CRIPTOMONEDAS, CRIPTOACTIVOS, BLOCKCHAIN, NFT, WEB3, DEFI

TEODORO GARCÍA EGEA

PRÓLOGO DE JUAN COSTA

₵RIPTO ECONOMÍA

MÁS ALLÁ DE BITCOIN: OPORTUNIDADES DEL NUEVO SISTEMA FINANCIERO

30 AÑOS

LID

Índice

Agradecimientos

Un libro escrito con conversaciones

En el verano de 2022 escuché cómo mi hija de siete años explicaba a una amiga qué es un bitcoin. En ese momento comprendí que tenía el apoyo de mi familia para avanzar con esta aventura. Quiero comenzar dando las gracias a mi mujer y a mis hijos porque, sin conocer profundamente el ecosistema cripto, me han acompañado y apoyado como siempre han hecho desde que estamos juntos. También quiero dar gracias a mis padres porque me han ayudado y apoyado en todo lo que he hecho en estos 37 años sin hacer muchas preguntas.

Mi vida siempre ha estado ligada a la tecnología. Aprendí a utilizar la línea de comandos de MS DOS antes que a poner bien las tildes. Entendí que estudiar ingeniería de telecomunicaciones era el desarrollo natural de mi vida. Por eso quiero dar las gracias a las muchas personas que a lo largo de estos años me han ayudado a avanzar en mi formación tecnológica. Estoy convencido de que las vocaciones científicas se forman de forma temprana; por eso intento inculcar en mis hijos el valor de la curiosidad y de la inquietud por aprender cosas nuevas cada día y de vivir una vida con propósito.

Este libro se ha construido a base de conversaciones. No solo quiero agradecer a todos aquellos que me han enseñado lo que sé, sino que quiero dar las gracias muy especialmente a todos aquellos que han escuchado pacientemente mis explicaciones sobre lo disruptivo que será el mundo con la llegada de la criptoeconomía sin entender nada de lo que hablaba. Gracias a todos aquellos que han aguantado estoicamente mis apasionadas conversaciones sobre tókenes, NFT, *exchanges* y algoritmos de consenso. Me han ayudado

mucho a conseguir mejorar mis explicaciones, crear nuevos ejemplos y conseguir desarrollar un tema complejo de forma más sencilla. Han sido especialmente esas personas que, sin tener ningún conocimiento del tema, han puesto todo de su parte para entenderlo quienes me han hecho avanzar. También aquellas que me han cuestionado de forma insistente haciendo razonamientos que, en alguna ocasión, me han puesto en apuros. Desde Eugenio Galdón, a quien agradezco sus análisis siempre certeros, hasta mis compañeros Juan María Vázquez y Juan Luis Pedreño, quienes desde un primer momento vieron el potencial por desarrollar de esta tecnología. Durante mis fines de semana en Murcia exploraba la criptoeconomía en conversaciones con amigos como Alfonso Carrasco, Antonio Beltrán o Javier M. Gilabert. Ellos también me han ayudado a avanzar. También quiero agradecer profundamente a Juan Costa su apoyo para escribir este libro y la visión global que siempre imprime a nuestras conversaciones.

En 2016 comencé a hablar con muchas personas que trabajaban en el ámbito de la *blockchain*. De todas las tecnologías que comenzaban su auge en aquel momento, esta llamó mi atención por encima del resto. A partir de 2017 comencé a dar charlas por toda España, y quiero agradecer a entidades como Cajamar, la Universidad de Sevilla, la Universidad Francisco de Vitoria, UDIMA, UPCT, FOM, Foment del Treball, Binance, Crypto Plaza, el Instituto Atlántico de Gobierno o ENAE Business School que contaran conmigo en estos meses como ponente en alguno de sus cursos para hablar sobre esta tecnología. Ocho años después de mis comienzos en este ámbito, en 2022 el responsable de FOM, Pablo Oliete, me invitó a inaugurar la cumbre de la Industria 4.0 en Valladolid, donde los mayores expertos del sector tecnológico se concentraban para hablar de tecnologías habilitadores. Aquella charla tuvo tal repercusión, que comenzaron a invitarme de distintos foros a participar como ponente repasando el estado de la situación del ecosistema cripto.

A todos vosotros, gracias por vuestro tiempo, porque este libro también lo habéis escrito vosotros a través de nuestras conversaciones.

En uno de estos encuentros me dieron referencias de un lugar especial en Madrid, un lugar en el que se concentraba todo el talento cripto del sur de Europa, una referencia obligada para los amantes de la tecnología en general y de la web3 en particular. Ahí conocí

a Alberto G. Toribio y a Jesús Pérez, fundadores de Crypto Plaza, y todo cambió. Sin ayudas públicas y solo con su talento y su tiempo habían creado un *hub* que conseguía atraer talento y empresas innovadoras en el ámbito cripto mundial. Desde que les conocí, en cada conversación con Jesús y Alberto sentía que aprendía tanto como en un programa corto de una escuela de negocios. Posteriormente tuvieron el apoyo de un referente del sector tecnológico y el emprendimiento en España, Carlos Barrabés, creando Crypto Plaza Tech by Barrabés y comenzaron a crecer. Gran parte de las reflexiones de este libro provienen de conversaciones con el ecosistema de Crypto Plaza. En el futuro, este espacio será reconocido como uno de los mayores casos de éxito en materia tecnológica en el ámbito europeo. Ellos fueron capaces de ver cosas que nadie veía en España.

Quiero dar las gracias especialmente a las personas que me han acompañado en la aventura de escribir este libro. A Daniel Romero-Abreu y al excelente equipo que ha conseguido forjar entorno a Thinking Heads. Gracias a Irene Alonso y a Elena Valerio por su ayuda y confianza desde el principio en que este proyecto merecía la pena. Sin su ayuda y sus consejos no hubiera podido finalizarlo con éxito.

Sin conocer personalmente a Manuel Pimentel, siempre he admirado su trabajo y su trayectoria profesional. Fue capaz de dedicar unos años al servicio público como ministro y continuar posteriormente con un apasionante y exitoso proyecto empresarial en el mundo de los libros. Una de las mejores cosas de escribir esta obra ha sido poder conocerlo, aprender y compartir tiempo con él. Ha conseguido crear un gran equipo de profesionales a su alrededor y ha sido un lujo compartir tiempo con personas de la talla humana y profesional de Gema Díaz Real y Laura Madrigal. Espero que este libro sea el primero de muchos sobre un tema que está captando la atención cada vez de más personas.

Prólogo

Madrid, otoño de 2012. Eran las 8 de la tarde y lloviznaba. Un buen amigo del Ministerio de Economía me había invitado a cenar con un grupo de diputados y jóvenes asesores parlamentarios. En España 2012 fue uno de los peores momentos de la crisis financiera. La economía retrocedió un 2.9 %, se destruyeron 850 000 empleos y el sistema financiero acabó con un rescate de más de 100 000 millones de euros.

La innovación financiera y la política monetaria de principios de la década de 2000 permitieron a muchas familias acceder al crédito y a una vivienda, pero al mismo tiempo crearon una burbuja en el mercado inmobiliario y en el suministro de crédito que sumió al mundo en lo que se conoció como *la Gran Recesión*. Todavía hoy vivimos las consecuencias de esa crisis que hizo a muchos perder la confianza en el sistema. Una fue la marea de populismo político que hemos vivido en Europa, en EE. UU. y en el mundo en la última década.

Actualmente vivimos una nueva ola de innovación financiera que puede conducirnos al fin del dinero tal como lo conocemos hoy. Y esa ola, al igual que la de innovación financiera que nos llevó a la crisis económica de 2008, puede traer, además de progreso y mejoras económicas, costes y desigualdad. La historia demuestra que la innovación, aparte de ventajas, también puede tener un lado oscuro.

Pero volvamos a Madrid. Entré en El Rincón de José, un restaurante bastante popular cercano al Congreso de los Diputados. Hicimos las presentaciones y allí conocí a Teodoro García Egea. Recuerdo aquella cena muy bien. Hablamos de la crisis financiera, pero también de otros temas, como ecología, tecnología, sostenibilidad y *blockchain*. Yo llevaba dos años trabajando para Ernst & Young (EY) en sostenibilidad. Teo estaba empezando a dar clases en la universidad al tiempo que centraba su trabajo como diputado nacional en el desarrollo de iniciativas para situar a España a la vanguardia de la Cuarta Revolución Industrial.

Durante estos años Teo y yo hemos continuado esa conversación en muchas ocasiones y hemos hablado de cómo la tecnología *blockchain* primero y la criptoeconomía después pueden cambiar la economía global.

La *blockchain* y la criptoeconomía se han presentado como una oportunidad para democratizar y descentralizar el mercado financiero, para limitar el poder de las grandes instituciones financieras y de los países más influyentes de la economía global; un sistema financiero donde los ciudadanos decidan y todos sean iguales y tratados de la misma manera. Los bitcoines y la *blockchain* pueden ayudar a crear un mercado financiero más inclusivo, un sistema de pagos veraz y una economía con menores costes de transacción.

La innovación financiera y la *blockchain* abren también nuevas oportunidades en las economías emergentes. En estos países, una parte amplia de la población carece de acceso al sistema bancario y la descentralización financiera puede hacer más asequible y accesible prestar servicios financieros de ahorro, crédito o seguro a todas las capas de la población.

Fenómenos como la creación de monedas electrónicas por los bancos centrales y la desaparición del dinero físico pueden contribuir también a luchar contra el fraude fiscal, la corrupción y las actividades ilícitas.

Finalmente, la criptoeconomía y las finanzas descentralizadas (DeFi) pueden ayudar a construir mercados globales y contribuir a hacer frente a retos como la protección de la biodiversidad y la lucha contra el cambio climático.

Sin embargo, existen también múltiples desafíos. El poder de la tecnología puede conducir asimismo a una mayor concentración del mercado entre unos pocos sistemas de pago y proveedores de servicios financieros. También existe el riesgo de que algunas grandes corporaciones o grandes economías utilicen las monedas electrónicas como un nuevo instrumento de colonización o dominio sobre economías más pequeñas o menos creíbles.

Por otra parte, las criptomonedas pueden afectar a la demanda de monedas fiduciarias y la capacidad de los bancos centrales para cumplir sus objetivos y tener implicaciones en los tipos de cambio y en la estructura del sistema monetario internacional.

La innovación financiera y la versión digital de las monedas fiduciarias abre además nuevos debates sociales. El anonimato y la

privacidad son principios esenciales en las sociedades occidentales. Si el dinero, tal y como lo conocemos, da paso a medios y sistemas de pagos digitales, el anonimato y la privacidad no solo pueden estar en peligro, sino que también puede comprometerse la credibilidad de los bancos centrales y de las instituciones financieras.

Veámoslo o no, el sistema financiero global se enfrenta a una era de cambio disruptivo. Detrás de ello se encuentra la tecnología, pero también una nueva visión de la sociedad y la economía global.

El efecto de esta nueva ola de innovación financiera puede ser eminentemente positivo. Puede facilitar el acceso al ahorro y al crédito a los más desfavorecidos y también a los emprendedores, quienes ven inviables muchos proyectos por la petición de garantías y colaterales de buena parte de la banca más tradicional. Al mismo tiempo, los pagos y transacciones nacionales e internacionales podrían ser más económicos y rápidos.

Sin embargo, actualmente hay más sombras que luces. La sucesión de fracasos corporativos que ha vivido la industria cripto durante los últimos 12 meses nos alerta de riesgos importantes, especialmente que algunos esquemas puedan acabar dañando a los más desfavorecidos económicamente.

¿Cómo podemos evitarlo? Como apunta Teo en este libro, la regulación no puede ser el único camino. Los gobiernos no están siendo capaces de dar soluciones a muchos de los desafíos a los que se enfrenta la economía global. El sector privado debe desempeñar un papel protagonista en la búsqueda de soluciones. Hoy el mundo debe aceptar que la solución es la cogobernanza. Muchos líderes sociales y empresariales están marcando el camino para construir un capitalismo más justo y liderando la lucha contra el cambio climático, la protección de la biodiversidad y la construcción de una economía más inclusiva. De igual forma, el ecosistema que está liderando la innovación financiera ha de recordar cuál es su propósito, su fin último, y desarrollar un catálogo de buenas prácticas capaces de contribuir a construir un sistema financiero justo e inclusivo.

Juan Costa
Ministro de Ciencia y Tecnología

Introducción

El 6 de julio de 2021 asistí a una charla del vicepresidente del Banco Central Europeo (BCE), Luis de Guindos, en los cursos de verano de El Escorial, en Madrid. Entre el público se encontraban cargos públicos, personas relevantes de la sociedad española y también algunos alumnos de la Universidad Complutense de Madrid. Al final de la conferencia, uno de los estudiantes levantó la mano e hizo una pregunta al ponente: «Sr. Guindos, ¿qué opina de las criptomonedas?». La respuesta resultó inesperada para mí y, seguramente, también para el joven: «Puedes invertir en criptomonedas o puedes ir al casino de Torrelodones. Para el caso, es lo mismo».

Con toda probabilidad, aquel estudiante había analizado la tecnología cadena de bloques *(blockchain)* que hay detrás de los criptoactivos, las ventajas de los contratos inteligentes o las oportunidades de las finanzas descentralizadas (DeFi) y buscaba una reflexión en profundidad del ponente. Por eso imagino que no esperaba que Luis de Guindos, un referente en el ámbito económico, respondiese como lo hizo.

A mí me sorprendió que un economista tan brillante tuviera esa concepción de las posibilidades de las criptomonedas. A raíz de su comentario, me pregunté cuántos economistas, políticos, empresarios, asesores financieros, etc., compartirían su punto de vista y si estaría más basado en un discurso imperfectamente construido desde los medios y las redes sociales que en un acercamiento en profundidad al mundo de las DeFi. En ese momento me di cuenta de que la criptoeconomía, las DeFi o la web3 iban a generar una brecha similar a la que supuso la llegada de Internet hace treinta años e iban a dejar a muchas economías atrás por no subirse a tiempo a la revolución del Internet del valor.

Me planteé entonces si intervenir en aquel foro. Cualquiera podría haberse levantado y comparar el casino de Torrelodones

con productos como las participaciones preferentes o las *subprime* vendidas sin la debida supervisión de los reguladores a personas que desconocían sus características. Pero nadie lo hizo, y yo tampoco. Sin embargo, desde ese momento llevo pensando en escribir este libro.

Las criptomonedas, los criptoactivos, los tókenes no fungibles (*Non Fungible Tokens* [NFT]) y, en definitiva, la web3 son conceptos cuyo desconocimiento está generando un gran problema para el futuro de nuestra economía. Los que conocen qué hay detrás de esta tecnología dedican parte de su tiempo a profundizar en las posibilidades que ofrece. Mientras, los que dudaron de su utilidad desde un primer momento se esfuerzan en desacreditarla. Es la nueva brecha digital, que enfrenta a partidarios y detractores de los criptoactivos; una brecha que se hace visible cuando un joven estudiante hace una pregunta al vicepresidente del BCE y evidencia la existencia de un nuevo mundo complejo que requiere grandes dosis de estudio, un análisis sosegado e importantes conocimientos tecnológicos.

Las siguientes páginas pretenden ser útiles para una gran variedad de público. Aquel que desconoce por completo la tecnología que hay detrás de los criptoactivos puede comenzar a entender por qué estaba equivocado al criticarla; el que es autodidacta en el difícil mundo de las DeFi podrá profundizar sobre conceptos y aplicaciones que le permitan mejorar su bagaje sobre el ecosistema, y, por último, quien conoce bien la tecnología y las potencialidades de los criptoactivos encontrará reflexiones y predicciones sobre su evolución en el futuro.

En definitiva, este trabajo es una llamada a la reflexión tanto para los que atacan las criptomonedas, por si sirve para que se replanteen su posición inicial, como para aquellos que creen que son la panacea. Los primeros podrán seguir atacándolas, pero sabiendo un poco más sobre su funcionamiento, y los segundos entenderán que aún hay mucho camino por recorrer.

1
La criptoeconomía anuncia la llegada de un nuevo mundo

Todo gran cambio tecnológico disruptivo genera cambios irreversibles en todos los sectores de la sociedad, normalmente basados en hechos sencillos. En el caso de la criptoeconomía, la posibilidad de enviar valor entre dos usuarios sin un intermediario abre un mundo de posibilidades. En este capítulo reflexionaremos sobre:

- Las características técnicas que hacen de la tecnología *blockchain* y la criptoeconomía algo disruptivo y no una mera transformación digital.
- La evolución que han venido sufriendo los criptoactivos y los protocolos con los que interacciona.
- ¿Qué hay detrás de las criptomonedas?

A lo largo de la historia, todo avance tecnológico generador de cambios sociales ha sido objeto de ataque. La llegada del telar mecánico provocó un 90 % de desempleo en el sector textil debido a la sustitución de la mano de obra por maquinaria. Este conflicto fue el germen del ludismo, un movimiento que llevó a los artesanos a rebelarse y a destruir las máquinas, a las que culpaban de su situación. Por su parte, la introducción del automóvil cambió radicalmente los métodos de transporte: transformó sectores enteros y obligó a los trabajadores a adquirir nuevas competencias profesionales. La llegada de

Internet, hace ya treinta años, originó una brecha digital que continúa abierta en algunos estratos de la población. La llamada *exclusión financiera* es solo una parte de esa brecha y afecta especialmente a personas de edad avanzada, quienes únicamente contemplan hacer trámites con su banco en una oficina física y rechazan frontalmente los medios tecnológicos no solo por desconfianza, sino también a causa de una forma determinada de entender el mundo.

La expansión de la *blockchain* y la criptoeconomía no estarán tampoco exentas de las dificultades que tuvieron que sortear otras tecnologías disruptivas en el pasado. Sin embargo, hay algo que las diferencia enormemente de cualquier mejora técnica anterior: en este caso no hablamos de comunicarnos, de perfeccionar nuestra movilidad o de ser más productivos, sino de crear «dinero». Y eso, hasta ahora, era competencia exclusiva de los Estados.

1. Un poco de historia

Entre 2020 y 2023 la gran mayoría de la población del mundo desarrollado ha oído hablar de la existencia de los criptoactivos, la *blockchain,* etc. Sin embargo, hemos de remontarnos a 1992 para encontrar el germen del fenómeno que vivimos hoy: el manifiesto criptoanarquista publicado por el estadounidense Timothy C. May. Según el autor, este movimiento tiene como objetivo la utilización de la criptografía asimétrica para hacer cumplir los principios de privacidad y libertad individual. La criptografía asimétrica es un tipo de cifrado en el que existen dos claves: la pública, que conoce todo el mundo, y la privada, que solo sabe el usuario. La combinación de ambas permite disponer de un sistema de cifrado robusto. Treinta años después de su redacción, el manifiesto demuestra que fue escrito por alguien con una visión de futuro que muy pocos tenían por aquel entonces.

El manifiesto criptoanarquista

Un espectro está surgiendo en el mundo moderno, el espectro de la criptoanarquía.

La informática está al borde de proporcionar la capacidad a individuos y grupos de comunicarse e interactuar entre ellos de forma totalmente anónima. Dos personas pueden intercambiar mensajes, hacer negocios y negociar contratos electrónicos sin saber nunca el nombre auténtico o la identidad legal de la otra. Las interacciones sobre las redes serán intrazables gracias al uso extendido de reenrutado de paquetes encriptados en máquinas a prueba de manipulación que implementen protocolos criptográficos con garantías casi perfectas contra cualquier intento de alteración. Las reputaciones tendrán una importancia crucial, mucho más en los tratos que las calificaciones crediticias actuales. Estos progresos alterarán completamente la naturaleza de la regulación del Gobierno, la capacidad de gravar y controlar las interacciones económicas, la capacidad de mantener la información secreta e incluso la naturaleza de la confianza y de la reputación.

La tecnología para esta revolución (y seguramente será una revolución social y económica) ha existido en teoría durante la última década. Los métodos están basados en el cifrado de clave pública, sistemas interactivos de prueba de cero-conocimiento y varios protocolos de *software* para la interacción, autenticación y verificación. El foco hasta ahora ha estado en conferencias académicas en Europa y EE. UU., monitorizadas de cerca por la Agencia de Seguridad Nacional. Pero solo recientemente las redes de computadores y ordenadores personales han alcanzado la velocidad suficiente para hacer las ideas realizables en la práctica. Y los próximos diez *años traerán suficiente velocidad adicional para* hacerlas factibles económicamente y, en esencia, imparables. Redes de alta

velocidad, ISDN, tarjetas inteligentes, satélites, transmisores de banda Ku, ordenadores personales multi-MIPS y chips de cifrado ahora en desarrollo serán algunas de las tecnologías habilitadoras.

El Estado intentará, por supuesto, retardar o detener la diseminación de esta tecnología, citando preocupaciones de seguridad nacional, el uso de esta tecnología por traficantes de drogas y evasores de impuestos y miedos de desintegración social. Cualquiera de estas preocupaciones será *válida; la* criptoanarquía permitirá la comercialización libre de secretos nacionales y la comercialización de materiales ilícitos y robados. Un mercado computarizado anónimo permitirá incluso el establecimiento de horribles mercados de asesinatos y extorsiones. Varios elementos criminales y extranjeros serán usuarios activos de la CryptoNet. Pero esto no detendrá la extensión de la criptoanarquía.

Al igual que la tecnología de impresión alteró y redujo el poder de los gremios medievales y la estructura del poder social, también los métodos criptológicos alterarán la naturaleza de las corporaciones y la interferencia del Gobierno en las transacciones económicas. La criptoanarquía, combinada con los mercados de información emergentes, creará un mercado líquido para cualquier material que pueda ponerse en palabras e imágenes. Y de la misma manera que una invención aparentemente menor como el alambre de púas hizo posible el cercado de grandes ranchos y granjas, alterando así para siempre los conceptos de tierra y los derechos de propiedad en las fronteras de Occidente, así también el descubrimiento aparentemente menor de una rama arcana de las matemáticas se convertirá en el alicate que desmantele el alambre de púas alrededor de la propiedad intelectual.

¡Levántate, no tienes nada que perder excepto tus propias vallas de alambres con púas!

May hablaba del desarrollo de un tipo de tecnología basada en clave asimétrica que permitía construir un mercado líquido para cualquier material. Y lo hacía mucho antes de que el bitcoin tuviera una capitalización de mercado suficiente para considerarse un activo líquido, es decir, que puede comprarse y venderse en cualquier momento al precio fijado por el mercado.

El manifiesto se publicó sin mucho ruido y así se mantuvo durante dos décadas, a pesar de que predijo de alguna forma la brecha social y cultural que iba a provocar la popularización de los criptoactivos. No fue hasta 2009 cuando Satoshi Nakamoto (pseudónimo del creador o grupo de creadores de Bitcoin) publicó un artículo[1] en el que describía un sistema de dinero electrónico completamente descentralizado a través del cual dos personas podían operar sin una autoridad de confianza o servidor central. Los comentarios que la comunidad hizo a aquella propuesta aún pueden leerse en el documento original y prueban el entusiasmo y el respeto por un texto que, ya entonces, intuían que iba a cambiar muchas cosas. Gracias a este artículo nació el bitcoin y los entusiastas del movimiento criptoanarquista recuperaron el manifiesto. Resulta curioso que, unos años después, Nakamoto dejara de publicar en foros y desapareciera por completo. Su identidad sigue siendo hoy un misterio.

A partir de 2009 las criptomonedas empezaron a evolucionar, tanto tecnológica como legalmente. Tras el nacimiento de las criptomonedas, uno de los retos que había que superar era la forma en la que se podían intercambiar monedas fiduciarias por bitcoines. En 2010 tuvo lugar la creación del primer gran *exchange* de criptomonedas, el MTGox. Un *exchange* de criptomonedas es una plataforma de intercambio que funciona exactamente igual que las casas de cambio que podemos encontrar en los aeropuertos para canjear euros por dólares o libras.

En España el bitcoin fue reconocido como objeto de derecho real al tiempo que la Dirección General de Ordenación del Juego consideraba que era dinero. Muchos se preguntarán por qué este órgano directivo del Ministerio de Consumo entró a valorar si este criptoactivo era dinero o no en sus primeros años de vida.

El motivo fue que algunos de los primeros entusiastas de la comunidad quisieron saber cómo consideraban las administraciones públicas las criptomonedas. En concreto, uno de los pioneros en este

ámbito en España, Alberto G. Toribio, creador de la primera *startup* del mundo con bitcoines dentro del capital social, hizo una consulta[2] a las administraciones para saber si una apuesta con bitcoin estaba sujeta a la misma regulación que el dinero. Es decir, si apostar con dinero era lo mismo que apostar con bitcoines. Pero antes de eso, durante la constitución de las primeras empresas dedicadas a los criptoactivos, se constató que esta moneda electrónica era un derecho real. En palabras de los impulsores:

> «Esa definición decía que era un objeto de derecho real. Eso quiere decir que es básicamente como una casa, una silla o una mesa, simplemente es un bien digital que tiene un valor. El hecho de que sea un objeto de derecho real es algo muy interesante, no ocurre con ningún otro bien digital. Para que luego sea objeto de derecho real tienes que tener propiedad exclusiva sobre él y eso no ocurre sobre una foto digital, porque puedes copiarla. Con el bitcoin no ocurre. O lo tienes tú o yo, pero no pueden tenerlo dos personas a la vez, a no ser que hablemos de multifirma, pero no se puede copiar el bien tantas veces queramos como ocurre con una foto. A eso se refiere un objeto de derecho real. En este caso, el bitcoin sí lo es. Fue complicado convencer al notario y al Registro Mercantil de que se trataba de derecho real y esto fue la primera definición jurídica que tuvo el bitcoin».

Una vez constatado que el bitcoin era un objeto de derecho real, el siguiente paso consistió en corroborar que se trataba de dinero. La Dirección General de Ordenación del Juego ratificó esta cuestión:

> «La Ley de Ordenación del Juego dice que si yo apuesto cantidades de cosas que no son dinero, no tengo por qué pagar impuestos. Así que nuestro argumento fue vamos a utilizar bitcoines para el juego en línea, pero nos vas a hacer pagar impuestos en contra de lo que dice la Ley. Entonces la Agencia Tributaria y la Dirección General de Ordenación del Juego dijeron que a pesar de que el bitcoin no es dinero, en este caso iban a actuar como si lo fuese. Este hecho marcó un punto de inflexión».

Estos acontecimientos sirvieron como base para comenzar a plantearse el tipo de impuestos que cabría asignar a activos como el bitcoin, dado que en aquel momento era el único criptoactivo en

el mercado. Fue entonces cuando el Tribunal de Justicia de la UE declaró que el bitcoin podía utilizarse como una moneda convencional y, por ende, su uso debía estar libre de impuestos en todos los países que comprendían la jurisdicción del tribunal[3].

En 2015 Vitálik Buterin y otros colaboradores lanzaron Ethereum, una plataforma o red digital que adoptaba la tecnología *blockchain* ideada por Nakamoto y cuya criptomoneda nativa denominaron *ether*. Crearon entonces la primera oferta inicial de criptomoneda (*Initial Coin Offering* [ICO]), un proceso de financiación mediante el cual buscaban obtener fondos para el propio crecimiento de la red. Para ello, pusieron los tókenes a la venta en el mercado. Este procedimiento lo utilizarían posteriormente muchísimos protocolos (dando servicios dentro del ecosistema cripto) para obtener financiación. De este proceso hablaremos en capítulos posteriores.

Hoy muchas personas creen que la caída en la valoración de los criptoactivos ocurrida a mediados de 2022 es la primera de la historia; sin embargo, en 2015 el bitcoin sufrió un desplome del 50 % en su valoración respecto al dólar, lo que llevó a MTGox, la primera plataforma de intercambio de criptomonedas *(exchange),* a la quiebra debido a la poca liquidez existente en aquellos años y a la insuficiente madurez del ecosistema de *exchanges*. Esto ha ocurrido y seguirá pasando, como ocurrió en el caso de FTX en enero de 2022.

A mediados de la década, las nuevas tendencias se fueron consolidando. Los grandes bancos empezaron a interesarse por la *blockchain* y las consultoras más importantes encargaron estudios sobre las posibilidades que ofrecía esta tecnología como parte de su estrategia de transformación digital. A partir de 2017 se impulsaron proyectos basados en el lanzamiento de tókenes para financiarse y nacieron muchas de los criptoactivos y plataformas que conocemos hoy.

En los últimos años han surgido nuevos conceptos, como los NFT, las finanzas descentralizadas y la web3. El paso de la web 2.0 a la 3.0 lo marca cómo nos identificamos en la Red: en el Internet de la información nuestra identidad está definida por la dirección IP y en el Internet del valor, por un monedero electrónico *(wallet),* que no es más que una cadena alfanumérica que representa una dirección en una red *blockchain* donde se almacenan criptoactivos.

El ecosistema ha pasado de tener menos de 800 000 usuarios en 2009 a contar con más de 40 millones en 2019, un número que se calcula según el de monederos electrónicos activos. La comunidad ha crecido y ya no solo la forman entusiastas de la criptografía, sino una auténtica red de profesionales que desarrollan servicios financieros para los poseedores de criptoactivos. El aumento de los servicios asociados durante los próximos diez años y su adopción por parte de la sociedad en general cambiarán nuestra manera de entender el mundo de la misma forma que nos cambió la popularización de Internet.

2. Del Internet de la información al Internet del dinero

Hace treinta años, la información escrita solo podía intercambiarse en mano. La llegada de Internet, la capacidad de miles de ordenadores interconectados y un lenguaje común con el que hablar (protocolo informático) permitieron a cualquier ciudadano sumarse a la Red e intercambiar mensajes y documentos de manera virtual. No era necesario conocer en detalle el funcionamiento del protocolo TCP/IP, la forma en la que se hacía la conversión analógica/digital o los protocolos de enrutamiento. Una interfaz en un PC era suficiente para recibir un correo electrónico y acceder a la información que otros habían enviado, y también al revés: entrar en Outlook, introducir la dirección de la persona a la que queríamos escribir y darle a Enviar. La tecnología se encargaba de transformar las letras en impulsos eléctricos bajo unas reglas que permitían a los ordenadores entenderse entre sí.

Sobre la base del intercambio de datos en Internet se construyeron empresas como Google o Amazon, las administraciones públicas idearon nuevas formas de relacionarse con los ciudadanos y las redes sociales permitieron a miles de personas ponerse en contacto. Había llegado la web2, la de las redes sociales. Se han construido infinidad de servicios que han hecho evolucionar la forma en la que interaccionamos, compramos, vendemos o pedimos una cita médica. Sin ellos, hoy la vida cotidiana sería más difícil.

De la misma manera, hasta hace poco la única forma de transferir dinero sin intermediarios era entregándolo en efectivo. La llegada

de la tecnología *blockchain* y su desarrollo posterior han permitido que, por primera vez en la historia, sea posible que dos personas que no se conocen y que no tienen garantías la una de la otra puedan intercambiar dinero directamente y con seguridad. Esta es la primera piedra sobre la que se construye el Internet del dinero. Esta es la base de la criptoeconomía.

La llegada de la tecnología *blockchain* ha permitido que, por primera vez en la historia, sea posible que dos personas que no se conocen y que no tienen garantías la una de la otra puedan intercambiar dinero directamente y con seguridad.

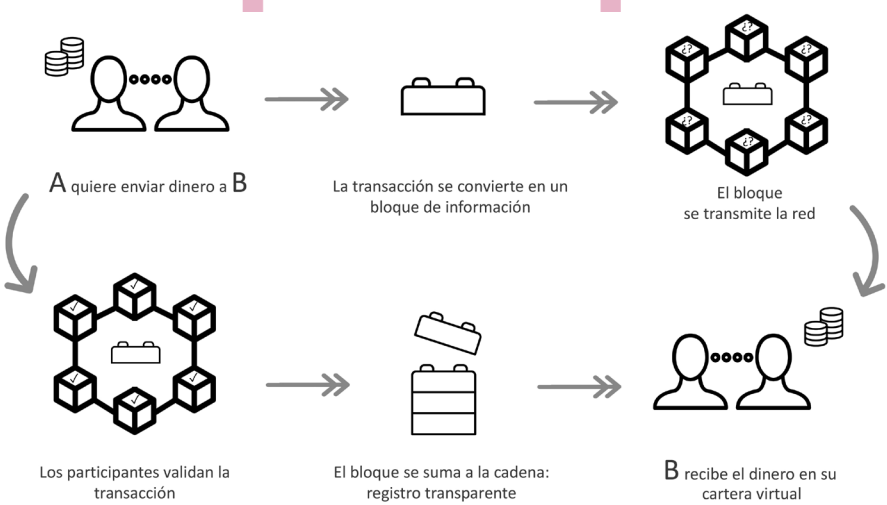
3. ¿Qué es la tecnología *blockchain*?

Hace muchos años que comencé a interesarme por la tecnología *blockchain*. Me atrajo tanto por la sencillez de sus planteamientos como por la complejidad de los desarrollos que podrían generarse a partir de ella.

La tecnología *blockchain,* cuya traducción habitual es «cadena de bloques», no es más que una base de datos descentralizada y recogida en miles de nodos. Para simplificarlo, imaginemos cientos de ordenadores conectados mediante una red. Usaremos estos ordenadores (nodos) para almacenar, por ejemplo, la información de los saldos de los clientes de un banco. En cada terminal hay una copia idéntica de estos datos. Para modificar el saldo de un cliente, tendríamos que cambiar la información en todos los ordenadores con el fin de que siempre fuera idéntica. Este sistema de gestión constituye una *estructura descentralizada* y es la base de la *blockchain,* que utiliza mecanismos de consenso para hacer el cambio en todos los nodos/ordenadores a la vez. Una de sus propiedades es que ofrece mayor seguridad que los sistemas centralizados, donde los datos se almacenan en un único dispositivo.

Por otro lado, las dos características principales de la tecnología *blockchain* son la garantía de la inmutabilidad de la información y la trazabilidad total. La información es inmutable porque es técnicamente imposible modificar un registro sin la clave privada del usuario. Y, una vez registrada en la red, nadie puede cambiarla sin dejar huella, ni siquiera su propietario. Además, todos los datos están unidos entre sí. En cualquier caso, si en algún momento alguien modificara una información pasada, la *blockchain* lo detectaría y no tendría en cuenta el nodo que hizo ese cambio. La trazabilidad total tiene que ver, por su parte, con el concepto de cadena: en lugar de sobreescribir la información y borrar las referencias anteriores, cada cambio (la modificación, la transacción o la introducción de datos inéditos) genera un nuevo bloque que se enlaza con el anterior y se une al histórico, que registra desde la primera hasta la última operación realizadas. Toda esa información se almacena, por tanto, como una cadena de bloques, enlazando continuamente las informaciones anteriores con las nuevas. Si volvemos al ejemplo, diríamos que el saldo de una cuenta forma una *blockchain* en cada uno de los ordenadores conectados. Por esta razón, esta tecnología aporta un valor importante en proyectos donde asegurar la trazabilidad de determinada información es un aspecto clave para el negocio.

Gráfico 1.1 Cómo funciona la *blockchain* para hacer pagos



Aunque hemos puesto como ejemplo el almacenamiento de los saldos de un usuario, sirve para recoger con integridad y trazabilidad cualquier dato que se desee. Los proyectos *blockchain* permiten guardar desde registros de tiempo atmosférico hasta los distintos tipos de viñas que los agricultores suministran a una bodega, de tal forma que se garantiza a los clientes que el vino que están tomando procede de una uva ubicada en una finca concreta. Si una *blockchain* almacena la información desde el origen, ni siquiera el dueño de dicha información podría alterar los registros. De esta forma, el consumidor tiene la certeza de que la trazabilidad del proceso es total. Bodegas como Emilio Moro se han lanzado a utilizar este sistema como experimento con buenos resultados[4].