

CARLOS DOMINGO

Todo lo que querías saber sobre

**BITCOIN,
CRIPTOMONEDAS
Y BLOCKCHAIN**

y no te atrevías a preguntar



,

Índice

Portada

Sinopsis

Dedicatoria

PRÓLOGO

La batalla de las ideas y los conceptos tras las criptomonedas

INTRODUCCIÓN

La siguiente revolución tecnológica

PRIMERA PARTE: ORO DIGITAL

1. UNA BREVE HISTORIA DEL DINERO

2. ¿QUÉ ES EL BITCOIN?

2008: estalla la crisis, nace el bitcoin

El economista visionario

El misterio Nakamoto

Red mundial descentralizada

¡Que no te roben la cartera!

¿Una moneda «de verdad»?

3. EL DINERO DIGITAL HA LLEGADO PARA QUEDARSE

Moneda en proceso

El valor de una pizza

En las profundidades de Internet

Una bola de nieve en crecimiento

Los caminos se bifurcan

SEGUNDA PARTE: LA NUEVA INTERNET DEL VALOR

4. BLOCKCHAIN: LA MAGIA TECNOLÓGICA DETRÁS DEL BITCOIN

5. CRIPTOMONEDAS ALTERNATIVAS: LOS HERMANOS Y PRIMOS DEL BITCOIN

Namecoin (NMC)

Litecoin (LTC)

Ripple (XRP)

Monero (XMR)

Hacia la segunda generación

6. ETHEREUM: LLEGA LA BLOCKCHAIN 2.0

Dinero programado

Propiedades digitalizadas y aplicaciones descentralizadas

Nuevas alternativas para financiar y monetizar

La revolución de la liquidez

TERCERA PARTE: EL FUTURO DE LA CRIPTOECONOMÍA

7. ALGUNOS MITOS Y MUCHAS EXPECTATIVAS

El año Netscape de la criptoeconomía

Desmontando mitos

La punta del iceberg

8. AFRONTANDO RETOS: EL UNIVERSO CRIPTO 3.0

Los grandes desafíos

Escalabilidad

Interoperabilidad

Usabilidad

Volatilidad

Se busca criptomoneda estable para realizar pagos

Blockchains de tercera generación

9. DE LA DISRUPCIÓN TECNOLÓGICA A LA REVOLUCIÓN FINANCIERA

Una casa en el extranjero
El rol de los reguladores
Impactos financieros, impactos globales

EPÍLOGO

Un futuro descentralizado

BIBLIOGRAFÍA

Créditos

¡Encuentra aquí tu próxima lectura!

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

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



Explora

Descubre

Comparte

CARLOS DOMINGO

TODO LO QUE QUERÍAS SABER SOBRE BI-
TCOIN, CRIPTOMONEDAS Y BLOCKCHAIN,
Y NO TE ATREVÍAS A PREGUNTAR

,

¿Ha llegado el dinero digital para quedarse definitivamente? ¿Es la blockchain la próxima revolución tecnológica? ¿Cómo va a afectar en nuestras vidas la llamada criptoconomía?

Casi no queda nadie que no haya oído hablar del bitcoin, las criptomonedas y la blockchain. Sin embargo, continúa siendo un universo sobre el que se mantienen demasiados mitos y que provoca muchas dudas y posiciones encontradas.

Carlos Domingo, una de las voces más autorizadas en esta materia y con un discurso comprensible y bien documentado, arroja luz sobre un tema que cada vez más nos afecta a todos. Desde el convencimiento de que estamos ante una auténtica disrupción, estas páginas nos acercan a la historia del bitcoin y otras criptomonedas de nueva generación y al enorme potencial de una tecnología que va a transformar numerosas industrias y revolucionar el sistema financiero.

A mi mujer Belinda Galiano, por la paciencia que tiene con mis locuras. Y por darme a mis hijos Olivia, Adrián y Mara, lo mejor de mi vida.

PRÓLOGO

LA BATALLA DE LAS IDEAS Y LOS CONCEPTOS TRAS LAS CRIPTOMONEDAS

Es propio de tiempos de cambio acelerados: los avances llegan sin anunciarse. O, mejor dicho, cuando se anuncian es porque ya se están aplicando. Lejos quedan otras etapas en las que íbamos teniendo noticia escalonada sobre los progresos en tal o cual técnica que nos permitiría disfrutar en pocos años de telégrafos, teléfonos, ordenadores personales, Internet o móviles inteligentes. Así fue durante la primera y la segunda Revolución Industrial, también durante los primeros años de las «puntocom», las redes sociales y la digitalización.

Pero la realidad dinámica de nuestros días nos habla, por poner un ejemplo, de la edición genómica a través de sus éxitos reales, no de sus expectativas de futuro; y lo mismo ocurre con avances científico-técnicos relacionados con la comunicación, la ingeniería aplicada o en ocupaciones menos venturosas, como la carrera armamentística en la que la inteligencia artificial permite a los guerreros no humanos independizar sus decisiones de acción. El futuro ya no es un vaticinio, sino el día a día, a veces el ayer.

En esta concepción temporal del progreso se incardina eso que se ha dado en llamar criptomonedas, que por ser la más conocida y extendida, el bitcoin representa ante el gran público con su nombre, sin ser la única. A su vez, la poderosa luz mediática de esta criptomoneda deja en la sombra la tecnología revolucionaria que la sostiene: la blockchain o cadena de bloques. No es tan sorprendente que

no sepamos qué son, sino que no sepamos qué son cuando ya son parte de la rutina de nuestro sistema. Han avanzado rápido y en silencio.

De iluminar esa zona oscura se encarga con énfasis didáctico y rigor técnico Carlos Domingo en el libro que el lector tiene entre sus manos. El autor desgrana su diagnóstico y no esconde su pronóstico: «Tengo claro que esto es el futuro», nos dice.

La aceleración del tiempo histórico ha sido tal que nos vemos impelidos a asumir conceptos nuevos, a normalizarlos en nuestra reflexión privada y conversación pública, sin saber realmente de qué estamos hablando. Conviene detenerse a pensar en la realidad y la potencialidad de las criptomonedas y la tecnología que la sustenta. Además, también es razonable pensar que el público general que lo asumirá y lo disfrutará —o padecerá, si se hace un mal uso—, necesita formarse, saber más y mejor de todo lo que implican estos cambios. La responsabilidad financiera individual es indisociable de la autoformación activa, y este libro, claro, directo y riguroso sobre qué es, qué cambios ha producido y cuáles puede producir la irrupción de las criptomonedas, facilita esta tarea.

Pero no es solo la propia aceleración de ese tiempo histórico la que hace que observemos los cambios con cierto vértigo y actitud recelosa por la exigencia de permanente puesta al día. Por un lado, no hace tanto que hemos sufrido una crisis tan severa que nos llevó a una gran recesión, de modo que los anticuerpos están en guardia ante cualquier innovación del sector financiero y bancario, o todo aquello tangencialmente relacionado con ellos. Por otro, la psicología cognitiva lleva años señalando los fundamentos neurológicos de las resistencias al cambio. Existen inercias que no solo es necesario vencer con argumentos técnicos irrefutables, sino con persuasión y pedagogía y finalmente con la práctica. Este libro también contribuye a ello.

¿Qué hace del bitcoin en particular, y de las criptomonedas en general, algo tan disruptivo? ¿Por qué tantos analistas, líderes políticos y de opinión mediáticos nos alertan de

su naturaleza tóxica y su aspecto de burbuja? Podríamos pensar que existen problemas con los fundamentos tecnológicos, pero como bien explica Domingo, hay pocas herramientas tan afinadas como la blockchain. Además, su aplicación ya va, y seguirá yendo, mucho más allá de las criptomonedas. Es un subyacente de primera. ¿Es su escasa consistencia económica? Tampoco. Las criptomonedas se basan, como las monedas de curso oficial, en la confianza. Desde que Richard Nixon decretara la ruptura del patrón dólar-oro allá por 1971, no ha existido ningún respaldo para nuestros intercambios, y nuestra reserva de valor, distinto al de la promesa del Estado de sustentar las monedas con las que se ejecutan, dinero fiat. Esto es, se basan en la confianza, y algunas veces más bien en la fe en el recto funcionamiento de las instituciones públicas.

Las criptomonedas no son distintas en esto por más que la minería del bitcoin lleva aparejado un coste que lo puede asimilar a la del oro, aunque sí parten de una desconfianza previa: la que sienten —no solo ellos, sino la gran mayoría de los usuarios— hacia las autoridades bancarias públicas y privadas y el monopolio estatal de la emisión de moneda. Y, bien pensado, no es una desconfianza caprichosa. ¿Por qué confiar en unos reguladores que no anticiparon —si es que no alimentaron— la crisis financiera? Por resumir, podemos decir que, en aparente paradoja, las criptomonedas se sustentan en la confianza —como el resto de monedas—, pero nacen de la desconfianza en los emisores y los gestores de la política monetaria. También en cierto valor añadido —su coste de fabricación— superior al mero apunte contable o el físico del papel.

Y entramos aquí en el gran escollo que deberán vencer las criptomonedas y en lo que explica la reacción, a veces sobreactuada, en su contra. Como hemos visto, las criptomonedas suponen una innovación tecnológica, de la herramienta, pero no de su finalidad; esto es, el intercambio de bienes y servicios y la reserva de valor. Sí son, en cambio, un competidor nuevo en un entorno dominado por monopolios de bancos centrales con varios siglos de antigüedad.

Las criptomonedas suponen una innovación técnica para facilitar operaciones económico-financieras, pero también son una disrupción jurídico-política que afecta al núcleo esencial del poder económico y monetario del orden westfaliano del Estado-Nación. De ahí la reacción cauta y, a veces, visceral en su contra desde tantos sectores. El fin del monopolio de la emisión de moneda por parte de los Estados es un problema político y jurídico, no tanto monetario o económico, mucho menos tecnológico.

Quedan incógnitas por resolver, pero no parece que vayamos a tardar mucho en despejarlas dado el ritmo de avances y cambios. En ese reto jurídico-político que mencionamos, está presente su utilización para fines delictivos en eso que se ha dado en llamar la *Deep Web* o Internet profunda. No son, en cualquier caso, problemas exclusivos de las criptomonedas. No obstante, habrá que prestar atención a este potencial uso nocivo del bitcoin que se ha constituido en el principal argumento para exigir su sometimiento al viejo esquema.

Queda por saber si será necesaria algún tipo de regulación. La propia naturaleza libertaria de las criptomonedas nos hace preguntarnos si funcionará eso que el economista Friedrich Hayek llamaba —aunque ya el taoísta Zhuangzi lo mencionara en el siglo IV a. C.— «orden espontáneo» y, por lo tanto, prosperará con independencia de cualesquiera regulaciones. O si operará la positiva «destrucción creadora» que Schumpeter veía en los procesos disruptivos. Será interesante ver de qué lado de la balanza política se inclinarán las criptomonedas. Porque frente a ese «orden espontáneo» y esa «destrucción creadora» de raíz liberal que se acaba imponiendo de abajo arriba frente al caos, la actual mayoría defiende que es necesario imponer una regulación normativista e intervencionista de arriba abajo. El dinero fiat, monopolio del Estado, librará una batalla casi final con las criptomonedas.

Es en esa batalla política de ideas y conceptos —y no de técnica, eficacia y oportunidad— donde se decidirá el futu-

ro de unas criptomonedas, cuyo potencial beneficioso quedan magistralmente explicadas en este libro tan necesario.

JUAN MARÍA NIN GÉNOVA

Consejero Delegado del Banco Sabadell (junio 2002-junio 2007)

Consejero Delegado de CaixaBank (julio 2011-julio 2014)
T_

INTRODUCCIÓN

LA SIGUIENTE REVOLUCIÓN TECNOLÓGICA

El bitcoin, las criptomonedas y la blockchain están de moda. O al menos, en boca de todos. Hoy por hoy me da la sensación de que ya no queda casi nadie que no haya oído hablar, aunque sea coloquialmente, de la famosa moneda digital o la nueva tecnología disruptiva que va a revolucionar el mundo. Además, a las personas nos gusta, sobre todo si algo es tan novedoso, lanzarnos a opinar enseguida sobre las cosas que irrumpen en nuestras vidas con tanta fuerza. De manera que, día sí y día también, nos encontramos en el debate público, ya sea con mayor o menor conocimiento de causa, conversaciones y pronósticos en torno al llamado dinero digital, el bitcoin y otras criptomonedas, y en torno a la tecnología que lo sustenta, la blockchain — lo cual no deja de ser un tanto sorprendente por cuanto entramos en un territorio técnico y económico un tanto complejo para la gran mayoría—.

Lo cierto es que estamos todos manejando una serie de conceptos novedosos y en última instancia bastante complejos que todavía distan mucho de tener unos cimientos bien asentados en nuestros mercados, pero que conforman desde ya un atractivo marco de actuación no exento de controversia. Tal es así que, a la que nos podemos referir como criptoeconomía, la están cortejando ya muchos desde una proliferación de miradas de muy diversa índole y posicionamientos completamente antagónicos.

Esa disparidad de opiniones es fácil de comprobar echando un vistazo a Internet. Tampoco es necesario inda-

gar demasiado, ya que estamos siendo constantemente bombardeados con noticias y artículos al respecto que, por un lado, nos dibujan un prometedor universo de posibilidades, pero por otro nos advierten de que todo esto no es sino una burbuja o un fraude —tal y como afirmó, haciéndose enseguida famosa esta interpretación, el consejero delegado de J. P. Morgan, Jamie Dimon. Más adelante se arrepintió públicamente de haberlo dicho—, una suerte de esquema Ponzi que va a terminar estallando, de manera que los bitcoins y otras criptomonedas, como algo puramente especulativo, van a dejar de tener el más mínimo valor.

El entusiasmo por parte de los primeros es significativo, rozando lo religioso: nos tratan de demostrar que esta no solo es la mejor inversión financiera que podíamos haber hecho en los últimos años, sino que todo este fenómeno que ahora apenas empieza a emerger representa la siguiente revolución tecnológica por llegar comparable a la propia irrupción de Internet, la nueva Internet del valor y la nueva Internet descentralizada. Para sus defensores, va a ser capaz de transformar no solo el dinero, la industria financiera y los mercados de capitales tal y como los conocemos en la actualidad; además, va a dar lugar a una nueva Internet descentralizada que rete el control vigente de la misma que tienen los grandes actores como son Google, Amazon, Facebook o Apple.

Frente a ellos, sin embargo, no dejan de alzarse voces agoreras, y no son pocos quienes se dedican a levantar obstáculos para limitar un desarrollo sin trabas de todo lo que concierne a la criptoconomía o a las plataformas públicas de blockchain.

De manera que no cabe sino hacerse la gran pregunta: ¿quién lleva razón? No voy a andarme con rodeos: yo tengo claro que esto es el futuro. Seguramente a mucha gente le atraerá la parte especulativa de la cuestión como vía para enriquecerse, dado el asombroso crecimiento de valor que, a pesar de ciertos altibajos y una gran volatilidad, ha experimentado el bitcoin y otras criptomonedas en menos de