundas de los discos, vídeo, biografía reciente», de manera que todas las demás partes, no sólo sellos discográficos, editores musicales y promotores de giras, sino también empresas que buscan música para anuncios, productores de televisión que buscan bandas sonoras, proveedores de servicios de telefonía móvil que buscan tonos de llamada y los muchos fans que hacen vídeos, podrían decidir si aceptar los términos de uso de Heap. «¿No sería estupendo sentir la presencia del artista, que éste pudiera decidir sobre su música y sentirlo casi físicamente, incluso de un día para otro? —dice—. Por ejemplo, puedo decidir que, como hoy es mi cumpleaños, toda mi música es gratis... O que los oyentes de menos de dieciséis años y de más de setenta no paguen... O enviar todo el dinero a los damnificados de alguna catástrofe, simplemente con cambiar unas palabras del contrato inteligente.»⁴³⁷

Ésta es la idea: crear un modelo de blockchain en el que el artista sea el centro, no las casas discográficas ni las distribuidoras tecnológicas. Los artistas podrían producir música y cobrar justamente por el valor que crean, y los amantes de la música podrían consumir, compartir, mezclar y, en fin, disfrutar de lo que les gusta y pagar un precio justo por ello. Este modelo no excluiría a los sellos discográficos ni a las distribuidoras digitales, pero sí haría de ellos miembros iguales y no dominantes del ecosistema.

Esto no es soñar despiertos. En octubre de 2015, Heap lanzó su primer experimento publicando en internet su canción *Tiny Human* y toda la información relacionada con ella: la versión instrumental, siete *stems* en estéreo, la imagen de portada, el vídeo musical, los comentarios sobre los músicos, el equipo, los créditos, las letras, los agradecimientos, enlaces útiles y la historia de la canción.⁴³⁸ Estos detalles harían más probable que posibles colaboradores la encontraran en internet.

Heap invitaba a los fans, desarrolladores y proveedores de servicios a subir la canción a sus distintas plataformas y compartir su trabajo. Les otorgaba derechos no exclusivos para crear un perfil de artista de Imogen Heap, con la condición de que le facilitaran las claves de entrada y los permisos cuando hubieran subido los archivos de ella a sus sistemas. Si esperaban ganancias, les pedía que ofrecieran modelos de pago, porcentajes y cantidades para que ella pudiera tenerlos en cuenta a la hora de analizar el experimento. Por último, daba la bienvenida a las donaciones que le hicieran a su dirección bitcoin y prometía destinar la mitad a su fundación benéfica, Mycelia, el nombre de este nuevo ecosistema. La información sobre el uso y el comportamiento de los participantes determinaría la siguiente etapa de desarrollo en la blockchain.

Varias empresas están trabajando en el diseño de esta plataforma y colaborando con Heap y otros músicos clarividentes. Este nuevo ecosistema tiene una serie de características que no tiene la industria actual:

Plantillas de contratos que respetan al artista y lo consideran un empresario y un socio a carta cabal en cualquier empresa, fundamental para la creación de valor. Adiós a los viejos contratos de papel que perpetúan los injustos comienzos. «Se acabó que nos quiten nuestros porcentajes de derechos de autor», dice Heap.

Derechos de autor inclusivos que reparten las ganancias equitativamente según la contribución de cada cual al proceso creativo, no sólo compositores e intérpretes, sino también otros artistas e ingenieros. Todo el mundo puede beneficiarse de un superventas, no sólo las casas discográficas y las distribuidoras.

Registros transparentes distribuidos en blockchain para que todo el mundo pueda ver cuánta ganancia produce una canción, el ritmo y la magnitud de las fuentes de ingresos y quién se lleva qué porcentaje. Se acabaron los viejos sistemas de contabilidad exclusivos y basados en el papel. Diferentes categorías según el tipo de ganancia, desde el trabajo hecho para contratar hasta los ingresos por derechos de autor. Fácil contabilidad, fácil auditoría, fácil pago de impuestos.

Posibilidad de microcontabilizar y microrrentabilizar la música para distribuir ingresos en el acto, no sólo la música. Si la música se contabilizara, de forma que los consumidores pudieran hacer micropagos cada vez que reproducen una canción, los pagos por derechos de autor podrían hacerse inmediatamente. Se acabaron los retrasos en los pagos, los cheques por derechos cada dos años o cada tres meses, las cláusulas crípticas. ¡Se acabaron los artistas pobres! El teórico de las blockchains Andreas Antonopoulos pone este ejemplo: «Streamium es un proveedor de vídeos de transmisión en línea argentino que permite a los productores de vídeo cobrar milésimas de céntimo por descargar, pongamos, doscientos milisegundos de vídeo. Usa sistemas de multifirma, de registro temporal de transacciones, de atomicidad y de integridad total para reforzar el esquema. Los productores sólo ofrecen los vídeos por los que han cobrado y los consumidores sólo pagan por los vídeos que han consumido. Renegocian automáticamente el contrato cinco veces por segundo. Si alguno de ellos se retira en algún momento, el contrato acaba y ambos cobran de acuerdo con la transacción más ventajosa que hubiera entre ellos».⁴³⁹

Bases de datos completas que pueden comunicarse entre sí y vincular el material sujeto a derechos —letras, composición y grabaciones— a toda la información que existe sobre ese material, los textos de los discos, material gráfico y fotográfico, los temas, los derechos que el compositor y el intérprete están dispuestos a vender, los términos de esa venta, la información de contacto, etc., y todo en un registro digital que todo el mundo puede ver. Se acabaron las bases de datos incompletas. ¡La disponibilidad de derechos al alcance de nuestros dedos! Los poseedores de los derechos serían fáciles de encontrar.

Análisis de uso de datos que por fin está al alcance de los artistas para atraer a los promotores y anunciantes deseados, organizar giras, preparar actos promocionales y buscar microfinanciación y colaboración creativa con otros artistas. Este modelo puede recuperar «mucha información perdida de todo el mundo, como dónde están nuestros fans, cuántos años tienen, cuáles son sus intereses —dice Heap—. Con esa información, podríamos planear giras a medida, ponernos en contacto con marcas e iniciativas que nos gusten, o promocionar a artistas, productos u organizaciones benéficas que apoyamos. No hablo de información como nombres y direcciones de correo electrónico, sino de una información más amplia pero igual de fundamental. Podríamos intercambiar esa información con otros grupos de música y usarla de mil maneras para bien tanto de los fans como de los artistas.»⁴⁴⁰

Gestión de derechos digitales, o sea, una forma de gestionar los derechos digitales que no sería como los programas de gestión vigentes, contrarios a los intereses del consumidor y que no contemplan más que restricciones al uso. Hablamos de la implantación de contratos inteligentes que gestionen los derechos y maximicen el valor de publicar, grabar, actuar, comercializar, etc. Esto incluye unos *términos de participación de terceros* dirigidos a sellos discográficos y distribuidoras: unos y otras podrían decidir aceptar los términos de uso y expectativas de servicio estipulados por los artistas. Si los artistas no quieren publicidad que interrumpa la experiencia musical, pueden prohibirla. Si quieren un porcentaje de los ingresos por publicidad, pueden estipularlo. Si quieren que una de esas grandes empresas se encargue de la venta y cobro de derechos y de la distribución en países como China, pueden hacerlo. También pueden fijar límites. Si las empresas no producen cierta cantidad de ganancias, los contratos se rescinden automáticamente. Los artistas también necesitan una *gestión de derechos subsidiarios automatizada*, allí donde sea posible o deseada, que permita a los posibles concesionarios aceptar o rechazar los términos de uso y pago estipulados por el artista. El mismo contrato aplica los acuerdos y puede notificar al artista violaciones o rescisiones.

Unos **mecanismos de subasta y fijación de precios** que permitan experimentar con promociones y versiones de contenido, incluso vincular porcentajes de derechos subsidiarios a peticiones de canciones. Por ejemplo, si un consumidor se descarga una canción de éxito, el anunciante que compró esa canción para un anuncio tiene automáticamente que pagar más cuando el anuncio se emita.

Un **sistema de reputación** que entresaca información del historial de transacciones de una dirección bitcoin y de los medios sociales y crea una reputación para esa dirección. Los artistas podrán establecer su propia credibilidad así como la de los posibles socios con los que traten, tanto si son artistas con los que colaboran, como si son consumidores,

casas discográficas, comerciantes, anunciantes, patrocinadores, concesionarios, etc. El uso de contratos inteligentes multifirma permitirá a los artistas abstenerse de tratar con entidades cuya reputación no alcance ciertos niveles o que no tengan bastante capital en sus cuentas.

La clave de esta nueva y justa industria musical es que los artistas están en el centro de su propio ecosistema y no en los márgenes de muchos otros. «Spotify y YouTube también tienen cabida, como la tiene el contenido que el usuario genere —dice Heap—. Tienen cabida las empresas de grabación porque seguimos necesitando personas que pasen por el tamiz los cientos de millones de horas de música, y los miles de millones de bits de música y arte que se crean a diario en todo el mundo.»⁴⁴¹ Con contratos informáticos, los artistas pueden colaborar con otros creadores, con las grandes casas discográficas, con las grandes distribuidoras y con los muchos intermediarios pequeños que decidan sumarse a las blockchains.

*Artistas que se lanzan a sí mismos:
señales del nuevo paradigma musical*

Una amiga de Heap, Zoë Keating, violonchelista y compositora de origen canadiense, siempre ha controlado su música. Posee todos los derechos de reproducción y los originales de sus grabaciones. Diseña personalmente su estrategia de comercialización, venta, cesiones y distribución. Dada la complejidad del sector, estamos muy impresionados. «Los artistas como yo no podríamos existir sin la tecnología. Puedo grabar mi música en mi casa y subirla a internet», ha declarado Keating a *The Guardian*. Según ella, internet ha dado grandes oportunidades a los artistas independientes, pero su experiencia con las distribuidoras de música en línea no difiere mucho de la de Imogen Heap con los sellos tradicionales. «No es justo que los proveedores de servicios repitan las formas de pago del pasado. No es justo aprovecharse de los que carecen de poder —dice Keating—. Las empresas son responsables no sólo ante sus accionistas, sino también ante el mundo y ante los artistas.»⁴⁴²

Keating se refiere al nuevo contrato que el YouTube de Google le ha ofrecido. Es un acuerdo de confidencialidad. Durante años, Keating ha distribuido su música en YouTube y rentabilizado subidas de material suyo por parte de terceros gracias a Content ID, un programa que automáticamente alerta a los poseedores de derechos de posibles infracciones de las leyes de propiedad intelectual. No le preocupa la piratería, que se compartan sus archivos ni las regalías. Para ella, la transmisión en línea es una manera de promocionarse, de llegar a nuevos públicos y de obtener información de uso que puede analizar. Los que han hecho mucho dinero ofreciendo catálogos enteros han sido los agregadores de música y los fabricantes de grandes éxitos. Ella no. La mayor parte de sus ganancias siempre han venido de sus fans más devotos, que pagan de veinte a cien dólares por un nuevo álbum. Primero subía su nuevo trabajo a Bandcamp, luego a iTunes, y al final hacía selecciones que ponía a disposición del público en otros sitios, como YouTube, Spotify o Pandora. Esta estrategia, llamada *windowing* en inglés, que consiste

en ofrecer contenido sólo en un canal durante un tiempo, se ha revelado eficaz para ella y para sus fans más devotos. Podía darles las gracias a sus partidarios y cultivar nuevas relaciones.

YouTube empezó a lanzar un nuevo servicio de suscripción, Music Key, en el que los usuarios pagan una cantidad para evitar publicidad. Si Keating quería seguir rentabilizando su trabajo en YouTube, tenía que aceptar los términos: incluir todo su catálogo y dejar de publicar en otras partes. Era o todo o nada. Sabía que a los sellos independientes no les gustaban las nuevas condiciones de cesión, pero aún les gustaban menos las consecuencias económicas. Keating quiso seguir controlando su música, con sus propias condiciones.

En la blockchain de bitcoin vio una tecnología que podría permitirle hacer eso, empezando porque es transparente. «Es que creo en la transparencia en todo —declaró a la revista *Forbes*—. ¿Cómo vamos a crear un ecosistema futuro si no sabemos cómo funciona el actual?»⁴⁴³ Por ejemplo, en YouTube Keating calcula que hay 15.000 vídeos —de bailes, de películas, de espectáculos televisivos, de proyectos de arte, de sesiones de juego— que usan su música a modo de banda sonora sin su autorización. Tendría que poder beneficiarse de todo este entusiasmo que despierta su trabajo, pero sólo YouTube sabe exactamente lo popular que es su música. Nielsen SoundScan no es sino un aspecto de una realidad que tiene muchas dimensiones.

Como Heap, Keating quiere registrar sus derechos de autor y beneficiarse de los correspondientes metadatos en una blockchain. De ese modo, la gente podría dar con ella, la poseedora de esos derechos, más fácilmente. Y ella podría encontrar a quienes usan su música a través de la blockchain. Con un archivo distribuido de metadatos musicales podríamos saber no sólo quién ha creado qué, sino quién más participó en esa creación. Keating podría visualizar formas de uso y relaciones, calcular el valor real de una canción para establecer un precio dinámico y realizar micropagos a colaboradores e inversores sin necesidad de cajas negras de terceros como ASCAP o BMI.⁴⁴⁴

Repetimos: no estamos diciendo que los sellos discográficos y las empresas tecnológicas no tengan su función, y que los artistas podrían arreglarse solos en un ecosistema de iguales. Hablamos más bien de un nuevo tipo de ecosistema centrado en los artistas, en el que éstos controlan su destino y reciben una compensación justa por el valor que crean. La tecnología blockchain no va a crear un nuevo modelo que diga cómo han de cobrar los artistas. Lo que hará será liberarlos para que elijan entre una infinita gama de soluciones aquella que más satisfaga sus necesidades y responda a sus creencias. Pueden ofrecer su trabajo gratis o microrrentabilizarlo todo, pero es algo que eligen ellos, no los sellos discográficos ni las distribuidoras.

Otros elementos del nuevo ecosistema musical

Registro básico de derechos de autor

Hay dos dimensiones fundamentales de los derechos de autor musicales. El primero es el derecho mundial a la composición original —las notas musicales y la letra— en cualquier forma o idioma, que normalmente tiene el compositor-letrista. La música y la letra

pueden tener derechos de autor independientes. El compositor-letrista cobra regalías siempre que alguien graba o interpreta la canción, compra la partitura, la adapta a otro género (por ejemplo, al de la música ambiental), la traduce a otro idioma o incluye la música en una antología o en un libro de texto. El segundo es el derecho mundial a la grabación de sonido, una interpretación grabada y guardada en algún soporte, como un archivo digital o un vídeo musical. Los derechos de autor de la grabación suele tenerlos el intérprete o los miembros de la banda, que perciben regalías cuando esa grabación se emite por radio, televisión, internet, o se vende en algún soporte físico como vinilo, CD o DVD.

El grado de autonomía de Zoë Keating animó a la banda de rock industrial de Toronto 22Hertz a recurrir a las blockchains. En Canadá, registrar los derechos de autor de una canción cuesta cincuenta dólares, y el certificado no contiene más que el título de la obra. El fundador de la banda, Ralf Muller, no creía que eso fuera a ayudarlo ante un tribunal, en caso de que alguien usara la letra o la melodía. Por eso decidió recurrir al sistema de hashes, y creó un hash de toda la canción con una herramienta llamada OP_RETURN y lo insertó en una blockchain. Si alguien usara su letra o su música, podría demostrar que es el propietario señalando la transacción en la blockchain, generando otro hash de la canción y comparando este segundo hash con el registrado en la blockchain. Serían idénticos. «Cuando codificamos un hash en OP_RETURN y sobre él se escriben sucesivos bloques, es imposible retroceder y cambiar nada. Para mí es algo estupendo.» Cuando se le pregunta por qué la tienda en línea de la banda acepta bitcoins y ofrece descuentos a los que pagan con esta moneda digital, Muller contesta rotundamente: «Porque no soy un negociante típico».⁴⁴⁵

Sistema de gestión de contenido digital

Colu es una original plataforma de gestión de contenido digital basada en la tecnología blockchain bitcoin, que ofrece a desarrolladores y empresas una serie de herramientas para acceder y gestionar activos digitales como derechos de autor, entradas de espectáculos y tarjetas regalo, algo que una industria musical realmente distribuida necesitaría. Colu se ha asociado con la empresa líder en tecnología musical Revelator para crear una «interfaz de programación de aplicaciones» (API, por sus siglas en inglés) para gestión de derechos. La idea es hacer realidad lo que Imogen Heap y Zoë Keating querían: poner orden en el mundo de la propiedad de derechos, la distribución digital y el uso real de la música. La API permitirá también a las empresas del sector ser más transparentes y eficientes, como se les exige. «Estamos muy entusiasmados por las posibilidades que la plataforma Colu ofrece de simplificar la gestión de derechos musicales, empezando por los de los compositores y sus canciones —dice Bruno Guez, fundador y consejero delegado de Revelator—. Colu ha hecho que la compleja tecnología blockchain pueda integrarse en plataformas como la nuestra, y estamos deseando explorar de qué manera puede eso mejorar el servicio que ofrecemos a nuestros clientes.»⁴⁴⁶

El nuevo departamento de «artistas y repertorio» (A&R)

Por último, un aspecto clave de toda industria creativa es la búsqueda y formación de talentos, función que, en las casas discográficas, desempeña el departamento llamado de «artistas y repertorio». Los músicos suelen aceptar de buen grado la idea del mentor y aspiran a ser descubiertos en concursos de canto como La Voz. El sistema blockchain apoya estas actividades de A&R con algoritmos de uso. Pensemos en la empresa PeerTracks, que, según dice en su portal de internet, es «la plataforma total» tanto para los artistas como para los amantes de la música. PeerTracks asocia sendos contratos inteligentes a las canciones que un artista sube a la plataforma, y esos contratos reparten automáticamente las ganancias según los acuerdos que el intérprete haya hecho con el letrista, el compositor y demás miembros de la banda. Los artistas crean sus propias monedas, que llevan su nombre y su cara, como los cromos de béisbol en Estados Unidos. Estas monedas son coleccionables. El artista establece el número de monedas disponibles. O sea, que puede haber ediciones limitadas, por así decirlo. La idea es simple: crear un depósito de valor, cuya cotización depende de la popularidad del artista.⁴⁴⁷

Los usuarios tienen acceso al catálogo completo de manera gratuita y sin interrupciones publicitarias. Pueden guardar canciones y listas de reproducción para oírlas sin conexión y descargarse cualquier canción o álbum del catálogo. A diferencia de Spotify o iTunes, los usuarios también pueden comprar monedas de artistas y comerciar con ellas como si fueran cromos. Cuando un artista tiene éxito, el valor de sus monedas sube, con lo que los usuarios podrían rentabilizar el apoyo dado a artistas antes de que se hagan famosos. Amar a un artista significa ser tratado privilegiadamente, recibir gajes y cosas gratis. Estos incentivos convierten a los oyentes, que serían pasivos en Spotify, en promotores activos y crean una base de fans duraderos y comprometidos. PeerTracks quiere pagar más a los artistas por descargas y transmisión en línea —concretamente el 95 por ciento de las ganancias— y pagarles instantáneamente con las blockchains. Los artistas pueden poner el precio que quieran a las descargas de música y a los artículos en venta. PeerTracks asegura que «multitud de cazatalentos/mentores en busca de la próxima estrella/ moneda de éxito» oirán la canción de un nuevo artista porque los usuarios de PeerTracks votarán por él.⁴⁴⁸

Artlery para amantes del arte: conectar a artistas y clientes

El mercado de arte tradicional es notoriamente exclusivo y opaco. Un número relativamente reducido de artistas y coleccionistas ocupa un porcentaje grandísimo del mercado, y las vías para que los artistas emergentes entren en el mundo del arte son pocas, estrechas y muchas veces tortuosas. Aun así, la índole abierta y, en general, poco regulada del mercado de arte hace posible experimentar con nuevos conceptos y medios, lo que democratiza tanto ese mercado como el mercado de capital, así como con el poder transformador y revolucionario de la blockchain bitcoin.

Artlery dice ser una comunidad de artistas que están dispuestos a compartir parte de sus ganancias con clientes e iguales que se comprometan socialmente con sus obras.⁴⁴⁹ El propósito de Artlery es acuñar en una blockchain una moneda que las obras de arte consideradas como activos respalden, haciendo que los amantes del arte participen a

modo de propietarios parciales y accionistas de la obra con la que interactúan. La idea es ofrecer incentivos a todos los actores del mercado —artistas, clientes, conservadores, galerías, museos, talleres y ferias—, en lugar de ofrecer incentivos perversos a uno de ellos en detrimento de los demás. Para aumentar la clientela y la reputación de un artista, Artlery lanza una oferta pública de venta inicial (IPO) de piezas digitales de la obra de ese artista. La aplicación de Artlery permite a artistas como JaZoN Frings, David Perea, Keith Hollander, Benton C Bainbridge y los Baazar Teens reproducir sus obras físicas digitalmente, dividiéndolas en muchas piezas como si fueran un puzzle, y repartirlas a los clientes según el grado de apreciación que les atribuya la aplicación. Mientras dura la oferta pública de venta de una obra, los compradores pueden acumular interés hasta un determinado porcentaje de la obra que el artista regaló a la comunidad. Cuando la plataforma se consolide, Artlery tiene previsto permitir la transferencia y venta de los intereses acumulados en las obras.

En el congreso sobre blockchain de Stanford de 2015 patrocinado por Artlery, Don decidió apoyar una obra de Anselm Skogstad titulada *EUR/USD 3081*, una reproducción artística de un billete de euro agrandado e impreso en un panel de aluminio Dibond de 147 por 111 centímetros.

Cómo comprar arte a través de la blockchain bitcoin

Para comprar la obra, Don abrió su cartera bitcoin y la usó para crear un mensaje que especificaba la cantidad de bitcoins que equivalían al precio de la obra, designó la clave pública de Artlery como la destinataria de esos bitcoins y usó su clave privada para «firmar» o autenticar el mensaje. Don se aseguró bien de que todos los datos eran correctos porque, a diferencia de los métodos de pago tradicionales, no hay posibilidad de revertir una transacción bitcoin. Por último, envió el mensaje no a su banco canadiense, sino a toda la red de ordenadores en los que está ejecutándose plenamente la blockchain bitcoin.

Hay personas que a estos ordenadores los llaman «nodos», y algunos de ellos ofrecen su capacidad procesadora para resolver problemas matemáticos asociados a la creación de los bloques. Como hemos explicado, la comunidad bitcoin llama «mineros» a estas personas, y a su actividad de resolver problemas la llama «minado», como si se tratara de una mina de oro. Es una analogía capciosa porque uno se imagina que son expertos cuyo talento puede darles alguna ventaja sobre los novatos. No es verdad. Cada minero ejecuta el programa como si fuera una utilidad del sistema y el programa hace todos los cálculos. Los mineros serios configuran sus ordenadores para optimizar la capacidad procesadora, minimizar el gasto de energía y aprovechar la conexión de alta velocidad de la red. Aparte de eso, no se necesita ninguna aptitud especial ni se toleran interferencias humanas.

No todos los nodos minan. De hecho, la gran mayoría de los nodos de la red bitcoin se limitan a realizar tareas de verificación de la información recibida antes de mandarla a los demás miembros de la red. Esta red verifica las dos informaciones —que Don controla la cantidad de bitcoins especificada y que autoriza la transacción— y reconoce

su mensaje como una transacción. Entonces los mineros disputan una carrera para convertir las transacciones no ordenadas ni registradas en transacciones ordenadas y registradas en un bloque de datos. Cada bloque ha de incluir la síntesis o hash del bloque de transacciones anterior, así como un número aleatorio llamado *nonce*. Para ganar esa carrera, un ordenador debe crear un hash del bloque, y este hash debe empezar con un número determinado, pero arbitrario, de ceros. Como es imposible saber qué *nonce* producirá un hash con el número correcto de ceros, los ordenadores han de probar con diferentes *nonces* hasta que den con el valor correcto. Es como ganar la lotería porque no depende de la habilidad. Sin embargo, un ser humano puede aumentar sus probabilidades de ganar la lotería comprando un procesador de última generación que se especialice en resolver problemas matemáticos de bitcoin; comprando más boletos, es decir, ejecutando muchos nodos importantes, o, como los seres humanos suelen hacer, uniendo sus nodos con otros —como hacen los colegas en el trabajo— y conviniendo en repartirse el premio si uno de esos nodos gana. Ganar, por tanto, depende de la suerte, de la capacidad procesadora que se tenga y de la cantidad de nodos que minen en común.

El «índice de hash» (*hash rate*) mide la capacidad de procesamiento total de la red bitcoin. Cuanto mayor es este índice, más difícil es dar con el *nonce* correcto. Cuando un minero encuentra un hash con el número correcto de ceros, comparte su prueba de trabajo con todos los demás mineros de la red. Esto constituye otro gran adelanto científico de la informática distribuida: el uso de pruebas de trabajo para alcanzar consenso en una red. Es lo que se llama el «problema de los generales bizantinos». Los demás mineros señalan que aceptan el bloque centrándose en recopilar el siguiente bloque, que tiene que incluir el hash del bloque recién creado. Del mismo modo que las claves pública y privada de Don son únicas y exclusivas de él, el hash de cada bloque es único: es como una huella dactilar criptográfica que permite verificar todas las transacciones incluidas en el bloque. No hay dos huellas dactilares iguales. El minero que gana recibe una cantidad de nuevos bitcoins como premio —el mismo programa acuña y asigna las nuevas monedas— y el bloque con su hash se añade a la cadena.

Pasados diez minutos, pues, desde que Don envió su mensaje, él y Artlery recibieron la confirmación de que la transacción de Don creó lo que se llama un *unspent transaction output* o «cantidad no gastada» que Artlery puede gastar haciendo justamente lo que hizo Don: publicar un mensaje especificando la cantidad a enviar y la dirección del destinatario, y autorizar la transacción con la clave pública de Artlery. Si el artista y los compradores conocen las claves públicas de Don y de Artlery, pueden saber que el acuerdo entre ellos se ha materializado y ver la cantidad de la transacción. Por eso decimos que es un «registro público» —todas las transacciones son transparentes— y anónimo, en el que podemos ver las direcciones de las partes, pero no los nombres de las personas. Todos los bloques que vengan a continuación constituirán sendas confirmaciones de esa transacción.

Perfil del comprador de arte de la nueva generación: el dinero redefinido

Ahora Don posee una participación porcentual de los derechos de una obra que representa un billete de euro. Cuando la obra física se venda, el artista, la sala, Don y todos los mecenas virtuales del artista recibirán una parte de la venta proporcionada a su grado de participación. En otras palabras, la participación de los mecenas es importante. Los mecenas que interactúan con el artista y la obra, que comparten su apreciación en redes sociales, que animan a otros a comprometerse con el artista y con el arte, y que, en fin, promocionan la «marca» del artista, reciben más de lo que recibe un mecenas pasivo que vio una vez una obra suya en línea y compró una participación. No sabemos si hablar de esto en este libro aumentará el valor de la participación de Don. Artlery quiere muestras de apreciación —en forma de menciones positivas de los artistas y de su obra— que incrementen el valor de la obra misma, y por eso es posible que en el futuro la plataforma tenga en cuenta ejemplos como el nuestro. Artlery se centra de momento en ofrecer un porcentaje por la venta de cada obra. En futuras versiones, la plataforma permitirá que los mecenas compren directamente participaciones de la obra, por ejemplo, ofreciendo suscripciones sobre las regalías o las ventas de derechos de la obra.

Como implica a muchos actores directamente en el proceso, incluidos los mecenas, y los convierte en accionistas, Artlery pone el foco de atención en la contabilidad. Las blockchains, que son un archivo público y distribuido, garantizan un procesamiento abierto, cuidadoso e instantáneo de las transacciones. Cuando los pagos superan la primera venta, la venta secundaria y derechos subsidiarios como reproducciones y otros productos mercadotécnicos, los artistas nunca actuarán solos. Tendrán una comunidad de mecenas que negociarán y harán valer los derechos contractuales que tengan.

Artlery utiliza la blockchain bitcoin de varios modos. En primer lugar, registra la procedencia de las obras de arte en forma de metadatos, lo que hace a través de otra empresa emergente de bitcoin, Ascribe.io, con la que se ha asociado y se comunica por medio de una interfaz de programación de aplicaciones o API. A continuación hace pública la relación de pagos para que todas las partes implicadas cobren según su participación, de una manera inmediata y transparente. Ahora está probando varias técnicas para codificar esta información, como la de incluir un script bitcoin en las transacciones. Aunque el mercado al que en principio se dirige es el mercado del arte, Artlery está imponiéndose en otras industrias de propiedad intelectual como la música, los libros, el cine, de las que se ocupará también mediante una interfaz de programación de aplicaciones propia.

La privacidad, la libertad de expresión, la libertad de prensa y las blockchains

La privacidad personal, la libertad de expresión y la libertad de prensa son fundamentales para crear una sociedad abierta, libre y próspera. Por un lado, los ciudadanos deben poder comunicarse de una manera privada y anónima. Por otro, deben poder hablar con libertad y seguridad y sin miedo a represalias. La censura en línea, el pirateo de grandes instituciones y organizaciones sociales, y las revelaciones por Edward Snowden de la existencia de una vigilancia masiva y del robo de datos han llevado a los ciudadanos de

democracias bien consolidadas a buscar el anonimato y tecnologías de cifrado. Estas herramientas les permiten ocultar su identidad y codificar los mensajes que envían y guardan para que sólo las personas autorizadas puedan acceder a ellos.

Y ésta es la cuestión: las tecnologías de cifrado o no son legales para uso individual o son de difícil acceso en aquellos países cuyos ciudadanos más las necesitan. El Acuerdo de Wassenaar, un convenio multilateral sobre control de exportaciones firmado por las naciones tecnológicamente avanzadas, regula la exportación de los llamados productos de «doble uso», es decir, aquellos productos que pueden usarse para bien y para mal. El propósito original del acuerdo era impedir que productos de alta tecnología cayeran en manos de dictadores como los de Corea del Norte, Libia, Irán e Iraq. Tecnologías de anonimato y cifrado como las infraestructuras de clave pública fueron consideradas de doble uso.

Hoy, en países como Rusia y China, tanto personas como empresas deben pedir autorización para usarlas. En países en los que su uso está permitido, los gobiernos —incluido el de Obama— han pedido a las empresas tecnológicas que incluyan una «puerta trasera», o sea, un medio secreto para saltarse el proceso de autenticación normal (que suele consistir en introducir una contraseña u otro código de seguridad) y tener acceso remoto a un ordenador y a sus datos *sin autorización ni detección*. Esto es mucho peor que el Gran Hermano, porque al menos todo el mundo sabía que el Gran Hermano nos observaba.⁴⁵⁰ Aquí se pide a las empresas tecnológicas que no revelen a los usuarios que hay una puerta trasera. Seguro que los piratas las buscan, las encuentran y las usan también.

«La tendencia que existe en materia de seguridad y privacidad en internet es muy preocupante», dice David Kaye, el relator especial de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. «La comunicación cifrada y anónima puede dificultar la aplicación de la ley y la tarea de los agentes antiterroristas, así como complicar la vigilancia, pero las autoridades del Estado no han sido capaces de identificar situaciones —ni siquiera generales, dada la exigencia de confidencialidad— en las que se ha necesitado aplicar una restricción para alcanzar un objetivo legítimo.»⁴⁵¹ Y añade que los encargados de aplicar la ley y las agencias antiterroristas han acabado descuidando el buen trabajo detectivesco de antes y la adopción de medidas de disuasión, incluyendo la cooperación internacional.⁴⁵²

No sorprende que, en la adopción de medidas globales para proteger los derechos personales y políticos —esto es, privacidad, libertad de expresión, de reunión y de prensa y tolerancia de otras religiones, inmigrantes, refugiados políticos y homosexuales—, Rusia ocupe el puesto 114 y China el penúltimo, de un total de 160 países.⁴⁵³ Por cierto, Estados Unidos tampoco puede cantar victoria: está en el puesto 28.

En esos países bloquear páginas web sin orden judicial se ha convertido en una cosa normal, y muchos censores han descubierto cómo inutilizar programas de redes privadas virtuales usados para evitar la censura.⁴⁵⁴ Según Reporteros sin Fronteras, Rusia lleva restringiendo la libertad de expresión y de información y bloqueando cada vez más sitios desde que Vladimir Putin volvió a la presidencia en 2012, entre ellos Wikipedia.⁴⁵⁵ China domina el arte del apagón informativo y censura la búsqueda de términos relacionados

con el movimiento prodemocrático Occupy Central de Hong Kong y con el 25.º aniversario de las protestas de la plaza de Tiananmen en Weibo, el equivalente chino de Twitter. Tiene bloqueado casi el 90 por ciento de los servicios Google. Encarcelar a las personas que publican en línea contenido que el gobierno considera sospechoso es también normal en estos países. A raíz de la caída de la bolsa china en julio de 2015, las autoridades detuvieron a más de cien personas por usar los medios sociales para difundir rumores que «causaron pánico, confundieron a la gente y provocaron desórdenes en la bolsa o en la sociedad».⁴⁵⁶

Los gobiernos que quieran acallar la voz de los ciudadanos y hayan secuestrado tecnologías como internet para silenciar a los disidentes y bloquear medios independientes comprobarán que la tecnología blockchain se resiste mucho más, por varias razones. La primera es que ciudadanos y periodistas podrían usar infraestructuras de clave pública para cifrar información y ocultar su identidad a posibles censores y atacantes. La segunda es que, cuando los gobiernos desalienten y priven de fondos al buen periodismo, los periodistas podrán reunir capital en las blockchains, creando una red más amplia para captar inversores afines a su causa, sobre todo inversores que prefieran permanecer anónimos. Por último, los gobiernos no podrían destruir o alterar la información registrada en la blockchain, por lo que podríamos usarla para pedirles responsabilidades a ellos y a otras instituciones.

Pensemos en la posibilidad de microfinanciar a los periodistas con el sistema blockchain. Si liberamos a los periodistas de las garras financieras de los medios de comunicación controlados por el Estado, podrían cubrir libremente la información política preservando el anonimato de los donantes. Los veteranos periodistas chinos podrían usar plataformas de micromecenazgo distribuidas como Koinify, Lighthouse o Swarm, que usan infraestructuras de clave pública y protegen la identidad del remitente y del destinatario mejor que sistemas basados sólo en internet. Otra gran herramienta de blockchain es la aplicación móvil gratuita de mensajería instantánea GetGems, que a la vez protege y rentabiliza los mensajes a través de bitcoin. Los usuarios pueden enviar toda clase de archivos con seguridad, porque GetGems funciona como un correo electrónico privado, no sólo como un SMS.⁴⁵⁷ Estas aplicaciones no son más que ejemplos de lo que se puede hacer.

Otra solución son las plataformas distribuidas que guardan artículos, crónicas, noticias, etc. en archivos inmutables y únicos, como la que Factom espera implantar en los países en vías de desarrollo. En Factom los autores pueden comprar «créditos de acceso» que les dan derecho a acceder al archivo y crear sus propias entradas. Igual que ocurre con el archivo de bitcoin, todo el mundo recibe la misma copia y puede contribuir, pero nadie puede alterar las entradas una vez que se han guardado. Factom usa lo que en criptografía se llama un «esquema de compromiso» (*commitment scheme*), que, en realidad, funciona como un mecanismo anticensura: en China, por ejemplo, los servidores no podrían impedir que, por su contenido, una entrada por lo demás válida se añada al archivo. Si el autor de la entrada ha asociado a ésta un crédito de acceso, la entrada quedará registrada. Un gobierno podría considerar ofensivas ciertas entradas, pero no

podría borrarlas ni bloquearlas como ha hecho el gobierno chino con Wikipedia. Si un tribunal oficial ordenara cambiar algo en el archivo, podría crear una entrada en la que hiciera constar el fallo, pero todo el mundo podría ver el historial.⁴⁵⁸

Otra solución son los sistemas de mensajería breve (*microblogging*) que no dependen de servidores centralizados. Stephen Pair, consejero delegado de BitPay, explica cómo reinventar Twitter o Facebook de manera que los usuarios controlen su información. «En lugar de haber una única empresa como Facebook, podría haber muchas conectadas a esa base de datos común [la blockchain] y que crearan su propia relación con el usuario. Algunas podrían pedirnos que compartiéramos con ellas cierta información que quisieran rentabilizar. Pero, como usuarios, tendríamos pleno control sobre la información que compartimos con esa empresa.»⁴⁵⁹ Existe Twister, una plataforma que funciona igual que Twitter desarrollada en 2013 por Miguel Freitas, programador e ingeniero de la Pontificia Universidad Católica de Río de Janeiro, Brasil. Twister usa programas gratuitos de los protocolos de bitcoin y de BitTorrent y cifrado de extremo a extremo para que los gobiernos no puedan espiar los mensajes de los usuarios.⁴⁶⁰

Que corra la voz: la función crucial de la educación

Joichi Ito es uno de esos empresarios triunfadores —como Bill Gates, Steve Jobs, Biz Stone o Mark Zuckerberg— que dejaron la universidad para inventar algo nuevo en la economía digital.⁴⁶¹ Una de las características de nuestra cultura empresarial es que la persecución de una idea —ir hasta el fondo y entender sus matices, como gusta decir Ito— lleva a un visionario a abandonar las aulas y ponerse a hacer negocios. Henry Ford y Walt Disney se dedicaron a su pasión sin títulos universitarios. Y por eso es una paradoja que el Instituto Tecnológico de Massachusetts (MIT) eligiera a Ito para dirigir su legendario Media Lab, en el epicentro de todo lo digital que tiene relevancia cultural.

La cosa no podía ser más oportuna. «La moneda digital es algo que me interesaba ya antes de entrar en Media Lab... Yo lancé uno de los primeros servidores de prueba digitales en los días de DigiCash, en la década de los noventa. Uno de los primeros libros que escribí fue en japonés y se titulaba *Dinero digital*, en colaboración con una persona que trabajaba en el Banco de Japón. Quiero decir que es un tema que me interesa desde hace mucho y precede a muchas de las cosas que estoy haciendo ahora.»⁴⁶²

Cuando entró en Media Lab, había varios profesores estudiando algún aspecto fundamental del sistema bitcoin —los modelos de consenso, el cifrado, la seguridad, los sistemas distribuidos, la economía—, pero ninguno se centraba concretamente en él. Vio que no había docentes investigándolo a fondo, aunque los estudiantes del MIT habían lanzado el MIT Bitcoin Project para dar cien dólares en bitcoins a los que aún no se habían licenciado.

Como Imogen Heap, Ito creyó que era urgente hacer correr la voz y formar equipos de trabajo sobre cuestiones legales, técnicas y creativas. Las tecnologías blockchain avanzaban mucho más rápido de lo que lo había hecho internet, pero sin gran participación académica. Los desarrolladores de los protocolos bitcoin estaban

recuperándose de los golpes que había recibido su reputación: la Fundación Bitcoin había quebrado y uno de sus directivos, Mark Karpeles, había sido detenido en Japón acusado de malversación de fondos por el escándalo de Mt. Gox. Ito fue rápido. Lanzó la Digital Currency Initiative (DCI) en el Media Lab y contrató a Brian Forde, exconsejero de la Casa Blanca, para que la dirigiera. Incorporó al proyecto a tres de los desarrolladores de bitcoin y les proporcionó recursos para que trabajaran con constancia en el código.

Creía que era importante crear una red de universidades que apoyaran el desarrollo de bitcoin y en eso está. «Impartimos cursos, estamos tratando de organizar la investigación, pero es sólo el principio —dice—. Acabamos de conseguir financiación para desarrollar el programa, y estamos tratando de despertar el interés de docentes y estudiantes.» En general, quiere que el MIT Media Lab reinvente la educación superior para que las personas como él no tengan que dejar la universidad y sepan lo que valen lugares como el Lab. Es una oportunidad de probar el futuro de la universidad.⁴⁶³

Melanie Swan, profesora y teórica destacada de las blockchains, tiene claro dónde hay que educar a los estudiantes sobre el sistema blockchain, y no es en las universidades tradicionales. *Es en el mismo sistema blockchain*. «Es una verdadera revolución que cambiará nuestra manera de hacer las cosas. La universidad no es el mejor lugar para estudiar cosas tan nuevas como las blockchains», dice. Por ejemplo, en lugar de enviar los artículos de investigación a las revistas académicas y esperar entre seis y dieciocho meses para que los rechacen o los publiquen, un estudioso podría publicarlos inmediatamente para un público limitado de especialistas, como hizo Satoshi Nakamoto, recibir críticas en tiempo real y ganarse el crédito necesario para dirigirse a un público más amplio. Los críticos pueden votar a favor o en contra de las críticas, como hacen los usuarios de Reddit, y así el estudioso sabe cuáles tomarse más en serio. El artículo podría leerse incluso gratis, pero otros científicos podrían suscribirse para recibir análisis más profundos o abrir un debate con el autor. El estudioso podría poner a disposición de sus colegas la información básica o compartirla con otros mediante contratos inteligentes. Si el artículo tuviera posibilidades comerciales, su autor podría proteger sus derechos por anticipado, teniendo en cuenta quién financió la investigación y cualquier reclamación que pudieran hacer del descubrimiento.

Swan es la fundadora del Institute for Blockchain Studies. «Estamos empezando a desarrollar una infraestructura educacional para promover el aprendizaje de estas tecnologías. Naturalmente, todas las reuniones, grupos de trabajo y encuentros de programadores son utilísimos —dice—. En todas las asesorías de contabilidad y estrategia hay ahora un grupo de especialistas en blockchain, y también hay centros educativos como la Blockchain University.»⁴⁶⁴ Ella misma imparte un taller sobre blockchain en la Singularity University.

Swan habla de un sistema educativo en el que los estudiantes universitarios serían lo que ella llama «sumilleres educativos», y en el que, según los intereses o las aptitudes que se necesitaran, se podrían elegir «cursos en línea abiertos y potencialmente masivos» (MOOC, por sus siglas en inglés). «La ventaja de los MOOC es una educación descentralizada. Podríamos seguir las clases de aprendizaje automático de Andrew Ng, de la Universidad de Stanford, a través de la página web Coursera. O cualquier otro curso

del MIT.» Así, los estudiantes podrían financiarse sus programas de desarrollo personal en cualquier parte del mundo y recibir la correspondiente acreditación. Swan explica: «Igual que cuando hago el examen de acceso a estudios de posgrado, o de administración de empresas, o de derecho, que me presento con mi carné de identidad y éste confirma que soy quien digo que soy y hago el examen», esa confirmación «podría formar parte de la infraestructura de los MOOC».

Swan ha estado trabajando en la manera de acreditar los MOOC y gestionar las deudas de los estudiantes con el sistema blockchain. Este sistema tiene tres elementos que podrían permitirnos conseguirlo: 1) un mecanismo fiable de prueba de la verdad, un oráculo, que confirma que los estudiantes que se apuntan a las clases de Coursera asisten a ellas, hacen los exámenes y dominan la materia; 2) un método de pago, y 3) unos contratos inteligentes que podrían ser como planes de estudio. Pongamos, por ejemplo, el caso del analfabetismo. «¿Por qué no ofrecemos ayuda económica para el desarrollo personal? Igual que hace Kiva, pero un Kiva que promoviera la alfabetización», dice Swan, con la diferencia de que todo sería perfectamente transparente y los participantes tendrían que dar cuentas. Los donantes podrían patrocinar a niños, invertir dinero en enseñarles e ir desembolsando según sus logros. «Por ejemplo, yo quiero financiar el programa de alfabetización de un niño de Kenia. Todas las semanas este niño tendría que presentar una prueba de que ha completado un módulo de lectura. Todo podría estar automatizado mediante una prueba en línea en la que el sistema blockchain confirmara la identidad del niño y registrara su progreso antes de ingresar la suma de la siguiente semana en lo que podríamos llamar la “cartera inteligente” de ese niño, y así éste podría seguir pagándose la escuela sin injerencia de nadie. El dinero destinado a la educación de una niña no podrían desviarlo para pagar la escuela del hermano», añade.⁴⁶⁵

La cultura, las blockchains y nosotros

Tras dos guerras mundiales libradas en una sola generación, los líderes mundiales admitieron que los acuerdos políticos y económicos no podían mantener una paz duradera. Esas condiciones cambiaban, a veces frecuentemente, otras drásticamente. La paz tiene que asentarse en algo más rico, más universal, en valores morales compartidos y en las libertades intelectuales de la sociedad. En 1945, tres docenas de países deciden fundar un organismo que cree una cultura de la paz, y que se conoce por el nombre de Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco). Su misión hoy es «crear las condiciones para el diálogo entre civilizaciones, culturas y pueblos».⁴⁶⁶

A través del prisma de las tecnologías blockchain, músicos, artistas, periodistas y educadores están viendo los perfiles de un mundo que protege, cuida y premia sus esfuerzos de una manera justa. Todos nosotros deberíamos tenerlo en cuenta. Somos una especie que sobrevive gracias a sus ideas, no a sus instintos. Que las industrias creativas marchen bien y que los mismos creadores vivan de su arte es algo que nos beneficia a todos. Además, estas industrias son los indicadores de nuestra economía, porque revelan antes que casi ningún otro cómo productores y consumidores adoptarán primero y

adaptarán después una tecnología a sus vidas. Los músicos han sido muchas veces los primeros en explotar innovaciones en provecho de muchas otras personas, y muchas veces a su costa. Estos abnegados miembros de nuestra sociedad nos inspiran, y los empresarios, funcionarios y demás dirigentes tienen mucho que aprender de ellos sobre los nuevos tiempos de la era digital.

TERCERA PARTE

Promesa y peligro

Capítulo X

Superar obstáculos: diez desafíos que hay que afrontar

Lev Serguéyevich Termén [León Theremin] fue un músico con talento, pero prefirió dedicarse a la física. Nacido en el seno de la aristocracia rusa a finales del siglo XIX, Termén se unió a los bolcheviques para acabar con la autocracia zarista. Una de sus primeras misiones fue crear un aparato que midiera la conductividad eléctrica y la capacidad de varios gases. Probó con bombillas llenas de gas, probó con un oscilador de alta frecuencia e incluso probó con la hipnosis.⁴⁶⁷ El oscilador acabó funcionando y el jefe de Termén lo animó a que le buscara otras aplicaciones. Dos de ellas se hicieron legendarias. La más curiosa de las dos empezó con dos polos de metal sin nada entre sí, como una bombilla sin cristal. Termén descubrió que si llenaba ese vacío con gas, podía conocer las propiedades eléctricas de ese gas. Su idea fue genial: sustituyó los diales por auriculares para poder hacer lecturas acústicas en lugar de visuales y controlar el tono que cada gas producía. El invento se adelantaba a su época, como los inventos del doctor Emmett Brown en *Regreso al futuro*.

Los aficionados a las charlas de la organización TED y los estudiantes de historia de la tecnología ya sabrán cómo acabó la cosa: Termén dio con un medio de hacer música de la nada. Cuando acercaba las manos a los polos de metal, el tono de la señal cambiaba. Comprobó que podía manipular el tono variando la posición y el movimiento de las manos. Llamó al aparato «eterófono», hoy conocido como theremín. La otra aplicación fue una versión a mayor escala del mismo artilugio, sensible al movimiento en un radio de varios metros. Fue el primer detector de movimiento: el centinela del éter. Hizo una demostración de los dos instrumentos en el Kremlin, y tocó su eterófono ante el camarada Lenin. Aunque Lenin disfrutó del eterófono, enseguida usó el detector para vigilar los alijos de oro soviéticos. Cuando alguien cruzaba la línea electromagnética que había en torno al oro, se activaba una alarma silenciosa. El Gran Hermano tenía de pronto ojos eléctricos.

La moraleja está clara: los inventos de Termén trajeron juntamente luz y oscuridad al mundo. En una interesantísima charla titulada «Nuestro camarada el electrón», Maciej Ceglowski señalaba estas dos vertientes de todos los inventos de Termén: en cuanto dieron forma a la nada aérea, las fuerzas oscuras se apropiaron de ellos. Lenin usó la electricidad en su propaganda, haciendo equivaler el comunismo al poder soviético más la electrificación del país.⁴⁶⁸ Pero fue Stalin quien acorraló a Termén y a sus colegas, los envió al gulag de Kolyma y los obligó a inventar instrumentos de tiranía.

Hemos visto cómo bitcoin se usaba con la misma grandilocuencia en campañas de todo tipo. Como toda tecnología revolucionaria, la blockchain bitcoin tiene sus pros y sus contras. En los capítulos anteriores hemos hablado de lo mucho que promete esta tecnología. Este capítulo se centrará en diez obstáculos: problemas y peligros. Pedimos perdón al lector si algunos son técnicamente complicados. Creemos que sería imprudente simplificar en exceso estas cuestiones: necesitamos cierto grado de detalle para ser rigurosos.

Por otro lado, después de leer esta sección, quizá el lector se sienta tentado de considerar inútil la labor de estos innovadores de las blockchains por los serios obstáculos con los que se encuentran. Lo animamos a que se pregunte si son razones para creer que las blockchains son una mala idea o si se trata de desafíos de la puesta en práctica que hay que vencer. Nosotros creemos que son esto último, y nos gustaría que los innovadores lo vieran como problemas importantes que debemos resolver en este momento de transición a la segunda era de internet. Para cada desafío proponemos algunas soluciones. En el último capítulo, exponemos lo que creemos que podemos hacer para que se cumpla la promesa que es el sistema blockchain.

1. La tecnología no está hecha para el gran público

En el momento en que escribimos esto, la mayoría de las personas sólo tiene una vaga idea de lo que es bitcoin, la criptomoneda, y muy pocos han oído hablar de la tecnología blockchain. Tú, lector, eres una de las pocas personas con visión de futuro. La palabra bitcoin hace pensar en cosas que van de una estafa piramidal a una ficha de lavandería automática, pasando por una especie de peaje financiero para circular por las autopistas del capital. En cualquier caso, la infraestructura no está hecha para el gran público.

El reto tiene varias facetas. La primera es, parafraseando al escritor de ciencia ficción William Gibson, que el futuro ya está aquí, sólo que su infraestructura está desigualmente repartida. Aunque los griegos hubieran conocido lo que era la moneda bitcoin durante su crisis económica de 2015, les habría seguido siendo muy difícil instalar una bolsa o un cajero bitcoin en algún sitio de Atenas. No habrían podido cambiar sus dracmas por bitcoins para protegerse del hundimiento de la moneda oficial. El científico informático Nick Szabo y el experto en seguridad de la información Andreas Antonopoulos afirman que es importante disponer de una infraestructura sólida y que ésta no puede improvisarse en medio de una catástrofe. Antonopoulos añade que en Grecia no había infraestructura blockchain ni suficiente liquidez de bitcoins para que todo un país cambiara su agitada moneda por bitcoins.

Por otro lado, la blockchain bitcoin tampoco está hecha para Grecia. Ésta es la segunda faceta: carece de los controles de seguridad necesarios para hacer frente a un uso tan masivo. «Al sistema le falta *capacidad transaccional* para acoger a diez millones de personas. Serían casi diez veces más usuarios de la noche a la mañana —dice Antonopoulos—. ¿Recordáis lo que pasó cuando AOL descargó 2,3 millones de cuentas de correo electrónico en internet? Enseguida descubrimos que internet, por carecer de protecciones contra el correo basura y de la debida etiqueta tecnológica, no estaba

preparado para absorber a 2,3 millones de neófitos. Esto no es bueno para una tecnología inmadura.»⁴⁶⁹ El sistema blockchain podría tener problemas de capacidad, fallos, virus imprevistos y, lo que quizá es peor, podría causar una gran decepción a los usuarios técnicamente no preparados, nada de lo cual se necesita en este momento.

Esto tiene que ver con la tercera faceta del problema: su *inaccesibilidad* para las personas normales y corrientes. No hay suficiente sostén de cartera, y muchas interfaces son difíciles de manejar porque requieren saber mucho de códigos alfanuméricos y conocer la jerga informática. La mayoría de las direcciones bitcoin son simples ristas de entre veintiséis y treinta y cinco caracteres que empiezan con un uno o con un tres, cosa muy fastidiosa de teclear. Como dice Tyler Winklevoss: «Cuando vamos a Google.com no tecleamos una ristra de números. No tecleamos una dirección IP. Tecleamos un nombre, una palabra que podemos recordar. Lo mismo debería ser con las direcciones bitcoin. Los usuarios normales no tendrían por qué ver las direcciones bitcoin. Cositas como éstas marcan la diferencia».⁴⁷⁰ Hay, pues, mucho trabajo que hacer para mejorar la interfaz y la experiencia del usuario.

Los críticos también han señalado la *falta de liquidez* a largo plazo, ya que la cantidad de bitcoins es finita —serán 21 millones en 2140— y el ritmo de minado disminuye. Es una política monetaria normativa cuyo propósito es impedir la inflación que unas políticas monetarias arbitrarias y discrecionales podrían provocar, un fenómeno frecuente con muchas monedas al uso. Satoshi escribió: «Es más típico de los metales preciosos. En lugar de que el suministro cambie para mantener el mismo valor, el suministro está predeterminado y el valor cambia. A medida que el número de usuarios crece, el valor por moneda aumenta. Puede ser un proceso que se retroalimenta: cuantos más usuarios hay, más aumenta el valor, lo que a su vez puede atraer a más usuarios deseosos de aprovechar el alza».⁴⁷¹

Por otro lado, los bitcoins guardados en carteras perdidas o que se hayan enviado a direcciones cuyos propietarios han extraviado sus claves privadas no pueden recuperarse y quedan inactivos en la blockchain, por lo que habrá menos de 21 millones en circulación. Los primeros usuarios de bitcoin tendían a guardar la moneda como guardaban el oro, esperando que con el tiempo aumentara de valor, y por tanto considerándola como un activo y no como un medio de intercambio. Según los economistas, una inflación baja o nula hace que los usuarios ahorren en lugar de gastar sus bitcoins. Sin embargo, si aumentan las transacciones de bitcoins fiables y los movimientos de los consumidores dentro y fuera de bitcoin, la frecuencia y el volumen del comercio podrían aumentar también. Si cada vez hay más comerciantes que aceptan bitcoins como método de pago, es probable que los que han guardado bitcoins empiecen a usarlos para sus compras, con lo que aumentará el número de bitcoins en circulación. Si los comerciantes empiezan a usar tarjetas regalo en bitcoins, la gente se familiarizará más con las criptomonedas y se acostumbrará a comprar y a vender con ellas. Y así, en teoría, tendrá menos razones para acumularlas. Los defensores del protocolo bitcoin afirman que, como los bitcoins pueden dividirse hasta ocho lugares decimales —la unidad más pequeña se llama satoshi y equivale a la centésima parte de la millonésima parte de un bitcoin—, los valores más pequeños se usarán más si la demanda de bitcoins aumenta.

También está la posibilidad de modificar los protocolos para incrementar la divisibilidad, y permitir, por ejemplo, picopagos (billonésimas partes de bitcoin), así como volver a minar los bitcoins que lleven un tiempo inactivos.

El quinto problema es el *largo periodo de latencia*: la red de la blockchain bitcoin tarda unos diez minutos en procesar y completar las transacciones, por lo que es mucho más rápida que la mayoría de los mecanismos de pago. Pero la cuestión no es completar instantáneamente las transacciones en el punto de venta; el verdadero problema es que diez minutos es un lapso de tiempo demasiado largo para el internet de las cosas, en el que los dispositivos tienen que actuar continuamente. El desarrollador Gavin Andresen dice que adaptar el sistema bitcoin a billones de objetos conectados requiere «una concepción del espacio diferente», un espacio en el que la brevedad del periodo de latencia sea vital y la posibilidad de fraude menor, o en el que las partes puedan establecer un grado de confianza aceptable sin la red bitcoin. Un periodo de latencia de diez minutos también es demasiado largo para transacciones financieras que dependen de la oportunidad de comprar un activo a un precio determinado, y expone a los negociantes a las debilidades del arbitraje basado en el tiempo, como son los ataques temporales, que aprovechan el tiempo que tarda un sistema en procesar una operación.⁴⁷² La solución inmediata que han encontrado los programadores ha sido bifurcar o ramificar el código fuente para lanzar una nueva blockchain con una «moneda alternativa» o *altcoin* que sirva de incentivo para participar. Litecoin es una popular moneda alternativa cuyos bloques tardan 2,5 minutos en crearse, y Ripple y Ethereum son plataformas blockchain totalmente reformadas con un periodo de latencia de segundos, no de minutos.

El sexto problema es la necesidad de un *cambio comportamental* que sea más profundo que la simple «netiqueta». Hoy, mucha gente confía en su banco, o en su empresa de tarjetas de crédito, e incluso quieren hablar con una persona real cuando cometen un error contable, olvidan sus contraseñas o pierden sus carteras o talonarios de cheques. La mayoría de las personas con cuenta bancaria no tiene costumbre de hacer copias de seguridad de sus contraseñas en una memoria USB o en otro dispositivo, de manera que no dependan de su proveedor de servicios para que se la restablezca, ni de guardar esas copias de seguridad en un lugar aparte para que, si se les pega fuego a la casa y pierden el ordenador y todas las demás pertenencias, no pierdan también su dinero. Sin esta disciplina, más les valdría guardar el dinero en el colchón. Cuanto mayor es la libertad —cuanto mayor es la privacidad, la seguridad y la independencia de terceros—, mayor es también la responsabilidad. Para aquellos consumidores que no son capaces de guardar copias de seguridad de sus claves privadas, hay proveedores de servicios que podrían guardarles esas copias.

La tercera faceta es el *cambio social*. El dinero sigue siendo un producto social que representa lo que la sociedad valora. Es inherente a esa sociedad, es un reflejo de las relaciones humanas y se adapta a la evolución de las necesidades del hombre. «No podemos ignorar el carácter social del dinero —dice Izabella Kaminska, del *Financial Times*—. Muchos de esos protocolos parecen ignorarlo al querer crear un sistema absolutista y muy cosificado. Así no reflejan el mundo tal y como es.» Señala el euro como ejemplo de sistema que no casa con todos los países,⁴⁷³ y recuerda lo que dice

Antonopoulos sobre la necesidad humana que tienen las sociedades de olvidar y perdonar para avanzar. «En el mundo financiero, hay una larga tradición de borrar registros porque, como sociedad, creemos que no está bien perseguir o discriminar a personas por algo que hicieron diez o quince años atrás. Tenemos esta mentalidad de perdonadeudores porque pensamos que la gente debería tener otra oportunidad. Crear un sistema que nunca olvide es un poco sociópata», dice.⁴⁷⁴

Esto nos lleva a la octava dimensión del problema, la *falta de recursos legales* en un mundo de transacciones irrevocables y contratos inteligentes inevitables. Según los juristas Primavera De Filippi y Aaron Wright, «las personas son libres, sí, de decidir a qué reglas quieren atenerse, pero, una vez tomada la decisión, ya no pueden apartarse de esas reglas, en la medida en que los contratos inteligentes, basados en un código tecnológico, las aplican automáticamente y al margen de la voluntad de las partes».⁴⁷⁵ Este altísimo grado de certidumbre —matemática— sobre el resultado de una transacción o un contrato inteligente no tiene precedentes en nuestra sociedad. Aumenta la eficiencia y conjura el riesgo de incumplimientos porque no tenemos posibilidad de infringir las normas. Pero esto tiene también su lado malo, y es que no da cabida a los seres humanos. Según Josh Fairfield, de la Facultad de Derecho de la Universidad de Washington & Lee, eso significa «más caos, no menos. Habrá más conflictos. “No reformaste de verdad mi casa, devuélveme el dinero.” Habrá más caos humano, aunque que haya más caos humano no significa que la tecnología sea mala».⁴⁷⁶

Pero la pregunta es: ¿llevará la gente a juicio a la otra parte? De Filippi calcula que, en el mundo analógico, el 80 por ciento de los incumplimientos de contrato no se persigue porque llevarlos a juicio resulta demasiado caro. ¿Por qué había de cambiar la cosa en el mundo de las blockchains? Cuando el código indica que el contrato se ha cumplido plenamente en lugar de lo contrario, si una parte no queda satisfecha con el resultado, ¿demandará esta parte a la otra? ¿Reconocerán los tribunales casos como éstos? ¿Se atreverá el pequeño empresario a contratar al gabinete legal de Dewey, Cheatham and Howe, o, con sus modestos medios, podrá siquiera identificar a la anónima parte contraria, de manera que pueda ponerle pleito?

2. La energía que se consume es insostenible

En estos días primeros de la blockchain bitcoin, el método de la «prueba de trabajo» descrita en el capítulo 2 ha sido fundamental para crear confianza en la gente. Dentro de unos años, volveremos la vista atrás y apreciaremos lo genial del proceso, desde la acuñación y destinación de nuevos bitcoins a la asignación de identidad y la prevención del doble gasto. Es algo muy notable. Y muy insostenible, según los críticos de las criptomonedas que usan la prueba de trabajo para mantener la red segura y anónima.

Hashear, el proceso de aplicar el algoritmo de hash seguro 256 (SHA-256) a las transacciones pendientes para validarlas y resolver un bloque, gasta muchísima electricidad. Algunos miembros del ecosistema blockchain hacen cálculos a ojo de buen cubero que se convierten en memes en la comunidad. Hay estimaciones que comparan el consumo energético de la red bitcoin con la electricidad que gastan unos setecientos

hogares medios estadounidenses, tirando por lo bajo, y con la que consume la isla de Chipre, tirando por lo alto.⁴⁷⁷ Eso supone más de 4.409.000 millones de kilovatios hora,⁴⁷⁸ una huella de carbono gigantesca, que es inherente al sistema: es lo que hace segura la red y garantiza que los nodos sean honrados.

A principios de 2015, *The New Republic* informaba de que la capacidad procesadora total de la red bitcoin era cientos de veces mayor que el rendimiento de los quinientos superordenadores más potentes del mundo juntos. «Procesar y proteger los más de 3 millones de dólares en bitcoins que hay en circulación requiere más de 100 millones de dólares anuales en electricidad, con el consiguiente volumen de emisiones de carbono.» El autor del artículo, Nathan Schneider, decía algo que desde entonces nos ha dado mucho que pensar: «Toda esa capacidad de procesamiento, que podría emplearse en curar el cáncer o explorar las estrellas, está encerrado en unas máquinas que no hacen más que procesar transacciones bitcoin».⁴⁷⁹

Como ciudadanos preocupados por nuestro planeta, todos deberíamos preocuparnos. Hay dos cuestiones, la de la electricidad que se consume para hacer funcionar las máquinas y la de la energía que se consume para enfriarlas para que no fallen. Puede decirse que por cada dólar que un ordenador consume en electricidad, gasta cincuenta céntimos en enfriarse.⁴⁸⁰ La fuerte sequía sufrida en California ha suscitado serias preocupaciones por el uso de una preciosa agua para enfriar centros de datos y operaciones de minado de bitcoins.

A medida que el valor del bitcoin aumenta, la competencia por el minado de nuevos bitcoins aumenta también. Cuanto mayor es la capacidad procesadora que se dedica al minado, más difíciles son los problemas que los mineros tienen que resolver. Una manera de medir la capacidad procesadora total de la red bitcoin es el ritmo de hash. Gavin Andresen explica: «Imaginemos que hay millones de transacciones por bloque y que por cada una de ellas se paga un dólar de comisión. Los mineros percibirán millones de dólares por bloque y gastarán un poco menos en la electricidad que necesitan para hacer ese trabajo. Así es como funciona la economía de la prueba de trabajo. En realidad es el precio del bitcoin y la recompensa que pueda haber en un bloque lo que determina el ritmo de hash».⁴⁸¹ El ritmo de hash ha crecido considerablemente en los últimos dos años, y en menos de un año se ha multiplicado por cuarenta y cinco. Y la tendencia es a usar más energía, no menos.

«El coste de esa energía es el coste de no tener una autoridad central», dice Eric Jennings, consejero delegado de Filament, una empresa de sensores inalámbricos.⁴⁸² Es un aspecto de la cuestión. La energía es lo que es, y puede compararse con lo que cuesta salvaguardar las monedas fiduciarias. «Cualquier forma de dinero guarda relación con la energía», dice Stephen Pair, de BitPay. Y lo compara con el oro. «Los átomos de oro son raros en la tierra porque se necesita mucha cantidad de energía para formarlos.» El oro es valioso por sus propiedades físicas, y estas propiedades derivan de la energía. Pair calcula que fabricar oro artificialmente requeriría fusión nuclear.⁴⁸³

Desde un punto de vista, todo este consumo de electricidad es razonable. Erik Voorhees, fundador de la plataforma de cambio de criptomonedas ShapeShift, dice que los críticos se equivocan cuando dicen que la energía que se gasta en minar bitcoins es

una pérdida. «Esa electricidad se gasta por algo. Se ofrece un servicio real: hacer seguros los pagos.» Pide a los críticos que lo comparen con la energía que gasta el actual sistema financiero. Que piensen en las grandes cámaras acorazadas, en la arquitectura como de búnker de los bancos y en sus majestuosas fachadas griegas, en los sistemas de climatización que refrigeran los relucientes vestíbulos, en las sucursales que hay en todas las esquinas, en los mil cajeros automáticos. «La próxima vez que veamos un furgón blindado de la compañía de seguridad Brink echando humo negro a la atmósfera, comparémoslo con la electricidad que se gasta en producir bitcoins. No está claro qué es peor», dice Voorhees.⁴⁸⁴

La segunda cuestión relacionada con la energía es la estructura informática misma. Para que pueda ser compatible con sistemas anteriores que cambian lentamente, nuestro portátil o PC es seguramente un ordenador con un conjunto de instrucciones complejas (CISC, por sus siglas en inglés) que pueden ejecutar una vasta gama de aplicaciones matemáticas que un usuario normal y corriente nunca usará. Cuando los ingenieros se dieron cuenta de eso, crearon unos ordenadores con un conjunto de instrucciones reducido (RISC, por sus siglas en inglés). Nuestro teléfono móvil es seguramente un dispositivo RISC avanzado (ARM, por sus siglas en inglés). Los mineros se dieron cuenta de que también podían aprovechar sus unidades de procesamiento gráfico (GPU, por sus siglas en inglés) para aumentar la velocidad de procesamiento. Como las modernas GPU tienen miles de microprocesadores en cada chip, son ideales para operaciones de computación que pueden hacerse en paralelo, como la de hashear que se realiza en el minado de bitcoins. Había algunas compensaciones, y estimar el consumo de energía de la máquina resultó algo más complicado, pero en general las GPU funcionaban bien.⁴⁸⁵

«Si puedo diseñar un ordenador RISC que sea tan rápido que pueda procesar en paralelo y al mismo tiempo tropecientos mil millones de códigos con poco o ningún gasto de electricidad, haré dinero de la nada»,⁴⁸⁶ dice Bob Tapscott, el hermano de Don y director de información. Es lo que ha hecho el grupo BitFury: crear un dispositivo paralelo masivo con circuitos integrados específicos de la aplicación (ASIC, por sus siglas en inglés) que son energéticamente eficientes y están diseñados exclusivamente para minar bitcoins. Su fundador y consejero delegado, Valery Vavilov, dice que las máquinas y las operaciones de minado en general serán cada vez más energéticamente eficientes y respetuosas con el medio ambiente. Eso depende en parte de que se emplacen en climas fríos en los que la energía es barata y preferiblemente renovable, como la hidráulica o geotérmica, y donde la madre naturaleza se encarga de la refrigeración o los fabricantes inventan una manera eficiente de capturar el calor. BitFury, por ejemplo, tiene dos centros de datos, uno en Islandia y otro en Georgia, planea instalar otros en Norteamérica y ha adquirido la empresa emergente con sede en Hong Kong Allied Control, especializada en tecnologías de refrigeración por inmersión.⁴⁸⁷ Así trabaja BitFury por reducir el impacto medioambiental de la infraestructura bitcoin.

Aunque estas iniciativas limitan la huella de carbono de la minería bitcoin, seguimos teniendo el problema del rápido consumo y disponibilidad de unos dispositivos que se actualizan constantemente. Los mineros que quieren dedicarse a ello han de actualizar y especializar sus sistemas constantemente. La mayor parte del equipo necesario para el

minado tiene una vida útil que va de tres a seis meses.⁴⁸⁸ Bob Tapscott compara empresas como BitFury con aquellos tenderos de Yukon de los tiempos de la fiebre del oro, que hacían fortunas vendiendo palas cada vez mejores a los mineros.⁴⁸⁹ Encontramos el testimonio de un minero que vendía su minador Cointerra TerraMiner IV con un chip ASIC que consumía tanta energía que la instalación eléctrica de su casa no daba abasto. «Vendo tres unidades porque mi casa es vieja y el cableado es de mala calidad. No quiero que salga ardiendo.» El precio de salida era de 5.000 dólares.⁴⁹⁰ Vendedores como MRI de Australia están aplicando nuevas formas de reciclaje, primero desarmando todos esos componentes en lugar de destrozarlos, y luego gestionando los residuos resultantes. Procesos creativos como éstos les permiten recuperar metales preciosos y reutilizar hasta el 98 por ciento del peso del producto.⁴⁹¹ Por desgracia, reciclar hardware sigue siendo difícil para la mayoría de los consumidores.

Para los desarrolladores de bitcoin, la preocupación es legítima y requiere una solución: «Si bitcoin se convierte de verdad en una red global, tendremos que ir renunciando a la prueba de trabajo como única forma de hacerla segura —dice Andresen—. A muy largo plazo, quizá tendremos que combinarla con alguna otra cosa.»⁴⁹²

Esto es lo que varias «cadenas alternativas» (*altchains*) han hecho: explorar otros algoritmos de consenso alternativos como la prueba de participación para hacer segura la red y que a la vez siga siendo descentralizada. El carácter abierto del protocolo bitcoin hace que sea técnicamente fácil. No olvidemos que el objeto de los algoritmos de consenso es distribuir el derecho de decidir el estado de la blockchain entre un conjunto descentralizado de usuarios. Según Vitalik Buterin, el visionario fundador de Ethereum, sólo hay tres clases de usuarios seguros y descentralizados, y a cada grupo le corresponde un conjunto de algoritmos de consenso: los *dueños de capacidad procesadora*, que usan el algoritmo de prueba de trabajo normal; los *participantes*, que usan varios algoritmos de prueba de participación en programas de cartera, y los *miembros de una red social*, que usan un algoritmo de consenso de tipo «federado».⁴⁹³ Obsérvese que sólo en uno de estos mecanismos de consenso figura la expresión «capacidad procesadora». La versión 2.0 de Ethereum se creará según un modelo de prueba de participación, y Ripple usa un modelo federado parecido al de SWIFT, el proveedor global de mensajería financiera segura, en el que un grupo autorizado de usuarios alcanza un consenso sobre el estado de la blockchain.⁴⁹⁴

Estos sistemas no gastan tanta electricidad como la cadena bitcoin. Bram Cohen, fundador de Tor, ha introducido una cuarta forma de resolver el problema del gasto de energía, y es la que él llama «prueba de disco», en la cual los *dueños de espacio de almacenamiento en disco* —gente que dedica parte de la memoria de su ordenador a mantener una red y desempeñar funciones reticulares— constituyen el grupo económico de usuarios. Austin Hill, de Blockstream, pone en guardia sobre estas alternativas a la prueba de trabajo para lograr consenso: «Experimentar con nuestro algoritmo de prueba de trabajo es peligroso, y es un nuevo campo de la ciencia informática».⁴⁹⁵ Y añade una dimensión a la innovación: los desarrolladores no sólo deben preocuparse por si sus

nuevas funciones y prestaciones funcionarán bien en sí mismas, sino que también deben comprobar que el algoritmo de consenso elegido las hace seguras y las distribuye entre el mejor grupo económico.

En general, aquí cuadra la expresión «querer es poder». Los tecnólogos más inteligentes del planeta están trabajando para encontrar soluciones creativas a la cuestión energética. Además, a medida que los ordenadores sean más inteligentes, aportarán sin duda sus propias soluciones. El inversor de riesgo Roger Ver, apodado el «Jesús del bitcoin», dice: «Supongamos que el ser humano más inteligente tiene un coeficiente intelectual de 200. Y ahora imaginemos una inteligencia artificial con un coeficiente intelectual de 250, o de 500, o de 5.000, o de 5 millones. Habrá soluciones, si los humanos las buscan».⁴⁹⁶

3. Los gobiernos lo reprimirán o lo utilizarán mal

A los libertarios y anarquistas, Satoshi Nakamoto les dijo: «No encontraréis una solución a los problemas políticos en la criptografía».⁴⁹⁷ Tendrían que buscar en otro sitio la panacea contra el Estado. Satoshi consideraba su experimento un paso dado en un nuevo territorio de libertad, no una revolución. Donde los gobiernos consiguieron decapitar redes con control centralizado como Napster, redes de iguales puras como Tor lograron sobrevivir. ¿Podría resistir la red blockchain bitcoin contra poderosas autoridades centrales?

Ésta puede ser la gran incógnita. ¿Qué harán los legisladores, reguladores y jueces con las tecnologías blockchain? «Los tribunales se equivocarán. Ya han empezado a equivocarse, al aplicar las leyes sobre propiedad intelectual a todo lo que es intangible. Creen que lo físico es la línea que separa la propiedad virtual de la propiedad intelectual, y no es así —dice Josh Fairfield—. No hay ningún elemento de propiedad intelectual, no hay ninguna parte en un bitcoin que sea propiedad intelectual, no hay ni pizca de creatividad que dé lugar a derechos de autor, no hay ideas que puedan patentarse, ni patente, ni marca de fábrica.»⁴⁹⁸ Según Stephen Pair, de BitPay, «la mayor amenaza que tiene bitcoin es que lo regulen tanto que en algún momento aparezca un competidor más privado y más anónimo y todo el mundo se pase a él».⁴⁹⁹ Una cosa es segura: «Sean cuales sean las normas, si no entendemos esta tecnología ni las implicaciones que tiene, estamos destinados a fracasar», dice Jerry Brito, de la plataforma Coin Center, dedicada al debate normativo sobre bitcoin. «Si no la entendemos, podemos dictar leyes y normas que la perjudiquen. Lo único que queremos es que se entienda lo que estamos haciendo.»⁵⁰⁰

El reto es, pues, formidable. Deben prever lo imprevisible. Deben evitar, por un lado, ahogar la innovación reaccionando exageradamente ante los peores usos, como el tráfico de seres humanos, de drogas y de armas, la pornografía infantil, el terrorismo, la evasión fiscal y la falsificación, por ejemplo; y, por otro, hacer un mal uso de nuevas pero no probadas aplicaciones como son las plataformas de gestión de la identidad basadas en blockchain, y utilizarlas para restringir las libertades civiles. Debe haber un planteamiento

equilibrado de la regulación, de la legislación y de la negociación internacional de tratados que minimice la inseguridad jurídica para que los inversores sigan sosteniendo el desarrollo global de esta tecnología.

La jurisdicción ya importa en lo que a bitcoin se refiere. Algunos gobiernos han prohibido esta moneda o han prohibido a los bancos del Estado que la cambien, como en China. Brito dice: «A la manera típicamente china, no es ilegal, pero podría serlo en cualquier momento y todos los saben».⁵⁰¹ China permite que florezca una comunidad profesional seria y esos grupos de mineros son muy influyentes en los debates sobre mejoras del protocolo bitcoin. ¿Qué pasaría con la seguridad de las blockchains si China prohibiera de pronto minar? Otras jurisdicciones han tratado de definir bitcoin con precisión, como ha hecho el Internal Revenue Service de Estados Unidos, que lo cataloga como un activo para calcular impuestos sobre la cotización del valor.

Los marcos legales también importan. Los juristas De Filippi y Wright no creen que el actual marco legal pueda dar respuesta a las cuestiones que plantea la propiedad inteligente globalizada. Los contratos inteligentes definen y gestionan los derechos de propiedad. Su código no prejuzga la asignación de derechos y no puede usurpar ni transferir esos derechos. Por ejemplo, si durante el proceso de asignación de tierras los funcionarios dan la propiedad de una parcela a alguien que no es el propietario legal, ese alguien tendría el derecho absoluto a esa parcela y el propietario legal simplemente no podría revocar esa asignación.

Josh Fairfield piensa más en el proceso: «No es que el derecho consuetudinario afecte al derecho tecnológico; es que el derecho consuetudinario *es* el derecho tecnológico. El derecho consuetudinario es el proceso de adaptar los sistemas humanos a los cambios tecnológicos... La verdadera lucha está en cómo adaptar rápida y eficazmente las viejas normas pensadas para la vieja tecnología a las nuevas tecnologías», de manera que esas normas sean reconocibles cuando empezamos a usarlas pero a la vez estén muy desarrolladas cuando la tecnología triunfe.⁵⁰²

Y, por último, pero no menos importante —y no debería sorprendernos—, la cuestión de la identidad también es crucial, o, al menos, la manera como la creamos en el sistema blockchain. «Tenemos una idea muy simplista de la identidad —dice Andreas Antonopoulos—. A mí me aterrorizan las implicaciones que pueda tener la identidad digital porque creo que la gente tomará atajos... Si trasladamos la identidad al mundo digital, donde las visiones son inflexibles, acabaremos construyendo algo que no se parecerá al producto social de la identidad, sino que será una terrible copia fascista de ella.»⁵⁰³

Si unimos una versión exactamente codificada de la identidad de una persona a una versión exactamente codificada de la sociedad, tenemos un mundo de novela de ciencia ficción o de película de Arnold Schwarzenegger. Los juristas De Filippi y Wright se imaginan unos «contratos automáticos, *jardines vallados* o *sistemas fiables* poseídos y administrados por una sofisticada red de organizaciones descentralizadas que dictan lo que la gente puede o no puede hacer, sin ningún tipo de garantía ni de restricción constitucional». En otras palabras, un régimen totalitario dirigido por máquinas.

El experto en inteligencia artificial Steve Omohundro nos deja esta frase: la *curva de aprendizaje del dictador*, o cómo los cavernícolas acabaron dominando la tecnología de la era espacial. Pensemos en todos los laboratorios de inteligencia artificial llenos de los más capaces científicos con acceso a los más poderosos ordenadores del mundo. Los científicos podrían bifurcar el código bitcoin o concebir un contrato inteligente que controlara la entrega de un paquete por un dron, y que retuviera el pago hasta el momento exacto en el que el paquete es entregado. Imaginemos que esos científicos suben ese programa a internet en forma de código abierto, porque así es como ellos hacen progresar sus ideas: compartiéndolas. Pues bien, el Estado Islámico no necesita un laboratorio de inteligencia artificial, ni un equipo de desarrolladores informáticos. Sólo tiene que sustituir el paquete por una bomba. En esto consiste la curva de aprendizaje del dictador, y no es brusca. Pero no culpemos al código ni a la cultura de compartir. El problema no es exactamente lo que hacemos con el código, es lo que no sabemos que haremos con él, es decir, las consecuencias no deseadas de un mundo sin conflictos.

4. Las poderosas empresas del viejo paradigma se adueñarán del nuevo

Muchos de nuestros temores sobre la primera generación de internet se han hecho realidad. Una serie de empresas poderosas se han apropiado de la tecnología y la usan en sus vastos imperios privados para quedarse con la mayor parte del valor. Han acabado con las oportunidades y privatizado gran parte de nuestra experiencia digital. Usamos tiendas privadas para comprar y usar nuevas aplicaciones en nuestros móviles, tabletas y ahora relojes. Los motores de búsqueda y los departamentos de venta interrumpen nuestro contenido con publicidad. Las grandes compañías que promueven la transparencia del consumidor y prosperan con ella, llevan sus actividades, planes, infraestructuras tecnológicas y activos informativos con manifiesto secreto. Es verdad que algunas empresas se han abierto voluntariamente, pero muchas otras no han hecho más que reaccionar a la luz arrojada sobre ellas por soplones y periodistas de investigación. Sus esfuerzos por ocultar operaciones y escamotear información contradicen estas aparentes muestras de transparencia.

Dicho llanamente, no han sabido administrar la confianza de la gente.

Ejemplo sobresaliente: la banca. «Tradicionalmente, los bancos son guardadores de secretos», dice Kaminska, del *Financial Times*. Y explica que los bancos juzgan con conocimiento de causa a quién prestar y cómo procesar los pagos cuando disponen de fácil acceso a información privada, que consiguen prometiendo que la mantendrán en secreto. Cuantos más secretos guardan, mayor es la asimetría informativa y mayores son sus ventajas, aunque estas ventajas tienen consecuencias perjudiciales para el sistema.⁵⁰⁴ ¿Qué podemos hacer, pues, para evitar que grandes empresas y Estados-nación poderosos se apropien de las tecnologías de las blockchains y las usen en su propio y estrecho interés? «Cualquier mecanismo de consenso que tengamos será susceptible de mercantilización, con lo que siempre habrá poderosos intereses que gastarán dinero en convencer a la gente de que haga una determinada cosa», dice Pair, de BitPay.⁵⁰⁵

Que quede claro que no estamos diciendo que las empresas y los gobiernos deberían dejar en paz esta tecnología. Después de todo, la tecnología blockchain está emergiendo como un importante recurso global que podría crear nuevas posibilidades. Es más, la sociedad necesita un Estado que preste servicios a sus ciudadanos y empresas que creen trabajo y riqueza. Pero eso es diferente de adueñarse de una tecnología revolucionaria y generosa y limitar así los grandes beneficios que podría tener para la sociedad.

Pensemos también en lo que los desarrolladores y las empresas de blockchain están ya haciendo para proteger sus redes, anticipándose y respondiendo a los peores escenarios. Por ejemplo, en 2014 unos ladrones robaron ocho millones de VeriCoins, una criptomoneda de prueba de participación, de la plataforma de cambio MintPal. Unos días después del ataque, los desarrolladores de VeriCoin hicieron público un nuevo código que bifurcaba la cadena de VeriCoin en un punto anterior al del ataque, retrocediendo, por así decirlo, en el tiempo, y colaboraron con las plataformas de cambio para cerciorarse de que adoptaban el nuevo código.⁵⁰⁶ Igualmente, «si el dinero y el poder tratan de apropiarse de la red, los mineros lo evitarán volviendo a la versión real de bitcoin e iniciando una bifurcación», dice Keonne Rodriguez, jefe de productos de Blockchain.⁵⁰⁷

¿Cómo podemos impedir que China decida dedicar toda la capacidad procesadora del Estado y todos sus grupos de mineros de la cadena bitcoin a lanzar un ataque del 51 por ciento o por lo menos a desestabilizar el sistema? Imaginemos que algún déspota rico decide que bitcoin, como antes internet, ha llegado a ser tan influyente que amenaza su poder. Este déspota podría adueñarse de toda la capacidad minadora que tenga a su alcance y comprar el resto a países que lo tolerasen, para llevar el ritmo de hash por encima del umbral del 50 por ciento. Entonces podría decidir qué transacciones incluir en los bloques y cuáles no. Con este poder de control, también podría decidir bifurcar el código para introducir nuevas prohibiciones, por ejemplo, vetando direcciones relacionadas con el mundo de las apuestas o con la libertad de expresión. ¿Qué harán los nodos honrados, aceptar esta bifurcación centralmente controlada o bifurcar a su vez para crear un nuevo código? Andrew Vegetabile, presidente de la asociación Litecoin, dice que no habría modo de escapar de ese escenario porque el déspota controlaría el 51 por ciento de la red. Y no tendría que ser un gobierno; podría ser una de las personas más ricas del mundo o un ejecutivo de una gran compañía con mucho poder adquisitivo.⁵⁰⁸

Otra posibilidad es que las grandes empresas defiendan su territorio y se asocien para exigir que la regulación que se les aplica a ellas se aplique a las emergentes, y para perseguir legalmente a cualquiera de éstas que sobreviva a la inquisición reguladora. Esta estrategia de buscar el conflicto y no innovar puede darles tiempo para preparar una línea de acción. O puede que deje a la gran empresa sin ningún valor real, si es que lo tuviera. Pensemos en esos dos tiranos gemelos, los sistemas heredados y la llamada «inercia activa». Los estudiosos han calculado los costes que a una empresa le supone seguir usando su vieja tecnología y los que le supone cambiar a una nueva, y han identificado los retos de la integración de sistemas después de una fusión. Las empresas que invierten mucho en la tecnología instalada son más susceptibles de gastar más dinero en su viejo sistema, que es como si afilaran un cuchillo para librar un combate a pistola, en lugar de experimentar estratégicamente con las blockchains.

5. Los incentivos no se adecuan a la colaboración masiva distribuida

Los mineros tienen un incentivo para mantener la infraestructura de bitcoin porque, si la red falla, todos los bitcoins no convertidos que han ganado (o podrían ganar) con el minado se perderían o no valdrían o, en cualquier caso, estarían en peligro. Antes de profundizar en el tema de los incentivos, aclaremos que el servicio que los mineros prestan *no* es validar transacciones. Cualquier nodo completo puede validar transacciones. Lo que hacen los mineros es preservar la distribución del poder: el poder de decidir qué transacciones incluir en cada bloque, el poder de acuñar monedas, el poder de votar lo que es verdadero.

¿ASÍ QUE QUIERES SER UN MINERO DE BITCOIN?

Como parte de nuestro estudio, le pedimos a Bob Tapscott —exdirector de inversiones bancarias, consejero de administración y hermano de Don— que se descargara toda la cadena bitcoin a principios de 2015. El experimento fue instructivo por el tiempo transcurrido, el esfuerzo requerido, la energía consumida y la (falta de) recompensa por minar por pasatiempo.

Bob dedicó a la tarea un Windows PC de dos núcleos y cuatro hilos de ejecución. Descargarse la blockchain le llevó tres días y consumió un 20 por ciento de la capacidad procesadora disponible. La operación de minado usa poco más de 200 MB de memoria y el 10 por ciento de la CPU para actualizarse.

Aunque el ordenador de Bob estaba perfectamente preparado para minar, entró en un grupo minero. En una sesión de 137 horas, el ordenador minó 152,8 microbitcoins (μBTC), más o menos tres céntimos y medio de dólar entonces. Pero, a diez céntimos por kilovatio-hora, el ordenador de Bob consumió unos catorce céntimos de electricidad. Bob concluyó: «Se acabó el minar bitcoins con nuestros PC».

Por tanto, cualquier cambio que se haga en el protocolo original de bitcoin, sea introduciendo una moneda alternativa, sea modernizando el sistema, debe ofrecer los debidos incentivos económicos para preservar la descentralización del minado, de manera que los mineros revaloricen la red a cambio de elevadas sumas de bitcoins. El desarrollador de bitcoin Peter Todd compara la tarea con la de diseñar un robot que pueda comprar leche en una tienda. «Si el robot no tiene olfato, el tendero pronto se dará cuenta de que no distingue entre la leche en buen estado y la leche en mal estado y nos timará, vendiéndonos leche en mal estado.»⁵⁰⁹ Para Todd, esto significa que los mineros más pequeños de lugares geográficamente dispersos deberían poder competir de igual a igual —tener el mismo olfato— que los mineros más grandes geográficamente centralizados, por ejemplo, grandes grupos mineros de Islandia o China.

La pregunta es si esto es posible. Como el número de monedas acuñadas se reduce a la mitad cada cuatro años, ¿qué pasará cuando la retribución caiga a cero? El ciclo de minado depende del precio de mercado del bitcoin. Cuando el precio cae, algunos mineros aparcen sus reservas pero siguen jugando a la lotería hasta que el precio aumenta. Otros no pueden permitírselo y suspenden el minado, o dedican su capacidad procesadora a otras monedas alternativas que podrían ser más rentables. Otros se unen a grupos mineros y comparten su capacidad procesadora con otros nodos esperando aumentar sus probabilidades de conseguir al menos una fracción de las ganancias. Y, por último, está la minería industrial. Valery Vavilov, de BitFury, estima que para su labor de minado dispondrá de una capacidad de al menos 200 megavatios a finales de 2016.

Una respuesta es cobrar comisiones. Satoshi escribió: «Habrà comisiones por transacción, y así los nodos [mineros] tendrán un incentivo para recibir e incluir todas las transacciones que puedan. Al final, cuando el total de monedas creadas alcance el límite predeterminado, los nodos serán recompensados sólo por las comisiones».⁵¹⁰ Así, cuando se hayan acuñado todos los bitcoins, surgirá seguramente un sistema de comisiones. Pensemos en que habrá miles de millones de micropagos. Como cada bloque tiene un tamaño máximo fijo, la cantidad de transacciones que un minero puede incluir es limitada. En consecuencia, los mineros agregarán primero las transacciones con las comisiones más altas, dejando que aquellas con comisiones bajas o nulas se disputen el espacio que quede. Si la comisión de nuestra transacción es lo bastante elevada, podemos esperar que algún minero la incluya en el siguiente bloque, pero si la red está ocupada y nuestra comisión es baja, podrían pasar dos, tres o más bloques antes de que un minero la registrara en la cadena.

¿Qué implica esto para aquellos que no pueden permitirse pagar comisiones? ¿No hará esto que la blockchain pierda su ventaja sobre los métodos de pago tradicionales? Según el empresario capitalista Pascal Bouvier, «las comisiones reflejan el coste marginal de verificar una transacción». Sin comisiones que incentiven a los mineros, y dado que la retribución por bloque sigue disminuyendo a la mitad, el ritmo de hash caerá. Y si el ritmo de hash cae, la seguridad de la red disminuye.⁵¹¹

Esto nos lleva de nuevo a la cuestión del ataque del 51 por ciento, que consiste en que un gran grupo minero o cártel de grupos mineros controla el 51 por ciento de la potencia de hash. Con ese arsenal, podrían constituir una mayoría de mineros que secuestrara la creación de bloques e impusiera su versión de la verdad al resto de la cadena. Eso no quiere decir que se hicieran ricos. Muy al contrario. Lo más que podrían hacer es deshacer sus propias transacciones, registradas en un bloque anterior, algo parecido al llamado contracargo en el caso de las tarjetas de crédito. Imaginemos que los atacantes hacen unas compras importantes a un mismo vendedor, esperan a que se las envíen y luego atacan la red para recuperar el dinero. Esto no significa que puedan añadir su propio bloque al cabo de la cadena. Significa que tienen que volver atrás y rehacer el bloque que contiene sus compras así como todos los bloques siguientes, incluidos los nuevos que la red va generando. Cuando la rama del cártel se alargue, pasará a ser la válida. Satoshi afirma que eso es mucho más costoso que minar nuevas monedas.

Si los ataques del 51 por ciento con modelos de prueba de trabajo proceden de la concentración de poder minero, los ataques con modelos de prueba de participación vienen de la concentración de control monetario, y las plataformas de cambio suelen ser las que más control tienen. En algunas jurisdicciones, necesitan un permiso y están reguladas. También se juegan su reputación, y por eso tienen muchos incentivos para proteger el valor de su marca y el de las monedas guardadas en carteras. Sin embargo, con más monedas en circulación, más diversidad de valor y más activos estratégicos registrados en blockchain de tipo prueba de trabajo o prueba de participación, un atacante puede no hacer caso de todos estos costes.

6. Las blockchains quitan empleo

En la reunión de 2015 del Foro Económico Mundial en Davos, Suiza, un grupo de ejecutivos de empresas tecnológicas como Microsoft, Facebook y Vodafone debatieron sobre el impacto que la tecnología tenía en el empleo. Todos coincidieron en que, si bien las innovaciones tecnológicas pueden alterar los mercados temporalmente, en conjunto crean nuevos empleos. «¿Por qué ahora habría de ser diferente?», se pregunta Eric Schmidt, presidente ejecutivo de Google.

La sustitución de trabajadores por máquinas no es nueva. Pensemos en el impacto que está teniendo internet en las agencias de viajes y en el mercado musical minorista. Uber y Airbnb producen ganancias a los conductores con tiempo libre y a los propietarios de inmuebles con habitaciones libres, pero no les ofrecen ni seguros médicos ni otros beneficios que suelen tener los empleados, y están sustituyendo puestos mejor pagados en los sectores del transporte y el alojamiento.

Las blockchains son una extraordinaria plataforma para la automatización radical del trabajo, en la que unos códigos informáticos y no los humanos hacen las tareas, gestionando recursos y personas. ¿Qué pasará cuando los vehículos automáticos reemplacen a los conductores de Uber? ¿O cuando las monedas digitales permitan prescindir de los 500.000 puntos de venta que tiene Western Union en todo el mundo?⁵¹² ¿O cuando una plataforma de servicios financieros de blockchain elimine los cientos de miles de empleos del sector de la administración contable y de la tecnología de la información? Mientras que el internet de las cosas creará muchas oportunidades y negocios nuevos, ¿aumentará también el desempleo, sobre todo en el mercado de trabajo no cualificado?

En el mundo en vías de desarrollo el sistema blockchain y las criptomonedas podrían permitir a los empresarios conseguir financiación, proteger activos y la propiedad intelectual y crear trabajo incluso en las comunidades más pobres. Cientos de miles de personas podrían convertirse en microaccionistas de nuevas empresas y participar en el intercambio económico. La tecnología podría mejorar drásticamente la entrega y distribución de ayuda humanitaria, aumentar la transparencia del Estado, reducir la corrupción y sentar las bases de un buen gobierno, que es una condición para crear trabajo en muchas partes del mundo.

Incluso en el mundo desarrollado las consecuencias son impredecibles. Una plataforma global que reduzca los costes transaccionales, en particular los costes de generar confianza y crear riqueza, podría atraer a muchos participantes.

Aunque esta tecnología nos permite hacer más cosas con menos mano de obra humana, sigue sin haber motivos para temer, frenar o detener su marcha. En última instancia lo que importa no es si existen o no nuevas posibilidades, sino hasta qué punto las sociedades las usan en beneficio de todos. Si las máquinas crean tanta riqueza, quizá es hora de establecer un nuevo contrato social que redefina el trabajo humano y cuánto tiempo deberíamos emplear en ganarnos la vida.

7. La dificultad de gestionar los protocolos

¿Cómo deberíamos administrar este nuevo recurso para realizar su potencial? A diferencia de internet, la comunidad bitcoin aún no tiene organismos de control oficiales como la ICANN, el Grupo de Trabajo de Ingeniería de Internet o el Consorcio World Wide Web que anticipen sus necesidades y guíen su desarrollo..., y la comunidad lo prefiere así. Esto conlleva incertidumbre. La gente que quiere que las blockchains sigan siendo descentralizadas, abiertas y seguras no se pone de acuerdo en cómo avanzar. Si no solucionamos el problema de su gestión, el movimiento podría desintegrarse en facciones enfrentadas y hundirse.

Hay muchísimas posibilidades. Los desarrolladores de bitcoin Gavin Andresen y Mike Hearn han venido defendiendo que el tamaño de los bloques pase de un megabyte a veinte. Bitcoin no es «una moneda para que gente rica especule con ella... Es una red de pago», dice Andresen.⁵¹³ Afirman que si bitcoin quiere convertirse en un mecanismo de pago global serio, debe prepararse para un uso masivo. No puede dejar de funcionar cuando de pronto el flujo de transacciones sobrepase la capacidad del sistema. Las comisiones que tendrían que pagar las personas que no quieran esperar meses o años para que sus transacciones se procesen se dispararían. O quizá saldría algún poder central a defender al consumidor y se encargaría de procesar el exceso. En agosto de 2015, estos desarrolladores se decidieron y lanzaron Bitcoin XT, una bifurcación de la cadena que permite crear bloques de ocho megabytes. Sigue siendo una medida controvertida.

Los oponentes afirman que la gente no tiene por qué usar bitcoins para pagar sus cafés con leche en Starbucks. «Hay desarrolladores que quieren que todas las personas del mundo ejecuten un nodo completo que valide todas las transacciones y no confíe en nadie —dice Andresen—. Los voluntarios que han hecho que el programa funcione los últimos

años están preocupados porque quizá no serán capaces de manejar bloques más grandes cuando el volumen de transacciones se dispare... No acaba de convencerme.»⁵¹⁴ En otras palabras, si la cadena bitcoin ha de crecer y ha de ser segura, no podemos tener las dos cosas. Habrá nodos que ejecuten protocolos completos y procesen más transacciones en bloques cada vez más grandes, y otros que ejecuten modelos de verificación de pago más simples confiando en que el 51 por ciento de los nodos completos se porte bien.

Los que más se oponen a Bitcoin XT son los grupos mineros que hay en China. Los mineros de bitcoin serios, como los jugadores de videojuegos en línea empedernidos, no sólo necesitan ordenadores potentes, sino también anchos de banda de alta velocidad para subir su trabajo rápidamente a la red. China es una excepción a la ley de Nielsen sobre internet: el ancho de banda no aumenta un 50 por ciento anual. Si el tamaño de los bloques crece demasiado, los mineros chinos, con anchos de banda más lentos, estarían en desventaja con respecto a los mineros de otras partes del mundo. Tardarían más en recibir nuevos bloques a partir de los cuales trabajar, así como en enviarlos al resto de la red. Este retraso acabaría haciendo que la red rechazara algunos de sus bloques y perderían ante mineros con más ancho de banda cuyos bloques se difundieran antes.

«Reiniciar o cambiar un protocolo de red es una tarea inmensa —dice Austin Hill—. No se pueden improvisar ni hacer precipitadamente cambios en un ecosistema que maneja riquezas y bienes por valor de entre 3.000 y 10.000 millones de dólares.»⁵¹⁵ Al fin y al cabo, dice Andresen, «ese modelo de gestión depende en gran medida del código que la gente quiera ejecutar, del nivel de calidad que quiera alcanzar en el material que venda». Dice que bitcoin, como internet, «vivirá un proceso de gestión igual de caótico que al final dependerá de qué código decidamos ejecutar».⁵¹⁶

Repetimos que no hablamos de regular sino de promover este recurso para que sea viable. La gestión incluye establecer normas de funcionamiento, adoptar políticas razonables, fomentar el conocimiento del potencial de la tecnología, desempeñar funciones de control y vigilancia, y, efectivamente, crear una infraestructura global. Hablamos de un modelo de gestión participativo en el siguiente capítulo.

8. Los agentes autónomos distribuidos serán Skynet

Hay empresas muy distribuidas que tienen buenos y malos actores. Anonymous es una red distribuida de voluntarios con intereses comunes compuesta de saboteadores, soplones y espías. Con el sistema blockchain, Anonymous podría recaudar bitcoins y guardarlos en una cartera. Ahora supongamos que un grupo de accionistas franceses quisiera dar ese dinero a unos asesinos para que encontraran y mataran a los terroristas que perpetraron la matanza de París. Necesitarían miles de firmantes para alcanzar un consenso y liberar ese dinero. En este caso, ¿quién controla legalmente ese capital? ¿Quién es responsable del resultado de la transacción? Si nosotros contribuimos con un voto entre diez mil, ¿cuál es nuestra responsabilidad?⁵¹⁷

Si las máquinas expendedoras están programadas para pedir los productos que produzcan más beneficios, ¿descubrirán un proveedor de bienes ilegales o drogas? ¿Venderá la máquina de caramelos éxtasis? ¿Cómo actuaría la ley con un vehículo

automático que matara accidentalmente a un ser humano? Para la revista *Wired*, dos piratas mostraron cómo secuestrar los sistemas de control de un Jeep Cherokee en una autopista. Chrysler respondió retirando 1,4 millones de vehículos, con la consiguiente alarma de conductores, fabricantes y políticos.⁵¹⁸ ¿Podrían los terroristas piratear dispositivos inteligentes para que realizaran acciones no deseadas con consecuencias desastrosas?

Los modelos de empresa distribuida tienen otros problemas. ¿Cómo gestiona la sociedad estas entidades? ¿Cómo pueden sus dueños ejercer el control en última instancia? Supongamos que somos dueños de una empresa de proveedores de servicios de internet en cuya administración todos los servidores tienen voz y voto. Un pirata humano o algún programa malicioso podrían simular que son un millón de servidores y vencer por mayoría a los legítimos servidores de la red. Cuando esta usurpación se produce en empresas tradicionales, los resultados pueden variar. Con un *agente autónomo distribuido* (DAE, por sus siglas en inglés), los resultados serán seguramente desastrosos. Una vez que esa entidad malévola controla nuestra empresa, podría desvalijarla. O podría hacer pública la información de otros servidores o retenerla hasta que los propietarios humanos pagáramos un rescate.

Cuando las máquinas tengan inteligencia y capacidad de aprender, ¿cuánto tardarán en volverse autónomas? ¿Decidirán los drones y robots militares, por ejemplo, atacar a los civiles? Según algunos estudios de inteligencia artificial, estas armas podrían empezar a fabricarse no en décadas, sino en años. En julio de 2015, un gran grupo de científicos e investigadores, entre los que estaban Stephen Hawking, Elon Musk y Steve Wozniak, publicó una carta abierta pidiendo que se prohibiera desarrollar armas ofensivas autónomas sin control humano.⁵¹⁹

«El titular de pesadilla sería para mí: “Cien mil frigoríficos atacan el Bank of America”», dice Vint Cerf, considerado el padre de internet. «Tendremos que pensar seriamente no sólo en la seguridad y la privacidad tecnológicas, sino también en cómo configurar y mejorar los dispositivos a gran escala», añade, observando que nadie quiere pasarse todo el fin de semana tecleando direcciones IP para todos y cada uno de los dispositivos domésticos.⁵²⁰

Nosotros no queremos que los DAE y el internet de las cosas estén muy regulados ni dependan de permisos oficiales. No queremos que los empresarios que están desarrollando aplicaciones tengan que identificar todas las consecuencias que esas aplicaciones puedan tener en la sociedad —buenas, malas o neutras— y alteren los códigos fuente y el diseño. Creemos que deberían consultar con aquellos que pudieran verse afectados por sus creaciones a fin de minimizar los riesgos de antemano, encontrar vías alternativas de progreso y conseguir apoyos.

9. El gran hermano sigue observándonos

«Habrá muchos intentos por controlar la red —dice Keonne Rodriguez, de Blockchain—. Las grandes empresas y los gobiernos se dedicarán a destruir la privacidad. La Agencia Nacional de Seguridad debe de estar analizando datos provenientes de blockchain» ahora

mismo.⁵²¹ Si bien las blockchains garantizan cierto anonimato, también ofrecen cierta apertura. Si el comportamiento del pasado dice algo de las intenciones futuras, debemos esperar que empresas conocidas por espiar y países conocidos por lanzar ciberataques redoblen sus esfuerzos, porque hay mucho valor en juego: dinero, patentes, acceso a derechos de explotación minera, títulos de propiedad de bienes inmuebles y del Tesoro. Es como si hubiéramos puesto una gran claraboya en lo alto de internet. Lo bueno es que todo el mundo podrá ver los chanchullos. Algunos pueden tener muchos motivos para denunciar el espionaje porque en un mercado de predicción han apostado por la probabilidad de que un determinado régimen esté atacando la blockchain.

¿Qué ocurre con la privacidad cuando el mundo físico empieza a recoger, comunicar y analizar infinitos datos que podrían perseguir a un individuo para siempre? En una conferencia dada en Webstock en 2014, Maciej Cegłowski criticó duramente la adquisición por Google de Nest, un fabricante de termostatos de lujo con sensores que recogen información de nuestras viviendas. Su viejo termostato no venía acompañado de una política de privacidad. Este termostato inteligente podía mandar información a Google, quizá incluso comerse la pizza que le sobraba como si fuera un compañero de piso poco fiable.⁵²² A muchos nos disgustan ya unos medios sociales que nos siguen allí donde vamos y nos bombardean con anuncios publicitarios. En el mundo de las blockchains, tendremos más control sobre esto, pero ¿seremos capaces de manejar bien nuestro régimen mediático?

Ninguno de estos problemas de privacidad es insuperable. Añade Cegłowski: «¡Lo bueno es que es cuestión de voluntad! Podemos crear un internet que sea distribuido, resistente, que irrite a todos los gobiernos y sea libre en el mejor sentido de la palabra», como queríamos que fuera en la década de los noventa del siglo pasado. Ann Cavoukian, del Privacy and Big Data Institute, señala siete principios que son «buenos para los negocios, buenos para los gobiernos y buenos para la gente». El primero es fundamental: hacer de la privacidad un elemento preferente. Rechazar las falsas dicotomías que oponen la privacidad a la seguridad; todos los sistemas tecnológicos, todas las prácticas de negocios y todas las infraestructuras deben poder funcionar plenamente. Los dirigentes han de prevenir más bien que reaccionar a las violaciones, operar siempre con transparencia y someter sus organizaciones a una verificación independiente. Las empresas se ganarán la confianza de la gente respetando la privacidad del usuario, haciendo de éste el eje de su desarrollo, garantizando la seguridad integral de sus datos y destruyéndolos cuando dejen de ser necesarios. Cavoukian dice: «Es un planteamiento en el que ganan las dos partes».⁵²³

Dice Cegłowski: «Pero eso necesitará esfuerzo y determinación. Habrá que rechazar una y otra vez modelos de negocio que se basen en la vigilancia masiva permanente, algo que escocerá a algunos. Habrá que forzar leyes a través de un sistema legal esclerótico. Tendremos que dar un poco la lata. Pero si no diseñamos este internet, si simplemente seguimos desarrollándolo, al final atraerá a ciertos visionarios que no nos van a gustar y no podremos hacer nada».⁵²⁴

10. Los delincuentes lo usarán

Al principio, los detractores de la moneda bitcoin la consideraron un instrumento para lavar dinero y comprar bienes ilícitos. Decían que, como esta tecnología es descentralizada, velocísima y distribuida, los delincuentes la explotarían. Puede ser, y el lector conocerá el caso de Silk Road, la plataforma digital de venta de drogas ilegales. En octubre de 2013, en su momento de mayor auge, la plataforma tenía 13.756 artículos con el precio en bitcoins. Los productos se enviaban por correo con un manual para evitar que las autoridades los detectaran. Cuando el FBI secuestró el sitio, el precio del bitcoin se desplomó y las monedas digitales fueron sinónimo de delincuencia. Fue la hora más negra de bitcoin.

Pero no hay nada especial en la tecnología de bitcoin o de las blockchains que la haga más efectiva para los delincuentes que otras tecnologías. Las autoridades, en general, creen que las monedas digitales podrían contribuir a aplicar la ley al proporcionar un registro de actividades sospechosas e incluso al ayudar a resolver multitud de delitos cibernéticos, ofreciendo desde servicios financieros hasta el internet de las cosas. Marc Goodman, autor de *Future Crimes*, decía hace poco: «Nunca ha habido un sistema informático que haya demostrado ser inatacable».⁵²⁵ Las ocasiones delictivas han aumentado con la tecnología. «La capacidad de una persona para afectar a muchas otras ha aumentado exponencialmente, y lo ha hecho tanto para bien como para mal.»⁵²⁶ Todo depende, por lo tanto, de que unos seres humanos quieran dañar a otros seres humanos. Los delincuentes usarán las últimas tecnologías para ello.

Sin embargo, bitcoin y la tecnología blockchain podrían disuadir a los delincuentes de usarlas. En primer lugar, también los delincuentes deben hacer públicas todas sus transacciones en la blockchain, con lo que la ley puede controlar los pagos en bitcoins más fácilmente que en efectivo, que sigue siendo el medio de pago preferido de los delincuentes. El viejo refrán del Watergate, «sigue el dinero» para dar con el ladrón, es mucho más factible en una blockchain que en cualquier otro método de pago. Hay reguladores que, por la naturaleza anónima de bitcoin, llaman a las monedas «futuros de cargo», porque pueden rastrearse e identificarse más fácilmente que el dinero en efectivo.

Después de cada asesinato en masa que se comete en Estados Unidos, los representantes cuyos electores y financiadores son miembros de la Asociación Nacional del Rifle se apresuran a decir: «¡La culpa de toda esta violencia no la tienen las armas!». Tendría gracia que esas mismas personas prohibieran la tecnología blockchain por los delitos que algunas personas puedan cometer con ella. La tecnología no tiene voluntad. No quiere nada ni se inclina por esto o por lo otro. El dinero es tecnología, después de todo. Cuando alguien atraca un banco, no culpamos del robo al dinero que se guarda en la caja fuerte. Que los delincuentes usen bitcoin dice más de la falta de una buena gestión, regulación, sostén y educación que de sus virtudes subyacentes.

Razones por las que las blockchains pueden fracasar, o los retos de su implementación

Los obstáculos, pues, son enormes. Ya empieza a surgir la computación cuántica, el llamado «error del milenio» de los criptógrafos, que combina la mecánica cuántica y la informática teórica para resolver problemas —por ejemplo, algoritmos criptográficos— mucho más rápido que los ordenadores de hoy. Dice Steve Omohundro: «Los ordenadores cuánticos, en teoría, pueden manejar números muy grandes muy rápida y eficazmente, y la mayoría de los sistemas criptográficos de clave pública se basan en tareas como ésa. Por eso, si al final se hacen realidad, toda la infraestructura criptográfica del mundo tendrá que cambiar radicalmente».⁵²⁷ El debate sobre la innovación tecnológica y el progreso viene de antiguo: ¿es la herramienta buena o mala? ¿Hace avanzar la condición humana o la degrada? Como observa el satírico James Branch Cabell, «los optimistas dicen que vivimos en el mejor de los mundos posibles; los pesimistas temen que sea verdad».⁵²⁸

Como muestra la historia de Lev Termén, las personas y las organizaciones pueden usar las innovaciones para bien o para mal, y así ha ocurrido con una gran variedad de tecnologías, desde la electricidad hasta internet. Yochai Benkler, autor del influyente libro *La riqueza de las redes*, nos dice: «La tecnología no se inclina sistemáticamente por la desigualdad y no impone una estructura del empleo; éstas son batallas sociales, políticas y culturales». Aunque la tecnología puede cambiar los negocios y la sociedad radical y rápidamente, Benkler cree que «no lo hace de una manera determinista, en un sentido o en otro».⁵²⁹

En general, el balance de la historia tecnológica ha sido positivo. Pensemos en los muchos adelantos que se han hecho en materia de alimentación y medicina, de la investigación y el desarrollo al tratamiento y la prevención: la tecnología ha contribuido a que exista más justicia, más capacidad productiva y más progreso social.

Nada indica que la tecnología blockchain no vaya a caer en la misma trampa en la que ha caído internet. Puede resistirse a la centralización y al control, pero si el interés económico y político es lo bastante grande, fuerzas poderosas tratarán de apoderarse de ella. Los líderes de este nuevo paradigma tendrán que volver por sus fueros e iniciar una ola de innovación económica e institucional para garantizar que todo el mundo tiene una oportunidad. Esta vez cumplamos la promesa. Lo que nos lleva a la cuestión de cómo hacerlo.

Capítulo XI

El liderazgo de la era que viene

Prolífico es un adjetivo que debería preceder a todos los títulos que se usen para describir al canadiense nacido en Rusia de veintiún años Vitalik Buterin, fundador de Ethereum. (O sea, *prolífico* fundador.) Pregunte el lector a su legión de seguidores sobre Ethereum y le dirán que es una «plataforma de guion (*script*), Turing completa, arbitraria y basada en el sistema blockchain»,⁵³⁰ plataforma que ha atraído a IBM, Samsung, UBS, Microsoft y al gigante automovilístico chino Wanxiang, así como a un ejército de desarrolladores de programas inteligentes de todo el mundo, todos los cuales piensan que Ethereum puede ser «el ordenador planetario» que lo cambie todo.⁵³¹

Cuando Buterin nos explica lo que significa que un sistema sea «arbitrario y Turing completo», es como si nos permitiera echar un vistazo a su mente. Escuchar música es muy diferente de leer un libro o calcular los ingresos y gastos del día, pero podemos hacer las tres cosas con nuestro teléfono inteligente, porque el sistema operativo de éste es «Turing completo». Eso significa que puede aceptar cualquier otro lenguaje que sea Turing completo. Los innovadores, pues, pueden crear casi cualquier aplicación digital imaginable con Ethereum: aplicaciones que desempeñen funciones muy distintas, y que sean desde contratos inteligentes y mercados de recursos informáticos hasta instrumentos financieros complejos y modelos de gestión distribuidos.

Buterin es políglota. Habla inglés, ruso, francés, cantonés (idioma que aprendió en dos meses durante unas vacaciones), latín y griego clásicos, BASIC, C++, Pascal y Java, por nombrar unos cuantos.⁵³² «Yo me especializo en muchas cosas», dice. También es polifacético, y además modesto. «Me interesaban todas esas cosas y de alguna manera me pareció que bitcoin era el punto de convergencia perfecto. Tiene matemáticas, tiene ciencia informática, tiene criptografía, tiene economía, tiene filosofía política y social. Enseguida me atrajo esta comunidad», dice. «Me pareció llena de posibilidades.» Entró en foros, buscó la manera de hacerse con unos bitcoins y descubrió a un tío que estaba lanzando un blog bitcoin. «Se llamaba *Bitcoin Weekly* y ofrecía cinco bitcoins por escribir artículos. Entonces eran unos cuatro dólares —cuenta Buterin—. Escribí unos cuantos artículos. Gané veinte dólares. Me gasté la mitad en una camiseta. Pasar por todo el proceso era como trabajar con las piedras fundacionales de la sociedad.»⁵³³

Y eso que, unos cinco años antes, había despreciado bitcoin. «En febrero de 2011 mi padre me dijo: “¿Has oído hablar de bitcoin? Es esa moneda que sólo existe en internet sin respaldo de ningún gobierno”. Inmediatamente pensé: “Ya, eso no tiene valor intrínseco, no puede funcionar”.» Como muchos adolescentes, Buterin «se pasaba un montón de tiempo en internet» leyendo sobre diferentes ideas que eran heterodoxas, fuera

de lo común. Si le preguntamos por sus economistas favoritos, contesta que son Tyler Cowen, Alex Tabarrok, Robin Hanson y Bryan Caplan. Puede hablar sobre el pensamiento del teórico del juego Thomas Schelling y de los economistas conductistas Daniel Kahneman y Dan Ariely. «Es realmente sorprendente lo mucho que podemos aprender por nosotros mismos debatiendo con otras personas en los foros, por ejemplo, sobre política. Es toda una experiencia educativa en sí misma», dice. Bitcoin seguía presente.

A finales de ese año Buterin dedicaba de diez a veinte horas semanales a escribir para otra publicación, *Bitcoin Magazine*. «Cuando llevaba unos ocho meses estudiando en la universidad me di cuenta de que aquello estaba atrapándome y de que quizá podía dedicarme a ello toda la vida. La Universidad de Waterloo era muy buena y el plan de estudios me parecía excelente. Dejé la universidad no porque no me gustara, sino porque me gustaba más lo otro. Era una de esas oportunidades que sólo se presentan una vez en la vida y no podía dejarla pasar.» Tenía sólo diecinueve años.

Buterin creó el proyecto de código fuente abierto Ethereum cuando se dio cuenta de que las blockchains podían ir mucho más allá de las monedas y los programadores necesitaban una plataforma más flexible que la que la blockchain bitcoin ofrecía. Ethereum permite una apertura radical y una privacidad radical en la red. Para él, esto no es una contradicción sino «una especie de síntesis hegeliana», una dialéctica entre ambas cosas que da como resultado una «transparencia voluntaria».

Ethereum, como muchas tecnologías de la historia, podría acabar con algunos empleos. Buterin cree que es un fenómeno natural que se da con muchas tecnologías y propone una solución novedosa: «Dentro de medio siglo habremos abandonado el modelo según el cual tenemos que trabajar ocho horas diarias para subsistir y llevar una vida decente».⁵³⁴ Sin embargo, en el caso de las blockchains, no cree que vaya a causar una pérdida de empleos masiva. Ethereum podría ofrecer nuevas oportunidades para crear valor y montar empresas. «Mientras que la mayoría de las tecnologías tienden a automatizar a los trabajadores y desplazarlos a la periferia para que hagan tareas poco cualificadas, las blockchains automatizan el centro —dice—. En lugar de quitarle el trabajo a un taxista, la blockchain se lo quita a Uber y deja que el taxista trabaje con el cliente directamente.» Las blockchains, más que eliminar trabajos, cambian la definición de trabajo. ¿Quién se verá afectado por esta gran revolución? «Sospecho y espero que las víctimas sean los abogados que ganan medio millón de dólares anuales más que las demás personas.»⁵³⁵ Así parafrasea Buterin el dicho de Shakespeare: «Lo primero que haremos es matar a los abogados».⁵³⁶

Ethereum tiene otra aparente contradicción. Es descaradamente individualista y privado pero depende de una comunidad vasta y distribuida que actúa abiertamente en su propio interés colectivo. Es más, la plataforma está diseñada de acuerdo tanto con su fe en que las personas harán lo correcto cuando se vean provistas de los instrumentos correctos, como con su sano escepticismo respecto de los motivos que mueven a las instituciones grandes y poderosas. Aunque pondera con gravedad los problemas de la sociedad contemporánea, lo hace con un tono de esperanza. «Hay muchas cosas que son injustas, pero cada vez acepto más el mundo como es y pienso en las oportunidades que puede

ofrecer el futuro.» Cuando se enteró de que 3.500 dólares permitirían a una persona luchar contra la malaria el resto de su vida, no lamentó que las personas, los gobiernos y las empresas no donaran, sino que se dijo: «¿Podemos salvar una vida por sólo 3.500 dólares? ¡Eso sí que es amortizar la inversión! Ahora mismo dono».⁵³⁷ Ethereum es su herramienta para cambiar efectivamente el mundo. «Participo de la tendencia general a perfeccionar la tecnología para que las cosas sean mejores para la sociedad.»

Buterin es un líder nato, en el sentido de que arrastra a la gente con sus ideas y su visión del mundo. Es el primer artífice de la red, el que más consenso logra en la comunidad Ethereum y el que mejor cultiva una comunidad mayor de desarrolladores brillantes que tienen fuertes opiniones sobre todo lo que es técnico. ¿Y si triunfa?

¿Quién liderará una revolución?

En 1992, el científico informático del MIT David Clark dijo: «Rechazamos a los reyes, a los presidentes y las votaciones. Creemos en los consensos básicos y en los códigos que funcionan».⁵³⁸ Éste fue el lema de los sostenedores de la primera generación de internet. Se proclamaba en un momento en el que la mayoría de las personas apenas podían imaginar hasta qué punto internet se convertiría en un nuevo medio de comunicación humana, que probablemente superaría a todos los anteriores por su importancia para la sociedad y la vida cotidiana. Las palabras de Clark reflejaban una idea sobre el liderazgo y la gestión de un recurso global que era radicalmente diferente a los otros pero que suponía un modelo de gestión bastante efectivo.

Desde el final de la segunda guerra mundial, una serie de instituciones basadas en Estados han administrado importantes recursos globales. Dos de los más poderosos —el Fondo Monetario Internacional (FMI) y la Organización Mundial del Comercio (OMC)— nacieron en la Conferencia de Bretton Woods de 1944. Las Naciones Unidas y otros organismos tutelados por ellas, como la Organización Mundial de la Salud (OMS), recibieron amplias facultades para ejercer su monopolio en la resolución de los problemas globales. Estas organizaciones eran jerárquicas por naturaleza, porque la jerarquía era el paradigma dominante en la primera mitad de un siglo marcado por la guerra. Pero estas soluciones a escala industrial responden mal a los desafíos de la era digital. El auge de internet marcó un punto de inflexión importante en la cultura del gobierno tradicional.

En 1992, la mayoría del tráfico de internet consistía en correos electrónicos. El navegador gráfico que hizo posible la extraordinaria «red informática global» vendría dos años después. La mayoría de la gente no estaba conectada ni entendía la tecnología. Muchas de las instituciones importantes que habrían de desarrollar este importante recurso global estaban en embrión o no habían nacido. El Grupo de Trabajo de Ingeniería de Internet, una comunidad internacional que gestiona muchos aspectos de la red, tenía apenas cuatro años. La Corporación de Internet para la Asignación de Nombres y Números (ICANN, por sus siglas en inglés), que presta servicios esenciales como el de asignar nombres de dominios, no se fundaría hasta seis años después, y Vint Cerf y Bob Kahn estaban reuniendo a gente para lo que al final sería la Sociedad de Internet.

La segunda generación de internet tiene el mismo espíritu y siente el mismo entusiasmo por la apertura y la misma aversión por las jerarquías, como se manifiesta en la escala de valores de Satoshi, Voorhees, Antonopoulos, Szabo y Ver. El código abierto es un gran principio organizador pero no es un *modus operandi* que sirva para seguir adelante. Por mucho que el código abierto haya transformado muchas instituciones de la sociedad, seguimos necesitando coordinación, organización y liderazgo. Proyectos de código abierto como Wikipedia o Linux, aunque basados en principios meritocráticos, siguen teniendo dictadores benevolentes como Jimmy Wales y Linus Torvalds.

Satoshi Nakamoto, dicho sea en su favor, reconcilió los incentivos de las distintas partes codificando principios de poder distribuido, integridad reticular, valor indiscutible, derechos de los participantes (como privacidad, seguridad y propiedad) e inclusión tecnológica. El resultado ha sido un gran desarrollo de la tecnología en los primeros años, fruto del cual son los ecosistemas que hoy conocemos. Sin embargo, este planteamiento, que hace de la no intervención una especie de dios, está empezando a crear tensiones. Como ocurre con todas las tecnologías revolucionarias, hay ideas encontradas sobre el ecosistema blockchain. Incluso los desarrolladores de blockchains se han dividido en varios bandos, cada uno con su propio criterio.

Brian Forde, ex empleado de la Casa Blanca y defensor de las blockchains que ahora dirige la Digital Currency Initiative del MIT, dice: «Si nos fijamos en el debate sobre el tamaño de los bloques, ¿realmente es sobre el tamaño de los bloques? En los medios de comunicación lo es, pero creo que lo que estamos viendo es un debate sobre la gestión».⁵³⁹ ¿Qué tipo de gestión y, más particularmente, qué tipo de liderazgo se necesita? Mike Hearn, por ejemplo, un destacado desarrollador bitcoin, causó un gran revuelo en enero de 2015 cuando escribió una carta de despedida a la industria en la que predecía la desaparición inminente de bitcoin. En esa carta, destacaba una serie de problemas acuciantes a los que se enfrentaba esta tecnología; el principal, que no se había respondido a importantes cuestiones técnicas y que había desacuerdo y confusión en las filas de la comunidad. La conclusión de Hearn era que estos problemas harían fracasar bitcoin. Discrepamos. De hecho, lo que Hearn quería que fuera una crítica condenatoria de los defectos de bitcoin es, a nuestro juicio, una de las más elocuentes defensas de la importancia de que exista una gestión participativa basada en la transparencia, el mérito y la colaboración. El código es sólo una herramienta. Para que esta tecnología siga avanzando y cumpla con su promesa a largo plazo, tienen que liderarla los humanos. Ahora es preciso que todas las partes implicadas se unan y resuelvan algunas cuestiones fundamentales.

Ya hemos señalado algunos de los problemas. No son baladíes. Pero constituyen desafíos que hay que superar para que esta revolución triunfe, no razones para oponerse a ella. Hasta ahora, muchas cuestiones siguen sin resolverse y muchas preguntas sin contestarse, y hay poco movimiento colectivo para buscarles una solución. ¿Cómo crecerá la tecnología? ¿Podremos hacerla crecer sin destruir el medio físico? ¿Habrá fuerzas poderosas que ahoguen la innovación o se apropien de ella? ¿Cómo resolveremos las cuestiones controvertidas sin volver a caer en la jerarquía?

Responder a estas cuestiones ha sido el objeto de nuestras investigaciones en los últimos dos años. Hemos descubierto que lo que necesitamos no son instituciones estatales, sino que la sociedad civil, el sector privado, el gobierno y los individuos colaboren en redes no estatales. Llamémoslas *redes para soluciones globales* (GSN, por sus siglas en inglés). Estas redes digitales están proliferando, creando nuevas formas de cooperación, cambiando la sociedad e incluso produciendo valor público global.

Una de las más importantes es internet mismo, organizado y administrado por un conjunto antes impensable de individuos, organizaciones de la sociedad civil y empresas, con el sostén tácito y a veces activo de los Estados. Pero ningún gobierno, país, empresa ni institución estatal controla internet. Y funciona. Así ha demostrado que varias partes implicadas pueden gestionar eficazmente un recurso global con inclusión, consenso y transparencia.

La lección está clara. La buena administración de estas innovaciones globales complejas no es tarea únicamente del Estado. Tampoco podemos dejarla en manos del sector privado: los intereses comerciales no bastan para garantizar que este recurso esté al servicio de la sociedad. Más bien necesitamos que todos los interesados colaboren globalmente y asuman el liderazgo.

El ecosistema blockchain: una alineación de jugadores

Aunque la tecnología blockchain surgió de la comunidad de código abierto, enseguida atrajo a muchas personas, cada una con su formación, intereses y motivaciones. Desarrolladores, inversores, empresarios, gobiernos y organizaciones no gubernamentales tienen su propia perspectiva y un papel que desempeñar. Empieza a haber indicios de que muchos de los participantes principales ven la necesidad de liderazgo y están dando un paso al frente. Veamos quiénes son:

Pioneros de la industria de las blockchains

Pioneros de la industria como Erik Voorhees y Roger Ver creen que cualquier forma de gestión oficial, regulación, protección o supervisión no es sólo absurda, sino contraria a los principios de bitcoin.⁵⁴⁰ Dice Voorhees: «Bitcoin está ya muy bien regulado por las matemáticas, las cuales no dependen de los caprichos de los gobernantes».⁵⁴¹ Sin embargo, conforme la industria se expande, muchos empresarios piensan que dialogar con los gobiernos y ampliar el enfoque de la gestión es bueno. Empresas como Coinbase, Circle o Gemini se han unido a organizaciones comerciales, y algunas incluso mantienen estrechas relaciones con instituciones gestoras emergentes, como la Digital Currency Initiative del MIT.

Inversores de riesgo

Lo que empezó siendo una camarilla de iniciados pronto creció hasta convertirse en el mayor inversor de riesgo de Silicon Valley, incluyendo a la venerable Andreessen Horowitz. Hoy, gigantes financieros se meten a inversores de riesgo: Goldman Sachs, NYSE, Visa, Barclays, UBS y Deloitte han invertido directamente en empresas emergentes o apoyado proyectos de nuevas empresas. Los fondos de pensiones también se apuntan. OMERS Ventures, la multimillonaria empresa inversora de uno de los más grandes fondos de pensiones públicos de Canadá, hizo su primera inversión en 2015. Jim Orlando, que dirige esa empresa, está buscando la próxima aplicación revolucionaria que «sea al sistema blockchain lo que los navegadores fueron a internet».⁵⁴² Las inversiones se han disparado: de 2 millones de dólares en 2012 a 500 millones en la primera mitad de 2015.⁵⁴³ El entusiasmo es palpable. Tim Draper nos dice que «los financieros subestiman el potencial de las blockchains».⁵⁴⁴ Las empresas inversoras relevantes pueden abogar por la tecnología y apoyar las instituciones gestoras incipientes, como Coin Center, financiado por Andreessen Horowitz. Digital Currency Group, una empresa fundada por Barry Silbert, ha incorporado a la directiva a académicos y a otros consejeros atípicos para acelerar el desarrollo de un sistema financiero mejor a través de la inversión y el apoyo activo.

Bancos y servicios financieros

Seguramente en ninguna otra industria se ha producido un cambio de opinión tan brusco. Durante mucho tiempo, la mayoría de las instituciones financieras rechazaron bitcoin acusándolo de ser una herramienta especulativa para jugadores y delincuentes, y apenas prestaron atención a lo que eran las blockchains. Hoy todo el mundo se ha apuntado. Es impresionante ver cómo ha ocurrido esto en 2015. Antes de este año, sólo unas cuantas instituciones financieras importantes anunciaron inversiones en el sector. Hoy, el Commonwealth Bank of Australia, el Banco de Montreal, la Société Générale, State Street, CIBC, RBC, TD Bank, Mitsubishi UFJ Financial Group, BNY Mellon, Wells Fargo, Mizuho Bank, Nordea, ING, UniCredit, Commerzbank, Macquarie y muchos otros están invirtiendo en la tecnología y participando en el debate sobre el liderazgo. La mayoría de los grandes bancos del mundo se han incorporado al consorcio R3 y muchos más se han asociado a la Fundación Linux para lanzar el proyecto Hyperledger. Los bancos deben participar en el debate sobre el liderazgo, pero los demás interesados han de estar prevenidos contra las grandes empresas que quieren controlar esta tecnología, como hicieron en los primeros tiempos de internet.

Desarrolladores

Los desarrolladores de la comunidad están divididos sobre aspectos técnicos básicos y la comunidad reclama coordinación y liderazgo. Gavin Andresen, el desarrollador bitcoin en torno al cual gira el debate sobre el tamaño de los bloques, nos dice: «Yo preferiría quedarme en la sala de máquinas, haciendo que el bitcoin marche»,⁵⁴⁵ en vez de pasarse

todo el rato defendiendo su postura. Pero, dada la falta de liderazgo, Andresen ha sido sin darse cuenta el centro de la atención. En el verano de 2015 nos dijo: «Mi trabajo de los próximos seis meses consistirá en mantener con vida bitcoin desde el punto de vista técnico para que siga funcionando dentro de dos o tres años y permita hacer una serie de operaciones: micropagos, compraventa de acciones, transferencia de propiedad y demás», lo que exige mucha labor de defensa y de promoción. Para él, la red de gestión de internet es un buen punto de partida. «Siempre busco modelos que seguir. El modelo por excelencia es el Grupo de Trabajo de Ingeniería de Internet.»⁵⁴⁶ La gestión de internet es «bastante caótica», dice, pero el caso es que funciona y es fiable.

El mundo académico

Las instituciones académicas financian laboratorios y centros de investigación para estudiar esta tecnología y colaborar con colegas de otras especialidades. Brian Forde nos dice: «Pusimos en marcha Digital Currency Initiative para catalizar algunos de los grandes recursos que tenemos en el MIT y dedicarlos al desarrollo de esta tecnología, porque creemos que será una de las más importantes transformaciones tecnológicas de los próximos diez años».⁵⁴⁷ Joichi Ito, director del Media Lab del MIT, ve una oportunidad para que el mundo académico dé un paso al frente: «El MIT y el ámbito académico pueden ser un lugar en el que podamos hacer valoraciones, investigación, y hablar de cosas como la escalabilidad de esta tecnología sin sesgos ni intereses particulares».⁵⁴⁸ Jerry Brito, uno de los juristas más destacados del sector —que primero trabajó en el Mercatus Center de la Universidad George Mason y ahora es director de Coin Center, un grupo de apoyo sin ánimo de lucro—, dice: «La gestión entra en juego cuando hay que tomar decisiones serias y se necesita un proceso para que se tomen».⁵⁴⁹ Recomienda empezar con el juramento hipocrático: lo primero, no causar daño. El planteamiento progresivo que tienen los desarrolladores de bitcoin «está mostrando ahora sus puntos débiles con el debate sobre el tamaño de los bloques. Va a ser muy difícil llegar a un acuerdo —dice Brito—. Queremos contribuir a desarrollar ese foro y crear una organización capaz de regularse a sí misma».⁵⁵⁰ Universidades importantes como la de Stanford, la de Princeton, la de Nueva York o la de Duke dan también cursos sobre las blockchains, bitcoin y las criptomonedas.⁵⁵¹

Gobiernos y legisladores

Los gobiernos de los distintos países del mundo actúan sin coordinación, y mientras que algunos aplican políticas de *laissez-faire*, otros intervienen activamente con normas y leyes como las del BitLicense de Nueva York. Algunos regímenes son abiertamente hostiles, pese a que cada vez son menos. Igualmente, la industria está dividiéndose en facciones, los que abogan por nuevas leyes y los que se oponen. Incluso quienes se resisten a admitir la intervención del Estado reconocen que los debates sobre su gestión los entusiasman. Adam Draper, un generoso inversor de riesgo que apuesta por el sector,

reconoce, aunque a regañadientes: «El respaldo del Estado favorece el respaldo de las instituciones, que es valioso».⁵⁵² Los bancos centrales de todo el mundo están dando pasos para entender esta tecnología. Benjamin Lawsky, exsupervisor de servicios financieros del estado de Nueva York, dice que una regulación fuerte es el primer paso que hay que dar para que esta industria crezca.⁵⁵³

Organizaciones no gubernamentales

El año 2015 ha sido fundamental para la transformación de la larga serie de ONG y organizaciones de la sociedad civil centradas específicamente en esta tecnología. Aunque la Digital Currency Initiative de Forde depende del MIT, la incluimos en esta serie. Otros grupos son el Coin Center de Brito y la Chamber of Digital Commerce de Boring. Estos grupos están teniendo protagonismo en la comunidad.

Usuarios

Usuarios como tú, lector, y como nosotros, gente que se preocupa por la identidad, la seguridad, la privacidad y demás derechos, por la viabilidad a largo plazo, por el reparto justo, y porque haya foros en los que podamos corregir errores y luchar contra los delincuentes que usan la tecnología para destruir lo que no queremos que se destruya. Todos parecemos divididos sobre cuestiones básicas como la clasificación y la categorización: cuando hablamos de blockchain, ¿nos referimos a la de bitcoin o a la tecnología en general? ¿Debemos hablar de blockchain o de una única blockchain? ¿Es una moneda, un servicio, una tecnología? ¿Es todas esas cosas o ninguna de ellas?

Liderazgo femenino

Como muchos han observado, el movimiento por las blockchains está lleno de hombres. En cuestión de tecnología e ingeniería, los hombres siguen siendo mucho más numerosos que las mujeres. Sin embargo, mujeres destacadas están fundando y administrando empresas del sector: Blythe Master, consejera delegada de Digital Asset Holdings; Cindy McAdam, presidenta de Xapo; Melanie Shapiro, consejera delegada de Case Wallet; Joyce Kim, directora ejecutiva de Stellar Development Foundation; Elizabeth Rossiello, consejera delegada y fundadora de BitPesa, y Pamela Morgan, consejera delegada de Third Key Solutions. Muchas de ellas han dicho que el sector acoge con gusto todas las voces, masculinas y femeninas. La inversión de riesgo en el sector también está diversificándose. Arianna Simpson, exdirectora de desarrollo de negocios en BitGo, es ahora una inversora. Jalak Jobanputra es una inversora que dedica su capital a las tecnologías descentralizadas.

Cuando se ha tratado de gestionar y promover este recurso global, las mujeres se han adelantado.

Primavera De Filippi, profesora adjunta del Berkman Center de Harvard e investigadora permanente del Centro Nacional de Investigación Científica de París, es una infatigable defensora de la tecnología blockchain y se ha revelado como una de las voces del mundo académico más claras y elocuentes sobre el tema de la gestión. Con Constance Choi, jurista metida a empresaria y otra destacada partidaria de la industria, De Filippi ha dirigido una serie de talleres sobre blockchain en Harvard, el MIT y Stanford, así como en Londres, Hong Kong y Sídney. Gracias a ellas, diversos miembros de la industria y de fuera de ella debaten sobre las grandes cuestiones. Nada es tabú y en los encuentros se dan cita gentes de diferente formación, convicciones y creencias.

Elizabeth Stark es otra voz destacada en el tema de la gestión. La catedrática de Derecho de Yale ha asumido el papel de coordinadora jefe del sector. Al igual que otra prominente mujer —Dawn Song, catedrática de Informática de Berkeley y becaria de la Fundación McArthur, y experta en seguridad cibernética—, Stark viene del mundo académico pero tiene otras ambiciones. Organizó Scaling Bitcoin, que reunió a desarrolladores, actores de la industria, expertos, funcionarios y otros interesados en Montreal. Fue un «momento constitucional» y Scaling Bitcoin sirvió para aclarar el debate sobre el tamaño de los bloques. Hoy Stark es también una empresaria destacada y colabora en el desarrollo de Bitcoin Lightning Network para resolver el problema de la «escalabilidad» de las blockchains.

Perianne Boring, experiodista y reportera de televisión, es la fundadora de Chamber for Digital Commerce, una asociación con sede en la ciudad de Washington. En un año ha conseguido reclutar en su directiva a figuras destacadas (como Blythe Masters, James Newsome o George Gilder). El movimiento necesitaba «saltar a la palestra de Washington e iniciar un diálogo con el gobierno», dice. Con su experiencia como periodista, Boring se centró en la comunicación y el posicionamiento y perfeccionamiento estratégico. Su organización está «abierta a todo aquel que se comprometa a hacer crecer la comunidad», dice, y es hoy una voz destacada en la política, la defensa y el conocimiento del floreciente ecosistema de gestión de las blockchains.⁵⁵⁴

Este creciente coro de líderes que abogan por la gestión es tan clarividente como necesario. Cuando hablamos de gestionar la tecnología blockchain no hablamos de regulación, al menos no exclusivamente. En concreto, hay serias limitaciones al uso de regulaciones para administrar un importante recurso global. Como dice Joichi Ito: «Podemos regular las redes, podemos regular las operaciones, pero no podemos regular el software».⁵⁵⁵ Es decir, la regulación será uno de los varios componentes importantes. Las blockchains no son como internet porque el dinero no es como la información. Blythe Masters, que conoció bien Wall Street y se ha convertido en una pionera de las blockchains, expresaba así su preocupación: «Los recién llegados pueden hacer cosas que las instituciones reguladoras no pueden hacer, pero tenemos que reflexionar detenidamente sobre el porqué de la existencia de esa regulación y sobre el propósito que tiene, antes de concluir que exponer a los consumidores a unas actividades financieras desreguladas es una buena cosa».⁵⁵⁶ En última instancia, el debate no es sobre qué clase de sociedad queremos, sino sobre las oportunidades que tienen los líderes para desarrollar un recurso global importante.

Un cuento con moraleja sobre la regulación de las blockchains

Benjamin Lawsky, exdirector de los servicios financieros del estado de Nueva York (NYDFS, por sus siglas en inglés), fue durante un tiempo el regulador bancario más poderoso de Estados Unidos. Para los políticos de Washington, Lawsky era conocido por las fotos que se hacía por las mañanas temprano cuando salía a correr por la ciudad. Pero para los gigantes de Wall Street era un luchador valiente y ambicioso (y muy celoso) que no dudaba en arremeter contra aquellos bancos que él creía que actuaban mal, dispuesto a darles su merecido.

Nombrado por el gobernador Andrew Cuomo, su amigo y viejo aliado político, Lawsky fue el primero en ocupar el cargo de vigilante supremo de los bancos en Estados Unidos. En 2012, cuando sólo llevaba un año en el cargo, fue noticia al llegar el NYDFS a un acuerdo de 340 millones de dólares con el banco británico Standard Chartered PLC, que había realizado transacciones por valor de más de 250 millones de dólares provenientes de Irán, prohibidas entonces por sanciones de Estados Unidos y de la Unión Europea. En el proceso, el NYDFS se adelantó al Departamento de Justicia, que quería imponer un castigo parecido.⁵⁵⁷

Para los que pensaban que la regulación bancaria era muy laxa, él era el nuevo *sheriff*, el temible justiciero y reformador de una industria que había enloquecido. Para los bancos, enseguida se convirtió en el enemigo público número uno. Lawsky no había hecho más que empezar.

Un día de mediados de 2013, estando Lawsky en su despacho, probablemente ocupado en algún otro sonado caso contra los grandes bancos, llamó a su puerta un economista de su equipo para debatir ciertas cuestiones inusuales. Según algunos abogados, varias empresas clientes estaban operando con una extraña moneda virtual llamada bitcoin. La primera reacción de Lawsky fue preguntar: «¿Qué diablos es bitcoin?». ⁵⁵⁸ El economista siguió explicando que dichas empresas tenían clientes que compraban, vendían, comerciaban y pagaban bienes y servicios con esa moneda digital y que los abogados, siempre cautelosos, querían saber si esas operaciones se consideraban transferencias de dinero, y si así era, qué debían hacer. En Nueva York, las transferencias de dinero están típicamente reguladas al mismo nivel, por lo que el NYDFS, siendo el organismo regulador de Nueva York, tenía el deber de controlar a todas las entidades implicadas en una transferencia de dinero. Pero ¿cómo hacerlo? Lawsky no sabía nada de esa tecnología y enseguida tuvo la sospecha de que iba a ser un reto completamente nuevo.

Casi inmediatamente, Lawsky se vio ante un problema de lo más común: que las tecnologías revolucionarias no encajan bien en los marcos regulatorios existentes, algo característico de la era digital. Bitcoin no encajaba en su mente. Bitcoin es de alcance global; los gobiernos federal y estatal verían limitada su capacidad de acción para controlarlo y regularlo. Además, es una tecnología igualitaria y descentralizada. Los organismos reguladores viven de controlar grandes intermediarios. Sus archivos centralizados contienen montones de datos, ideales para preparar un caso. Y en la era digital, los gobernantes nunca o pocas veces disponen de la información necesaria para tomar decisiones en interés público. Muchas veces carecen de recursos para gestionarla

con eficacia y pueden estar mal informados sobre innovación. Lawsky empezaba a asumir algo con lo que gobiernos y organismos reguladores llevaban luchando veinte años. Gracias a la suerte, la previsión y un marco regulador nuevo, internet pudo crecer y prosperar. Las criptomonedas eran otro ejemplo de cómo la tecnología digital escapaba al control de los responsables tradicionales, incluidos los gobiernos.

Con todo, Lawsky tenía que hacer su trabajo. Tras revisar los estatutos existentes, los encontró completamente inapropiados. Al principio, el departamento quiso regular esta tecnología aplicando normativas de los tiempos de la guerra civil. Aquellas leyes sobre transferencias dinerarias no podían aplicarse a ninguna clase de tecnología digital como internet, y menos aún a las monedas digitales o a la seguridad cibernética. «Cuanto más aprendía, más veía lo poderosa que es esta tecnología y las muchas aplicaciones y plataformas que podrían ir creándose con el tiempo», dice. Si «pudiéramos regularla de tal manera que evitáramos las malas cosas que podrían ocurrir en el ecosistema, pero que al mismo tiempo esa regulación no fuera demasiado autoritaria, entonces podríamos contribuir a que una tecnología muy potente mejorara seriamente nuestro sistema».⁵⁵⁹ Lawsky concluyó: «¿No necesitaríamos un marco regulador nuevo para tratar con algo cualitativamente diferente?».⁵⁶⁰ Su propuesta, el BitLicense, fue el primer intento serio de regular el sector. Ley controvertida, demostró hasta qué punto una regulación bienintencionada puede tener consecuencias inesperadas. Cuando BitLicense entró en vigor, hubo un éxodo masivo de empresas como Bitfinex, GoCoin o Kraken que salieron de Nueva York; la causa, según estas empresas, eran los prohibitivos costes de la licencia. Las pocas que se quedaron estaban bien capitalizadas y más consolidadas.

Los beneficios, como una supervisión mejor y más protección del consumidor, son considerables. Plataformas de cambio con licencia, como Gemini, han ganado terreno, quizá porque su clientela institucional sabe que ahora están tan reguladas como los bancos. Pero con menos competidores, ¿no ahogará BitLicense la innovación y el crecimiento? Brito alega que BitLicense se equivoca porque aplica viejas soluciones a problemas nuevos. Y pone el ejemplo de la ley de BitLicense según la cual se necesita una licencia para custodiar fondos de consumidores. «Con bitcoin y otras monedas digitales, tenemos tecnologías como la de la multifirma, que, por primera vez, introduce el concepto de control compartido. Si los tres tenemos una clave de una dirección multifirma que necesita las otras dos, ¿quién custodia los fondos?»⁵⁶¹ En este caso, el concepto de custodia, que antes estaba legalmente muy claro, ahora es ambiguo.

«Creo que los próximos cinco o diez años van a ser unos de los tiempos más dinámicos e interesantes de la historia de nuestro sistema financiero», dice Lawsky.⁵⁶² Dimitió de su cargo en el NYDFS para dedicarse a una serie de cuestiones importantes en el seno de este mundo dinámico. «Disfrutaría de mi carrera si tuviera que trabajar en medio de lo que creo que va a ser una época tremendamente transformadora, dinámica e interesante... Hablamos de una tecnología casi completamente desregulada que choca con el que probablemente es el sistema más regulado del mundo, el sistema financiero. Nadie sabe a ciencia cierta lo que resultará de ese choque —dice—. Lo sabremos en los próximos cinco o diez años y quiero estar en medio de ese choque.»⁵⁶³

El senador que cambiaría el mundo

El Senado canadiense sorprendió a mucha gente cuando, en junio de 2015, el Comité sobre la Banca, la Industria y el Comercio hizo público un informe detallado e inequívocamente positivo: «Monedas digitales. Las monedas que no se pueden lanzar al aire».⁵⁶⁴ El informe, que incluía opiniones de muchos miembros del ecosistema blockchain, explicaba por qué los gobiernos debían adoptar esta tecnología.⁵⁶⁵

«Podría ser el próximo internet», decía Doug Black, el senador canadiense por la ciudad de Calgary, provincia de Alberta, y uno de los principales autores del informe. «Podría ser el próximo televisor, el próximo teléfono. Queremos que se sepa en Canadá y fuera de Canadá: fomentamos la innovación y la capacidad de empresa.»⁵⁶⁶ Como Ben Lawskey, Black es un veterano abogado. Hizo carrera en el mundo del petróleo, representando a productores de gas y petróleo como socio de uno de los gabinetes legales más prestigiosos del país. El senador Black discrepa, sin embargo, de Lawskey por su resistencia a aplicar nuevas regulaciones. «¡El Estado no debería meterse!», nos dice.⁵⁶⁷ Como miembros del Senado canadiense, Black y sus colegas no desempeñan ninguna función legislativa, pero pueden influir en cuestiones importantes dando directrices o haciendo recomendaciones al gobierno. Aunque, con una media de edad de sesenta y seis años, no parecía que las probabilidades de que el Senado canadiense adoptara esta tecnología de vanguardia fueran las mayores, eso es exactamente lo que han hecho.

Reflexionando sobre el proceso, Black recuerda que pensaba: «¿Cómo podemos crear un ambiente que aliente la innovación en lugar de asfixiarla?... No es normal que un gobierno adopte este punto de vista desde el principio». Según Black, los gobiernos «tienden a querer mantener el control y minimizar el riesgo».⁵⁶⁸ Aunque reconoce el riesgo que toda nueva tecnología supone para los consumidores y las empresas, Black explica: «Hay riesgo en todo; hay riesgo en las monedas fiduciarias. Podemos controlar el riesgo hasta cierto punto, pero también debemos crear un ambiente en el que pueda promoverse la innovación».⁵⁶⁹

Con este informe, Black cree que han dado en el clavo.

El informe hace muchas recomendaciones, pero dos destacan sobre las demás. La primera, que el gobierno debería empezar a usar blockchains para relacionarse con los canadienses. Black dice: «Las blockchains son un vehículo más confidencial para proteger la información»; en consecuencia, «el gobierno debería ir pensando en usar esta tecnología, con lo que daría un poderoso mensaje».⁵⁷⁰ Esto es decir mucho: si queremos ser un foco de innovación y unos pioneros en el sector, prediquemos con el ejemplo y empecemos a innovar nosotros.

La segunda recomendación es incluso más sorprendente: el Estado debería ir con cuidado en materia reguladora. No pocos juristas respetados que se interesan por la tecnología blockchain han defendido lo mismo. Aaron Wright, de la Facultad de Derecho Cardozo de la Universidad de Yeshiva, aboga por leyes tipo *safe harbor* (literalmente «puerto seguro») que permitan a los innovadores seguir innovando y minimicen la

regulación legal hasta que la tecnología avance.⁵⁷¹ Josh Fairfield, de la Facultad de Derecho de la Universidad Washington & Lee, dice: «Necesitamos una regulación que sea como la tecnología: humilde, experimental e iterativa».⁵⁷²

Los bancos centrales en una economía descentralizada

Las finanzas pueden ser el segundo oficio más viejo del mundo, pero la banca central es un fenómeno relativamente moderno. La Reserva Federal de Estados Unidos (la Fed), el banco central más poderoso del mundo, celebró su centenario en 2013.⁵⁷³ Los bancos centrales, en su relativamente breve historia, han atravesado varias etapas, la última de las cuales ha sido la de pasar del patrón oro a un sistema de monedas fiduciarias de tasa variable. Como las monedas digitales amenazan el papel de los bancos centrales en la economía, es de esperar que se opongan a la tecnología blockchain. Sin embargo, estos bancos vienen mostrando desde hace años voluntad de innovación. La Fed fue pionera en la liquidación de capitales al apostar por el sistema de la Cámara de Compensación Automatizada (ACH, por sus siglas en inglés) cuando todos los cheques se extendían y cobraban manualmente. Como otros bancos centrales, la Fed no ha vacilado en experimentar con cosas nuevas. Ha adoptado políticas poco ortodoxas y arriesgadas, como el famoso (para bien o para mal, según se mire) programa de expansión cuantitativa que aplicó a raíz de la crisis financiera de 2008, cuando emitió moneda para comprar activos financieros como bonos del Estado por una cantidad sin precedentes.

No es de extrañar que los bancos centrales hayan sido de los primeros en entender la importancia de la tecnología blockchain para la economía de sus respectivos países. Por dos razones es importante. La primera, porque esta tecnología es una nueva herramienta para mejorar los servicios financieros, alterar el funcionamiento de muchas instituciones financieras y potenciar el papel de los bancos centrales en la economía global.

La segunda razón, y la más importante, es que las blockchains suscitan preguntas sobre la misma existencia de los bancos centrales. ¿Cómo podrán desempeñar eficazmente su función en un mercado global en el que haya una o muchas criptomonedas que ellos no controlen? Después de todo, la política monetaria es un utensilio clave de los bancos centrales para manejar la economía, sobre todo en tiempos de crisis. ¿Qué pasará cuando esa moneda no la emita un gobierno sino que exista globalmente como parte de una red distribuida?

Los bancos centrales de todo el mundo están explorando estas cuestiones. Carolyn Wilkins, gobernadora adjunta del Banco de Canadá y una veterana de la banca central, nos dice: «Hoy por hoy confiamos en nuestro paradigma, pero entendemos que muchos paradigmas tienen fecha de caducidad: funcionan bien durante unos años pero luego empiezan a fallar. Al principio se pueden ajustar, pero al final hay que cambiarlos por otra cosa». Ella cree que las blockchains pueden ser esta otra cosa. «Es difícil no dejarse fascinar por algo tan transformador. El uso que está dándose a esta tecnología afecta a todas las funciones que desempeña la banca central», dice.⁵⁷⁴

Ben Bernanke, expresidente de la Fed, dijo en 2013 que la tecnología blockchain podría «propiciar un sistema de pago más rápido, más seguro y más eficiente».⁵⁷⁵ Hoy, tanto la Fed como el Banco de Inglaterra (y probablemente otros bancos centrales que no han sido tan explícitos) tienen equipos dedicados a esta tecnología.

Para entender por qué los bancos centrales están tan interesados, veamos primero lo que hacen. En términos generales, estas augustas instituciones desempeñan tres funciones. Primera, dictan la política monetaria estableciendo las tasas de interés, controlando la oferta de dinero y en circunstancias excepcionales inyectando capital directamente en el sistema. Segunda, procuran garantizar la estabilidad financiera, lo que significa que actúan como banqueros del gobierno y de los bancos: son los prestamistas de último recurso. Por último, los bancos centrales suelen compartir con otros organismos del Estado la responsabilidad de regular y controlar el sistema financiero, particularmente la actividad de los bancos que manejan el ahorro y el crédito del consumidor medio.⁵⁷⁶ Invariably, todas estas funciones están interrelacionadas y son interdependientes.

Empecemos por la estabilidad financiera. «Como banco central, nuestra función es proveer de liquidez como último recurso. Eso lo hacemos en dólares canadienses. Por tanto, los dólares canadienses, como fuente de liquidez, son importantes para el sistema financiero canadiense», dice Wilkins. ¿Qué ocurre si las transacciones son en otra moneda como bitcoin? «Nuestra capacidad para hacer préstamos se vería limitada.»⁵⁷⁷ ¿La solución? Los bancos centrales podrían empezar a guardar reservas en bitcoins, como hacen con otras monedas, y activos como oro. Y también podrían pedirles a las instituciones financieras que guardaran reservas de esas monedas no estatales en el banco central. Estas reservas permitirían a los bancos centrales desempeñar su función monetaria tanto en monedas fiduciarias como en criptomonedas. Parece prudente, ¿no?

Hablando de la estabilidad financiera en relación con la política monetaria, Wilkins dice: «Las consecuencias [en la política monetaria] del dinero electrónico dependen de cómo se lo denomine». En una reciente conferencia, afirmaba que el «e-dinero», como ella lo llamaba, podía ser denominado por el gobierno en una moneda nacional o como criptomoneda.⁵⁷⁸ Una moneda digital denominada en dólares canadienses sería fácil de manejar, decía. Por ejemplo, ello ayudaría a que un banco central respondiera más rápidamente. Lo más probable es que veamos una combinación de las dos cosas: los bancos centrales guardarán y manejarán monedas alternativas basadas en blockchains, igual que tienen reservas extranjeras, y explorarán la posibilidad de convertir moneda fiduciaria en el llamado e-dinero a través de un registro basado en blockchains. Este nuevo mundo será muy diferente.

¿Y qué pasa con los bancos centrales considerados como organismos reguladores y de vigilancia? Tienen un poder regulador considerable en sus respectivos países, pero no operan aisladamente. Se coordinan y colaboran con otros bancos centrales y con instituciones mundiales como el Consejo de Estabilidad Financiera, el Banco de Pagos Internacionales, el FMI, el Banco Mundial y otras. Necesitamos más coordinación global para solucionar los problemas de las blockchains. Hoy, los bancos centrales plantean importantes cuestiones. Carolyn Wilkins dice: «Es fácil decir que la regulación debe ser

proporcionada al problema, pero ¿cuál es el problema? ¿Y qué tipo de innovación queremos?». ⁵⁷⁹ Son grandes cuestiones que podríamos resolver más eficazmente en un ambiente inclusivo.

Bretton Woods es un buen modelo. ¿Por qué no convocar otro encuentro por el estilo, pero no en habitaciones humosas tras puertas cerradas, sino en un foro abierto en el que participen las partes interesadas, incluidos el sector privado, la comunidad tecnológica y las instituciones de gobierno? Wilkins dice: «El Banco de Canadá trabaja con otros bancos centrales para entender lo que es esta tecnología y lo que significa. Hemos organizado congresos a los que han asistido gobernadores de bancos centrales, personas del mundo académico y representantes del sector privado». ⁵⁸⁰

De hecho, la historia de los bancos centrales revela algo más importante: los gobiernos carecen muchas veces del conocimiento práctico necesario para responder a un mundo en rápida transformación. Los bancos centrales tienen sin duda mucho que decir en este debate, pero deberían tener en cuenta a las demás partes y a otros bancos centrales de todo el mundo para poner en común ideas, colaborar en cuestiones de liderazgo y avanzar en la agenda.

Regulación frente a gestión

No cabe duda de que el valor y el dinero son cosas distintas de lo que es la información tradicional. Hablamos de ahorros, de una pensión, del pan diario de las personas, de su empresa, de sus acciones, de su economía, y esto afecta a todo el mundo. ¿No necesitamos regulación, y rápido? ¿Pueden y deben los gobiernos abstenerse de intervenir en vista de los enormes cambios que se avecinan?

Están produciéndose cambios importantes que revelan los límites del Estado en una época de innovación acelerada. Por ejemplo, la crisis financiera de 2008 mostró hasta qué punto la velocidad y la complejidad del sistema económico global hacen cada vez más ineficaces los organismos legislativos centralizados tradicionales. Pero una regulación más fuerte tampoco es el remedio. Los gobiernos no pueden pretender controlar y regular todos los rincones del mercado financiero, de la tecnología o de la economía, simplemente porque hay demasiados actores, innovaciones y productos. Lo que sí pueden hacer, como la experiencia demuestra, es obligar a las partes a que se comporten con transparencia y favorecer el cambio. Los gobiernos pueden exigir, por ejemplo, que las actuaciones de los bancos en internet sean transparentes y permitir que los ciudadanos y otras partes interesadas contribuyan con sus propios datos y observaciones. Los ciudadanos también pueden contribuir a que se respete la regulación cambiando, por ejemplo, su comportamiento a la hora de comprar o, debidamente informados, organizando campañas públicas que denuncien y condenen a los transgresores.

Evidentemente, los gobiernos deben ser una parte clave y principal de la gestión. También tienen que admitir que su papel en la gestión de las blockchains será fundamentalmente diferente del papel que históricamente han desempeñado en la política

monetaria y en la regulación financiera. Durante milenios, el Estado ha tenido el monopolio del dinero. ¿Qué pasa cuando el «dinero» no lo emite exclusivamente una autoridad central sino que es (al menos en parte) creado por una red distribuida mundial?

Aunque en general positiva, la respuesta de Estados Unidos ha parecido a veces contradictoria. «En Estados Unidos hay conciencia, tanto en el Congreso y el ejecutivo como en los distintos organismos, incluidos los legislativos, de que esta tecnología tiene usos serios y legítimos», dice Jerry Brito.⁵⁸¹ De hecho, internet ha demostrado que, por su espíritu y por su naturaleza institucional, Estados Unidos no sólo tolera sino que acoge de buen grado la innovación que traspasa fronteras. Pero también la acota a través de leyes, algunas de las cuales pueden ser desacertadas y casi siempre son prematuras.

Los riesgos de regular prematuramente —antes de entender bien las implicaciones— pueden tener profundas consecuencias. En la Inglaterra victoriana, las llamadas locomotoras automáticas (esto es, los automóviles) debían ir acompañadas por ley de un hombre que iba por delante agitando una bandera roja para advertir a los transeúntes y caballos de que se acercaba aquel extraño armatoste. Steve Beauregard, consejero delegado de GoCoin, una empresa líder en el sector, describe los peligros de regular demasiado pronto: «Cuando empezaron a aparecer las primeras páginas web, los organismos reguladores se preguntaron qué régimen regulador debía aplicárseles. Surgió la idea de que las personas que crearan y alojaran páginas web debían sacarse un permiso de banda de radio ciudadana porque uno está “transmitiendo”. ¿Te imaginas tener que sacarse un permiso de esos para poder crear una página web?». ⁵⁸² Por suerte la propuesta no prosperó.

Seamos claros: la regulación no es lo mismo que la gestión. Regular es dictar leyes que controlen la conducta. Gestionar es promover, colaborar e incentivar para actuar de común acuerdo. Pero la experiencia indica que los gobiernos deberían regular las tecnologías con cuidado, actuando más como colaboradores de otros sectores sociales que como el pesado brazo de la ley. Deben participar como actores en un ecosistema de gestión que vaya de abajo arriba más que como ejecutores de un régimen de control jerarquizado.

Brito, de Coin Center, afirma que los gobiernos deben tener un papel, pero han de actuar con cuidado. Aboga por una solución participativa que empieza por la educación, «informando a la gente en el Congreso, en los organismos, en los medios de comunicación, y respondiendo a sus preguntas o dirigiéndolos a las personas que sepan contestarlas de una manera comprensible». ⁵⁸³

Un nuevo marco para gestionar las blockchains

En lugar de limitarse a regular, los gobiernos pueden mejorar el comportamiento de las industrias haciéndolas más transparentes y potenciando el compromiso cívico, no como sustituto de una regulación mejor, sino como un complemento de los sistemas existentes. Nosotros creemos que una regulación efectiva y, por extensión, una gestión efectiva es fruto de un planteamiento común en el que la transparencia y la participación pública

valgan y pesen más a la hora de tomar decisiones. Por primera vez en la historia de la humanidad, están formándose unas redes no estatales y participativas para resolver problemas globales.

En las últimas décadas ha habido dos grandes avances que han sentado las bases de un nuevo modelo. Primero, el advenimiento de internet ha permitido que participantes de todos los tamaños, desde los más grandes hasta simples individuos, se comuniquen, compartan recursos y coordinen acciones. Ya no necesitamos funcionarios del Estado que nos convoquen para que unamos esfuerzos y acordemos objetivos. Segundo, empresarios, académicos, ONG y otros participantes no estatales han adquirido la capacidad de desempeñar un papel importante en el esfuerzo cooperativo global. No había empresarios, ONG ni participantes no estatales en la mesa de Bretton Woods. Hoy, todos ellos colaboran a diario con los gobiernos para resolver problemas de todo tipo, desde gestionar un recurso global como internet hasta solucionar cuestiones como el cambio climático o el tráfico de seres humanos.

La combinación de estos factores hace posible el nuevo modelo. Para hacer frente a un número creciente de desafíos globales, la colaboración autoorganizativa permite ahora cooperar, gestionar y resolver problemas a nivel global, así como progresar más rápidamente que las instituciones estatales.

Para crear una red de gestión basada en las blockchains, planteamos una serie de cuestiones críticas y desarrollamos un marco para responder a ellas:

- ¿Cómo diseñamos esa red de gestión?
- ¿Creamos esa nueva red desde cero o aprovechamos alguna institución ya consolidada y con experiencia en cuestiones financieras internacionales?
- ¿Cuál será el mandato de esta red? ¿Tendrá poder para aplicar políticas?
- ¿En interés de quién actuará una red de gestión basada en las blockchains y ante quién tendrá que responder?
- Y, cuestión fundamental, ¿cederán las naciones-Estado autoridad a una red global?

En general, el ecosistema que gobierna internet es muy aleccionador. Que se haya convertido en un recurso global en tan poco tiempo es asombroso, y ha sido así debido en no pequeña medida a un liderazgo y a una gestión fuertes, y a pesar de las poderosas fuerzas que se le oponían.

¿Quién, pues, gobierna la primera generación de internet y cómo la gobierna? Un vasto ecosistema de empresas, organizaciones sociales, desarrolladores informáticos, académicos y gobiernos, principalmente el de Estados Unidos, que actúa de una manera abierta, distribuida y colaborativa que nada tiene que ver con el modelo tradicional de las jerarquías y cadenas de mando. Ni gobiernos ni grupos de gobiernos controlan internet, aunque algunas agencias del gobierno de Estados Unidos lo financiaran alguna vez.⁵⁸⁴

En los albores de internet, los gobiernos mostraron a la vez moderación y clarividencia. Mostraron moderación al limitar la regulación y el control mientras internet evolucionaba, y clarividencia al permitir que el ecosistema prosperara antes de intentar imponer normas y regularlo. Esta red participativa ha funcionado en el caso de internet, pero hemos de reconocer que las normas desempeñarán un papel importante en la

tecnología blockchain. Mientras que internet ha democratizado la información, las blockchains democratizan el valor y revolucionan industrias tradicionales como la banca. Es evidente que tendrá que haber una regulación que proteja a consumidores y ciudadanos. Pero nuestra investigación indica que el modelo de gestión de internet es bueno.

Sigue habiendo dudas sobre si el nuevo liderazgo vendrá de la vieja comunidad de internet. Vint Cerf, que coinventó el mismo internet y lideró la creación de la Sociedad de Internet y del Grupo de Trabajo de Ingeniería de Internet (IETF, por sus siglas en inglés), que ha creado casi todos los estándares de la red, cree que un punto de partida para las blockchains sería crear un grupo de interés o BOF (*birds of a feather*, literalmente «pájaros del mismo plumaje») dentro del IETF.⁵⁸⁵ Al principio, muchas organizaciones involucradas en la gestión de internet consideraron que las monedas digitales y las tecnologías blockchain quedaban fuera de su esfera, pero esto está cambiando. El Consorcio de la Red Informática Global, el W3C, ha hecho de los pagos por internet una prioridad, y las blockchains son esenciales en este debate.⁵⁸⁶ Además, el Foro de Gestión de Internet (IGF, por sus siglas en inglés) ha organizado encuentros sobre las blockchains y bitcoin, en los que los participantes han explorado los nuevos marcos de gestión descentralizada que esta tecnología hace posible.⁵⁸⁷ Las fronteras entre lo viejo y lo nuevo son permeables, y muchos de los líderes de la red de gestión de internet, como Pindar Wong, el pionero de internet, exvicepresidente de la ICANN y consejero de la Sociedad de Internet, han sido también los líderes más destacados en materia de gestión de las blockchains.⁵⁸⁸

¿Cómo es la nueva red de gestión? Hay diez tipos de «redes para soluciones globales», y todas consisten en una combinación de empresas, gobiernos, ONG, académicos, desarrolladores e individuos. Ninguna de ellas está controlada por el Estado ni por instituciones estatales como las Naciones Unidas, el FMI, el Banco Mundial o el G8. Todas desempeñarán un papel importante en el liderazgo y la gestión de la tecnología blockchain.



1. Redes de conocimiento

La primera función de las redes de conocimiento es desarrollar nuevas formas de pensar, investigaciones, ideas y políticas que contribuyan a resolver los problemas globales. Cuanto mejor informados estén los usuarios, mejor podrán protegerse de robos y fraudes y proteger su privacidad, así como entender plenamente el valor de esta revolucionaria tecnología, participar más en la prosperidad global y contribuir a una mayor conectividad financiera.⁵⁸⁹ Las redes de conocimiento deben promover una cultura abierta e inclusiva, ser transparentes y constar de muchos participantes.

Implicaciones para las blockchains: Las redes de conocimiento son focos en los que se generan nuevas ideas para crear nuevas redes para soluciones globales y un mundo más amplio. Son clave para evitar fallos y superar obstáculos. El conocimiento preparará a los participantes para hacer mejor promoción, crear o cocrear políticas y difundir información crítica a los usuarios. Compartir el conocimiento permite que haya un diálogo fructífero con el gobierno. Según Jerry Brito, de Coin Center, sea cual sea la política que se adopte, si los gobiernos «no entienden la tecnología ni sus implicaciones, están abocados al fracaso».⁵⁹⁰ Muchos claman por la creación de espacios en los que se compartan y debatan ideas e información. «Debería haber un foro en el que hacer propuestas y presentar ideas», dice Tyler Winklevoss.⁵⁹¹ La Digital Currency Initiative del MIT es una red de conocimiento destacada, que trata de unir y animar a académicos y universidades de todo el mundo. Encuentros informales menos conocidos como el de desarrolladores de San Francisco o el de Nueva York también están dando prioridad al conocimiento. Blockchainworkshops.org es otro grupo que reúne a las partes para divulgar conocimiento y enseñanzas clave. Reddit, el foro y comunidad en línea, es también un buen foco de conocimiento del sector.

2. Redes de distribución

En realidad, lo que estas redes distribuyen es el cambio que buscan, complementando e incluso superando el trabajo de instituciones tradicionales. Por ejemplo, la ICANN desempeña un papel fundamental en la red de gestión de internet, distribuyendo soluciones en forma de nombres de dominio.

Implicaciones para las blockchains: ¿Cómo sabemos que los incentivos son adecuados para fomentar la colaboración masiva distribuida y que la tecnología está preparada para su uso masivo? Seguramente habrá un «momento ICANN» en las blockchains, en el que se formarán organizaciones para desempeñar funciones esenciales. Pero mientras que la ICANN y otras redes para soluciones globales de la red de gestión de internet son estadounidenses, los líderes de las blockchains deben intentar internacionalizar estas organizaciones. Joichi Ito dice: «Creo que tenemos que hacer un gran esfuerzo para conseguir que la gestión salga de Estados Unidos y se haga internacional desde el principio, porque una cosa que hemos aprendido de la ICANN es que, una vez que empezamos desde Estados Unidos, cuesta salir de ahí».⁵⁹² La Coalición para las Aplicaciones Legales Automatizadas (COALA, por sus siglas en inglés) es una organización global que desempeña una serie de funciones clave: divulga el

conocimiento, influye en las políticas, defiende la tecnología blockchain y promueve el desarrollo y la difusión de aplicaciones basadas en blockchain, todo lo cual es fundamental para superar los grandes obstáculos que podrían presentarse.⁵⁹³

3. Redes de política

A veces las redes crean políticas gubernamentales, incluso cuando consisten en actores no gubernamentales. Las redes de política fomentan el desarrollo de políticas o crean alternativas a ellas, las apoyen o no los gobiernos. El objetivo de estas redes no es arrebatarse a los gobiernos el control del proceso de elaboración de políticas, sino transformar el modelo de transmisión jerárquica tradicional de la responsabilidad en un modelo consultivo y colaborativo.

Implicaciones para las blockchains: Hoy está surgiendo una incipiente red política. Coin Center, un grupo político sin afán de lucro con sede en la ciudad de Washington, se centra en cinco pilares básicos: innovación, protección del consumidor, privacidad, licencias de comercialización y protocolos contra el blanqueo de dinero y de conocimiento del cliente (AML y KYC, por sus siglas en inglés, respectivamente). La Cámara de Comercio Digital, una organización comercial, promueve la aceptación y el uso de las monedas digitales.⁵⁹⁴ El Reino Unido tiene su propia Asociación de Moneda Digital, como la tienen Australia y Canadá, que defiende la industria. Con la contratación de John Collins, exconsejero del gobierno de Estados Unidos, Coinbase se convirtió en la primera empresa con un defensor político permanente.⁵⁹⁵ Promover y unir muchas voces potentes en la arena política garantizará que las blockchains tengan más posibilidades de realizar su potencial. Por ejemplo, sabemos que el minado consume mucha energía y que el cambio climático es un gran problema. Una política responsable será fundamental para construir un futuro sostenible, y los gobiernos no pueden hacerlo solos.

4. Redes de defensa

Las redes de defensa se proponen cambiar las agendas o las políticas de los gobiernos, las empresas y otras instituciones. Internet ha reducido los costes de colaborar, y ahora estamos viendo el surgimiento de redes de defensa cada vez más poderosas y que son más globales, más distribuidas y tecnológicamente más sofisticadas de lo que lo han sido nunca.

Implicaciones para las blockchain: Las redes de defensa surgen por la decepción que causan las instituciones políticas y civiles tradicionales, lo que las convierte en ideales para la comunidad blockchain, que está tratando de cambiar la manera como estas instituciones tradicionales resuelven los problemas. Sin embargo, en estos primeros días, las redes de defensa deben trabajar con el gobierno. Las redes de defensa están estrechamente unidas a las redes políticas, por lo que no es extraño que Coin Center y la Cámara de Comercio Digital sean líderes en esta área. También podríamos incluir aquí a COALA, la Digital Currency Initiative del MIT y otros. La protección y defensa es fundamental para expandir la tecnología blockchain. Sin fuertes defensores que protejan a los interesados y sus derechos, los gobiernos y otras instituciones poderosas podrían querer ahogar, tergiversar o usurpar esta poderosa red abierta en provecho propio, que es otro de los peligros que corre.

5. *Redes de vigilancia*

Estas redes examinan a las instituciones para comprobar que se comportan adecuadamente, en temas como los derechos humanos, la corrupción, el medio ambiente, los servicios financieros y demás. En el proceso, promueven el debate público, fomentan la transparencia y provocan movimientos en favor del cambio. La función de los vigilantes está íntimamente relacionada con la de las redes de defensa y de política. Las redes políticas colaboran con los gobiernos para establecer políticas que funcionen. Los vigilantes garantizan que la industria cumple con las políticas. Los gobiernos que traicionen la confianza pública también pueden ser controlados y responsabilizados.

Implicaciones para las blockchains: La Blockchain Alliance es una asociación de fuerzas de orden público, ONG, organizaciones comerciales y empresas privadas y la primera red de defensa que se ha creado en el sector. Coin Center y la Cámara de Comercio Digital, con el apoyo de BitFury, Bitfinex, BitGo, Bitnet, Bitstamp, Blockchain, Circle, Coinbase y otros, se han asociado con agencias de orden público como el Departamento de Justicia, el FBI, el Servicio Secreto y el Departamento de Seguridad Nacional de Estados Unidos. Ya hemos señalado en el capítulo anterior la amenaza que supone que los delincuentes se apropien de las blockchains a gran escala. Estos vigilantes tienen también una importante función defensiva que desempeñar. A raíz de los ataques terroristas de París, algunos legisladores y agentes de seguridad culparon a bitcoin de ser una fuente de financiación del terrorismo. La Blockchain Alliance pidió paciencia: «No legislemos por miedo», dijeron.⁵⁹⁶ En el momento de escribir esto, no sabemos hasta qué punto les han hecho caso, pero de lo que no cabe duda es que sin ellos, y con los gobiernos decidiendo sobre el asunto unilateralmente, las cosas habrían sido peores. Aparte de las normas que los miembros de la comunidad se dan a sí mismos al reunirse, colaborar y debatir en foros y en Reddit, pocas otras redes de vigilancia han surgido. La asociación con las fuerzas y cuerpos de seguridad del Estado es un buen comienzo, pero el ecosistema blockchain necesita organizaciones completamente independientes, como serían, por ejemplo, Amnistía Internacional y Human Rights Watch, para que vigilen a gobiernos, empresas y otras grandes instituciones. Si no es así, nos exponemos a ser víctimas de otro peligro: que las blockchains se conviertan en una nueva y poderosa herramienta que gobiernos corruptos y sin escrúpulos usen para vigilarnos.

6. *Plataformas*

La era digital ha permitido que las organizaciones sean algo más que instituciones cerradas; también pueden ser plataformas que creen valor, innoven y contribuyan a resolver problemas globales. Organizaciones como Change.org hacen posible que las personas lancen campañas de apoyo a causas sociales relacionadas con los derechos humanos, el cambio climático y muchas más. Una «plataforma de petición» que aprovecha la fuerza colectiva de millones de personas y la cataliza para que tenga un impacto duradero. Las plataformas de datos abiertos pueden usarse para muchos propósitos, desde el cambio climático hasta las blockchains.⁵⁹⁷

Implicaciones para las blockchains: Conforme la tecnología blockchain adquiera importancia global, las partes implicadas deberán ser capaces de agregar y examinar información. La blockchain bitcoin puede ser radicalmente abierta y transparente, pero también puede haber blockchains cerradas que se usen en cualquier ámbito, desde el de los servicios financieros hasta el del internet de las cosas, que no lo sean. Imaginemos una plataforma que permita que los ciudadanos normales y corrientes agreguen y examinen información. Sería un gran medio de salvar los obstáculos que pudieran surgir a su expansión, impedir que los gobiernos se apropiaran de ella y combatir el uso insostenible de energía. Con plataformas así, todos nos convertiríamos en vigilantes y podríamos pedir más responsabilidades a las instituciones y empresas y abrir debates constructivos.

7. Redes de patrones

Las redes de patrones son organizaciones no estatales que desarrollan especificaciones y patrones técnicos para casi cualquier cosa, incluido internet. Determinan los patrones que forman los bloques fundamentales para el desarrollo de productos y hacen posible la innovación que permita dar el salto a la adopción masiva. Para que las redes de patrones globales funcionen, deben contar con la participación de personas, instituciones, organizaciones civiles y, sobre todo, empresas privadas. El Grupo de Trabajo de Ingeniería de Internet, uno de los organismos de creación de patrones más importantes de la red de gestión de internet, destaca por incorporar los muchos puntos de vista de las distintas partes.

Implicaciones para las blockchains: Al principio, la Fundación Bitcoin financió el desarrollo del protocolo bitcoin, los patrones comúnmente usados por la comunidad. Sin embargo, la casi quiebra de la fundación (debida a la mala gestión y al despilfarro) demostró que era necesario buscar soluciones administrativas reticulares. Reconociendo la profunda importancia de esta tecnología y la necesidad de protegerla y promocionarla, el MIT creó la Digital Currency Initiative, que desde entonces ha financiado a los desarrolladores de bitcoin para que puedan seguir trabajando. «Enseguida dimos un paso al frente y les proporcionamos un puesto en el Media Lab, para que pudieran continuar trabajando independientemente y contribuyendo al desarrollo de bitcoin», dice Brian Forde.⁵⁹⁸ Para los desarrolladores, poder trabajar de una manera autónoma era fundamental.

Gavin Andresen es uno de los desarrolladores que trabajan en el MIT. Cree que se necesita liderazgo para que el proyecto avance con patrones comunes, como en la muy debatida cuestión del tamaño de los bloques. «Quizá se puedan diseñar otras cosas sin orden ni concierto, pero no patrones informáticos», dice. Y hablando de los primeros tiempos de la red, añade: «El modelo de internet demuestra que puede haber tecnologías en las que se produzca consenso, incluso cuando no hay un claro líder», pero que «siempre hay una persona o un proceso que acaba en una persona. Tiene que haber o una cosa o la otra».⁵⁹⁹ Los mecanismos de consenso solos no bastan para desarrollar patrones.

Scalingbitcoin.org es una organización que reúne a ingenieros y académicos para solucionar importantes cuestiones técnicas, incluidas las referidas a los patrones. Pindar Wong, que preside el Comité de Planificación de Scalingbitcoin.org (entre muchas otras funciones directivas), ha sido líder en la tarea de unir a participantes clave y salvar

obstáculos técnicos. En materia de servicios financieros, tanto R3 como el Hyperledger Project se ocupan de cuestiones de patrón fundamentales. Naturalmente, tendrá que haber redes de patrones en una serie de cosas, desde el protocolo blockchain que constituya la base de la industria de los servicios financieros del futuro, hasta patrones básicos de privacidad y pago en el internet de las cosas.

Aunque todos estos grupos abordan el problema desde diferentes ángulos y con diferentes agendas, todos comparten un objetivo común: preparar esta tecnología para que la use todo el mundo, lo que se consigue construyendo infraestructura, desarrollando patrones y favoreciendo su expansión.

8. Instituciones reticulares

Algunas redes ofrecen tal variedad de prestaciones que las llamamos «instituciones reticulares». No son instituciones estatales sino verdaderas redes participativas. El valor que crean va desde el conocimiento hasta las soluciones, pasando por la defensa y las normativas.

Implicaciones para las blockchains: El Foro Económico Mundial (WEF, por sus siglas en inglés), una institución reticular señera, ha sido partidario activo de la tecnología blockchain. Esta tecnología fue uno de los ejes de la reunión de enero de 2016 en Davos. Jesse McWaters, director de innovación financiera del WEF, cree que la tecnología blockchain es una tecnología de uso general, como internet, que podemos emplear para mejorar radicalmente la eficiencia de los mercados y el acceso a los servicios financieros. El WEF predijo que dentro de una década podríamos almacenar el 10 por ciento del PIB global en blockchains.⁶⁰⁰ Como organización, el WEF ha puesto sobre la mesa grandes cuestiones como la desigualdad económica, el cambio climático e incluso los giros de dinero. Otras instituciones reticulares, desde grupos pequeños hasta las mayores fundaciones del mundo, como la Fundación Clinton o la Fundación Bill and Melinda Gates, harían bien en abogar por esta tecnología para abordar temas tan importantes como la inclusión financiera y los servicios sanitarios. Las instituciones reticulares pueden desempeñar muchas veces un gran papel a la hora de influir en las políticas gubernamentales, lo que hace de ellas un eslabón fundamental y un socio estratégico para superar obstáculos serios.

9. Diásporas

Las diásporas son comunidades globales formadas por personas que han salido de sus países y que se sienten unidas por la cultura y la identificación con sus lugares de origen. Gracias a internet, estas personas y las organizaciones afiliadas pueden colaborar en redes participativas. Una de las funciones de muchas de las diásporas de hoy es contribuir a resolver problemas globales comunes.

Implicaciones para las blockchains: Las diásporas son fundamentales para el futuro de las blockchains. Para empezar, éstas hacen que el proceso de enviar dinero sea más simple y más barato. Lejos de destruir empleos, las blockchains ganan tiempo y ahorran recursos para que esas personas busquen otros empleos o emprendan nuevos proyectos. Aunque se han creado pocas empresas en lugares como Filipinas o Kenia, las diásporas deben hacer más para acelerar el conocimiento, la adopción y la aceptación de

los métodos de pago basados en blockchains. Hoy, la mayoría de las empresas que han aprovechado la oportunidad, como Abra o Paycase, tienen su sede en Estados Unidos, el Reino Unido, Canadá o China.

10. Redes de gestión

La red de gestión de blockchains será una combinación de todas las características y atributos de los otros nueve tipos de redes para soluciones globales. En definitiva, una red de gestión de blockchains ha de ser inclusiva y estar abierta a la participación de todos los colectivos implicados importantes. La red debería ser meritocrática, esto es, que la comunidad debería apoyar las propuestas que sean viables, independientemente del rango y condición del que las haga. También debería ser transparente y poner a disposición toda la información, documentación y actas de reuniones para el escrutinio público. Por último, las decisiones deberían tomarse, en la medida de lo posible, por consenso, a fin de que el resultado fuera lo más legítimo posible.

Una agenda nueva para la próxima era digital

Una red de gestión de blockchains es fundamental para administrar este recurso global. Pero ¿cómo podemos garantizar que esta nueva generación de internet cumple con lo que promete?

La siguiente época de la era digital ofrece posibilidades ilimitadas, peligros notables, obstáculos desconocidos, desafíos formidables y un futuro que dista de estar claro. La tecnología, especialmente la distribuida, crea oportunidades para todo el mundo, pero son los seres humanos los que determinan el resultado. Como dice Constance Choi, «esta tecnología entraña una promesa y un peligro. Todo depende de cómo la utilicemos».⁶⁰¹ Como hemos visto en este capítulo, todo el mundo tiene que poner de su parte para que se cumpla la nueva promesa de la era digital.

En otros momentos de transición, las sociedades decidieron actuar para desarrollar nuevas mentalidades, leyes e instituciones. Estas transformaciones culturales llevaron tiempo, normalmente siglos, y muchas estuvieron salpicadas de conflictos y hasta de revoluciones.

Hoy la situación es diferente. Los cambios se producen infinitamente más rápido. Y, lo que es más importante, el *ritmo de cambio*, como indica la Ley de Moore, se acelera exponencialmente. Nos acercamos a la proverbial «segunda mitad del tablero de ajedrez», donde el crecimiento exponencial llega a lo inconcebible.⁶⁰² La consecuencia es que nuestras infraestructuras reguladoras y normativas son muy inapropiadas y se adaptan muy lentamente o no se adaptan a los requisitos de la era digital. Los cambios actuales se producen tan rápido que superan la capacidad de las personas y de las instituciones para entenderlas y aún más para controlar su impacto. Nuestras instituciones e instrumentos democráticos fueron diseñados para la era industrial, y, de hecho, tuvieron su origen precisamente en la transformación de las sociedades feudales en Estados capitalistas industriales.

¿Cómo podemos acelerar la transformación humana para seguir el ritmo de la innovación y la revolución tecnológicas? ¿Cómo podemos evitar un trastorno social masivo o algo peor? Para que no se nos acuse de ser deterministas tecnológicos o utopistas, decimos que es hora de suscribir un nuevo contrato social para la era digital. Gobiernos, sector privado, sociedad civil e individuos debemos colaborar para forjar una nueva conciencia.

Ahora que entramos en esta segunda generación de internet, es hora de lanzar un manifiesto de la era digital. Llamémoslo «Declaración de interdependencia». Los ciudadanos de la era digital tenemos *derechos*: acceso a las infraestructuras digitales, alfabetización, alfabetización digital, aprendizaje vitalicio y renovada libertad de expresión en línea sin miedo a la vigilancia.

La economía y la sociedad digitales deberían ser gobernadas por *principios*. Por supuesto, los que trabajan deberían participar de la riqueza que crean. Si los ordenadores pueden hacer el trabajo, entonces la semana laboral, no nuestro nivel de vida, debería reducirse. De hecho, los principios generales implícitos de Satoshi para la revolución de las blockchains deberían servirnos bien: necesitamos instituciones que actúen con integridad, seguridad, privacidad, inclusión, protección de derechos y reparto de poder. Trabajemos para distribuir las oportunidades y la prosperidad en su origen, no simplemente para redistribuir la riqueza después de que haya sido creada por las estructuras de clase tradicionales.

La tecnología blockchain puede reducir el coste y el tamaño del Estado, pero seguiremos necesitando *leyes* en muchas áreas. Hay soluciones tecnológicas y de modelo de negocio para los desafíos que plantean la propiedad intelectual y la propiedad de derechos. Por eso deberíamos reescribir o descartar leyes viejas que asfixian la innovación con una protección excesiva de las patentes. Mejores acciones antimonopolistas deben detener la tendencia a los monopolios, de manera que nadie pague excesivamente por, digamos, servicios básicos de internet o financieros. El 80 por ciento de los estadounidenses no puede elegir a sus proveedores de servicios de internet, lo que quizá explique por qué el ancho de banda es uno de los más caros y lentos del mundo desarrollado. Los que amañan y manipulan cualquier cosa, desde el cambio de divisas hasta la emisión de contaminantes, deben ser perseguidos y castigados debidamente.

Necesitaremos una *transformación institucional* en todos los ámbitos. Los bancos centrales tendrán que cambiar su funcionamiento en materia de administración de divisas y de política monetaria y colaborar multilateralmente con más participantes en la economía y la sociedad. Necesitamos escuelas y universidades con un dominio colaborativo de la información en blockchains que esté enfocado al estudiante y personalizado, y que permita a estudiantes y profesores participar en pequeños grupos que debatan y elaboren proyectos. Necesitamos un registro universal de pacientes en blockchains que garanticen una salud colaborativa cuando queramos administrar nuestro bienestar fuera del sistema. Cuando usemos el sistema de salud, no deberíamos sufrir por ignorar la interacción de fármacos o por medicamentos no probados. Los políticos tendrán que adaptarse a un mundo transparente en el que los contratos inteligentes los

obligarán a rendir cuentas ante sus electores. ¿Cómo gestionaremos el cambio que se producirá cuando las monedas digitales acaben con un mercado de giros postales que mueve 500.000 millones de dólares?

La tecnología blockchain puede crear nuevas *infraestructuras físicas* que requieran nuevas asociaciones y acuerdos entre los interesados. ¿Qué pasará con los millones de conductores de Uber cuando SUber los deje sin trabajo? ¿Qué pueden hacer las ciudades para que en 2025 los ciudadanos confíen en los sistemas de transporte inteligente? ¿Cómo podemos avanzar hacia una red eléctrica basada en blockchain y en la que los hogares participen de la generación de energía y no sólo sean consumidores? ¿Dónde encontraremos el liderazgo para implantar un sistema personal de intercambio de créditos de carbono?

El protocolo fiable y nosotros

¿Se cumplirá la ley de los paradigmas, según la cual a los que más les cuesta adoptar lo nuevo es a los líderes de lo viejo? Pensemos en los líderes que respaldaron el libro de Don de 1994 *La economía digital*: los consejeros delegados de Nortel Networks, MCI, Nynex, Ameritech y General Electric Information Services, todas empresas desaparecidas. Menos mal que no incluyó a los consejeros delegados de Kodak, Borders, Blockbuster o Circuit City. (Otra moraleja para aviso de los amables promotores de este libro.)

¿Por qué no creó Rupert Murdoch *The Huffington Post*? ¿Por qué no lanzó AT&T Skype, ni Visa creó PayPal? La CNN podría haber creado Twitter, visto que de frases cortas e impactantes como titulares se trata, ¿no? General Motors o Hertz podrían haber lanzado Uber, y Marriott, Airbnb. Gannett podría haber creado Craigslist o Kijiji. Yellow Pages podría haber fundado perfectamente eBay. Microsoft tenía la posibilidad de crear Google o cualquier modelo de negocio basado en internet más que en el ordenador personal. ¿Por qué no inventó la NBC YouTube? Sony podría haberse adelantado al iTunes de Apple. ¿Dónde estaba Kodak cuando se inventaron Instagram o Pinterest? ¿Y si *People* o *Newsweek* hubieran creado *BuzzFeed* o *Mashable*?

Como escribimos al principio de este libro: «Parece que el genio de la tecnología ha salido otra vez de la botella... se ha puesto ahora a nuestro servicio para dar un nuevo salto hacia delante: transformar el sistema del poder económico y el viejo orden de los asuntos humanos. Si es que queremos». Como la primera generación de internet, la revolución blockchain promete subvertir los modelos de negocios y transformar las industrias. Pero eso no es más que el principio. La tecnología blockchain nos arrastra a una nueva era, basada en la apertura, el mérito, la descentralización y la participación global.

Nos esperamos que haya un periodo de volatilidad, especulación y mal uso de la tecnología. También nos esperamos que haya un avance firme y continuado, un abrirse paso con dificultad junto a las vacas sagradas de la industria. Nadie sabe qué impacto tendrá esta tecnología en los servicios financieros. ¿Tiene razón Ben Lawskey cuando dice que la industria puede ser irreconocible dentro de cinco o diez años? Tim Draper dice:

«Bitcoin es al dólar lo que internet al papel».⁶⁰³ ¿Podría ocurrir que los más ardientes defensores de las blockchains *subestimen* en realidad el potencial que esta tecnología tiene a largo plazo? ¿Serán las blockchains el mayor salto hacia delante en materia de eficiencia industrial y de valor desde la invención de la contabilidad por partida doble y de las empresas de sociedad anónima? Hernando de Soto dice que las blockchains pueden incorporar a 5.000 millones de personas a la economía global, cambiar la relación entre el Estado y los ciudadanos (a mejor) y convertirse en una poderosa plataforma que impulse la prosperidad global y garantice los derechos individuales. Para él, «la idea de la paz por la ley, la idea de una familia humana, es que consigamos consenso sobre valores comunes. Deberíamos pensar en cómo la Declaración Universal de los Derechos Humanos podría ser más real con las blockchains».⁶⁰⁴ ¿Cómo podemos lograr este futuro mejor?

La mayoría de las personas que lideran esta revolución son desconocidas, a excepción de veteranos como el padre de Netscape, Marc Andreessen. Es probable que el lector nunca haya oído hablar de la mayor parte de las personas que se mencionan en este libro. Pero decimos lo mismo: ¿quién conocía al inmigrante iraní Pierre Omidyar o al programador de Wall Street Jeff Bezos en 1994? Todo depende de cómo los líderes de la industria se suban al carro. ¿Son las blockchains una alternativa a Facebook o Twitter realmente viable o responderán los gigantes del sector satisfaciendo las demandas de los usuarios sobre propiedad de información y privacidad? No importa. En ambos casos ganan los consumidores. ¿Se debilitará Visa o cambiará su modelo de negocio para adoptar el poder de las blockchains? ¿Cómo responderá Apple a una industria musical que se centre en el artista? ¿Qué pensarán los dictadorzuelos de un internet descentralizado que no puedan suprimir o controlar? ¿Pueden las blockchains hacer accesible la tecnología a los 2.000 millones de personas que hay en el mundo sin servicios bancarios?

El índice de fracaso de las empresas emergentes es alto, y por eso esperamos que muchas de las que hemos estudiado aquí fracasen, no porque la tecnología blockchain sea mala, sino porque —para cada uno de los ejemplos que hemos puesto— hay mucha competencia. No todas las empresas emergentes pueden sobrevivir. Creemos que las que sigan los principios de Satoshi tendrán más posibilidades de hacerlo que las que no.

Corren tiempos emocionantes y peligrosos. Como hombres de negocios, usemos *La revolución blockchain* como si fuera un manual, sí, pero sabiendo que las reglas del juego cambian. Pensemos en nuestro negocio, en nuestra industria, en nuestro trabajo: ¿cómo nos afectará a nosotros y qué podemos hacer? No caigamos en la trampa que nos han tendido muchos cambios de paradigma a lo largo de la historia. Los líderes de hoy no pueden permitirse ser los perdedores de mañana. Nos jugamos demasiado y necesitamos tu ayuda, lector. Únete a nosotros, por favor.

Agradecimientos

Este libro es fruto del concurso de dos mentes y de dos trayectorias vitales. Don había dirigido un programa de investigación financiado con 4 millones de dólares que se llamaba Redes para Soluciones Globales (GSN, por sus siglas en inglés) y que se desarrolló en la Facultad de Administración y Dirección de Empresas Rotman de la Universidad de Toronto. La idea era investigar modelos de red nuevos que facilitaran soluciones y una gestión globales. Don estudió el ecosistema que gobierna internet, compuesto de muchos participantes, y se interesó por las monedas digitales y su gestión. Alex, por su parte, era un ejecutivo del banco de inversiones Canaccord Genuity y cuando, en el año 2013, vio el creciente entusiasmo que despertaba el fenómeno de bitcoin y de las blockchains, que entonces estaba en sus inicios, decidió orientar los esfuerzos de su empresa hacia ese sector. Un día, en un viaje que padre e hijo hicimos a la estación de esquí de Mont-Tremblant, en 2014, mientras cenábamos, resolvimos colaborar en el tema y Alex accedió a dirigir una investigación sobre gestión de monedas digitales que culminó en un libro blanco titulado *A Bitcoin Governance Network*. Cuanto más profundizábamos en el asunto, más nos parecía que aquello iba a ser la siguiente gran revolución.

A todo esto, nuestro agente, Wes Neff, del Leigh Bureau, y el editor de Don, Adrian Zackheim, de Portfolio/Penguin (*Wikinomics*, *Macrowikinomics*), estaban pidiéndole a Don que fuera pensando en la idea de otro libro. Al ver que todo el mundo reconocía que el de Alex era un libro pionero en este campo, Don le propuso que escribieran uno juntos. Adrian, dicho sea en su honor, nos hizo una oferta que no pudimos rechazar y el libro no salió a subasta, como ocurre normalmente.

Tomamos entonces la que, vista retrospectivamente, fue una excelente decisión. Nos pusimos en contacto con el mejor editor que conocíamos, Kirsten Sandberg, que había trabajado en la Harvard Business School Press, y le pedimos que editara nuestro libro. Hizo un gran trabajo y la colaboración fue tan buena que le pedimos que formara parte plenamente del equipo de investigación del libro. Kirsten participó en más de cien entrevistas y nos ayudó a entender las mil cuestiones que se planteaban y a desarrollar fórmulas que nos permitieran explicar estos grandes adelantos a un público no especializado. Contribuyó a dar vida al proyecto y por eso es también coautora de este libro, que sin ella no habría visto la luz, al menos en su comprensible forma presente. Por todo ello, por su estímulo y su buen humor, le estamos muy agradecidos.

También damos nuestras más sentidas gracias a toda la gente que enumeramos a continuación, que compartió generosamente su tiempo y sus conocimientos con nosotros y sin la cual este libro no existiría. Por orden alfabético:

Jeremy Allaire, fundador, presidente y consejero delegado de Circle

Marc Andreessen, cofundador de Andreessen Horowitz
 Gavin Andresen, científico jefe de la Fundación Bitcoin
 Dino Angaritis, consejero delegado de Smartwallet
 Andreas Antonopoulos, autor de *Mastering Bitcoin*
 Federico Ast, fundador de CrowdJury
 Susan Athey, catedrática de Economía de la Tecnología, Escuela de Posgrado de Negocios, Universidad de Stanford
 Adam Back, cofundador y presidente de Blockstream
 Bill Barhydt, consejero delegado de Abra
 Christopher Bavitz, director gerente de Cyberlaw Clinic, Facultad de Derecho de la Universidad de Harvard
 Geoff Beattie, presidente de Relay Ventures
 Steve Beauregard, fundador y consejero delegado de GoCoin
 Mariano Belinky, socio gerente de Santander InnoVentures
 Yochai Benkler, catedrático Berkman de Estudios Empresariales, Facultad de Derecho de la Universidad de Harvard
 Jake Benson, fundador y consejero delegado de LibraTax
 Tim Berners-Lee, inventor de World Wide Web
 Doug Black, senador del gobierno de Canadá
 Perianne Boring, fundadora y presidenta de la Cámara de Comercio Digital
 David Bray, *fellow* 2015 de la Fundación Eisenhower y ejecutivo residente de la Universidad de Harvard
 Jerry Brito, director ejecutivo de Coin Center
 Paul Brody, director de estrategia para América del grupo de tecnología de EY (el antiguo «internet de las cosas» de IBM)
 Richard G. Brown, director de tecnología de R3 CEV (exdirector ejecutivo de innovación industrial y desarrollo de negocios de IBM)
 Vitalik Buterin, fundador de Ethereum
 Patrick Byrne, consejero delegado de Overstock
 Bruce Cahan, profesor visitante de la Facultad de Ingeniería de la Universidad de Stanford y cofundador de la Iniciativa de Banca Sostenible de Stanford
 James Carlyle, ingeniero jefe y director gerente de R3 CEV
 Nicolas Cary, cofundador de Blockchain Ltd.
 Toni Lane Casserly, consejero delegado de CoinTelegraph
 Christian Catalini, profesor agregado de la Facultad de Administración y Dirección de Empresas del Instituto Tecnológico de Massachusetts (MIT)
 Ann Cavoukian, directora ejecutiva del Instituto Privacy and Big Data de la Universidad de Ryerson
 Vint Cerf, cocreador de internet y director de promoción de internet de Google
 Ben Chan, ingeniero superior de programación de BitGo
 Robin Chase, cofundador y exconsejero delegado de Zipcar
 Fadi Chehadi, consejero delegado de la ICANN
 Constance Choi, directora de Seven Advisory

John H. Clippinger, consejero delegado de ID3 y científico investigador del Media Lab del MIT

Bram Cohen, creador de BitTorrent

Amy Cortese, periodista y fundadora de Locavest

J.-F. Courville, jefe de operaciones de RBC Wealth Management

Patrick Deegan, director de tecnología de Personal BlackBox

Primavera De Filippi, investigadora permanente del CNRS y profesora adjunta del Berkman Center de Harvard

Hernando de Soto, presidente del Instituto para la Libertad y la Democracia

Peronet Despeignes, miembro del grupo de operaciones especiales de Augur

Jacob Dienelt, programador de blockchain y director financiero de itBit y Factom

Joel Dietz, fundador de Swarm Corp

Helen Disney, exmiembro de la Fundación Bitcoin

Adam Draper, fundador y consejero delegado de Boost VC

Timothy Cook Draper, inversor y fundador de Draper Fisher Jurvetson

Andrew Dudley, fundador y consejero delegado de Earth Observation

Joshua Fairfield, catedrático de Derecho de la Universidad Washington & Lee

Grant Fondo, socio de Securities Litigation and White Collar Defense Group, Privacy and Data Security Practice, Goodwin Procter LLP

Brian Forde, exconsejero de la Casa Blanca y director de Digital Currency del Media Lab del MIT

Mike Gault, consejero delegado de Guardtime

George Gilder, fundador y socio de Gilder Technology Fund

Geoff Gordon, consejero delegado de Vogogo

Vinay Gupta, coordinador de publicación de Ethereum

James Hazard, fundador de Common Accord

Imogen Heap, cantante y compositora ganadora de un premio Grammy

Mike Hearn, exingeniero de Google y fundador de Vinumeris/ Lighthouse

Austin Hill, cofundador de Blockstream

Toomas Hendrik Ilves, presidente de Estonia

Joichi Ito, director del Media Lab del MIT

Eric Jennings, cofundador y consejero delegado de Filament

Izabella Kaminska, periodista financiera del *Financial Times*

Paul Kemp-Robertson, cofundador y director editorial de Contagious Communications

Andrew Keys, cofundador de Consensus Systems

Joyce Kim, directora ejecutiva de la Fundación Stellar Development

Peter Kirby, cofundador y consejero delegado de Factom

Joey Krug, desarrollador de Augur

Haluk Kulin, consejero delegado de Personal BlackBox

Chris Larsen, consejero delegado de Ripple Labs

Benjamin Lawsky, exsuperintendente de servicios financieros del estado de Nueva York y consejero delegado de The Lawsky Group

Charlie Lee, creador, director de tecnología y exingeniero administrativo de Litecoin

Matthew Leibowitz, socio de Plaza Ventures
 Vinny Lingham, consejero delegado de Gyft
 Juan Llanos, vicepresidente ejecutivo de Strategic Partnerships y director de transparencia de Bitreserve.org
 Joseph Lubin, consejero delegado de Consensus Systems
 Adam Ludwin, fundador de Chain.com
 Christian Lundkvist, fundador de Balanc3
 David McKay, presidente y director ejecutivo de RBC
 Janna McManus, directora de relaciones públicas de BitFury
 Mickey McManus, presidente de Maya Institute
 Jesse McWaters, especialista en innovación financiera del World Economic Forum
 Blythe Masters, consejera delegada de Digital Asset Holdings
 Alistair Mitchell, socio gerente de Generation Ventures
 Carlos Moreira, fundador, director y consejero delegado de WISeKey
 Tom Mornini, fundador y defensor del consumidor de Subledger
 Ethan Nadelmann, director ejecutivo de Drug Policy Alliance
 Adam Nanjee, director de Fintech Cluster de MaRS
 Daniel Neis, consejero delegado y cofundador de KOINA
 Kelly Olson, directora de New Business Initiative de Intel
 Steve Omohundro, presidente de Self-Aware Systems
 Jim Orlando, director gerente de OMERS Ventures
 Lawrence Orsini, cofundador y presidente de LO3 Energy
 Paul Pacifico, consejero delegado de Featured Artists Coalition
 Jose Pagliery, periodista de investigación de CNNMoney
 Stephen Pair, cofundador y consejero delegado de BitPay Inc.
 Vikram Pandit, exconsejero delegado de Citigroup, inversor de Coinbase y cofundador de Portman Square Capital
 Jack Peterson, desarrollador de Augur
 Eric Piscini, asesor de banca y tecnología de Deloitte Consulting
 Kausik Rajgopal, director de la oficina de McKinsey & Co. en Silicon Valley
 Suresh Ramamurthi, presidente y director de tecnología de CBW Bank
 Sunny Ray, consejero delegado de Unocoin.com
 Caterina Rindi, gerente de comunidad de Swarm Corp
 Eduardo Robles Elvira, director de tecnología de Agora Voting
 Keonne Rodriguez, director de productos de Blockchain Ltd.
 Matthew Roszak, fundador y consejero delegado de Tally Capital
 Colin Rule, presidente y consejero delegado de Modria.com
 Marco Santori, abogado de Pillsbury Winthrop Shaw Pittman LLP
 Frank Schuil, consejero delegado de Safello
 Barry Silbert, fundador y consejero delegado de Digital Currency Group
 Thomas Spaas, director de Belgium Bitcoin Association
 Balaji Srinivasan, consejero delegado de 21 y socio de Andreessen Horowitz
 Lynn St. Amour, expresidente de The Internet Society

Brett Stapper, fundador y consejero delegado de Falcon Global Capital LLC
Elizabeth Stark, profesora visitante de la Facultad de Derecho de la Universidad de Yale
Jutta Steiner, fundadora de Ethereum/Provenance
Melanie Swan, fundadora del Institute for Blockchain Studies
Nick Szabo, catedrático de Derecho de la Universidad George Washington
Ashley Taylor, directora de cultura de Consensus Systems (ConsenSys)
Simon Taylor, vicepresidente de sociedades empresariales de Barclays
David Thomson, fundador de Artlery
Michelle Tinsley, directora de Mobility and Payment Security de Intel
Peter Todd, contradictor jefe de CoinKite
Jason Tyra, fundador de CoinDesk
Valery Vavilov, consejera delegada de BitFury
Ann Louise Vehovec, vicepresidenta de Strategic Projects de RBC Financial Group
Roger Ver, el «Jesús del Bitcoin», fundador de Memorydealers KK
Akseli Virtanen, gerente de fondos de inversión de Robin Hood Asset Management
Erik Voorhees, fundador y consejero delegado de ShapeShift
Joe Weinberg, cofundador y consejero delegado de Paycase
Derek White, director digital y de diseño de Barclays Bank
Ted Whitehead, director gerente de Manulife Asset Management
Zooko Wilcox-O'Hearn, consejero delegado de Least Authority Enterprises
Carolyn Wilkins, gobernadora adjunta del Banco de Canadá
Robert Wilkins, consejero delegado de myVBO
Cameron Winklevoss, fundador de Winklevoss Capital
Tyler Winklevoss, fundador de Winklevoss Capital
Pindar Wong, pionero de internet y presidente de VeriFi
Gabriel Woo, vicepresidente de Innovación de RBC Financial Group
Gavin Wood, director de tecnología de la Fundación Ethereum
Aaron Wright, catedrático de la Facultad de Derecho Cardozo de la Universidad de Yeshiva
Jonathan Zittrain, catedrático de Derecho de la Universidad de Harvard

También damos las gracias especialmente a unas cuantas personas que se esforzaron de verdad por ayudarnos. Anthony Williams y Joan Bigham, del proyecto Global Solutions Networks, trabajaron estrechamente con Alex en el texto original sobre gestión de monedas digitales. Joan McCalla, ejecutivo de Cisco, investigó a fondo para los capítulos sobre el «internet de las cosas» y sobre gobierno y democracia. Nuestra familia nos prestó una grandísima ayuda. Bob Tapscott, ejecutivo de IT, se pasó días enteros realizando descargas y estudiando la blockchain de bitcoin para proporcionarnos conocimientos de primera mano sobre algunas cuestiones técnicas. Bill Tapscott, empresario tecnológico, nos sugirió la revolucionaria idea de crear un sistema de compraventa personal de bonos de carbono basado en la tecnología blockchain, y Niki Tapscott, ejecutiva tecnológica, y su marido, James Leo, analista financiero, han dado gran publicidad al proyecto. Katherine MacLellan, del Grupo Tapscott (abogada, lo que nos vino muy bien), se ocupó de solucionar las cuestiones más complicadas de los

contratos digitales (*smart contracts*) y de organizar las entrevistas. Phil Courneyeur estuvo todos los días al tanto de material jugoso y David Ticoll nos instruyó sobre el estado actual de la era digital. Wes Neff y Bill Leigh, del Leigh Bureau, nos ayudaron a definir la idea del libro (¿cuántos libros queréis escribir, tíos?). Como siempre (y desde hace ahora más de veinte años), Jody Stevens se encargó, con una diligencia intachable, de organizar y coordinar todo el proyecto —bases de datos, cuestiones financieras, gestión documental—, además de ocuparse del proceso de revisión y producción del texto... un trabajo a tiempo completo que se sumó a los demás trabajos a tiempo completo que desempeña en el Grupo Tapscott.

Damos especialmente las gracias a Dino Mark Angaritis, el consejero delegado de la compañía de blockchain Smartwallet; a Joseph Lubin, consejero delegado del taller de desarrollo Consensus Systems de Ethereum, y a Carlos Moreira, de la próspera compañía de seguridad WISeKey, porque pasaron mucho tiempo con nosotros debatiendo ideas. Los tres son geniales y muy amables por echarnos una mano. Ahora podemos disfrutar del éxito que tienen sus proyectos en este campo. Damos también las gracias al gran equipo de Penguin Random House encabezado por nuestro editor Jesse Maeshiro y supervisado por Adrian Zackheim.

Sobre todo, queremos agradecer de todo corazón a nuestras esposas, Ana Lopes (Don) y Amy Welsman (Alex), que toleraran que nos pasáramos casi un año entero obsesionados con roer el durísimo hueso que ha sido este libro. Los dos somos muy afortunados de tener unas compañeras tan maravillosas.

Escribir este libro ha sido una experiencia gozosa para ambos y podemos asegurar que hemos disfrutado de cada minuto que empleamos en hacerlo. Como dijo un famoso: «Si dos están de acuerdo en todo, uno sobra». Nosotros nos confrontamos a diario para poner a prueba nuestras creencias y presupuestos, y este libro es la prueba de esta colaboración sana y vigorosa. Claro es que colaborar parece fácil cuando dos personas comparten tanto ADN y se han pasado treinta años explorando el mundo juntas. Esperamos que el fruto de esta colaboración sea importante y provechoso.

DON TAPSCOTT y ALEX TAPSCOTT,

enero de 2016

Notas

1. <<https://www.technologyreview.com/s/419452/moores-outlaws/>>.
2. <<https://cryptome.org/jya/digicrash.htm>>.
3. «How DigiCash Blew Everything», traducido del neerlandés al inglés por Ian Grigg y colegas y enviado por correo electrónico a la lista de direcciones de Robert Hettinga, 10 de febrero de 1999. Cryptome.org. John Young Architects. Web, 19 de julio de 2015, <<https://cryptome.org/jya/digicrash.htm>>. «How DigiCash Alles Verknalde», <<http://www.nextmagazine.nl/ecash.htm>>. *Next! Magazine*, enero de 1999. Web, 19 de julio de 2015, <<https://web.archive.org/web/19990427/http://nextmagazine.nl/ecash.htm>>.
4. <<http://nakamotoinstitute.org/the-god-protocols/>>.
5. Brian Fung, «Marc Andreessen: In 20 Years, We'll Talk About Bitcoin Like We Talk About the Internet Today», *The Washington Post*, 21 de mayo de 2014, <www.washingtonpost.com/blogs/the-switch/wp/2014/05/21/marc-andreessen-in-20-years-well-talk-about-bitcoin-like-we-talk-about-the-internet-today/>, consultado el 21 de enero de 2015.
6. Entrevista a Ben Lawskey, 2 de julio de 2015.
7. <www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>.
8. <www.coindesk.com/bitcoin-venture-capital/>.
9. Fung, «Marc Andreessen».
10. <www.coindesk.com/bank-of-england-economist-digital-currency/>.
11. Véase el informe de Leigh Buchanan para la Fundación Kauffman «American Entrepreneurship Is Actually Vanishing», <www.businessinsider.com/927-people-own-half-of-the-bitcoins-2013-12>.
12. Esta definición se desarrolla en Don Tapscott y David Ticoll, *The Naked Corporation: How the Age of Transparency Will Revolutionize Business*, Free Press, Nueva York, 2003.
13. <www.edelman.com/news/trust-institutions-drops-level-great-recession/>.
14. <www.gallup.com/poll/1597/confidence-institutions.aspx>.
15. Entrevista a Carlos Moreira, 3 de septiembre de 2015.
16. Don Tapscott es miembro del consejo asesor de WISEKey.
17. Don Tapscott ha sido uno de los muchos autores que han escrito sobre el lado oscuro de la era digital, por ejemplo en *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*, McGraw Hill, Nueva York, 1995. [Hay traducción castellana: *La economía digital. Las nuevas oportunidades y peligros en un mundo empresarial u personal interconectado en red*, McGraw Hill/Interamericana de Colombia, 1997.]
18. Entrevista a Carlos Moreira, 3 de septiembre de 2015.
19. Tom Peters, «The Wow Project», *Fast Company*, Mansueto Ventures LLC, 30 de abril de 1999, <<http://www.fastcompany.com/36831/wow-project>>.
20. Entrevista a Carlos Moreira, 3 de septiembre de 2015.
21. El «yo virtual» es una expresión popularizada por Ann Cavoukian y Don Tapscott en *Who Knows: Safeguarding Your Privacy in a Networked World*, McGraw-Hill, Nueva York, 1997.
22. Scott McNealy, entonces consejero delegado de Sun Microsystems, fue el primero en decirlo en 1999.
23. Entrevista a Andreas Antonopoulos, 20 de junio de 2015.
24. Entrevista a Joseph Lubin, 30 de julio de 2015.
25. Ni siquiera los sistemas de encuesta sofisticados podrán leer nuestra información personal porque se les dará encriptada, aunque sí podrán contestar preguntas relacionadas con ella interrogando esa misma información encriptada mediante técnicas de encriptación homomórfica.
26. Pensadores destacados tienen una idea de la prosperidad que va más allá del crecimiento del PIB. Michael Porter, de la Universidad de Harvard, ha creado un imperativo de progreso social, <<http://www.socialprogressimperative.org>>. El economista Joseph Stiglitz y otros han investigado medidas que trascienden el PIB, <http://www.insee.fr/fr/publications-et-services/dossiers_web/stiglitz/doc>.

- [commission/RAPPORT_anglais.pdf](#)>. Hay otros intentos de mejorar el PIB pero sin separarse de la economía familiar, <<http://www.forbes.com/sites/realspin/2013/11/29/beyond-gdp-get-ready-for-a-new-way-to-measure-the-economy/>>.
27. Entrevista a Vitalik Buterin, 30 de septiembre de 2015.
 28. Luigi Marco Bassani, «Life, Liberty and...: Jefferson on Property Rights», *Journal of Libertarian Studies* 18(1), invierno de 2004, p. 58.
 29. Entrevista a Hernando de Soto, 27 de noviembre de 2015.
 30. *Ibid.*
 31. <www.theguardian.com/music/2013/feb/24/napster-music-free-file-sharing>, consultado el 12 de agosto de 2015.
 32. <www.inc.com/magazine/201505/leigh-buchanan/the-vanishingstartups-in-decline.html>.
 33. *Naked City* («Ciudad Desnuda») fue una serie de televisión policiaca que se emitió de 1958 a 1963 en la cadena estadounidense ABC.
 34. Un informe de octubre de 2015 del Foro Económico Mundial asegura que no será mayoritariamente usado hasta 2027.
 35. Entrevista a David Ticoll, 12 de diciembre de 2015.
 36. Entrevista a Ann Cavoukian, 2 de septiembre de 2015.
 37. Guy Zyskind, Oz Nathan y Alex «Sandy» Pentland, «Enigma: Decentralized Computation Platform with Guaranteed Privacy», libro blanco, Instituto Tecnológico de Massachusetts, 2015. 10 de junio de 2015. Web, 3 de octubre de 2015, <arxiv.org/pdf/1506.03471.pdf>.
 38. Entrevista a Ann Cavoukian, 2 de septiembre de 2015.
 39. *Ibid.*
 40. Entrevista a Austin Hill, 22 de julio de 2015.
 41. Entrevista a Ann Cavoukian, 2 de septiembre de 2015.
 42. Vitalik Buterin, «Proof of Stake: How I Learned to Love Weak Subjectivity», *Ethereum blog*, Fundación Ethereum, 25 de noviembre de 2014. Web, 3 de octubre de 2015, <blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity>.
 43. Dino Mark Angaritis, archivo adjunto de correo electrónico, 27 de noviembre de 2015. Hace este cálculo «suponiendo que el ritmo de hash es de 583.000.000 Gh/s (Gh/s = mil millones de hashes por segundo). En diez minutos hay seiscientos segundos. $600 \times 583.000.000 = 349.800.000.000$ miles de millones de hashes en diez minutos. O sea, 350 quintillones, o 350.000.000.000.000.000, o 350 millones de millones de miles de millones».
 44. La «prueba de destrucción» (*proof of burn*) requiere que los mineros envíen monedas a direcciones sin salida en las que no se pueden convertir. A cambio de «destruir» estas monedas, los mineros participan en una lotería en la que, en principio, ganan más de lo que han destruido. No es un mecanismo de consenso sino un mecanismo de confianza.
 45. Entrevista a Paul Brody, 7 de julio de 2015.
 46. Franklin Delano Roosevelt, «Executive Order 6102-Requiring Gold Coin, Gold Bullion and Gold Certificates to Be Delivered to the Government», *The American Presidency Project*, Gerhard Peters y John T. Woolley eds., 5 de abril de 1933, <www.presidency.ucsb.edu/ws/?pid=14611>, consultado el 2 de diciembre de 2015.
 47. Entrevista a Josh Fairfield, 1 de junio de 2015.
 48. El Tamagotchi es un juguete digital creado por Bandai que requiere que los usuarios cuiden de él y lo protejan. Si no lo hacen, muere.
 49. Joseph E. Stiglitz, «Lessons from the Global Financial Crisis of 2008», *Seoul Journal of Economics* 23(3), 2010.
 50. Ernst & Young LLP, «The Big Data Backlash», diciembre de 2013, <www.ey.com/UK/en/Services/Specialty-Services/Big-Data-Backlash>; <<http://tinyurl.com/ptfm4ax>>.
 51. Este tipo de ataque se llamó «Sybil» por el seudónimo de una mujer a la que diagnosticaron un trastorno de identidad disociativo descrito en un libro de 1973 del mismo título. El amante de los gatos e informático John «JD» Douceur popularizó el nombre en un artículo de 2002.
 52. Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», www.bitcoin.org, 1 de noviembre de 2008, <www.bitcoin.org/bitcoin.pdf>, sección 6, «Incentive».
 53. Nick Szabo, «Bit gold», sin especificar, Nick Szabo, 27 de diciembre de 2008. Web, 3 de octubre de 2015, <<http://unenumerated.blogspot.com/2005/12/bit-gold.html>>.
 54. Entrevista a Austin Hill, 22 de julio de 2015.

55. Neal Stephenson, *Snow Crash*, 1992. [Hay traducción castellana: *Snow Cash*, Ediciones Gigamesh, Barcelona, 2008.] Alusión al mundo virtual de la novela *Snow Crash*, cuyo protagonista y héroe es Hiro Protagonist. Hiro es uno de los principales hackers del Metaverso. Los kongbucks son como los bitcoins: los franchulates (empresas estatales, mezcla de *franchise* y *consulate*) acuñan su propia moneda.
56. Ernest Cline, *Ready Player One*, Crown, Nueva York, 2011. [Hay traducción castellana: *Ready Player One*, Ediciones B, Barcelona, 2016.]
57. Entrevista a Austin Hill, 22 de julio de 2015.
58. John Lennon, *Imagine*, en «Imagine». Productores John Lennon, Yoko Ono y Phil Spector. 11 de octubre de 1971. <www.lyrics007.com/John%20Lennon%20Lyrics/Imagine%20Lyrics.html>.
59. Andy Greenberg, «Banking's Data Security Crisis», en *Forbes*, noviembre de 2008. Web, 3 de octubre de 2015, <www.forbes.com/2008/11/21/data-breaches-cybertheft-identity08-tech-cx_ag_1121breaches.html>.
60. Ponemon Institute LLC, «2015 Cost of Data Breach Study: Global Analysis», patrocinado por IBM, mayo de 2015, <www-03.ibm.com/security/data-breach>.
61. Ponemon Institute LLC, «2014 Fifth Annual Study on Medical Identity Theft», patrocinado por Medical Identity Fraud Alliance, 23 de febrero de 2015, <Medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft>.
62. Entrevista a Andreas Antonopoulos, 20 de julio de 2015.
63. Michael Melone, «Basics and History of PKI», *Mike Melone's blog*, Microsoft Corporation, 10 de marzo de 2012. Web, 3 de octubre de 2015, <<http://tinyurl.com/ngxuupl>>.
64. «Why Aren't More People Using Encrypted Email?», *Virtru blog*, Virtru Corporation, 24 de enero de 2015. Web, 8 de agosto de 2015, <www.virtu.com/blog/aren-t-people-using-email-encryption>.
65. Entrevista a Andreas Antonopoulos, 20 de julio de 2015.
66. Entrevista a Austin Hill, 22 de julio de 2015.
67. *Ibíd.*
68. Entrevista a Ann Cavoukian, 2 de septiembre de 2015.
69. *Ibíd.*
70. David McCandless, «Worlds Biggest Data Breaches», *Information Is Beautiful*, David McCandless, 2 de octubre de 2015. Web, 3 de octubre de 2015, <www.informationisbeautiful.net/visualizations/worlds-biggest-databreaches-hacks/>.
71. Entrevista a Haluk Kulin, 9 de junio de 2015.
72. Entrevista a Austin Hill, 22 de julio de 2015.
73. Política de privacidad de Coinbase, <www.coinbase.com/legal/privacy>, 17 de noviembre de 2014, consultado el 15 de julio de 2015.
74. Véase Don Tapscott y David Ticoll, *The Naked Corporation: How the Age of Transparency Will Revolutionize Business*, Free Press, Nueva York, 2003.
75. Entrevista a Haluk Kulin, 9 de junio de 2015.
76. ProofofExistence.com, 2 de septiembre de 2015, <www.prooffofexistence.com/about/>.
77. Entrevista a Steve Omohundro, 28 de mayo de 2015.
78. Entrevista a Andreas Antonopoulos, 20 de julio de 2015.
79. *Ibíd.*
80. Entrevista a Stephen Pair, 11 de junio de 2015.
81. Edella Schlarger y Elinor Ostrom, «Property-Rights Regimes and Natural Resources: A Conceptual Analysis», *Land Economics* 68(3), agosto de 1992, pp. 249-262; <www.jstor.org/stable/3146375>.
82. Entrevista a Haluk Kulin, 9 de junio de 2015.
83. John Paul Titlow, «Fire Your Boss: Holacracy's Founder on the Flatter Future of Work», *Fast Company*, Mansueto Ventures LLC, 9 de julio de 2015, <www.fastcompany.com/3048338/the-future-of-work/fire-your-boss-holacracys-founder-on-the-flatter-future-of-work>.
84. Banco Mundial, 2 de septiembre de 2015, <www.worldbank.org/en/news/press-release/2015/04/15/massive-drop-in-number-of-unbanked-says-new-report>.
85. «Bitcoin Powers New Worldwide Cellphone Top-Up Service», *CoinDesk*, 15 de febrero de 2015, <www.coindesk.com/bitcoin-powers-new-worldwide-cellphone-top-service/>, consultado el 26 de agosto de 2015. FAQs, BitMoby.com, mHITs Ltd., n/a, <www.bitmoby.com/faq.html>, consultado el 14 de noviembre de 2015.
86. Entrevista a Gavin Andresen, 8 de junio de 2015.
87. Entrevista a Austin Hill, 22 de julio de 2015.
88. Jakob Nielsen, «Nielsen's Law of Internet Bandwidth», Nielsen Norman Group, 5 de abril de 1998, <www.nngroup.com/articles/law-of-bandwidth/>, consultado el 26 de agosto de 2015.

130. <www.youtube.com/watch?v=A6kJfvuNqtg>.
131. Entrevista a Jeremy Allaire, 30 de junio de 2015.
132. *Ibíd.*
133. *Ibíd.*
134. *Ibíd.*
135. Lo que se anunció como otra señal de que la industria estaba «creciendo», <www.wsj.com/articles/goldman-a-lead-investor-in-funding-round-for-bitcoin-startup-circle-1430363042>.
136. Entrevista a Jeremy Allaire, 30 de junio de 2015.
137. Entrevista a Stephen Pair, 11 de junio de 2015.
138. Alex Tapscott ha sido consejero de Vogogo Inc.
139. Entrevista a Suresh Ramamurthi, 28 de septiembre de 2015.
140. Correo electrónico de Blythe Masters, 14 de diciembre de 2015.
141. Entrevista a Tom Mornini, 20 de julio de 2015.
142. Estas ideas ya las examinaban Don Tapscott y David Ticoll en su libro *The Naked Corporation: How the Age of Transparency Will Revolutionize Business*, Free Press, Nueva York, 2003.
143. *Ibíd.*
144. <www.accountingweb.com/aa/auditing/human-errors-the-top-corporate-tax-and-accounting-mistakes>.
145. *Ibíd.*
146. Entrevista a Simon Taylor, 13 de julio de 2015.
147. *Ibíd.*
148. Entrevista a Jeremy Allaire, 30 de junio de 2015.
149. Entrevista a Christian Lundkvist, 6 de julio de 2015.
150. Entrevista a Austin Hill, 22 de julio de 2015.
151. Entrevista a Eric Piscini, 13 de julio de 2015.
152. <www2.deloitte.com/us/en/pages/about-deloitte/articles/facts-and-figures.html>.
153. Entrevista a Eric Piscini, 13 de julio de 2015.
154. *Ibíd.*
155. Entrevista a Tom Mornini, 20 de julio de 2015.
156. *Ibíd.*
157. <www.calpers.ca.gov/docs/forms-publications/global-principles-corporate-governance.pdf>.
158. Entrevista a Izabella Kaminska, 5 de agosto de 2015.
159. <<http://listedmag.com/2013/06/robert-monks-its-broke-lets-fix-it/>>.
160. El movimiento por el derecho al olvido va ganando fuerza, sobre todo en Europa, <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf>.
161. <www.bloomberg.com/news/articles/2014-10-07/andreessen-on-finance-we-can-reinvent-the-entire-thing>.
162. <<http://www.nytimes.com/2015/12/24/business/dealbook/banks-reject-new-york-city-ids-leaving-unbanked-on-sidelines.html>>.
163. Entrevista a Patrick Deegan, 6 de junio de 2015.
164. *Ibíd.*
165. <<https://btcjam.com/>>.
166. Entrevista a Erik Voorhees, 16 de junio de 2015.
167. <www.sec.gov/about/laws/sa33.pdf>.
168. <<http://www.wired.com/2015/12/sec-approves-plan-to-issue-company-stock-via-the-bitcoin-blockchain/>>.
169. <<http://investors.overstock.com/mobile.view?c=131091&v=203&d=1&id=2073583>>.
170. <<https://bitcoinmagazine.com/21007/nasdaq-selects-bitcoin-startup-chain-run-pilot-private-market-arm/>>.
171. James Surowiecki, *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations*, Doubleday, Nueva York, 2014. [Hay traducción castellana: *Cien mejor que uno: la sabiduría de la multitud o por qué la mayoría es más inteligente que la minoría*, Urano, Barcelona, 2005.]
172. <www.augur.net>.
173. Correos electrónicos del personal de Augur: Jack Peterson, desarrollador; Joey Krug, desarrollador; Peronet Despeignes, operaciones especiales.
174. Entrevista a Andreas Antonopoulos, 8 de diciembre de 2014.
175. Entrevista a Barry Silbert, 22 de septiembre de 2015.
176. Entrevista a Benjamin Lawsky, 2 de julio de 2015.
177. Entrevista a Joseph Lubin, 13 de julio de 2015.

178. Empresas como Apple y Spotify podrán usar también la nueva plataforma. La idea es que sea propiedad de muchas entidades de la industria musical, sobre todo de artistas. Será más fácil ganar fichas si creamos contenido que si vendemos contenido ajeno.
179. <<https://slack.com/is>>.
180. <<https://github.com>>.
181. Coase escribía: «Una empresa funcionará en el sistema económico si... las transacciones pueden realizarse dentro de la empresa a menor coste que si esas mismas transacciones se realizaran fuera, en el mercado. El límite del tamaño de una empresa se alcanza cuando los costes de realizar transacciones dentro de esa empresa superan los costes de realizarlas en el mercado». Citado en Oliver Williamson y Sydney G. Winter, eds., *The Nature of the Firm*, Oxford University Press, Nueva York y Oxford, 1993, p. 90.
182. Oliver Williamson, «The Theory of the Firm as Governance Structure: From Choice to Contract», *The Journal of Economic Perspectives* 16(3), verano de 2002, pp. 171-195.
183. Ibid.
184. Peter Thiel y Blake Masters, *Zero to One: Notes on Startups, or How to Build the Future*, Crown Business, Nueva York, 2014. [Hay traducción castellana: *De cero a uno: cómo inventar el futuro*, Gestión 2000, Barcelona, 2015.]
185. Lord Wilberforce, *The Law of Restrictive Trade Practices and Monopolies*, Sweet & Maxwell, Londres, 1966, p. 22.
186. Entrevista a Yochai Benkler, 26 de agosto de 2015.
187. John Hagel y John Seely Brown, «Embrace the Edge or Perish», *Bloomberg*, 28 de noviembre de 2007; <<http://www.bloomberg.com/bw/stories/2007-11-28/embrace-the-edge-or-perishbusinessweek-business-news-stock-market-and-financial-advice>>.
188. Entrevista a Vitalik Buterin, 30 de septiembre de 2015.
189. Entrevista a Andreas Antonopoulos, 20 de julio de 2015.
190. La única excepción es Way Back Machine, que nos permite ver una historia más completa.
191. Oliver E. Williamson, «The Theory of the Firm as Governance Structure: From Choice to Contract», *Journal of Economic Perspectives* 16 (3), verano de 2002.
192. Ibid.
193. Michael C. Jensen y William H. Meckling, «Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure», *Journal of Financial Economics* 305 (1976), pp. 310-311 (donde afirma que una empresa es un conjunto de relaciones consensuadas entre accionistas, acreedores, directivos y demás); véase también, más en general, Frank H. Easterbrook y Daniel R. Fischel, *The Economic Structure of Corporate Law*, Harvard University Press, Cambridge, 1991.
194. Vitalik Buterin, «Bootstrapping a Decentralized Autonomous Corporation: Part I», *Bitcoin Magazine*, 19 de septiembre de 2013; <<https://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i/>>.
195. Nick Szabo, «Formalizing and Securing Relationships on Public Networks», <<http://szabo.best.vwh.net/formalize.html>>.
196. <<http://szabo.best.vwh.net/smart.contracts.html>>.
197. Entrevista a Aaron Wright, 10 de agosto de 2015.
198. Los criptógrafos empezaron a usar los nombres de «Alice» y de «Bob» en lugar de «Parte A» y «Parte B» porque parecía más conveniente para hablar de intercambios entre ellos y hacía más claro y familiar el debate sobre encriptación informática. Parece ser que la costumbre se remonta al artículo de Ron Rivest de 1978 «Security's Inseparable Couple», *Communications of the ACM. Network World*, 7 de febrero de 2005; <<http://www.networkworld.com/news/2005/020705widernetaliceandbob.html>>.
199. GitHub.com, 3 de enero de 2012; <<https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki>>, accesible el 30 de septiembre de 2015.
200. <www.coindesk.com/hedgy-hopes-tackle-bitcoin-volatility-using-multi-signature-technolog/>.
201. <<https://books.google.ca/books?id=VXIDgGjLHVgC&pg=PA19&lpg=PA19&dq=a+workman+moves+from+department+Y+to+department+X&sc=urq>>.
202. Elliot Jaques, «In Praise of Hierarchy», *Harvard Business Review*, enero-febrero de 1990.
203. Entrevista a Yochai Benkler, 26 de agosto de 2015.
204. Tapscott y Ticoll, *The Naked Corporation: How the Age of Transparency Will Revolutionize Business*, Free Press, Nueva York, 2003.
205. Werner Erhard y Michael C. Jensen, «Putting Integrity into Finance: A Purely Positive Approach», 27 de noviembre de 2015, Harvard Business School NOM Unit Working Paper No. 12-074; Barbados Group Working Paper No. 12-01; European Corporate Governance Institute (ECGI)-Finance Working Paper No. 417/2014.

206. La rentabilidad media del capital del Bank of America desde el 31 de diciembre de 2009 es menor del 2 por ciento; <https://ycharts.com/companies/BAC/return_on_equity>.
207. Entrevista a Steve Omohundro, 28 de mayo de 2015.
208. Entrevista por correo electrónico a David Ticoll, 9 de diciembre de 2015.
209. Entrevista a Melanie Swan, 14 de septiembre de 2015.
210. <<<https://hbr.org/1990/05/the-core-competence-of-the-corporation>>.
211. Michael Porter, «What Is Strategy?», *Harvard Business Review*, noviembre-diciembre de 1996.
212. Entrevista a Susan Athey, 20 de noviembre de 2015.
213. Para evitar correos basura, es posible que las claves públicas nuevas (identidades) con reputación baja tengan que pagar una cantidad de dinero para publicar sus anuncios. Esa cantidad puede guardarse en una cuenta de plica y devolverse al usuario cuando éste haya alquilado su propiedad o, tras un tiempo, decida retirar el anuncio. Archivos pesados como fotos se guardarán en plataformas como IPFS o Swarm, pero el hash de esos documentos y la información que identifica la identidad de su propietario quedarán registrados en la blockchain como parte del contrato suscrito con bAirbnb.
214. Usando, por ejemplo, el protocolo de Whisper.
215. Con formato y notas en Lenguaje de Marcas de Hipertexto (HTML, por sus siglas en inglés).
216. David McCandless, «World's Biggest Data Breaches», *Information Is Beautiful*, 2 de octubre de 2015; <www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>, consultado el 27 de noviembre de 2015.
217. Como define Vitalik Buterin: «Criptoconomía es un término técnico que viene a significar que es descentralizada, que usa criptografía de clave pública para autenticaciones y que emplea incentivos económicos para asegurar que siga funcionando y no retroceda en el tiempo ni sufra ningún otro fallo técnico», «The Value of Blockchain Technology, Part I», <<https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/>>.
218. <www.youtube.com/watch?v=K2fhwMKk2Eg>.
219. <<http://variety.com/2015/digital/news/netflix-bandwidth-usage-internet-traffic-1201507187/>>.
220. Entrevista a Bram Cohen, 17 de agosto de 2015.
221. Stan Franklin y Art Graesser, «Is It an Agent, or Just a Program? A Taxonomy for Autonomous Agents», <www.inf.ufrgs.br/~alvares/CMP124SMA/IsItAnAgentOrJustAProgram.pdf>.
222. *Ibid.*, p. 5.
223. Vitalik Buterin, <<https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>>. «Los agentes autónomos son lo contrario de la automatización; en un agente autónomo no hay necesidad de ninguna intervención humana específica, es decir, aunque sí sea necesario cierto esfuerzo humano para fabricar el hardware en el que el agente se ejecuta, no hace falta ningún humano que sea consciente de la existencia del agente.»
224. *Ibid.*
225. Un detalle técnico: como almanenar información directamente en blockchain es muy caro, lo más probable es que haya un hash de esa información, y que ésta se guarde en alguna red de almacenamiento de información como Swarm o IPFS.
226. Entrevista a Vitalik Buterin, 30 de septiembre de 2015.
227. Entrevista a Andreas Antonopoulos, 20 de julio de 2015.
228. *Ibid.*
229. Don Tapscott y Anthony D. Williams, *Wikinomics: How Mass Collaboration Changes Everything*, Portfolio/Penguin, Nueva York, 2007. [Hay traducción castellana: *Wikinomics: la nueva economía de las multitudes inteligentes*, Paidós Ibérica, Barcelona, 2011.] En *Wikinomics* se definían siete de estos modelos de negocio. Aquí hemos alargado la lista.
230. La «producción entre iguales basada en el común» es un concepto desarrollado por el catedrático de Derecho de la Universidad de Harvard Yochai Benkler en su seminal artículo «Coase's Penguin», *The Yale Law Journal*, 2002; <www.yale.edu/yalelj/112/BenklerWEB.pdf>.
231. <<http://fortune.com/2009/07/20/information-wants-to-be-free-and-expensive/>>.
232. Entrevista a Yochai Benkler, 26 de agosto de 2015.
233. Entrevista a Dino Mark Angaritis, 7 de agosto de 2015.
234. Andrew Lih, «Can Wikipedia Survive?», *The New York Times*, 20 de junio de 2015; <www.nytimes.com/2015/06/21/opinion/can-wikipedia-survive.html>.
235. <<http://techcrunch.com/2014/05/09/monegraph/>>.
236. <<http://techcrunch.com/2015/06/24/subscribe-raises-2-million-to-ensure-you-get-credit-for-your-art/>>.
237. <www.nytimes.com/2010/04/15/technology/15twitter.html?_r=0>.

238. <<http://techcrunch.com/2014/05/09/monegraph/>>.
239. <www.verisart.com/>.
240. <<http://techcrunch.com/2015/07/07/verisart-plans-to-use-the-blockchain-to-verify-the-authenticity-of-artworks/>>.
241. Entrevista a Yochai Benkler, 26 de agosto de 2015.
242. Entrevista a David Ticoll, 7 de agosto 2015.
243. Entrevista a Yochai Benkler, 26 de agosto de 2015.
244. <www.nytimes.com/2013/07/21/opinion/sunday/friedman-welcometo-the-sharing-economy.html?pagewanted=1&_r=2&partner=rss&emc=rss&>.
245. Sarah Kessler, «The Sharing Economy Is Dead and We Killed It», *Fast Company*, 14 de septiembre de 2015; <www.fastcompany.com/3050775/the-sharing-economy-is-dead-and-we-killed-it#1>.
246. «Prosumidor» es un término inventado por Alvin Toffler en *Future Shock* (1980). [Hay traducción castellana: *El shock del futuro*, Plaza & Janés, Barcelona, 1999.] En *The Digital Economy* (1994), Don Tapscott desarrolló el concepto de «prosumo».
247. Entrevista a Robin Chase, 2 de septiembre de 2015.
248. <<https://news.ycombinator.com/item?id=9437095>>.
249. Este escenario lo expuso por primera vez Don Tapscott en «The Transparent Burger», *Wired*, marzo de 2004, <http://archive.wired.com/wired/archive/12.03/start.html?pg=2%3ftw=wn_tophead_7>.
250. Entrevista a Yochai Benkler, 26 de agosto de 2015.
251. Lo que en *Wikinómia* se llamó «el lugar de trabajo wiki».
252. Captcha significa *Completely Automated Public Turing Test to Tell Computers and Humans Apart*, «Prueba de Turing completamente automática para distinguir entre ordenadores y seres humanos».
253. Entrevista a Joseph Lubin, 13 de julio de 2015.
254. *Ibid.*
255. No son sus verdaderos nombres. La historia se basa en conversaciones con personas que han vivido esa situación.
256. Primavera De Filippi, «It's Time to Take Mesh Networks Seriously (and Not Just for the Reasons You Think)», *Wired*, 2 de enero de 2014.
257. Entrevista a Eric Jennings, 10 de julio de 2015.
258. *Ibid.*
259. Entrevista a Lawrence Orsini, 30 de julio de 2015.
260. Don predijo el desarrollo de estas redes en Don Tapscott y Anthony Williams, *Macrowikinomics: New Solutions for a Connected Planet*, Portfolio/ Penguin, Nueva York, 2010; edición actualizada: 2012. [Hay traducción castellana, *Macrowikinomics: Nuevas fórmulas para impulsar la economía mundial*, Paidós Ibérica, Barcelona, 2011.]
261. Entrevista a Lawrence Orsini, 30 de julio de 2015.
262. Puja Mondal, «What Is Desertification? Desertification: Causes, Effects and Control of Desertification», UNEP: *Desertification*, Programa Medioambiental de las Naciones Unidas, n/a, <<https://desertification.wordpress.com/category/ecology-environment/unep/>>, consultado el 29 de septiembre de 2015.
263. <www.internetlivestats.com/internet-users/>, consultado el 1 de diciembre de 2015.
264. Cadie Thompson, «Electronic Pills May Be the Future of Medicine», CNBC, 21 de abril de 2013, <<http://www.cnbc.com/id/100653909>>; y Natt Garun, «FDA Approves Edible Electronic Pills That Sense When You Take Your Medication», *Digital Trends*, 1 de agosto de 2012, <www.digitaltrends.com/home/fda-approves-edible-electronic-pills/>.
265. Mark Jaffe, «IOT Won't Work Without Artificial Intelligence», *Wired*, noviembre de 2014, <www.wired.com/insights/2014/11/iot-wont-work-without-artificial-intelligence/>.
266. IBM, «Device Democracy», 4.
267. Allison Arieff, «The Internet of Way Too Many Things», *The New York Times*, 5 de septiembre de 2015.
268. IBM, «Device Democracy», 10.
269. Entrevista a Dino Mark Angaritis, 11 de agosto de 2015.
270. Entrevista a Carlos Moreira, 3 de septiembre de 2015.
271. *Ibid.*
272. Entrevista a Michelle Tinsley, 25 de junio de 2015.
273. *Ibid.*
274. McKinsey Global Institute, «The Internet of Things: Mapping the Value Beyond the Hype», junio de 2015.
275. Entrevista a Eric Jennings, 10 de julio de 2015.

276. IBM Institute for Business Value, «The Economy of Things: Extracting New Value from the Internet of Things», 2015.
277. Cadie Thompson, «Apple Has a Smart Home Problem: People Don't Know They Want It Yet», *Business Insider*, 4 de junio de 2015, <www.businessinsider.com/apple-homekit-adoption-2015-6>.
278. McKinsey Global Institute, «The Internet of Things: Mapping the Value Beyond the Hype», junio de 2015.
279. Entrevista a Eric Jennings, 10 de julio de 2015.
280. IBM, «Device Democracy», 9.
281. Ibid., 13.
282. McKinsey Global Institute, «The Internet of Things». Este instituto definió nueve ajustes con valor potencial.
283. <www.wikihow.com/Use-Uber>.
284. <<http://consumerist.com/tag/uber/page/2/>>.
285. Mike Hearn, «Future of Money», Turing Festival, Edimburgo, Escocia, 23 de agosto de 2013, subido a la red el 28 de agosto de 2013, <www.youtube.com/watch?v=Pu4PAMFPo5Y&feature=youtu.be>.
286. McKinsey, «An Executive's Guide to the Internet of Things», agosto de 2015; <www.mckinsey.com/Insights/Business_Technology/An_executives_guide_to_the_Internet_of_Things?cid=digital-eml-alt-mip-mck-oth-1508>.
287. <<http://datatopics.worldbank.org/financialinclusion/country/nicaragua>>.
288. <www.budde.com.au/Research/Nicaragua-Telecoms-Mobile-and-Broadband-Market-Insights-and-Statistics.html>.
289. «Property Disputes in Nicaragua», embajada de Estados Unidos, <http://nicaragua.usembassy.gov/property_disputes_in_nicaragua.html>. Se estima que hay 30.000 propiedades sujetas a disputa.
290. Entrevista a Joyce Kim, 12 de junio de 2015.
291. Ibid.
292. Ibid.
293. <www.worldbank.org/en/news/press-release/2015/04/15/massive-drop-in-number-of-unbanked-says-new-report>; y C.K. Prahalad, *The Fortune at the Bottom of the Pyramid: Eradicating Poverty Through Profits*, Wharton School Publishing, Filadelfia, 2004. [Hay traducción castellana: *La fortuna en la base de la pirámide: cómo crear una vida digna y aumentar las opciones mediante el mercado*, Granica, Barcelona, 2005.] Esta cifra es una estimación.
294. Entrevista a Joyce Kim, 12 de junio de 2015.
295. <www.ilo.org/global/topics/youth-employment/lang--en/index.htm>.
296. Thomas Piketty, *El capital en el siglo XXI*, Fondo de Cultura Económica de España, Madrid, 2014.
297. <www.brookings.edu/~media/research/files/papers/2014/05/declining%20business%20dynamism%20litan/declini>.
298. Ruth Simon y Caelainn Barr, «Endangered Species: Young U.S. Entrepreneurs», *The Wall Street Journal*, 2 de enero de 2015, <www.wsj.com/articles/endangered-species-young-u-s-entrepreneurs-1420246116>.
299. World Bank Group, Doing Business, <www.doingbusiness.org/data/exploretopics/starting-a-business>.
300. Entrevista a Hernando de Soto, 27 de noviembre de 2015.
301. <www.tamimi.com/en/magazine/law-update/section-6/june-4/dishonoured-cheques-in-the-uae-a-criminal-law-perspective.html>.
302. <www.worldbank.org/en/topic/poverty/overview>. Para ser exactos, había 1.910 millones en 1990.
303. <<http://digitalcommons.georgefox.edu/cgi/viewcontent.cgi?article=1003&context=gfsb>>.
304. <<http://reports.weforum.org/outlook-global-agenda-2015/top-10-trends-of-2015/1-deepening-income-inequality/>>.
305. Ibid.
306. Entrevista a Tyler Winklevoss, 9 de junio de 2015.
307. Congo, Chad, República Centroafricana, Sudán del Sur, Nigeria, Madagascar, Guinea, Camerún, Burkina Faso, Tanzania, <http://data.worldbank.org/indicator/FB.CBK.BRCH.P5?order=wbapi_data_value_2013+wbapi_data_value+wbapi_data_value-last&sort=asc>.
308. <www.aba.com/Products/bankcompliance/Documents/SeptOct11CoverStory.pdf>.
309. <<http://www.nytimes.com/2015/12/24/business/dealbook/banks-reject-new-york-city-ids-leaving-unbanked-on-sidelines.html>>.
310. Correspondencia electrónica con Joseph Lubin, 6 de agosto de 2015.
311. David Birch, *Identity Is the New Money*, London Publishing Partnership, Londres, 2014, p. 1.
312. Correspondencia electrónica con Joseph Lubin, 6 de agosto de 2015.
313. Entrevista a Joyce Kim, 12 de junio de 2015.

314. Entrevista a Hernando de Soto, 27 de noviembre de 2015.
315. Entrevista a Haluk Kulin, 9 de junio de 2015.
316. Correspondencia electrónica con Joseph Lubin, 6 de agosto de 2015.
317. Entrevista a Balaji Srinivasan, 29 de mayo de 2014.
318. <www.doingbusiness.org/data/exploretopics/starting-a-business>.
319. Entrevista a Haluk Kulin, 9 de junio de 2015.
320. Analie Domingo nos permitió que la acompañáramos en su rutina de enviar dinero a su madre en Filipinas. Analie ha sido empleada de Don Tapscott y Ana Lopes durante veinte años y es también una buena amiga.
321. <www12.statcan.gc.ca/nhs-enm/2011/dp-pd/prof/details/page.cfm?Lang=E&Geo1=PR&Code1=01&Data=Count&SearchText=canada&SearchType=Begins&SearchPR=01&A1=Al>.
322. <https://remittanceprices.worldbank.org/sites/default/files/rpw_report_june_2015.pdf>.
323. El mercado de los giros postales mueve 500.000 millones de dólares; el 7,7 por ciento de comisión media equivale a unos 38.500 millones de dólares en este concepto.
324. Dilip Ratha, «The Impact of Remittances on Economic Growth and Poverty Reduction», *Migration Policy Institute* 8, septiembre de 2013.
325. Adolf Barajas *et al.*, «Do Workers' Remittances Promote Economic Growth?», *IMF Working Paper*, <www10.iadb.org/intal/intalcdi/pe/2009/03935.pdf>.
326. «Aid and Remittances from Canada to Select Countries», Canadian International Development Platform, <<http://cidpnsi.ca/blog/portfolio/aid-and-remittances-from-canada/>>.
327. World Bank Remittance Price Index, <<https://remittanceprices.worldbank.org/en>>.
328. 2011 National Household Survey Highlights, Canadian Census Bureau, <www.fin.gov.on.ca/en/economy/demographics/census/nhsh11-1.html>.
329. <<https://support.skype.com/en/faq/FA1417/how-much-bandwidth-does-skype-need>>.
330. Entrevista a Eric Piscini, 13 de julio de 2015.
331. <http://corporate.westernunion.com/Corporate_Fact_Sheet.html>.
332. Cuando escribimos esto Abra no funcionaba en Canadá, pero pudimos probar su tecnología con Analie y su madre con la ayuda de la empresa.
333. Entrevista a Bill Barhydt, 25 de agosto de 2015.
334. *Ibid.*
335. *Ibid.*
336. «Foreign Aid and Rent-Seeking», *The Journal of International Economics*, 2000, p. 438, <<http://conferences.wcfia.harvard.edu/sites/projects.iq.harvard.edu/files/gov2126/files/1632.pdf>>.
337. *Ibid.*
338. <www.propublica.org/article/how-the-red-cross-raised-half-a-billion-dollars-for-haiti-and-built-6-homes>.
339. «Mortality, Crime and Access to Basic Needs Before and After the Haiti Earthquake», *Medicine, Conflict and Survival* 26(4), 2010.
340. <<http://unicoins.org/>>.
341. Jeffrey Ashe y Kyla Jagger Neilan, *In Their Own Hands: How Savings Groups Are Revolutionizing Development*, Berrett-Koehler Publishers, San Francisco, 2014.
342. E. Kumar Sharma, «Founder Falls», *Business Today* (India), 25 de diciembre de 2011; <www.businesstoday.in/magazine/features/vikram-akula-quits-sks-microfinance-loses-or-gains/story/20680.html>.
343. Ning Wang, «Measuring Transaction Costs: An Incomplete Survey», *Ronald Coase Institute Working Papers* 2, febrero de 2003; <www.coase.org/workingpapers/wp-2.pdf>.
344. <www.telesurtv.net/english/news/Honduran-Movements-Slam-Repression-of-Campesinos-in-Land-Fight-20150625-0011.html>.
345. USAID, Millennium Challenge Corporation y la Organización de las Naciones Unidas para la Alimentación y la Agricultura (FAO).
346. Paul B. Siegel, Malcolm D. Childress y Bradford L. Barham, «Reflections on Twenty Years of Land-Related Development Projects in Central America: Ten Things You Might Not Expect, and Future Directions», Knowledge for Change Series, International Land Coalition (ILC), Roma, 2013; <<http://tinyurl.com/oekhzos>>, consultado el 26 de agosto de 2015.
347. *Ibid.*
348. Embajador Michael B.G. Froman, Oficina del Representante del Comercio de Estados Unidos, «2015 National Trade Estimate Report on Foreign Trade Barriers», USTR.gov, 1 de abril de 2015, <<https://ustr.gov/sites/default/files/files/reports/2015/NTE/2015%20NTE%20Honduras.pdf>>.
349. Entrevista a Hernando de Soto, 27 de noviembre de 2015.
350. <<http://in.reuters.com/article/2015/05/15/usa-honduras-technology-idINKBN0001V720150515>>.

351. Entrevista a Kausik Rajgopal, 10 de agosto de 2015.
352. Banco Mundial, «Doing Business 2015: Going Beyond Efficiencies», Washington, D.C., Banco Mundial, 2014; DOI: 10.1596/978-1-4648-0351-2, License Creative Commons Attribution CC BY 3.0 IGO.
353. «ITU Releases 2014 ICT Figures», www.itu.int/net/pressoffice/press_releases/2014/23.aspx#.VEfalovF_Kg.
354. www.cdc.gov/healthliteracy/learn/understandingliteracy.html.
355. www.proliteracy.org/the-crisis/adult-literacy-facts.
356. CIA World Factbook, estadísticas sobre alfabetización, www.cia.gov/library/publications/the-world-factbook/fields/2103.html#136.
357. http://europa.eu/about-eu/countries/member-countries/estonia/index_en.htm; <http://www.citypopulation.de/Canada-MetroEst.html>.
358. Conversación entre el presidente estonio Toomas Hendrik Ilves y Don Tapscott en la cumbre del Consejo de la Agenda Global del Foro Económico Mundial en Abu Dhabi, Emiratos Árabes Unidos, octubre de 2015.
359. www.socialprogressimperative.org/data/spi#data_table/countries/com6,dim1,dim2,dim3,com9,idr35,com6,idr16.
360. <https://e-estonia.com/the-story/the-story-about-estonia/>. Estonia está muy orgullosa de sus iniciativas electrónicas y ha publicado mucha información en la red. Toda la información y las estadísticas empleadas en esta sección proceden de la página web del gobierno de Estonia.
361. «Electronic Health Record», e-Estonia.com, n/a, <https://e-estonia.com/component/electronic-health-record/>, consultado el 29 de noviembre de 2015.
362. «e-Cabinet», e-Estonia.com, n/a, <https://e-estonia.com/component/e-cabinet/>, consultado el 29 de noviembre de 2015.
363. «Electronic Land Register», e-Estonia.com, n/a, <https://e-estonia.com/component/electronic-land-register/>, consultado el 29 de noviembre de 2015.
364. Charles Brett, «My Life Under Estonia's Digital Government», *The Register*, www.theregister.co.uk/2015/06/02/estonia/.
365. Entrevista a Mike Gault, 28 de agosto de 2015.
366. «Keyless Signature Infrastructure», e-Estonia.com, n/a, <https://e-estonia.com/component/keyless-signature-infrastructure/>, consultado el 29 de noviembre de 2015.
367. Olga Kharif, «Bitcoin Not Just for Libertarians and Anarchists Anymore», *Bloomberg Business*, 9 de octubre de 2014, www.bloomberg.com/bw/articles/2014-10-09/bitcoin-not-just-for-libertarians-and-anarchists-anymore. A decir verdad, en el conjunto de la sociedad estadounidense hay una fuerte tendencia libertaria. Según el Pew Research Center, el 11 por ciento de los estadounidenses dicen ser libertarios y saben lo que la palabra significa. «In Search of Libertarians», www.pewresearch.org/fact-tank/2014/08/25/in-search-of-libertarians/.
368. «Bitcoin Proves the Libertarian Idea of Paradise Would Be Hell on Earth», *Business Insider*, www.businessinsider.com/bitcoin-libertarian-paradise-would-be-hell-on-earth-2013-12#ixzz3kQqSap00.
369. Human Rights Watch, «World Report 2015: Events of 2014», www.hrw.org/sites/default/files/wr2015_web.pdf.
370. Entrevista a Hernando de Soto, 27 de noviembre de 2015.
371. Seymour Martin Lipset, *Political Man: The Social Bases of Politics*, 2.^a ed., Heinemann, Londres, 1983, p. 64. [Hay traducción castellana: *El hombre político: las bases sociales de la política*, Tecnos, Madrid, 1987.]
372. Entrevista a Hernando de Soto, 27 de noviembre de 2015.
373. Hernando de Soto, «The Capitalist Cure for Terrorism», *The Wall Street Journal*, 10 de octubre de 2014, www.wsj.com/articles/the-capitalist-cure-for-terrorism-1412973796, consultado el 27 de noviembre de 2015.
374. Entrevista a Hernando de Soto, 27 de noviembre de 2015.
375. Entrevista a Carlos Moreira, 3 de septiembre de 2015.
376. Melanie Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, Sebastopol (California), enero de 2015, p. 45.
377. Emily Spaven, «UK Government Exploring Use of Blockchain Recordkeeping», *CoinDesk*, 1 de septiembre de 2015, www.coindesk.com/uk-government-exploring-use-of-blockchain-recordkeeping/.
378. J.P. Buntinx, «“Blockchain Technology” Is Bringing Bitcoin to the Mainstream», *Bitcoinist.net*, 29 de agosto de 2015, <http://bitcoinist.net/blockchain-technology-bringing-bitcoin-mainstream/>.
379. Melanie Swan, citado en Adam Stone, «Unchaining Innovation: Could Bitcoin's Underlying Tech Be a Powerful Tool for Government?», *Government Technology*, 10 de julio de 2015, www.govtech.com/state/Unchaining-Innovation-Could-Bitcoins-Underlying-Tech-be-a-Powerful-Tool-for-Government.html.
380. Véanse, por ejemplo, www.partnerships.org.au/ y www.in-control.org.uk/what-we-do.aspx.

381. Entrevista a Perianne Boring, 7 de agosto de 2015. Véase también Joseph Young, «8 Ways Governments Could Use the Blockchain to Achieve “Radical Transparency”», *CoinTelegraph*, 13 de julio de 2015, <<http://cointelegraph.com/news/114833/8-ways-governments-could-use-the-blockchain-to-achieve-radical-transparency>>.
382. <www.data.gov>.
383. <www.data.gov.uk>.
384. Ben Schiller, «A Revolution of Outcomes: How Pay-for-Success Contracts Are Changing Public Services», *Co.Exist*, <www.fastcoexist.com/3047219/a-revolution-of-outcomes-how-pay-for-success-contracts-are-changing-public-services>. Véase también: www.whitehouse.gov/blog/2013/11/20/building-smarter-more-efficient-government-through-pay-success.
385. R.C. Porter, «Can You “Snowden-Proof” the NSA?: How the Technology Behind the Digital Currency – Bitcoin– Could Stop the Next Edward Snowden», *Fortuna’s Corner*, 3 de junio de 2015, <<http://fortunascorner.com/2015/06/03/can-you-snowden-proof-the-nsa-how-the-technology-behind-the-digital-currency-bitcoin-could-stop-the-next-edward-snowden/>>.
386. Elliot Maras, «London Mayoral Candidate George Galloway Calls for City Government to Use Block Chain for Public Accountability», *Bitcoin News*, 2 de julio de 2015, <www.cryptocoinsnews.com/london-mayoral-candidate-george-galloway-calls-city-government-use-block-chain-public-accountability/>.
387. Don Tapscott, *The Digital Economy*, op. cit., p. 304.
388. Al Gore, discurso en la conferencia de We Media, 6 de octubre de 2005; <www.fpp.co.uk/online/05/10/Gore_speech.html>.
389. Ibid.
390. «The Persistence of Conspiracy Theories», *The New York Times*, 30 de abril de 2011, <www.nytimes.com/2011/05/01/weekinreview/01conspiracy.html?pagewanted=all&_r=0>.
391. <www.nytimes.com/2014/07/06/upshot/when-beliefs-and-facts-collide.html>.
392. «Plain Language: It’s the Law», Plain Language Action and Information Network, n/a, <www.plainlanguage.gov/plLaw/>, consultado el 30 de noviembre de 2015.
393. <<https://globalclimateconvergence.org/news/nyt-north-carolinas-election-machine-blunder>>.
394. <http://users.ensc.concordia.ca/~clark/papers/2012_fc.pdf>.
395. <http://link.springer.com/chapter/10.1007%2F978-3-662-46803-6_16>.
396. <<http://blogs.wsj.com/digits/2015/07/29/scientists-in-greece-design-cryptographic-e-voting-platform/>>.
397. <<http://nvbloc.org/>>.
398. <<http://cointelegraph.com/news/114404/true-democracy-worlds-first-political-app-blockchain-party-launches-in-australia>>.
399. <www.techinasia.com/southeast-asia-blockchain-technology-bitcoin-insights/>.
400. Ibid.
401. <www.washingtonpost.com/news/wonkblog/wp/2014/08/06/a-comprehensive-investigation-of-voter-impersonation-finds-31-credible-incidents-out-of-one-billion-ballots-cast/>.
402. <www.eac.gov/research/election_administration_and_voting_survey.aspx>.
403. <<http://america.aljazeera.com/opinions/2015/7/most-americans-dont-vote-in-elections-heres-why.html>>.
404. Entrevista a Eduardo Robles Elvira, 10 de septiembre de 2015.
405. <www.chozabu.net/blog/?p=78>.
406. <<https://agoravoting.com/>>.
407. Entrevista a Eduardo Robles Elvira, 10 de septiembre de 2015.
408. <http://cointelegraph.com/news/111599/blockchain_technology_smart_contracts_and_p2p_law>.
409. Aplicación Patentada de David Chaum, «Random Sample Elections», 19 de junio de 2014, <<http://patents.justia.com/patent/20140172517>>.
410. <<https://blog.ethereum.org/2014/08/21/introduction-futarchy/>>.
411. Federico Ast (@federicoast) y Alejandro Sewrjugin (@asewrjugin), «The CrowdJury, a Crowdsourced Justice System for the Collaboration Era», <<https://medium.com/@federicoast/the-crowdjury-a-crowdsourced-court-system-for-the-collaboration-era-66da002750d8#e8yyynqipo>>.
412. <<http://crowdjury.org/en/>>.
413. Todo el proceso se expone en Ast y Sewrjugin, «The CrowdJury».
414. Véase una breve descripción del proceso de selección del jurado en la antigua Atenas en <www.agathe.gr/democracy/the_jury.html>.
415. Véase el informe completo y las recomendaciones, incluida una exposición de modelos de otras partes del mundo, en <www.judiciary.gov.uk/reviews/online-dispute-resolution/>.
416. <<http://blog.counter-strike.net/index.php/overwatch/>>.

417. Fondo para la Defensa del Medio Ambiente, <www.edf.org/climate/how-cap-and-trade-works>.
418. Melanie Swan, *Blockchain: Blueprint for a New Economy*, op. cit.
419. Entrevista a Andreas Antonopoulos, 20 de julio de 2015.
420. «2015 Women in Music Honours Announced», *M Online*, PRS for Music, 22 de octubre de 2015, <www.m-magazine.co.uk/news/2015-women-in-music-honours-announced/>, consultado el 21 de noviembre de 2015.
421. Entrevista a Imogen Heap, 16 de septiembre de 2015.
422. David Byrne, «The Internet Will Suck All Creative Content Out of the World», *The Guardian*, 20 de junio de 2014, <www.theguardian.com/music/2013/oct/11/david-byrne-internet-content-world>, consultado el 20 de septiembre de 2015.
423. Entrevista a Imogen Heap, 16 de septiembre de 2015.
424. Conversación entre Paul Pacifico y Don Tapscott en casa de Imogen Heap, 8 de noviembre de 2015.
425. *Hide and Seek*, interpretada por Ariana Grande, YouTube, Love Ariana Grande Channel, 17 de octubre de 2015, <www.youtube.com/watch?v=2SdJ5wjsRsOs>, consultado el 21 de noviembre de 2015.
426. Entrevista a Imogen Heap, 16 de septiembre de 2015.
427. David Byrne et al., *Once in a Lifetime*, «Remain in Light», Talking Heads, 2 de febrero de 1981.
428. Entrevista a Imogen Heap, 16 de septiembre de 2015.
429. Johan Nylander, «Record Labels Part Owner of Spotify», *The Swedish Wire*, n/a, <www.swedishwire.com/jobs/680-record-labels-part-owner-of-spotify>, consultado el 23 de septiembre de 2015. Según Nylander, Sony posee el 5,8 por ciento; Universal, el 4,8 por ciento, y Warner, el 3,8 por ciento. Antes de su liquidación, EMI poseía el 1,9 por ciento.
430. Entrevista a Imogen Heap, 16 de septiembre de 2015.
431. David Johnson, «See How Much Every Top Artist Makes on Spotify», *Time*, 18 de noviembre de 2014, <<http://time.com/3590670/spotify-calculator/>>, consultado el 25 de septiembre de 2015.
432. Micah Singleton, «This Was Sony Music's Contract with Spotify», *The Verge*, 19 de mayo de 2015, <www.theverge.com/2015/5/19/8621581/sony-music-spotify-contract>, consultado el 25 de septiembre de 2015.
433. Stuart Dredge, «Streaming Music: What Next for Apple, YouTube, Spotify... and Musicians?», *The Guardian*, 29 de agosto de 2014, <www.theguardian.com/technology/2014/aug/29/streaming-music-apple-youtube-spotify-musicians>, consultado el 14 de agosto de 2015.
434. Ed Christman, «Universal Music Publishing's Royalty Portal Now Allows Writers to Request Advance», *Billboard*, 20 de julio de 2015, <www.billboard.com/articles/business/6634741/universal-music-publishing-royalty-window-updates>, consultado el 24 de noviembre de 2015.
435. Robert Levine, «Data Mining the Digital Gold Rush: Four Companies That Get It», *Billboard* 127(10), 2015, pp. 14-15.
436. Entrevista a Imogen Heap, 16 de septiembre de 2015.
437. Imogen Heap, «Panel Session», *Guardian Live*, «Live Stream: Imogen Heap Releases Tiny Human Using Blockchain Technology, Sonos Studio London», 2 de octubre de 2015, <www.theguardian.com/membership/2015/oct/02/live-stream-imogen-heap-releases-tiny-human-using-blockchain-technology>. Pasaje editado por Imogen Heap, correo electrónico, 27 de noviembre de 2015.
438. Ibid.
439. Entrevista a Andreas Antonopoulos, 20 de julio de 2015.
440. Entrevista a Imogen Heap, 16 de septiembre de 2015.
441. Ibid.
442. Stuart Dredge, «How Spotify and Its Digital Music Rivals Can Win Over Artists: "Just Include Us"», *The Guardian*, 29 de octubre de 2013, <www.theguardian.com/technology/2013/oct/29/spotify-amanda-palmer-songkick-vevo>, consultado el 14 de agosto de 2015.
443. George Howard, «Bitcoin and the Arts: An Interview with Artist and Composer, Zoe Keating», *Forbes*, 5 de junio de 2015, <www.forbes.com/sites/georgehoward/2015/06/05/bitcoin-and-the-arts-and-interview-with-artist-and-composer-zoe-keating/>, consultado el 14 de agosto de 2015.
444. Ibid.
445. Joseph Young, «Music Copyrights Stored on the Bitcoin BlockChain: Rock Band 22HERTZ Leads the Way», *CoinTelegraph*, 6 de mayo de 2015, <<http://cointelegraph.com/news/114172/music-copyrights-stored-on-the-bitcoin-blockchain-rock-band-22hertz-leads-the-way>>, consultado el 14 de agosto de 2015.
446. Comunicado de prensa, «Colu Announces Beta Launch and Collaboration with Revelator to Bring Blockchain Technology to the Music Industry», *Business Wire*, 12 de agosto de 2015.
447. Gideon Gottfried, «How "the Blockchain" Could Actually Change the Music Industry», *Billboard*, 5 de agosto de 2015, <www.billboard.com/articles/business/6655915/how-the-blockchain-could-actually-change-the-music-industry>.

448. PeerTracks Inc., 24 de septiembre de 2015; <<http://peertracks.com/>>.
449. «About Us», Artlery: Modern Art Appreciation, 3 de septiembre de 2015, <<https://artlery.com>>.
450. Ellen Nakashima, «Tech Giants Don't Want Obama to Give Police Access to Encrypted Phone Data», *The Washington Post*, 19 de mayo de 2015, <www.washingtonpost.com/world/national-security/tech-giants-urge-obama-to-resist-backdoors-into-encrypted-communications/2015/05/18/11781b4a-fd69-11e4-833c-a2de05b6b2a4_story.html>.
451. David Kaye, «Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression», Consejo de las Naciones Unidas sobre los Derechos Humanos, sesión vigésima novena, número de tema 3, borrador editado, 22 de mayo de 2015, <www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>, consultado el 25 de septiembre de 2015.
452. El informe de las Naciones Unidas remite al lector al Centre for International Governance Innovation y a Chatham House, *Toward a Social Compact for Digital Privacy and Security: Statement by the Global Commission on Internet Governance* (2015).
453. Social Progress Imperative, *Social Progress Index 2015*, 14 de abril de 2015, <www.socialprogressimperative.org/data/spi#data_table/countries/com9/dim1,dim2,dim3,com9>, consultado el 24 de septiembre de 2015. Nuestra clasificación se basa en la puntuación de componentes, no en la general de oportunidades.
454. «Regimes Seeking Ever More Information Control», *2015 World Press Freedom Index*, Reporteros sin Fronteras, 2015, <<http://index.rsrf.org/#/!themes/regimes-seeking-more-control>>.
455. Reporteros sin Fronteras, «Has Russia Gone So Far as to Block Wikipedia?», 24 de agosto de 2015, <<https://en.rsrf.org/russia-has-russia-gone-so-far-as-to-block-24-08-2015,48253.html>>, consultado el 25 de septiembre de 2015.
456. Scott Neuman, «China Arrests Nearly 200 over “Online Rumors”», 30 de agosto de 2015; <www.npr.org/sections/thetwo-way/2015/08/30/436097645/china-arrests-nearly-200-over-online-rumors>.
457. GetGems.org, 2 de septiembre de 2015, <<http://getgems.org/>>.
458. «Factom: Business Processes Secured by Immutable Audit Trails on the Blockchain», <www.factom.org/faq>.
459. Entrevista a Stephen Pair, 11 de junio de 2015.
460. Miguel Freitas, About Twister, <http://twister.net.co/?page_id=25>.
461. Mark Henricks, «The Billionaire Dropout Club», *CBS MarketWatch*, CBS Interactive Inc., 24 de enero de 2011, actualizado el 26 de enero de 2011, <www.cbsnews.com/news/the-billionaire-dropout-club/>, consultado el 20 de septiembre de 2015.
462. Entrevista a Joichi Ito, 24 de agosto de 2015.
463. *Ibid.*
464. Entrevista a Melanie Swan, 14 de septiembre de 2015.
465. *Ibid.*
466. «Introducing UNESCO: What We Are», web, consultado el 28 de noviembre de 2015, <<http://www.unesco.org/new/en/unesco/about-us/who-we-are/introducing-unesco>>.
467. Lev Serguéyevich Termén [León Theremin], «Erhöhung der Sinneswahrnehmung durch Hypnose [Incremento de la percepción sensorial por hipnosis]», *Erinnerungen an A. F. Joffe*, 1970. «Theremin, Leon», *Encyclopedia of World Biography*, 2005, *Encyclopedia.com*, <www.encyclopedia.com>, consultado el 26 de agosto de 2015.
468. Maciej Ceglowski, «Our Comrade the Electron», charla dada en Webstock 2014, teatro St. James, Wellington, Nueva Zelanda, 14 de febrero de 2014, <www.webstock.org.nz/talks/our-comrade-the-electron/>, consultado el 26 de agosto de 2015. El comienzo de este capítulo se inspira en la charla de Ceglowski.
469. Entrevista a Andreas Antonopoulos, 20 de julio de 2015.
470. Entrevista a Tyler Winklevoss, 9 de junio de 2015.
471. Satoshi Nakamoto, <P2pfoundation.ning.com>, 18 de febrero de 2009.
472. Ken Griffith e Ian Grigg, «Bitcoin Verification Latency: The Achilles Heel for Time Sensitive Transactions», libro blanco, 3 de febrero de 2014, <<http://iang.org/papers/BitcoinLatency.pdf>>, consultado el 20 de julio de 2015.
473. Entrevista a Izabella Kaminska, 5 de agosto de 2015.
474. *Ibid.*
475. Primavera De Filippi y Aaron Wright, «Decentralized Blockchain Technology and the Rise of Lex Cryptographia», *Social Sciences Research Network*, 10 de marzo de 2015, p. 43.
476. Entrevista a Josh Fairfield, 1 de junio de 2015.

477. Izabella Kaminska, «Bitcoin's Wasted Power—and How It Could Be Used to Heat Homes», *FT Alphaville*, *Financial Times*, 5 de septiembre de 2014.
478. CIA, «The World Factbook», <www.cia.gov>, 2012, <<http://tinyurl.com/noxwvle>>, consultado el 28 de agosto de 2015. Téngase en cuenta que las emisiones de carbono de Chipre en el mismo periodo ascendieron a 8.801 millones de megatonnes (2012).
479. «After the Bitcoin Gold Rush», *The New Republic*, 24 de febrero de 2015, <www.newrepublic.com/article/121089/how-small-bitcoin-miners-lose-crypto-currency-boombust-cycle>, consultado el 15 de mayo de 2015.
480. Entrevista a Bob Tapscott, 28 de julio de 2015.
481. Entrevista a Gavin Andresen, 8 de junio de 2015.
482. Entrevista a Eric Jennings, 10 de julio de 2015.
483. Entrevista a Stephen Pair, 11 de junio de 2015.
484. Entrevista a Erik Voorhees, 16 de junio de 2015.
485. Sangjin Han, «On Fair Comparison Between CPU and GPU», blog, 12 de febrero de 2013, <www.eecs.berkeley.edu/~sangjin/2013/02/12/CPU-GPU-comparison.html>, consultado el 28 de agosto de 2015.
486. Entrevista a Bob Tapscott, 28 de julio de 2015.
487. Entrevista a Valery Vavilov, 24 de julio de 2015.
488. Hass McCook, «Under the Microscope: Economic and Environmental Costs of Bitcoin Mining», CoinDesk Ltd., 21 de junio de 2014, <www.coindesk.com/microscope-economic-environmental-costs-bitcoin-mining/>, consultado el 28 de agosto de 2015.
489. Entrevista a Bob Tapscott, 28 de julio de 2015.
490. my-mr-wanky, eBay.com, 8 de mayo de 2014, <www.ebay.com/itm/3-Cointerra-TerraMiner-IV-Bitcoin-Miner-1-6-TH-s-ASIC-Working-Units-in-Hand-/331192098368>, consultado el 25 de julio de 2015.
491. «PC Recycling», *MRI of Australia*, MRI (Australia) Pty Ltd. Web, 28 de agosto de 2015, <<http://www.mri.com.au/pc-recycling.shtml>>.
492. Entrevista a Gavin Andresen, 8 de junio de 2015.
493. Vitalik Buterin, «Proof of Stake: How I Learned to Love Weak Subjectivity», *Ethereum blog*, 25 de noviembre de 2014, <<https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/>>.
494. Stefan Thomas y Evan Schwartz, «Ripple Labs' W3C Web Payments», documento de posición, 18 de marzo de 2014, <www.w3.org/2013/10/payments/papers/webpayments2014-submission_25.pdf>.
495. Entrevista a Austin Hill, 22 de julio de 2015.
496. Entrevista a Roger Ver, 30 de abril de 2015.
497. Satoshi Nakamoto, «Re: Bitcoin P2P E-cash Paper», *The Mail Archive*, 7 de noviembre de 2008, <www.mail-archive.com/>, <<http://tinyurl.com/oofvok7>>, consultado el 13 de julio de 2015.
498. Entrevista a Josh Fairfield, 1 de junio de 2015.
499. Entrevista a Stephen Pair, 11 de junio de 2015.
500. Entrevista a Jerry Brito, 29 de junio de 2015.
501. *Ibid.*
502. Entrevista a Josh Fairfield, 1 de junio de 2015.
503. Entrevista a Andreas Antonopoulos, 20 de julio de 2015.
504. Entrevista a Izabella Kaminska, 5 de agosto de 2015.
505. Entrevista a Stephen Pair, 11 de junio de 2015.
506. Andrew Vegetabile, «An Objective Look into the Impacts of Forking Blockchains Due to Malicious Actors», The Digital Currency Council, 9 de julio de 2015; <www.digitalcurrencycouncil.com/professional/an-objective-look-into-the-impacts-of-forking-blockchains-due-to-malicious-actors/>.
507. Entrevista a Keonne Rodriguez, 11 de mayo de 2015.
508. Andrew Vegetabile, «An Objective Look».
509. Peter Todd, «Re: [Bitcoin-development] Fwd: Block Size Increase Requirements», *The Mail Archive*, 1 de junio de 2015, <www.mail-archive.com/>, <<http://tinyurl.com/pk4ordw>>, consultado el 26 de agosto de 2015.
510. Satoshi Nakamoto, «Re: Bitcoin P2P E-cash Paper», lista de correo, *Cryptography*, Metzger, Dowdeswell & Co. LLC, 11 de noviembre de 2008. Web, 13 de julio de 2015, <www.metzdowd.com/mailman/listinfo/cryptography>.
511. Pascal Bouvier, «Distributed Ledgers Part I: Bitcoin Is Dead», *FiniCulture blog*, 4 de agosto de 2015, <<http://finiculture.com/distributed-ledgers-part-i-bitcoin-is-dead/>>, consultado el 28 de agosto de 2015.
512. Western Union, «Company Facts», Western Union, Western Union Holdings, Inc., 31 de diciembre de 2014. Web, 13 de enero de 2016, <http://corporate.westernunion.com/Corporate_Fact_Sheet.html>.
513. Entrevista a Gavin Andresen, 8 de junio de 2015.

514. *Ibíd.*
515. Entrevista a Austin Hill, 22 de julio de 2015.
516. Entrevista a Gavin Andresen, 8 de junio de 2015.
517. Andreas Antonopoulos, «Bitcoin as a Distributed Consensus Platform and the Blockchain as a Ledger of Consensus States», entrevista a Andreas Antonopoulos, 9 de diciembre de 2014.
518. Andy Greenberg, «Hackers Remotely Kill a Jeep on the Highway— with Me in It», *Wired*, 21 de julio de 2015.
519. International Joint Conference on Artificial Intelligence, 28 de julio de 2015, Buenos Aires, Argentina, <http://futureoflife.org/AI/open_letter_autonomous_weapons#signatories>.
520. Lisa Singh, «Father of the Internet Vint Cerf's Forecast for "Internet of Things"», *Washington Exec*, 17 de agosto de 2015.
521. Entrevista a Keonne Rodriguez, 11 de mayo de 2015.
522. Maciej Ceglowski, «Our Comrade the Electron».
523. Entrevista a Ann Cavoukian, 2 de septiembre de 2015.
524. Maciej Ceglowski, «Our Comrade the Electron».
525. <<http://www.lightspeedmagazine.com/nonfiction/interview-marc-goodman/>>.
526. Marc Goodman, *Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It*, Doubleday, Nueva York, 2015. (Hay traducción castellana: *Los delitos del futuro: todo está conectado, todos somos vulnerables, ¿qué podemos hacer al respecto?*, Ariel, Barcelona, 2015.)
527. Entrevista a Steve Omohundro, 28 de mayo de 2015.
528. *The Silver Stallion*, capítulo 26, <www.cadaeic.net/cabell.htm>, consultado el 2 de octubre de 2015.
529. Entrevista a Yochai Benkler, 26 de agosto de 2015.
530. Stephan Tual, «Announcing the New Foundation Board and Executive Director», *Ethereum blog*, Fundación Ethereum, 30 de julio de 2015; <<https://blog.ethereum.org/2015/07/30/announcing-new-foundation-board-executive-director/>>, consultado el 1 de enero de 2015.
531. *Ethereum: The World Computer*, producido por Ethereum, YouTube, 30 de julio de 2015; <www.youtube.com/watch?v=j23HnORQXvs>, consultado el 1 de diciembre de 2015.
532. Entrevista a Vitalik Buterin, 30 de septiembre de 2015.
533. *Ibíd.*
534. *Ibíd.*
535. *Ibíd.*
536. *Enrique VI*, segunda parte, acto 4, escena 2.
537. Correspondencia electrónica con Vitalik Buterin, 1 de octubre de 2015.
538. David D. Clark, «A Cloudy Crystal Ball», presentación, IETF, 16 de julio de 1992, <http://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf>.
539. Entrevista a Brian Forde, 26 de junio de 2015.
540. Entrevista a Erik Voorhees, 16 de junio de 2015; entrevista a Andreas Antonopolous, 20 de julio de 2015.
541. Entrevista a Erik Voorhees, 16 de junio de 2015.
542. Entrevista a Jim Orlando, 28 de septiembre de 2015.
543. <<http://www.coindesk.com/bitcoin-venture-capital/>>.
544. Correspondencia electrónica con Tim Draper, 3 de agosto de 2015.
545. Entrevista a Gavin Andresen, 8 de junio de 2015.
546. *Ibíd.*
547. Entrevista a Brian Forde, 26 de junio de 2015.
548. Entrevista a Joichi Ito, 24 de agosto de 2015.
549. Entrevista a Jerry Brito, 29 de junio de 2015.
550. *Ibíd.*
551. <www.cryptocoinsnews.com/us-colleges-universities-offering-bitcoin-courses-fall/>.
552. Entrevista a Adam Draper, 31 de mayo de 2015.
553. Entrevista a Benjamin Lawsky, 2 de julio de 2015.
554. Entrevista a Perianne Boring en *Money* 20/20, 26 de octubre de 2015.
555. Entrevista a Joichi Ito, 24 de agosto de 2015.
556. Entrevista a Blythe Masters, 29 de julio de 2015.
557. Para una lista completa de las victorias que Lawsky obtuvo siendo director del NYDFS, véase <www.dfs.ny.gov/reportpub/2014_annualrep_summ_mea.htm>.
558. Entrevista a Benjamin Lawsky, 2 de julio de 2015.
559. *Ibíd.*

560. *Ibíd.*
561. Entrevista a Jerry Brito, 29 de junio de 2015.
562. Entrevista a Benjamin Lawskey, 2 de julio de 2015.
563. *Ibíd.*
564. Lectura obligada para quien quiera oír una opinión fresca de un organismo gubernamental típicamente conservador: <www.parl.gc.ca/Content/SEN/Committee/412/banc/rep/rep12jun15-e.pdf>.
565. *Ibíd.*
566. Entrevista al senador canadiense Doug Black, 8 de julio de 2015.
567. *Ibíd.*
568. *Ibíd.*
569. *Ibíd.*
570. *Ibíd.*
571. Entrevista a Aaron Wright, 10 de agosto de 2015.
572. Entrevista a Josh Fairfield, 1 de junio de 2015.
573. La Reserva Federal no fue el primer banco nacional de Estados Unidos. El Primer Banco Nacional, creado por el Congreso en 1791 y puesto en marcha por el primer secretario del Tesoro de Estados Unidos, Alexander Hamilton, tuvo un alcance mucho más limitado y al final el presidente Andrew Jackson suprimió a su sucesor, el Segundo Banco Nacional, en 1836.
574. Entrevista a Carolyn Wilkins, 27 de agosto de 2015.
575. <<http://qz.com/148399/ben-bernanke-bitcoin-may-hold-long-term-promise/>>.
576. En Canadá: <www.bankofcanada.ca/wpcontent/uploads/2010/11/regulation_canadian_financial.pdf>; en Estados Unidos: <www.federalreserve.gov/pf/pdf/pf_5.pdf>.
577. Entrevista a Carolyn Wilkins, 27 de agosto de 2015.
578. «Money in a Digital World», comentarios de Carolyn Wilkins, gobernadora adjunta del Banco de Canadá, Universidad Wilfred Laurier, Waterloo, Ontario, 13 de noviembre de 2014.
579. Entrevista a Carolyn Wilkins, 27 de agosto de 2015.
580. *Ibíd.*
581. Entrevista a Jerry Brito, 29 de junio de 2015.
582. Entrevista a Steve Beauregard, 30 de abril de 2015.
583. Entrevista a Jerry Brito, 29 de junio de 2015.
584. Don Tapscott y Lynne St. Amour, «The Remarkable Internet Governance Network—Part I», Global Solution Networks Program, Martin Prosperity Institute, Universidad de Toronto, 2014.
585. Correspondencia electrónica con Vint Cerf, 12 de junio de 2015.
586. <www.w3.org/Payments/>.
587. <www.intgovforum.org/cms/wks2015/index.php/proposal/view_public/239>.
588. <www.internet-society.org/inet-bangkok/speakers/mr-pindar-wong>.
589. Adam Killick, «Knowledge Networks», Global Solution Networks Program, Martin Prosperity Institute, Universidad de Toronto, 2014.
590. Entrevista a Jerry Brito, 29 de junio de 2015.
591. Entrevista a Tyler Winklevoss, 9 de junio de 2015.
592. Entrevista a Joichi Ito, 24 de agosto de 2015.
593. <http://coala.global/?page_id=13396>.
594. <www.digitalchamber.org/>.
595. <<https://blog.coinbase.com/2014/10/13/welcome-john-collins-to-coinbase/>>.
596. <<http://www.digitalchamber.org/assets/press-release---g7---for-website.pdf>>.
597. Anthony Williams, «Platforms for Global Problem Solving», Global Solution Networks Program, Martin Prosperity Institute, Universidad de Toronto, 2013.
598. Entrevista a Brian Forde, 26 de junio de 2015.
599. Entrevista a Gavin Andresen, 8 de junio de 2015.
600. <www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf,7>.
601. Entrevista a Constance Choi, 10 de abril de 2015.
602. La revolución digital ha pasado a la «segunda mitad del tablero de ajedrez», ingeniosa frase acuñada por el inventor y escritor estadounidense Ray Kurzweil. Se refiere a la historia del emperador de China que, encantado con el juego de ajedrez, ofreció a su inventor concederle lo que deseara. El inventor pidió arroz. «Quisiera un grano de arroz en la primera casilla del tablero de ajedrez, dos en la segunda, cuatro en la tercera, y así hasta la última casilla», dijo. Pensando que serían un par de sacos de arroz, el emperador accedió de buen grado. Se

equivocaba. Aunque pequeña al principio, la cantidad de arroz ascendía a más de 2.000 millones de granos a mitad del tablero. En la última casilla tendría que haber más de 18 trillones de granos de arroz... bastantes para cubrir toda la superficie del planeta.

603. Entrevista por correo electrónico con Timothy Draper, 3 de agosto de 2015.

604. Entrevista a Hernando de Soto, 27 de noviembre de 2015.

La revolución blockchain

Don Tapscott y Alex Tapscott

No se permite la reproducción total o parcial de este libro, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio, sea éste electrónico, mecánico, por fotocopia, por grabación u otros métodos, sin el permiso previo y por escrito del editor. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (Art. 270 y siguientes del Código Penal)

Diríjase a CEDRO (Centro Español de Derechos Reprográficos) si necesita reproducir algún fragmento de esta obra.

Puede contactar con CEDRO a través de la web www.conlicencia.com o por teléfono en el 91 702 19 70 / 93 272 04 47

Título original: *Blockchain Revolution*

© del diseño de la portada, Sylvia Sans Bassat, 2017

© Don Tapscott y Alex Tapscott, 2017

© de la traducción, Juan Manuel Salmerón, 2017

© Centro Libros PAPF, S. L. U., 2017

Deusto es un sello editorial de Centro Libros PAPF, S. L. U.

Grupo Planeta, Av. Diagonal, 662-664, 08034 Barcelona (España)

www.planetadelibros.com

Primera edición en libro electrónico (epub): febrero de 2017

ISBN: 978-84-234-2715-4 (epub)

Conversión a libro electrónico: Newcomlab, S. L. L.

www.newcomlab.com

¡Encuentra aquí tu próxima lectura!

EMPRESA



ECONOMÍA



¡Síguenos en redes sociales!



El impacto del blockchain en nuestras vidas será tan significativo
como el que representó la aparición de internet

LA REVOLUCIÓN BLOCKCHAIN

DESCUBRE CÓMO
ESTA NUEVA TECNOLOGÍA
TRANSFORMARÁ
LA ECONOMÍA GLOBAL

DON TAPSCOTT

Autor del bestseller *Wikinomics*

ALEX TAPSCOTT

*Posiblemente el mejor tratado
escrito hasta el momento
sobre blockchain.*

Del prólogo de ENRIQUE DANS,
profesor de innovación en IE Business School

DEUSTO