Índice

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

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].