

# Perspectivas y retos de Bitcoin y la revolución Blockchain

Luis Torras (@TorrasLuis) y Albert Castellana (@kstellana)

*“Dentro de veinte años hablaremos de Blockchain como ahora hablamos de Internet.”*

**Marc Andreessen**, fundador de Netscape<sup>1</sup>

*“I do think Bitcoin... has the potential to do something like to change the world.”*

**Peter Thiel**

## Introducción

La aparición de Internet constituye un punto de inflexión de magnitud y relevancia comparable a la máquina de vapor que marca un antes y un después en hasta el entonces incipiente mundo digital. La red de redes ha supuesto cambios en todos los ámbitos que incluyen una importante carga sociológica y filosófica. Internet ha permitido un aplanamiento de las estructuras a todos los niveles, en línea con la propia naturaleza dispersa del conocimiento. Esta descentralización ha favorecido unos crecimientos de la productividad nunca vistos antes: la revolución digital ha alumbrado un nuevo escenario con unos *costes de transacción* cada vez más bajos (tendemos en muchos aspectos al coste marginal cero<sup>2</sup>), más descentralizado, más libre y, a la postre, con mayor potencial para generar valor. Con todo, rápidamente quedó visto que todas estas promesas de un mundo más plano, rápido, transparente y descentralizado tenía límites.

El mundo digital se planteaba la solución a múltiples retos también presentes en el mundo físico: por ejemplo la confianza, la privacidad, la seguridad o la trazabilidad y control de los datos. En el mundo físico, donde nos vemos las caras, esto era un problema relativo y en donde la identidad no era un problema. En el mundo digital, donde una persona puede tener múltiples perfiles la cosa cambiaba radicalmente. En una célebre viñeta del *The New Yorker*, **Peter Steiner** ironizaba con el problema de la identidad que nacía con Internet a principios de los 90s donde se ve un perro chateando en Internet que le dice a otro: *"On the Internet no one knows you're a dog."*

El ejemplo que ponemos de la identidad, asegurarnos de que hablamos con Paco y no con Carmen (o llegado al extremo con un perro), limitaba el intercambio de valor en la red que se tenía que realizar utilizando la muleta de terceras partes. En efecto, para suplir estas limitaciones el mercado se ha apoyado en grandes compañías: no nos fiamos de Pepe si nos quiere vender un libro de segunda mano, pero sí de Amazon; no nos fiamos de María a la hora de alquilar un piso, pero sí de la plataforma AirBnB. Y así miles de ejemplos.

---

<sup>1</sup> Véase también **Marc Andreessen**, “Why Bitcoin Matters”, *New York Times*, 21 de Enero de 2014: <http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters>.

<sup>2</sup> **Jeremy Riffkin**, *La sociedad de coste marginal cero*, Paidós, 2014.

La economía mutaba pero solo de traje: sustituíamos viejos gigantes como *IBM, Johnson & Johnson, Citibank, Bank of America* o *ExxonMobile*, por los nuevos colosos de Silicon Valley: Google, Apple, Facebook y Amazon que se convertían en un relativamente corto periodo de tiempo en las mayores compañías por capitalización bursátil. Internet generó poco a poco su propia *metaestructura* que hoy genera no pocas suspicacias y recelos sobre su opacidad o las muchas asimetrías que se han acumulado entre estos grandes almacenes de datos y los usuarios.<sup>3</sup> La existencia de economías de escala, –de red, en el mundo digital–, favoreció, como en el mundo *pre-Internet*, la existencia de grandes corporaciones donde ahora la clave no era tanto la posesión de recursos o monopolios clave, sino simplemente información. Esto ha hecho que algunas de las tempranas advertencias de **Moisés Naím** en *El fin del poder*, que refleja las consecuencias de un mundo *totalmente plano*, aún no se hayan materializado del todo.<sup>4</sup>

Internet tenía una revolución pendiente, una revolución capaz de mejorar la trazabilidad de la información de manera que el usuario pudiera tener un control transparente sobre el flujo de estos “datos”, –lo más parecido al petróleo del siglo XXI–, como se monetizan y con qué propósitos. Una tecnología capaz, en definitiva, de ampliar los límites de la desintermediación, alumbrando una nueva era de prosperidad. Blockchain es este *protocolo fiable* que permite un Internet verdaderamente descentralizado (distribuido), transparente, seguro y abierto.

### La tecnología Blockchain

La tecnología Blockchain, *cadena de bloques*, es una base de datos distribuida, no centralizada en ningún punto, encriptada, y con un componente dinámico –la cadena se va incrementando con cada nuevo bloque de manera que cada nuevo paquete de datos tiene que ser validado de forma descentralizada por todos (o una parte significativa) del resto de miembros (nodos) que configuran la red antes de, finalmente, unirse a la cadena de bloques–; de ahí su nombre. Este elemento dinámico y su descentralización hace que esta tecnología sea extremadamente eficiente a la hora de almacenar de forma creciente datos ordenados en el tiempo y sin posibilidad de revisión o modificación. Al final, cada base de datos blockchain (Bitcoin es la más famosa, pero no la única), es algo similar a un gran libro contable abierto (*Distributed Ledger Technologies*), seguro, y donde se utilizan sofisticadas técnicas de encriptación para garantizar la no manipulación del archivo. Lo anterior dota de una gran seguridad, transparencia y trazabilidad con respecto a los datos por parte de todos los usuarios. De ahí también su gran potencial que tiene una infinidad de aplicaciones.

---

<sup>3</sup> **Don Tapscott**, *La economía digital*, McGraw-Hill, o **Ann Cavoukian** y **Don Tapscott**, *Who Knows: Safeguarding Your Privacy in a Networked World*, McGraw-Hill, 1997. **Eri Perinser**, *El filtro burbuja*, Taurus, 2017. Los problemas de seguridad en el Internet 1.0. han sido objeto de múltiples discusiones. Véase, por ejemplo, **Tom Slee**, *Lo tuyo es mío*, Taurus, 2016. Véase también **Luis Torras**, “El problema del filtro burbuja”, 13 de mayo de 2017: <https://medium.com/@TorrasLuis/un-libro-importante-sobre-un-tema-fundamental-3429841203db>

<sup>4</sup> **Moises Naím**, *El fin del poder*, Debate, 2011.

## Centralización, Descentralización y Distribución

Cada *Blockchain* es una *base de datos distribuida*, –un Internet sofisticado y mejorado si se quiere–, con un propósito concreto. Cada blockchain, Bitcoin o Ethereum por poner dos de los ejemplos más conocidos, pero también podemos hablar de NEM, Ripple, o IOTA (de las más complejas), esta compuesta por un conjunto de ordenadores/servidores llamados *nodos* que utilizan todos ellos un mismo sistema de comunicación, *protocolo*, para validar y añadir nueva información a la red. Con cada nuevo bloque, –transacción, actualización o dato–, la cadena se actualiza por completo y se valida por todos los usuarios siguiendo este protocolo de manera que quedan registradas todas las transacciones de manera segura y abierta. Cada red Blockchain tiene su propio *consenso*, es decir unas normas y reglas, que fijan y establecen el funcionamiento de la Blockchain para todos los usuarios. A partir de este consenso se pueden verificar los datos de forma distribuida lo que ofrece un control sobre los datos antes desconocido en el mundo de Internet, antes dependiente de grandes bases de datos centralizadas y muy opacas. Blockchain es la tecnología que permite asegurar que un Bitcoin es de un usuario concreto y de nadie más. Esto es posible, como decíamos, gracias al elemento *dinámico*, –similar al latido de un corazón–, que permite aproximar el mundo digital a la realidad y naturaleza de los procesos de mercado dinámicos por definición.

Si Internet suponía favorecer estructuras que tenían un mejor encaje con la naturaleza dispersa del conocimiento<sup>5</sup>, este nuevo cambio que supone Blockchain tiene un cierto paralelismo con la mejora a la teoría de la eficiencia estática neoclásica que supone la teorías de la *eficiencia dinámica* desarrolladas por el profesor **Jesús Huerta de Soto**.<sup>6</sup> De ahí también la fuerza, la revolución, que puede llegar a suponer blockchain en los años venideros si somos capaces de vencer las resistencias, obstáculos y riesgos que ineluctablemente conlleva siempre cualquier mejora disruptiva.

La irrupción de Internet cambió para siempre nuestras vidas alumbrando un mundo digital más descentralizado, accesible y abierto. Se trataba de una tecnología con un impacto transversal que sirvió de base a nuevos modelos de negocio y nuevos productos y servicios. Estos cambios no solo tuvieron un impacto en la dimensión económica sino que han supuesto una mutación radical en los modelos de liderazgo, sistemas de gestión, formas de comunicación e incluso la manera en la que hacemos política. Aún es pronto para aventurar hasta donde esta nueva tecnología podrá cumplir sus promesas, pero sí podemos afirmar que está en disposición de convertirse en una nueva revolución como lo fue Internet en la década de los 90s.

Gracias a las posibilidades técnicas que alumbró la tecnología de las *cadena de bloques*, en el horizonte apuntan nuevas maneras de optimizar procesos y relaciones, haciéndolas más transparentes y directas, nuevos modelos de negocio para ahorrar costes administrativos y burocráticos o generar entornos que permitan una mayor cooperación entre personas. Blockchain alumbró una nueva era en donde el mundo digital pasará de permitir el libre intercambio de datos, a un mundo digital en donde será posible el libre intercambio directo de

---

<sup>5</sup> **F.A. Hayek**, «The Use of Knowledge in Society», *The American Economic Review*, vol. 35, No. 4 (1945), pp. 519-530.

<sup>6</sup> **Jesús Huerta de Soto**, «La teoría de la eficiencia dinámica». *Procesos de Mercado: Revista Europea de Economía Política*, Vol. I, No. 1, Primavera 2004, pp. 11-71.

valor, un intercambio de valor hoy únicamente posible vía terceras partes que “centralizan la confianza” y validan las operaciones del sistema. Debido a estas grandes posibilidades no es de extrañar que desde la aparición de la primera Blockchain coincidiendo con la Gran Crisis Financiera su interés no haya parado de crecer pese a que los retos, como veremos al final, no son pocos.

*"I think that Internet is going to be one of the major forces for reducing the role of government. The one thing that's missing, but soon will be developed, is a reliable e-cash."*

**Milton Friedman**

### **Bitcoin: la nueva divisa digital**

El 18 de agosto de 2008, en plena crisis de las hipotecas subprime, y poco antes de que el sistema financiero se aproximase al abismo de su colapso con la quiebra de Lehman Brothers, se registró en Internet el dominio [bitcoin.org](http://bitcoin.org). Poco después, bajo el pseudónimo (o no) de **Satoshi Nakamoto** se hacía público un completo documento en donde se explicaba en que consistía Bitcoin, una moneda digital, encriptada utilizando la posibilidad de contar con bases de datos distribuidas lo que permitía el intercambio directo (*'peer-to-peer'*), sin necesidad de que intermedien terceras partes (el gran objetivo), igual que un pago en efectivo pero con todas las ventajas de desarrollarse en un entorno digital.<sup>7</sup> Bitcoin hoy es la red Blockchain más extendida y desarrollada del mundo, aunque no la única –ya que es un campo en donde los cambios se suceden a velocidad de vértigo–, pero sí que, junto con Ethereum, Ripple, o NEM, las principales y más sofisticadas redes de blockchain hoy en día, han ayudado a extender el uso de esta tecnología en un primer momento.

Pensemos en el correo postal. Un amigo quiere enviarte un mensaje a otro y quiere que el contenido de la carta sea una cosa exclusiva de ambos. Para ello mete la carta en un sobre y la sella. El sobre y una regulación estricta que estipula como delito contra la intimidad abrir el correo ajeno, es el binomio tecnología/instituciones que han permitido la comunicación privada entre personas durante siglos. Reto similar es el que se planteaba en el caso de Bitcoin, reto únicamente soluble gracias a la tecnología *blockchain*.

Bitcoin es, hoy por hoy, la gran criptomoneda a nivel global. Se trata de una divisa con una oferta limitada, como el oro, fijada en 21 millones de bitcoins (a día de hoy se han “minado” ya algo más de 16,3 millones), y que gracias a la tecnología blockchain que permite un intercambio seguro que protege esta oferta de cualquier manipulación política o arbitraria por cualquier poder político.

El Bitcoin también tiene su propio coste de obtención, un coste que se adapta automáticamente en base al tiempo de validación histórico de los bloques, pudiendo incrementarse o disminuir. Esta circunstancia guarda un cierto paralelismo con los costes de obtención del oro, la forma de dinero por excelencia, pero en un entorno digital. Todas estas características le dan a esta forma de dinero un enorme potencial. Para los divulgadores de temas tecnológicos **Don** y **Alex Tapscott**, Blockchain en el ámbito de la moneda y la contabilidad de transacciones económicas supone una revolución tan importante como el que supuso la invención de la contabilidad de

---

<sup>7</sup> <http://bitcoin.org/bitcoin.pdf>

partida doble por parte de **Luca Pacioli** en la Italia de la baja edad media.<sup>8</sup>

El desarrollo de Bitcoin no se puede entender sin aproximar la salida en falso a la crisis, su alargamiento innecesario<sup>9</sup>, y la devaluación de las grandes divisas ha servido de importante acicate y ha ido despertando el interés de los inversores de manera creciente a los grandes retos que dicha divisa plantea, criptomoneda como Bitcoin han despertado el interés general de muchos inversores y han logrado atraer importantes flujos de dinero, especialmente intenso por parte de algunos países (como India y China) especialmente sensibles a una devaluación severa de sus divisas como "*salida fácil*" a su elevada posición de deuda.

Lo anterior supone incrementar los riesgos de una confiscación masiva del ahorro derivado de una gestión fraudulenta de la moneda. Ante este escenario, el oro, y ahora el Bitcoin (entre otras divisas digitales), se han erigido como principales bastiones de protección contra la inflación. En el corto plazo, ambas propuestas presentan importantes diferencias: la primera, ha crecido de forma más lenta en tanto en cuando es una más que probada, –ahí están ya más de 5.000 años de historia documentada con el oro como principal y más perfecta forma de dinero–, mientras que la segunda es todavía pronto para saber cómo y de qué manera se convertirá en una nueva forma de proteger y defender el ahorro.

Entender la dinámica inflacionista de la actual arquitectura financiera es también importante para analizar el potencial y posibilidades de Bitcoin (y también de algunas otras criptomoneda). Los diseñadores de Bitcoin quisieron solucionar alumbrando una moneda deflacionaria en el medio-largo plazo mediante el diseño de su consenso reduce a la mitad la recompensa a los mineros cada cuatro años lo que reduce la emisión de nueva moneda de forma automática.

La gran fuerza de Bitcoin es que la oferta monetaria esta descentralizada, por lo tanto más *antifrágil*, y también más segura, privada (garantiza la intimidad de comprador y vendedor como los pagos en efectivo) y ajena a procesos inflacionistas.<sup>10</sup>

## Retos y dudas de Bitcoin

Bitcoin (y el resto de criptomoneda), también plantean dudas. Algunas sobre su seguridad pero el tiempo esta demostrando como, al tratarse de un registro exhaustivo y descentralizado, en un sistema blockchain todo queda registrado y cambiar el registro de la cadena si bien es técnicamente posible, esto requiere la existencia de consensos.<sup>11</sup> La principal es ver si logrará

---

<sup>8</sup> **Don Tapscott, Alex Tapscott**, *La revolución blockchain*, Deusto, 2017. Véase también **Albert Castellana**, “Introducción a la tecnología Blockchain”, BigDataWeek16: <https://www.youtube.com/watch?v=QuK3mVdojPg>

<sup>9</sup> Véase, por ejemplo, **James Rickard**, *The Death of Money*, Penguin Books, 2015; **Daniel Lacalle**, *Escape from the Central Bank Trap: How to Escape From the \$20 Trillion Monetary Expansion Unharmed*, Business Experts Press, 2017.

<sup>10</sup> **Nassim N. Taleb** (2013): *Antifrágil. Las cosas que se benefician del desorden*, Paidós, Barcelona.

<sup>11</sup> Véase por ejemplo el caso del cyber ataque por parte de WannaCry en donde la trazabilidad de las criptomoneda mostró su fortaleza. **Andreu Rodríguez**, “¿Acertaron los creadores de WannaCry pidiendo el rescate en bitcoins?”, *El País*, 17 de mayo de 2017: [http://retina.elpais.com/retina/2017/05/17/tendencias/1495036335\\_828145.html?platform=hootsuite](http://retina.elpais.com/retina/2017/05/17/tendencias/1495036335_828145.html?platform=hootsuite). Véase también “Understanding the DAO attack”: <https://www.coindesk.com/understanding-dao-hack-journalists/>

convertirse en una nueva divisa global libre de inflación, es decir, un depósito de valor verdaderamente sólido, como hoy es el oro físico. Falta ver como evolucionará la aceptación de esta tecnología disruptiva tanto por parte de los agentes económicos como por parte de los reguladores y el sector público. Sí sabemos seguro que será un proceso de consolidación no exento de turbulencias como lo ha demostrado los vaivenes experimentados no únicamente por Bitcoin, también el conjunto de todas las redes blockchain, debido a su carácter novedoso, la dificultad de establecer estimaciones sobre el tema, y debido a qué el estadio de desarrollo de esta tecnología es aún embrionario.

Con respecto a Bitcoin en concreto, persiste la duda sobre si, como decíamos, esta nueva red que quiere ser una forma de pago digital se convertirá finalmente en un *proxy digital*, –por lo tanto, mejorado–, de dinero (una forma de dinero lo más parecido a oro en el mundo digital); o sí, por el contrario, la fiebre del Bitcoin es únicamente una nueva *Tulipomanía*.<sup>12</sup>

El éxito futuro de Bitcoin descansa en la capacidad que tenga en generar confianza en su seguridad y utilización para convertirse, finalmente, en un extendido modo de pago como reza la definición de dinero clásica del economista austriaco **Carl Menger**.<sup>13</sup> Está por ver si Bitcoin se convertirá o no en una nueva forma de *dinero*, –es decir, sí va más allá de ser un método alternativo de pago (bastante ineficiente en algunos aspectos) como es hoy en día–, es hoy la gran incertidumbre sobre la moneda virtual según el experto en temas monetarios **George Selgin**.<sup>14</sup> Otros se muestran más optimistas como el filósofo libanés **Nassim Taleb**, el emprendedor **Peter Thiel**, o los autores de temas digitales **Dominic Frisby** o **Nathiel Popper**, por poner solo algunos ejemplos.<sup>15</sup>

Sin embargo, las criptomonedas están demostrando su sólida seguridad y, debido a su oferta limitada, el valor de la misma está creciendo de manera exponencial a medida que se ha ido incrementando la oferta. El valor de cualquier moneda tradicional según la *Teoría Monetaria Moderna* (TMM), –que tiene no pocas vías de agua–, pasa, principalmente por la capacidad de exigir exacciones (es decir, tributos e impuestos) por parte de un estado que ejerce una autoridad en un territorio. De esta forma, las economías nacionales están forzosamente “nominadas” en una divisa nacional, o supranacional como el Euro, lo que asegura su demanda. Otra de las grandes críticas a monedas como Bitcoin, con una oferta monetaria teóricamente limitada, deriva de la confusión de los nuevos monetaristas keynesianos de confundir oferta

---

<sup>12</sup> **Peter Schiff** ha mostrado cierto escepticismo con respecto a Bitcoin por tener un bajo valor intrínseco, en este caso el coste de la energía que consumen los servidores de Internet en el proceso de ‘*mining*’, y su poca, de momento, utilización/aceptación. <https://news.bitcoin.com/peter-schiff-bitcoin-digital-fools-gold/>.

<sup>13</sup> **Carl Menger**, “On the Origins of Money,” trans. C.A. Foley, *The Economic Journal* 2 (1892), pp. 239– 55.

<sup>14</sup> **George Selgin** (2014): *Bitcoin: Problems and Prospects*, Center for Monetary and Financial Alternatives, The Cato Institute, Washington DC. Véase “Gold Bug Peter Schiff Calls Bitcoin ‘Digital Fool’s Gold’”, Bitcoin.com, 1 de marzo de 2017. **Javier Santacruz**, “¿Son tan buenas como el oro las monedas virtuales tipo Bitcoin”: <https://www.oroymas.com/2014/01/buenas-como-oro-monedas-virtuales-bitcoin/>. Véase también **Luis Torras**, “Bitcoin: ¿el nuevo oro digital?”, *World Economic Forum*, 22 de mayo de 2017;

<sup>15</sup> Véase **Dominic Frisby** (2014): *Bitcoin: The Money of the Future?*, Unbound; **Nathaniel Popper** (2016): *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*, Harper. Véase también **Valentin Schmid**, “Bitcoin is money”, *The Epoch Times*, 21 de Junio de 2017 o **Dr. Saifedean Ammous**, *The Bitcoin Standard: Sound Money in a Digital Age*, DRAFT Junio 2017, pendiente de publicación.

monetaria con liquidez.<sup>16</sup>

Bitcoin es un gran libro contable abierto, seguro –gracias a la tecnología Blockchain–, que se valida de forma descentralizada, lo que permite el intercambio entre dos partes sin intermediarios. Un pago en efectivo en el entorno digital. Con todo, las limitaciones técnicas de Bitcoin (también de otras criptomonedas) no son pocos, y persisten muchas incertidumbres aún por solventar de las que deriva también el comportamiento por momentos errático y extremadamente volátil del grueso de las criptomonedas. Algunos de los problemas actuales de bitcoin hacen referencia a unos costes de transacción que siguen siendo muy altos y a la capacidad del conjunto del sistema sigue siendo limitada, especialmente si lo comparamos con el sistema actual capaz de procesar varios miles de operaciones al segundo. Otro tema polémico es el referente al control que pueden ejercer ciertos grupos de “mineros” en donde se sitúa el origen del “hard fork” entre Bitcoin y Bitcoin Cash. Por último, persiste todavía un consumo energético muy alto.<sup>17</sup> Todos ellos son retos de tipo técnico y tecnológico que, por el momento, hacen de Bitcoin una solución interesante en muchos aspectos pero que dista de ser perfecta en otros.

### **Blockchain: más allá de Bitcoin**

Los grandes desarrollos de Blockchain hasta el momento se han dado en el ámbito de la moneda con la aparición de Bitcoin y resto de criptomonedas, pero el potencial de la tecnología de encriptación va mucho más allá y sus aplicaciones impactan de forma transversal en muchos otros ámbitos en donde la tecnología blockchain, en suma, permite tener un registro seguro permitiendo asegurar la identidad en el entorno digital. Esto es, por ejemplo, lo que ya está haciendo la *Svrin Foundation*, una de las primeras iniciativas orientadas a resolver el problema de las “identidades múltiples” que se dan típicamente en el entorno digital.<sup>18</sup>

En el mundo físico cuando entramos en una discoteca y nos piden demostrar nuestra mayoría de edad simplemente tenemos que mostrar nuestro DNI. No hace falta conectarse con la base de datos del Departamento del Interior, el mismo documento verifica esta identidad sin necesidad de terceras partes. Esto mismo es lo que Blockchain también quiere solventar en el futuro y que hasta ahora, en Internet, no era posible. De esta manera, y de igual manera que sucede con las monedas virtuales, podremos intercambiar datos con seguridad sin la necesidad de un tercero que nos valide.

Esta no es la única iniciativa. Bitnation, por ejemplo, comenzó a usar la cadena de bloques para emitir su propia versión de un pasaporte estatal independiente del estado en 2014, proyecto que descansa sobre la prometedora red blockchain Ethereum que también soporta otra herramienta de administración de identidad llamada uPort. Civic está construyendo un proyecto similar con

---

<sup>16</sup> Véase **Paul Krugman**, “Bitcoin Is Evil”, *The New York Times*, 28 de diciembre de 2013. Una buena crítica a la TMM se puede encontrar en **George Selgin**, *The Theory of Free Banking: Money Supply under Competitive Note Issue* (1988): <http://oll.libertyfund.org/titles/selgin-the-theory-of-free-banking-money-supply-under-competitive-note-issue>. Véase también **J.R. Rallo**, *Contra la Teoría Monetaria Moderna*, Deusto, 2017.

<sup>17</sup> **Mark van Rijmenan**, “Why Bitcoin Will Ultimately Fail and What Will Come Next”, LinkedIn del auto, 12 de septiembre de 2017.

<sup>18</sup> **Matthew Griffin**, “New blockchain tools are helping people reclaim control of their online identities”, 16 de mayo de 2017: <http://www.globalfuturist.org/2017/05/new-blockchain-tools-help-people-reclaim-control-of-their-online-identities/>

Bitcoin en otra red Blockchain, en este caso Windley. Otras redes de Blockchain como la prometedora NEM, tienen el potencial de convertirse en base para nuevos negocios en los próximos años al permitir de manera fácil para el usuario, entre otras funcionalidades, distribuir los registros de cualquier base de datos a partir de redes blockchain privadas, un paso intermedio a la ahora de adaptar esta tecnología como en su día con Internet fueron el diseño de redes cerradas o Intranets.

Al margen de las dificultades técnicas, operativas y regulatorias, lo cierto es que la expansión de blockchain exige importantes cambios en los modelos de gestión, el liderazgo público y privado, e incluso plantea la necesidad de una nueva cultura ciudadana y democráticas. Por añaduría, y como ha señalado el profesor de la UPF **Benito Arruñada**, las promesas de esta nueva tecnología que promete un *intercambio sin intermediarios* mediante los llamados “*Smart contracts*”<sup>19</sup>, están limitadas a la propia naturaleza del intercambio contractual y el funcionamiento de la economía. Generar *confianza*, paso previo ineluctable previo a cualquier intercambio, a veces incluye elementos de naturaleza *intangibles*, tácita, difícilmente articulable en código de programación, elemento que suele quedar muchas veces infravalorado en el grueso de análisis de impacto sobre Blockchain.<sup>20</sup>

De lo anterior podemos concluir que Blockchain, *a priori*, va a tener un mayor impacto en mercados contractualmente organizados y relativamente estandarizados: por ejemplo, en todo lo relacionado con el Internet de las cosas (donde la demanda de seguridad es un punto clave), en comparación con otros ámbitos en donde la confianza se genera por otras vías y canales.<sup>21</sup> Las mejoras del blockchain incorporan una importante promesa de mayor control y transparencia, de lo que deriva mejores prácticas contractuales para reducir la corrupción o el coste de la burocracia entre otros cambios.<sup>22</sup>

Como siempre sucede, el cambio tecnológico es más rápido que el social o cultural. Si ya la irrupción de modelos de negocio como Uber, una plataforma “agregadora” (es decir, una de estas “terceras partes” necesarias en el actual mundo digital para verificar identidades y datos), han topado con fuertes barreras políticas y sociales, qué barreras no encontrara una tecnología que supone una descentralización de la economía de una magnitud veinte veces mayor. Como ya pasó con el Internet 1.0., –el del comercio online, las redes sociales y la (mal llamada) “*economía colaborativa*–, el gran perdedor de esta nueva revolución es (sobre todo) los poderes Públicos y el Estado, paroxismo de poder centralizado, que ve como las nuevas tecnologías lo

---

<sup>19</sup> El primero en utilizar la expresión “*smart contract*” fue Nick Szabo. **Nick Szabo**, *The Idea of Smart Contracts*, MANUSCRIPT (1997) [http://szabo.best.vwh.net/smart\\_contracts\\_idea.html](http://szabo.best.vwh.net/smart_contracts_idea.html). Véase también **Nick Szabo**, *Secure Property Titles with Owner Authority*, <http://szabo.best.vwh.net/securetitle.html>

<sup>20</sup> **Benito Arruñada**, “Blockchain’s Struggle to Deliver Impersonal Exchange”, próxima publicación en *Minnesota Journal of Law, Science & Technology*. Véase también **Benito Arruñada**, *Property as Sequential Exchange: The Forgotten Limits of Private Contract*, 13 J. INST. ECON, 2017; **Vili Lehdonvirta**, “The Blockchain Paradox: Why Distributed Ledger Technologies May Do Little to Transform the Economy”, *The Policy and Internet Blog*, 21 de noviembre, 2016, <http://blogs.oxi.ac.uk/policy/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/>

<sup>21</sup> Véase también, a este respecto, **César Hidalgo**, *El triunfo de la información*, Debate, 2017, pp. 127-43. Para un estudio amplio sobre la complejidad de la confianza véase **Francis Fukuyama**, *Trust: The Social Virtues and the Creation of Prosperity*, Free Press, 1995.

<sup>22</sup> **Mark Walport**, *Executive Summary and Recommendations*, en DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN 8, 2016.



adelantan por la izquierda, derecha, por arriba y por abajo, dando lugar a un escenario en donde quienes salen ganando, –tienen más libertad–, son los consumidores, inversores, empresarios y ciudadanos en general.

El gran reto es de gobernanza y liderazgo como ha señalado con razón, **Klaus Schwab** en su libro *La cuarta revolución industrial*.<sup>23</sup> **Manuel Castells** recuerda: “*En momentos de grandes cambios tecnológicos, las personas, empresas e instituciones se pueden sentir superadas por estos cambios por la ignorancia sobre sus efectos.*”<sup>24</sup> Es cierto que quedan muchos problemas de tipo técnico por resolver, pero las limitaciones de este cambio tecnológico, al margen de las relacionadas con la propia naturaleza del intercambio, tienen mucho que ver con nuestra capacidad personal de cambio y de adaptación a este nuevo escenario. De nosotros depende pues limitar los miedos que derivan de esta ignorancia y saber capitalizar las posibilidades que ofrece el mundo digital descentralizado y distribuido en el futuro que siguen siendo muchas al margen de las limitaciones y retos aquí descritos.

### **Bibliografía seleccionada**<sup>25</sup>

Antonopoulos, A. (2016): *The Internet of Money*, Merkle Bloom.

Arruñada, B. (2017): “Blockchain’s Struggle to Deliver Impersonal Exchange”, próxima publicación en *Minnesota Journal of Law, Science & Techonolgy*.

Cavoukian, A., Tapscott, D. (1997): *Who Knows: Safeguarding Your Privacy in a Networked World*, McGraw-Hill, Nueva York.

Coase, R.H. (1937): “The Nature of the Firm”, *Economica* 4, n 16, pp. 386-450.

Hayek, F.A. (1945): «The Use of Knowledge in Society», *The American Economic Review*, vol. 35, No. 4 (Sept.), pp. 519-530.

Hidalgo, C. (2017): *El triunfo de la información*, Debate, 2017.

Huerta de Soto, J. (2008): *The Theory of Efficient Dynamics*, Routledge, Londres.

Frisby, D. (2014): *Bitcoin: The Future of Money*, Unbound.

Fukuyama, F. (1995): *Trust: The Social Virtues and the Creation of Prosperity*, Free Press.

Lacalle, D. (2017): *Escape from the Central Bank Trap: How to Escape From the \$20 Trillion Monetary Expansion Unharmred*, Business Experts Press, Londres.

Mougayar, W. (2016): *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, Wiley.

Naím, M. (2011): *El fin del poder*, Debate, Barcelona.

---

<sup>23</sup> **Klaus Schwab**, *La cuarta revolución industrial*, Debate, 2016.

<sup>24</sup> **Luis Torras**, “Vivir en tiempos de la cuarta revolución industrial”, *World Economic Forum Blog*, 9 de febrero de 2017.

<sup>25</sup> Adicionalmente, para el lector interesado, pueden consultarse estas otras fuentes relevantes en relación a este tema: <https://steemit.com/books/@luistorras/44-books-to-help-to-understand-the-implications-of-blockchain-bitcoin>

Narayanan, A., Bonneau, J., Felten, E., Miller, A., y Goldfeder, S. (2016): *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (borrador disponible: [https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton\\_bitcoin\\_book.pdf?a=1](https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1))

Perinser, E. (2017): *El filtro burbuja*, Taurus, Barcelona.

Popper, N. (2016): *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*, Harper.

Rickards, J. (2015): *The Death of Money*, Penguin Books, Nueva York.

Schawb, K. (2016): *La cuarta revolución industrial*, Debate, Barcelona.

Schiff, P. (2012): *The Real Crash*, St. Martin Press.

Selgin, G. (1988): *The Theory of Free Banking: Money Supply under Competitive Note Issue*: <http://oll.libertyfund.org/titles/selgin-the-theory-of-free-banking-money-supply-under-competitive-note-issue>.

Slee, T. (2016): *Lo tuyo es mío*, Taurus, Barcelona.

Taleb, N.N. (2013): *Antifrágil. Las cosas que se benefician del desorden*, Paidós, Barcelona.

Tapscott, D. y Tapscott, A. (2017): *La revolución Blockchain*, Deusto, Barcelona.

Vigna, P. y Casey, M. (2016): *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order*, Picador, Nueva York.

## Autores



**Luis Torras**, es consultor financiero y gestor de fondos (Panda Agriculture and Water Fund y Japan Deep Value), profesor visitante en ESADE Business School y miembro del Observatorio de Divulgación Financiera del IEF.



**Albert Castellana**, ingeniero informático es co-fundador y Presidente de Atraura Blockchain, consultora pionera en España en el diseño e implementación de soluciones basadas en la tecnología Blockchain, y es miembro del Consejo de la Fundación NEM.