Camila Russo

LA MÁQUINA INFINITA

Cómo un ejército de *cripto-hackers* crea el Internet del futuro con Ethereum

Traducción del inglés:
Hugo A. Cañete

la esfera de los libros

Índice

PARTE III
EL LANZAMIENTO

PARTE IV
ÓRBITA LUNAR

PARTE V
A PUNTO DE ALUNIZAR

PARTE VI
DE VUELTA A LA TIERRA

Prólogo a esta edición

Vivimos un momento interesante para la criptografía y descentralización. Científicos, ingenieros y matemáticos llevaban más de tres décadas trabajando en su avance sin resultados notables cuando la creación del consenso distribuido en forma de Bitcoin, probaría ser la pieza del puzle que faltaba para el siguiente salto evolutivo de estas tecnologías.

La creación de la primera infraestructura de pagos digital de titularidad privada y descentralizada, basada en la inmutabilidad de los datos, transparencia y resistencia a la censura, marcaría un antes y un después en el uso de redes y ordenadores como herramientas de preservación de la privacidad y defensa de la libertad individual.

Debido a la pérdida de confianza del público en las instituciones derivada de la crisis *subprime*, el año 2008 fue el momento perfecto para que surgiera Bitcoin como alternativa que atraería a aquellos desencantados con los fallos de los sistemas financieros y monetarios tradicionales.

En los primeros años tras su aparición, las narrativas se centrarán en su capacidad como divisa digital y sistema de pago alternativo libre de la injerencia de los poderes establecidos, pero al cabo del tiempo, la idea de utilizar parte del paquete tecnológico subyacente para algo más que la transferencia de valor, pronto caló en la ferviente comunidad de usuarios tempranos que entendían la descentralización como elemento imprescindible para el avance de la «sociedad de la información».

En 2013, un fan de Bitcoin de 19 años prácticamente desconocido, Vitalik Buterin, empezaría a viajar, escribir y compartir detalles de un proyecto sobre el que había estado trabajando, Ethereum, la gran

iteración del consenso distribuido en forma de red descentralizada de Smart Contracts (Contratos Inteligentes), el límite de la frontera tecnológica y abstracción computacional última.

La declinación de la capacidad del consenso distribuido en forma de red donde se pudiera programar o llevar a cabo cualquier cálculo en un sistema Turing Complete, supondría el siguiente salto evolutivo en el estado de la criptografía y descentralización.

De la misma forma en que el anónimo Satoshi Nakamoto hizo historia al crear Bitcoin, Vitalik, hijo de científicos rusos emigrados a Canadá a mediados de los 90 tras el colapso de la Unión Soviética, acabaría lanzando Ethereum para grabar su nombre de forma indeleble en los anales de ciencia y tecnología.

Su visión casi onírica del futuro digital, la consiguiente conceptualización, captación del grupo de jóvenes hackers que le acompañará en el desarrollo y lanzamiento de Ethereum, así como los desvelos por financiar el proyecto y sus rocambolescos inicios, son tan ricos en matices y complejos en su ambición y alcance, que su aventura está a la altura de titanes científicos y empresariales de la talla de Alan Turing, Henry Ford, Steve Jobs o Elon Musk.

En la actualidad Ethereum se ha convertido en la segunda red por capitalización de mercado, solo por detrás de Bitcoin, así como líder indiscutible del desarrollo tecnológico de vanguardia, sustentando una miríada de proyectos, equipos de ingenieros y programadores que avanzan constantemente el estado del arte en forma de aplicaciones descentralizadas, NFTs, protocolos DeFi y demás.

El trabajo de documentación llevado a cabo por Camila Russo y su extraordinaria capacidad para traducirlo en una narrativa fluida, reflejan de forma fiel el poso cultural tecnológico y libertario que sirvió como caldo de cultivo para el surgimiento y desarrollo de estas tecnologías, convirtiendo a *La máquina infinita* en referencia indiscutible sobre la historia de Ethereum y favorita de la comunidad descentralizada, siendo lectura obligada para todos aquellos que estén interesados en la explosión cámbrica digital que promete dar forma al futuro exponencial que en breve nos arrollará.

Francisco Gordillo

Un apunte para mis lectores

No me considero una *nerd* de la informática. No paso horas y horas pegada a mi ordenador haciendo hackeos. Tampoco estoy metida en la especulación financiera. Me encanta verlo desde la distancia y escribir sobre ello. Poner mi dinero —y mi estómago— en esos nauseabundos altibajos, no tanto.

Entonces, ¿por qué pasar años de dedicación a las criptomonedas? La respuesta es, como mínimo, ligeramente diferente para todas las personas a las que he hecho esta pregunta. Para mí, se trata de la libertad. Si me insistes un poco más, podría decir incluso que se trata de una revolución.

La primera vez que supe de Bitcoin fue en 2013. Vivía en Buenos Aires y era corresponsal del mercado argentino para Bloomberg News. Pero no solo estaba informando sobre ello, lo estaba viviendo. Mientras escribía sobre una inflación de doble dígito, los pesos que ganaba por esas crónicas se depreciaban rápidamente. Comencé a cambiar mi salario a dólares tan pronto como me lo ingresaban, hasta el día que la presidenta se levantó y dijo ¡Ni hablar! Ya no puedes hacerlo más.

¿Era posible que el gobierno pudiese prohibir la compra de dólares norteamericanos, algo que había estado haciendo con un simple clic en la página web de mi banco? Fui a comprobarlo y, desde luego, la opción de cambiar los pesos de mi cuenta corriente local a dólares y transferirlos a mi cuenta corriente en el extranjero había desaparecido. Un día estaba allí y al día siguiente ya no. El gobierno estaba depreciando su moneda con políticas populistas y ahora ni siquiera iba a dejarme proteger mis propios ahorros de la mala gestión económica. Y era perfectamente legal. El gobierno lo estaba haciendo.

¿A quién podía recurrir? Por ese tiempo, un colega de otro medio me dijo algo sobre una extraña moneda digital llamada Bitcoin que estaban utilizando los argentinos para solventar el problema. Decidí escribir sobre ello. La gente con la que hablé para mi artículo había estado conviviendo con cierta forma de inflación y/o controles de moneda toda su vida, al igual que sus padres. Entendían lo importante que era poder comprar una moneda que no estuviese controlada por nadie y que, por tanto, no pudiese ser congelada o confiscada. Su tasa de emisión era dictada por algoritmos y código de programación, no por los caprichos de políticos y bancos centrales.

Pensé que esta innovación era increíblemente potente y continué observando Bitcoin y el mercado en auge de las criptomonedas hasta que en 2017 tuve la oportunidad de escribir de nuevo sobre ello. Pero esta vez residía en Nueva York, aún con una corresponsalía de cobertura de los mercados para Bloomberg News, y me di cuenta de que lo de las criptomonedas se estaba animando. Comencé cubriendo este extraño mercado, al principio de forma esporádica, pero a medida que los precios continuaban su ascenso, se emitían más *tokens*, las *startups* de criptomonedas recaudaban millones en segundos y todo el mundo, desde celebridades hasta gestores de fondos y CEO de empresas, hablaba sobre ello, no tardó en ocupar la mayor parte de mi tiempo. Hacia finales de año era evidente que éramos testigos de una auténtica burbuja. Una de las fiebres especulativas más fantásticas jamás presenciadas por el mundo y yo tuve el privilegio de cubrirla desde uno de los medios de comunicación financieros más prestigiosos.

A finales de 2017, cuando hice balance de lo que acababa de presenciar en el sector de las criptomonedas, pensé, esto tiene que quedar documentado. Desde muy joven, mi sueño había sido escribir sobre el mundo real con el drama y la emoción de la ficción. Me propuse encontrar la mejor historia que contar sobre las criptomonedas. Descubrí que, aunque ya se habían escrito algunos grandes libros sobre Bitcoin del tipo del que yo quería escribir, no había todavía una historia de Ethereum, la segunda criptomoneda basada en *blockchain* (cadena de bloques) más importante, culpable de buena parte de la locura del año anterior. Y lo que era más importante, Ethereum era única en el senti-

do de que trataba de llevar la tecnología de *blockchain* en que se basa Bitcoin un poco más allá de lo que lo había hecho la primera criptomoneda. Bitcoin quería ser dinero entre particulares (P2P). Ethereum pretendía serlo todo entre particulares. Quería ser la «computadora mundial» que estuviese detrás de un mundo más libre y descentralizado. Aun en el caso de que fracasase en su ambición, la innovación en sí misma y el frenesí causado eran merecedores de un libro.

Así fue como me propuse escribir el primer libro de la historia de Ethereum.

Para hacerlo, comencé realizando entrevistas al pequeño grupo fundador de esta red, los primeros cofundadores —aunque, en seguida, leerás que existe cierta controversia en torno a ese término—, incluido el propio creador de la plataforma, Vitalik Buterin. Desde las primeras conversaciones, establecí una cronología básica de cómo se había desarrollado Ethereum, los principales hitos y demás cuestiones. Luego busqué a los protagonistas de cada una de las grandes fases del proyecto, aquellos que fueron testigos presenciales de cómo se desarrollaba su historia. Estos me propiciaron el contacto con otros miembros estrechamente implicados que, a su vez, me facilitaron que pudiese hablar con más protagonistas. Luego regresé y volví a hablar con muchos de ellos de nuevo. Así es como, tras dos años de trabajo, con unos seis meses centrada en la investigación a tiempo completo, compilé más de cien entrevistas y muchas más horas de conversaciones grabadas.

También hice todo lo que pude por seguirlos allí donde se reunían. La comunidad de Ethereum vive en todo el mundo por razones obvias, así que las conferencias y los cursos de *hackeo* son especialmente importantes, ya que constituyen las pocas ocasiones del año en las que muchos ven a sus colegas y compañeros *Etherianos* en persona. En alrededor de una docena de eventos a los que asistí en Estados Unidos, Sudamérica, Europa y Asia, tuve la oportunidad de conocer a más gente aún y de obtener una percepción más amplia de cómo es la comunidad, desde los temas de los que hablan a cómo se visten y se divierten. En otras palabras, le vi color —y son un grupo muy colorido—.

Algunas de mis fuentes fueron también lo suficientemente generosas como para compartir conmigo sus correos electrónicos, fotogra-

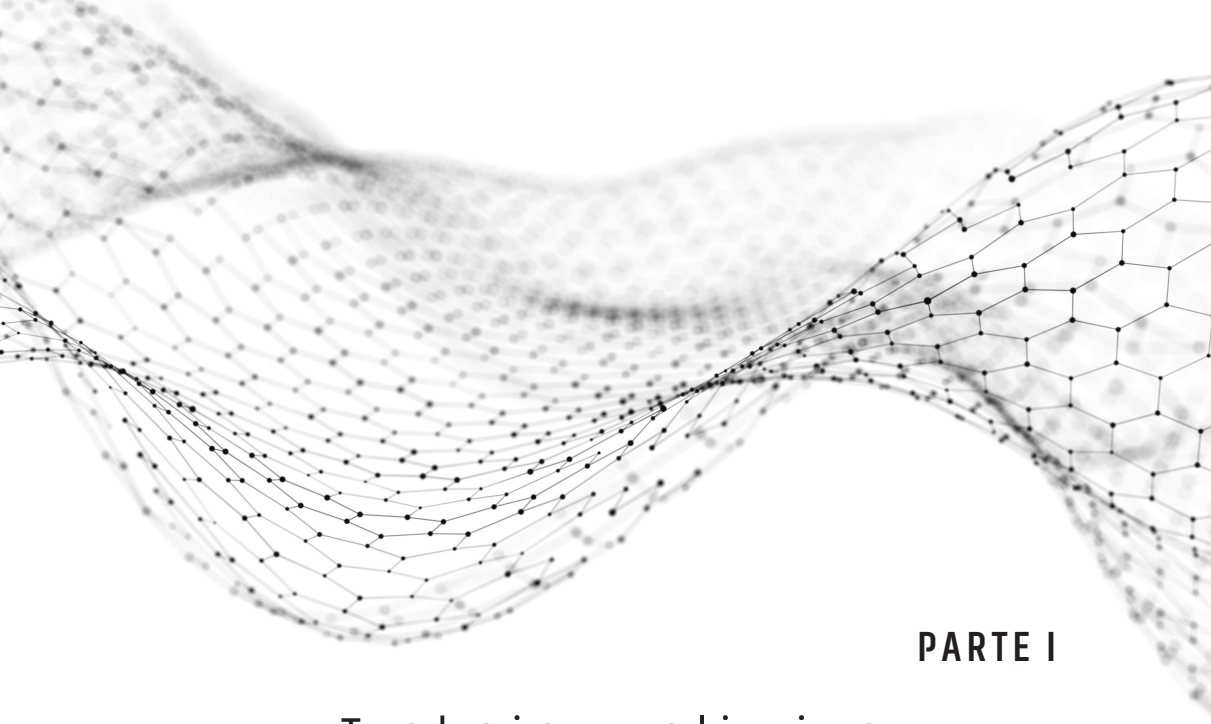
fías, conversaciones de chat y conversaciones grabadas de aquellos momentos. Además, me basé también en otros materiales primarios, como páginas webs archivadas, entradas de blog y vídeos.

Mi objetivo en esta investigación era reconstruir la historia de Ethereum del modo más preciso y cercano posible a la realidad. Todo lo que narro está basado en entrevistas con gente que estaba allí y con material del momento. No he reconstruido ni condensado escenas que persigan el dramatismo. Los elementos más cercanos a la ficción son los diálogos, que elaboré a partir de cómo recordaban los protagonistas de esas conversaciones el modo en que sucedieron los acontecimientos. Todas las personas del libro son reales y los nombres empleados son sus verdaderos nombres. No he creado personajes compuestos, suma de varios, o de ficción. Solo en una ocasión acepté la petición de que utilizase un pseudónimo, al ser un personaje secundario y no tener la exclusión de su nombre un impacto importante en la documentación de la historia de Ethereum. Se hace mención de ello en el libro.

Uno de los mayores desafíos a la hora de escribir esta historia fue decidir una única versión de los hechos cuando los implicados la recordaban de diferente manera. Esto entrañó especial dificultad cuando no había otro material que lo sustentase más que las entrevistas. En esas ocasiones opté por la versión compartida por la mayoría de los participantes y por la que, según mi propia investigación, tenía más sentido. Los lectores tendrán que fiarse de mi juicio en esos pocos casos. Hice todo lo que estuvo en mi mano para tomar esas decisiones de una manera responsable.

Por supuesto, es de esperar que los entusiastas disfruten aprendiendo aún más sobre la red que apoyan y en la que trabajan, y vean cómo se desarrolló desde sus primeros días. Pero si no eres una persona experta en tecnología, como yo, y aun en el caso de que nunca hayas oído la palabra «Ethereum» hasta ahora, este libro es para ti. Mi intención es que cualquiera, en cualquier lugar, pueda adentrarse en él sin ningún conocimiento previo de la tecnología de *blockchain* y quedar cautivado por una historia fascinante: un héroe idealista, su banda de inadaptados sociales y los retos a los que se enfrentan para hacer realidad un sueño increíblemente ambicioso.

Cuando llegues a las páginas finales, espero que hayas aprendido más sobre este sueño, sobre cómo este ejército de *hackers* está construyendo una alternativa al modo en el que funciona el mundo en la actualidad, esto es, concentrado en las manos de unas pocas entidades poderosas. Buscan poner ese poder en manos de la gente, de modo que esta pueda tener un mayor control de las cosas que posee, desde los activos a los datos, y más libertad para hacer uso de ello en el modo que elijan —eso es lo que pretendía decir cuando dije que las criptomonedas son una revolución—. Espero que también aprendas sobre esta tecnología, que, en mi opinión, ha venido para quedarse y será cada vez más relevante en el futuro.



PARTE I

Trabajo preliminar

1

Hasta la Luna

La semana del 11 de mayo de 2018. Nueva York

En una fiesta con abundancia de alcohol y EDM [música *dance* electrónica] en un yate con vistas a la estatua de la Libertad, dos invitados seleccionados al azar fueron agraciados con sendos Aston Martin al final de la noche. Un coche tenía estampada una «B» de Bitcoin en su puerta; el otro mostraba un logo de Ethereum. En otro evento en un almacén de Brooklyn, el sushi servido era publicitado como «parte de la *blockchain*», mientras que el gurú del bienestar Deepak Chopra dirigía sesiones de meditación y un gato digital, vivo solo gracias a las líneas de código y píxeles, era vendido en una subasta de arte por 140.000 dólares. En un local patrocinado por una empresa de criptomonedas, Snoop Dogg se fumó un canuto en el escenario y lo compartió con el público. Los banqueros de Wall Street, convertidos en inversores de criptomonedas, cortejaban a los fracasados de Silicon Valley convertidos en emprendedores de criptomonedas en un ático del barrio neoyorquino del SoHo. En otra fiesta *after*, los entusiastas de Bitcoin levantaron sus copas de champán ante bailarinas en tanga en un célebre club de estriptis del centro de la ciudad, mientras un rapero cantaba canciones sobre la criptomoneda flanqueado por aceitosas barras de estriptis.

Tres Lamborghini aparcados frente al Hilton, cerca de Times Square, daban la bienvenida a unos 8.500 asistentes que habían pagado 2.000 dólares por entrada para tener la oportunidad de ser parte de la fiebre del oro de las criptomonedas. Decenas de veinteañeros, que habían ganado millones de dólares de la noche a la mañana vendiendo

sus propias monedas digitales, ocupaban puestos coloridos y engalanados para el evento.

Todo lo anterior sucedió en un periodo de siete días en una sola ciudad. Era la «Blockchain Week» de Nueva York, en la que se había reunido la comunidad de las criptomonedas para asistir a las fiestas y conferencias que convierten las promesas en fortunas.

De hecho, en esos siete días, dieciséis *start-ups* recaudaron casi 300 millones de dólares mediante un instrumento de *crowdfunding* conocido como oferta inicial de moneda (ICO), con el que cualquiera, de cualquier parte del mundo, puede emitir criptomonedas y venderlas a inversores igualmente repartidos por todo el orbe.

Aun así, el mercado había caído con fuerza después de un repunte espectacular y la pregunta que todo el mundo se hacía era si esa bajada reciente era un retroceso temporal o el principio del fin. La exuberancia estaba impregnada de un tufillo de desesperación, lo que hizo que los desmesurados espectáculos sugiriesen más urgencia aún. La mayoría de las *start-ups* que recaudaban dinero y se presentaban en conferencias no eran más que meras promesas en una página web. Los Lamborghini habían sido alquilados.

El punto álgido había llegado apenas unos meses antes, en diciembre de 2017, cuando el precio de Bitcoin, la primera criptomoneda y la más importante, se disparó hasta casi 20.000 dólares desde un precio de 1.000 dólares a comienzos de año. Los veteranos se tomaron el retroceso con calma, recordando que, desde el lanzamiento de la moneda digital en 2009, su precio había pasado en tres ocasiones por subidas y bajadas exponenciales. Durante esos picos anteriores, Bitcoin había aglutinado la mayor parte del mercado de criptodivisas. Pero esta vez fue diferente.

Ethereum, cuya moneda digital se llama ether, había sido lanzada en 2015 y dos años más tarde su precio se disparaba a mayor ritmo que el de Bitcoin. Había alcanzado un máximo en enero de 2018 de unos 1.400 dólares, desde apenas 10 dólares doce meses antes. Eso significaba que cualquiera que hubiese comprado 10.000 dólares de ether a principios de 2017 y los hubiese vendido en máximos se había hecho millonario. En cierto punto de la subida, algunos inversores especula-

ron que podía superar a Bitcoin en capitalización de mercado, al tener una mayor tasa de crecimiento que la primera criptomoneda.

Y había una buena razón, argumentaban algunos, para que el ether se disparase hasta la Luna. Ethereum no es solo una red para su moneda digital, el ether. Se pretende que sea la capa base en la que los desarrolladores creen cualquier aplicación que puedan soñar, incluida la emisión de su propia moneda. Todo lo que tenían que hacer era introducir unas cuantas líneas de código y ya podían acuñar criptomonedas y cambiarlas por bitcoins o por ether, que podían ser cambiados a continuación por dólares —el llamado mecanismo de financiación ICO que eliminaba las barreras entre aquellos que buscaban recaudar dinero y los que deseaban emplearlo para acceder a la posibilidad de hacerse rico—. Gracias a esta novedosa forma de recaudar dinero fueron surgiendo miles de nuevas monedas que intensificaron el frenesí del fenómeno cripto.

Los inversores —en realidad, cualquiera con una conexión a Internet— no dejaban de meter dinero en estas criptomonedas y en los jóvenes desarrolladores que las diseñaban. Las ICO habían finalizado en el transcurso de minutos, en ocasiones de segundos —esa era la rapidez con la que estas *start-ups* de tecnología de *blockchain* alcanzaban sus objetivos multimillonarios—. No había mucho que puedas hacer con estas monedas, que solo existen en Internet y que son negociadas en plataformas online escasamente reguladas. No son aceptadas por la mayoría de los comerciantes y las aplicaciones descentralizadas, o «drapps», para las que fueron diseñadas son todavía experimentales y poco fiables. Pero su uso no era en realidad el objetivo, sino comprarlas antes de que el precio se disparase y luego deshacerse de ellas en el nuevo máximo. Al menos, esa era la teoría.

En 2017, la cantidad de dinero recaudado en las ICO superó por primera vez a la financiación tradicional de capital riesgo para *start-ups* de tecnología de *blockchain*. A finales de 2018 habían pasado casi 10 mil millones de dólares por este mecanismo de *crowdfunding* solo en ese año. Por ponerlo en perspectiva, eso es más o menos lo que recaudaron las compañías en los mercados de valores de Canadá, México y Brasil juntos en ese periodo. Acababa de nacer una nueva forma de reunir

capital para empresas en fase inicial de emprendimiento y una nueva vía para invertir en empresas tecnológicas que antes no estaba al alcance de la gente normal.

A medida que el dinero se acumulaba, algunas criptomonedas más pequeñas se dispararon incluso más rápido que Bitcoin y el ether. De visitar páginas web de seguimiento de sus precios, todo lo que verías serían números coloreados en verde y flechas apuntando hacia el cielo. Todas las líneas de los gráficos eran parabólicas. No parecía importar la moneda que eligieses, cualquiera de ellas multiplicaba su valor varias veces.

Todo el mundo quería ser un criptomillonario. Las búsquedas de Google para Bitcoin superaban a las de Donald Trump. Las celebridades, algunas de las cuales eran recompensadas por las compañías de criptomonedas anticipando una suculenta retribución, comenzaron a apoyar a las ICO en sus redes sociales. Paris Hilton retuiteó «Deseando participar en la nueva @LydianCoinLtdToken! #ThisIsNotAnAd #CryptoCurrency #BitCoin #ETH #BlockChain», y Floyd Mayweather posteó en Instagram «Voy a ganar una jodida tonelada [$hit T$n en el original] de dinero el 2 de agosto en la ICO de Stox.com».

No solo las celebridades estaban prestando atención. De repente, los grandes banqueros y los CEO de las compañías más cotizadas comenzaron a verter opiniones sobre las criptomonedas y la tecnología subyacente de la *blockchain*. «Creo en ello», dijo Abigail Johnson, de Fidelity Investments. «Es un fraude», dijo Jamie Dimon de JP Morgan. Lloyd Blankfein, CEO de Goldman Sachs, declaró no estar «dispuesto a menospreciarlas», mientras que Warren Buffett, que no se anda con rodeos, dijo que Bitcoin «es probablemente veneno para ratas al cuadrado».

Entre tanto, con millones de dólares en el aire, el regulador se apresuró a ver el modo de lidiar con estos instrumentos novedosos, si es que se daba el caso. ¿Eran valores? ¿*Software*? ¿Nuevas monedas? ¿Mercancías? Abundan las historias de antiguos fundadores de criptomonedas que huyeron con el botín de su empresa, *hackers* que robaron bitcoins de los monederos digitales de las ICO y las plataformas, y de bots que patrullan las redes sociales tratando de engañar a la gente para

que les envíe sus criptomonedas. Era el ambiente perfecto para los estafadores, los piratas y los rumores estrambóticos.

Y también estaban aquellos que realmente querían crear aplicaciones que cambiasen el mundo utilizando la tecnología de la *blockchain*. Querían construir un mundo que dejase a un lado las instituciones tradicionales y permitiese a los usuarios transferir valor directamente entre sí, sin tener que contar con la intermediación de los bancos o de otros intermediarios. Querían devolver el control del dinero y los datos a los usuarios, en lugar de depositarlos en cámaras y servidores informáticos de entidades centralizadas. Para ellos, la tecnología de la *blockchain* (y Bitcoin y Ethereum) menguarían el poder de las grandes corporaciones que controlan la tecnología y las finanzas, y lo devolverían a las manos de la gente.

Por supuesto, nadie se estaba preparando en realidad para derrocar gobiernos, protestar frente a los bancos o enfrentarse a la policía en las calles. Más bien, se trataba de una revolución basada en la tecnología y la criptografía, que se desarrollaría en un universo paralelo en el que no se aplicaban las leyes financieras tradicionales y todo se estaba construyendo desde cero. Al principio, nadie notaría, o se preocuparía, por estos *hackers* marginados, según su lógica, hasta que fuese demasiado tarde. La revolución había comenzado con Bitcoin y ahora Ethereum presentaba todo un nuevo arsenal en esta lucha subterránea hacia un futuro descentralizado.

Al menos ese era el sueño que tenían muchos de estos desarrolladores cuando lo dejaron todo y se unieron al ejército creciente de Ethereum.

Para escribir este libro me infiltré en ese ejército.

La primera vez que escribí sobre Bitcoin para Bloomberg News fue en 2013, cuando vivía en Argentina y veía cómo las personas ordinarias empleaban las monedas digitales para proteger sus ahorros de la inflación y sortear los controles de moneda. Para cuando me trasladé a la oficina de Bloomberg News en Nueva York en 2017, el término «blockchain» estaba en la boca de casi todo el mundo, hasta el punto de convertirse en una palabra de moda vacía. Por entonces, yo era una de las pocas periodistas de Bloomberg, y de los medios de

comunicación financiera en general, que cubrían el día a día de las criptomonedas y de la *blockchain*. A final de año tuve que darme un respiro después de cubrir una de las burbujas más locas que el mundo haya presenciado. Decidí que esta explosión debía ser documentada con mayor atención y que Ethereum era la historia más importante que contar.

Realicé más de cien entrevistas, de varias horas de duración cada una de ellas, con todos los fundadores y desarrolladores originales que trabajaron en el protocolo en los primeros días y lo que lo hacen ahora. Hablé con inversores, abogados, reguladores, comunicadores, diseñadores e investigadores que también han contribuido a moldear Ethereum. Aquellos que hablaron conmigo fueron lo suficientemente generosos como para ayudarme a aflorar viejos correos electrónicos, registros de chat, documentos y fotografías. También escudriñé a fondo en foros online, entradas de blog y páginas web archivadas. Seguí a este colorido y brillante grupo de idealistas a sus conferencias y «*hackathons*» en Praga, Buenos Aires, Toronto, Berlín, Denver, París, Nueva York, San Francisco y Osaka.

Me sentía como Alicia siguiendo al Conejo Blanco por un mundo de sueños imposibles: banca sin bancos, cría de gatos digitales, empresas autoorganizadas sin directores y hablar de volar a la Luna. Jóvenes desarrolladores desaliñados, sea porque abandonasen módulos de ciencia computacional o dejasen compañías que estaban en la misma orilla de un mismo río, eran los magos que intentaban hacer realidad estos sueños en medio de un remolino de memes de Internet, arcos iris, unicornios y líneas de código informático.

En el centro de este círculo de *nerds* tecnológicos, financieros, inadaptados y renegados estaba Vitalik Buterin, un genio de diecinueve años y *hacker* al que se le ocurrió la idea que acabaría materializándose en Ethereum. Su sueño provocó que una legión de seguidores de diferentes rincones del planeta y diversos y orígenes dispares se uniese a él para hacerlo realidad. Están trabajando en una tecnología destinada a cambiar, en su esencia, el modo en que funciona el mundo y esta gran visión ha atraído a más gente incluso, de modo que en este momento hay varios miles de personas desarrollándola. Hay todavía más que tra-

tan de beneficiarse, de forma legítima o ilegítima, de ella. Tras cinco años en el empeño va camino de cambiar el mundo con la red multimillonaria que ayudó a crear, pero ha sido un viaje turbulento, con ataques maliciosos de *hackers* envidiosos, alucinantes desafíos técnicos, luchas intestinas en el seno del equipo inicial y el atractivo de una riqueza casi obscena, circunstancias todas que amenazan a Vitalik con descarrilar en su búsqueda idealista.

El crecimiento del mercado de las criptomonedas ocupa un lugar destacado en la lista de dificultades. En el punto álgido del mercado en los primeros días de 2018, el valor de los activos digitales se había disparado por encima de los 800 mil millones de dólares desde la cota de 15 mil millones de dólares del año anterior. Miles de nuevas criptomonedas habían surgido en ese tiempo. Pero Vitalik no estaba contento.

«Así que la capitalización total del mercado de criptomonedas acaba de alcanzar hoy los 0,5 billones de dólares. Pero, ¿nos lo hemos ★ganado★?», tuiteó Vitalik el 12 de diciembre de 2017.

«¿A cuánta gente sin bancarizar hemos bancarizado?», escribió, y continuó preguntándose ¿cuántas aplicaciones tienen un número significativo de usuarios o están moviendo grandes cantidades de volumen? ¿A cuánta gente se ha protegido de la hiperinflación? Se preguntó en una serie de tuits hasta qué punto era el impacto de las criptomonedas suficiente hasta ese momento para justificar el tamaño del mercado.

«Definitivamente, la respuesta a todas estas cuestiones no es cero y en algunos casos es bastante significativa», escribió. «Pero no lo suficiente para decir que es un nivel significativo de 0,5 billones de dólares. No lo suficiente».

En el momento en el que este libro va a la imprenta, el valor del ether cotiza por debajo de los 200 dólares, diez veces menos que su récord de principios de 2018. Muchos especuladores han hecho caja, pero los verdaderos devotos como Vitalik y los de su clase continuarán adelante con su versión. Como en generaciones previas de revoluciones basadas en Internet, resulta difícil mantener esa visión pura y prístina. Con demasiada frecuencia se vuelve turbia, confusa y desordenada frente a la realidad. Los visionarios como Vitalik sueñan con viajar

hasta la Luna y más allá, con frecuencia subestimando el empuje gravitacional que pueden ejercer fuerzas mundanas como la ambición, la codicia y el miedo. Resulta que revolucionar los sistemas financieros podría ser más fácil que superar la fragilidad humana. No hay aplicación (o drapp) para eso todavía, aunque sin duda algún genio de la tecnología esté trabajando también en ello en algún lugar.

2

EL SUEÑO FEBRIL DE LOS *CYPHERPUNKS*

En 2008, cinco años antes de que se materializase la idea de Ethereum en un libro blanco (*white paper*), se creó Bitcoin. Pero ni siquiera Bitcoin surgió de la nada. Los criptógrafos habían estado tratando de crear una moneda privada entre particulares (P2P) desde al menos la década de 1980. El científico de la computación David Chaum vio cómo la llegada de los pagos electrónicos podía amenazar la privacidad y centró su investigación en modos de evitarlo. Diseñó el sistema de «firma digital ciega», que permitía los pagos digitales sin tener que facilitar información personal, y empleó esa tecnología en la creación de eCash en 1983, una moneda digital anónima.

eCash no era un sistema plenamente descentralizado. Dependía de los bancos para firmar la moneda digital, de modo que aún podía ser susceptible de censura y corrupción. Aun así, la innovación de Chaum lideró lo que se convertiría en un movimiento. Sus humildes orígenes pueden remontarse hasta una oficina en el área de la bahía de San Francisco, donde un pequeño grupo de científicos e ingenieros de la computación se reunían para hablar de cómo podría contribuir la criptografía a garantizar que la privacidad de los usuarios no fuese violada en los albores de Internet y de los ordenadores personales.

La *hacker* Jude Milhon, más conocida por su seudónimo St. Jude, combinó las palabras «cypher» [cifra] (un modo de encriptar la información) y «cyberpunk» (un subgénero de ciencia ficción que describe mundos altamente tecnológicos en los que la sociedad se ha desmoronado) para bautizar a este grupo emergente como los «cypherpunks». Para los *cypherpunks*, la criptografía sería la herramienta con la que lograr un mayor cambio social y político. Algunos de ellos abogaban

incluso por la criptoanarquía, una creencia según la cual la criptografía haría posible un mundo libre del control de las corporaciones o del estado. La tecnología sería «la cizalla que corta el alambre de espino que rodea la propiedad intelectual», escribió el criptógrafo Timothy May en el manifiesto. El dinero digital privado entre particulares (P2P) estaría en el núcleo de su ruptura con los bancos y los gobiernos.

Poco después de las reuniones iniciales se creó una lista de correo para que el debate pudiese ampliarse más allá de San Francisco, y creció rápidamente conseguir cientos de suscriptores.

Mientras los *cypherpunks* continuaban adelante, también crecía el movimiento de *software* de código abierto, que también influiría en el desarrollo de la tecnología de la *blockchain*. Supuestamente, todo comenzó gracias a una impresora atascada en el Instituto de Tecnología de Massachussets a finales de la década de 1970. Richard M. Stallman, un programador de plantilla de la universidad, había escrito código para la impresora del laboratorio, que estaba en otra planta, con el fin de ahorrar tiempo haciendo que la máquina enviase un mensaje al ordenador principal del laboratorio cuando la impresora se atascase. Eventualmente, la impresora fue sustituida y cuando Stallman trató de aplicar el mismo *hack*, descubrió que no podía modificar el código porque era información con derechos de propiedad.

En 1983, Stallman respondió con la creación de un sistema operativo llamado GNU, que sería libre y accesible para todo el mundo. A continuación, Stallman fundó la Fundación por el Software Libre [Free Software Foundation] y la Licencia General Pública GNU, que declaraba que cualquiera era libre de utilizar, copiar, distribuir y modificar *software* creado con esa licencia. El único requisito era que los cambios en el código tenían que ser compartidos. Linux, un sistema operativo que funciona con licencia GNU, comenzó a despegar a mediados de la década de 1990.

En 1997, Eric S. Raymond publicó el ensayo «La catedral y el bazar», comparando dos modelos de desarrollo de *software*: la catedral, donde el desarrollo de código está restringido a un grupo exclusivo de desarrolladores, y el bazar, donde el código es público y se desarrolla en Internet. El ensayo fue considerado el empujón final para que

Netscape publicase el código fuente de su navegador web Mozilla en 1998. En las décadas que siguieron, el código abierto siguió creciendo y dio lugar al sistema operativo móvil más popular del mundo con Android, al igual que empresas multimillonarias como Red Hat y Git-Hub, mientras que Linux es empleado en la actualidad en la mayoría de los servidores. «El *software* está destinado a ser gratuito» sigue siendo un grito de guerra para programadores de todo el mundo.

Por ese tiempo, en 1999, se lanzó Napster. La página web, ya desaparecida, permitía a los usuarios compartir archivos digitales entre una red de participantes, posibilitando la disponibilidad gratuita de cientos de miles de canciones en MP3 en cualquier parte del mundo. Entonces, en 2001 se lanzó BitTorrent, posibilitando para películas y archivos de mayor tamaño lo que Napster había hecho con la música. Podría decirse que popularizaron las aplicaciones entre particulares (P2P). Las redes P2P conectan nodos que ostentan los mismos privilegios, permitiendo a los usuarios compartir y transferir datos sin necesidad de una entidad administrativa centralizada. Los sistemas que emplean esta arquitectura son resilientes contra la censura, los ataques y la manipulación. Igual que la hidra mitológica, no hay cabeza que puedas cortar que la mate, fortaleciéndose después de cada ataque.

La visión original de la World Wide Web, tal y como se la imaginó su creador, Tim Berners-Lee, buscaba una mayor similitud a una red P2P que el modo en que funciona hoy en día, esto es, detrás de una serie de cortafuegos y traída a nosotros a través de Google, Facebook y puede que otro puñado de megacorporaciones. Berners-Lee ha lamentado públicamente el estado actual en que se halla la red. La visión original es la que inspiró y motivó a los *cypherpunks*. Querían una red P2P para el dinero.

En las décadas de 1980 y 1990 había problemas primordiales que los *cypherpunks* estaban tratando de resolver antes de poder conseguirlo. Uno es que las monedas digitales, a diferencia del dinero en efectivo, no son más que código informático que puede ser fácilmente replicado y falsificado. El problema, conocido como «doble gasto», puede solucionarse empleando una entidad centralizada que mantenga un registro de las monedas y las autentique, pero el desafío era transferir

valor sin tener que mediar la intervención de un tercero de confianza. Otra cuestión a abordar en sistemas seudoanónimos entre particulares eran los ataques Sybil. Igual que las monedas pueden ser replicadas en un mundo digital, también pueden serlo las identidades. Esto es un problema en una red entre iguales, porque un atacante podría crear un gran número de identidades seudoanónimas con el fin de conseguir una influencia desproporcionadamente grande.

Los investigadores Cynthia Dwork y Moni Naor lograron el primer avance en la resolución de estos problemas cuando inventaron el concepto «prueba de trabajo» en 1993. Prueba-de-trabajo pretende disuadir los ataques o el *spam* en una red requiriendo a los usuarios del servicio hacer algún trabajo, de modo que sea inviable desde el punto de vista económico crear información inútil o maliciosa. Su estudio se centró en la prevención del correo basura al requerir al remitente que gastase cierta cantidad de potencia computacional para solucionar una función o un problema matemático. Cinco años más tarde, el criptógrafo Adam Back propuso una versión de prueba-de-trabajo llamada Hashcash, que empleaba funciones criptográficas Hash para probar que se había realizado el trabajo.

En 1998, los científicos de la computación Wei Dai y Nick Szabo concibieron B-money y Bit Gold respectivamente. Ambos propusieron esquemas que permitían a una red de usuarios realizar transacciones con dinero digital sin la necesidad de intermediarios, pero estos no fueron nunca implantados al no resolver completamente los problemas de doble gasto y el ataque Sybil.

Para aquellos que vivían en naciones democráticas y desarrolladas, con monedas relativamente estables e instituciones de confianza, la obsesión de los *cypherpunks* por el dinero que no necesita bancos y que está liberado de los controles gubernamentales podría parecer desconcertante. Todo apunta a que se trata de un esquema para narcotraficantes y evasores de impuestos, ¿cierto? Pero en buena parte del mundo la estabilidad y la seguridad financiera no son todavía la norma.

Considérese el caso de Álvaro Yermak, un empleado de banca en una ciudad lejana de Argentina.

La semilla que llevaría a Álvaro a buscar un dinero inmune a los controles gubernamentales o al despilfarro se plantó en diciembre de 2001. Como había estado haciendo durante los seis años anteriores trabajando como cajero en un banco de Tucumán, una región montañosa del norte de Argentina, fichó poco antes de las ocho de la mañana y ocupó su puesto detrás del mostrador. Dio un sorbo a su mate, que se le revolvió en el estómago cuando miró a la puerta. La gente había comenzado ya a hacer cola fuera de la oficina y la inundaría tan pronto como abriese en unos minutos. Tanto él como las otras decenas de cajeros que se sentaban junto a él sabían que sería un día difícil.

Era lunes, 3 de diciembre, y el gobierno argentino había aprobado un decreto durante el fin de semana prohibiendo a los ahorradores retirar más de 250 dólares o 250 pesos por semana y la mayoría de las transferencias de dinero internacionales. En esencia, significaba que los ahorros de la gente quedaban atrapados en el sistema bancario nacional. También drenaría liquidez de la economía, paralizando el comercio y dejando sin ingresos a los que trabajaban en la economía sumergida, alrededor de la mitad de la población.

Era el intento del gobierno de detener una fuga de depósitos, ya que los argentinos, que temían una crisis económica inminente, pretendían sacar sus pesos, comprar dólares y enviarlos, los que pudiesen, a cuentas bancarias en el extranjero.

El país estaba de resaca después de que los gobiernos anteriores hubieran vendido una enorme cantidad de bonos denominados en dólares y su hubiesen lanzado a un frenesí de gasto. El pago creciente de la deuda y el aumento del déficit eran ya insostenibles y el mercado comenzó a temer la llegada de un incumplimiento de la deuda. El peso argentino tenía paridad con el dólar (una equivalencia uno a uno), lo que funcionó para frenar la inflación, pero también hizo que las exportaciones nacionales perdiesen competitividad y se ralentizase el crecimiento. El gobierno de Fernando de la Rúa había prometido al Fondo Monetario Internacional severos recortes en el gasto a cambio de un préstamo que ayudase a sacar del apuro a la economía. Estas medidas provocaron una mayor contracción de una economía ya de por sí deprimida.

Hacia finales de 2001, los argentinos, que ya habían vivido antes los espectaculares altibajos cíclicos, se preparaban para lo peor. Ese fin de semana de primeros de diciembre, el decreto que restringía las retiradas era la confirmación que estaban esperando: había comenzado la crisis.

La multitud se abalanzó hacia el banco y Álvaro miraba con pavor cómo la cola de clientes inquietos se extendía a lo largo de tres manzanas. Todas las personas que venían querían sacar sus ahorros, pero Álvaro no tenía más opción que seguir las nuevas reglas y contestar «Solo puedo darle 250». Aguantó la oleada de insultos y gritos de ayuda lo mejor que pudo. Comprendía a las personas de la otra parte de la mampara de cristal; también él era una de ellas.

Álvaro no había acabado sus grados de economía y tecnología de la información y buscó un puesto de trabajo de menor cualificación en el banco para mantener a su esposa e hijo. Era como muchos otros argentinos de treinta y pocos años, pero, de repente, se había convertido en la cara del desplome de la economía del país. Aquellos que habían decidido que el mejor modo de lidiar con la crisis era dictar lo que la gente podía hacer con su propio dinero se ocultaban en algún lugar del interior de los palacios barrocos gubernamentales de Buenos Aires, como generales cobardes en tiempos de guerra, mientras él era apostado en primera línea.

El país se sumió en el caos mientras todo el mundo, desde los ricos de las urbanizaciones cerradas hasta los pobres de las *villas*, marchaba por las principales avenidas, golpeando cacerolas y sartenes para crear un estruendo metálico. Multitudes furiosas incendiaron cosas y destruyeron todo lo que se encontraron a su paso, particularmente corporaciones extranjeras y bancos.

Álvaro temía ir a trabajar. Fijó sus ojos en los zapatos mientras caminaba junto a la muchedumbre enfadada, tratando de ignorar los insultos cuando alguien se daba cuenta de que trabajaba en el banco. La oficina bancaria mantuvo medio cerradas durante el día las persianas de acero que protegían la entrada, dejando entrar solo a diez personas a la vez. Algunos días, simplemente no abrían.

De la Rúa decretó el estado de emergencia otorgando más poder a las fuerzas armadas, pero todo lo que consiguió fue un clamor aún ma-

yor. La policía recurrió a la violencia, golpeando a los manifestantes y abriendo fuego finalmente. El presidente dimitió el 20 de diciembre y, poco después, un fuerte estruendo ahogó a las miles de personas reunidas cerca de la Plaza de Mayo, frente al palacio presidencial. Miraron hacia arriba y vieron un helicóptero que volaba sobre ellas. La multitud experimentó una subida de adrenalina cuando descendió sobre la Casa Rosada. Presumieron que había venido a por De la Rúa. Se mantuvo muy cerca del tejado del palacio presidencial y en vuelo estático, sin que las palas dejasen de rotar, De la Rúa subió a su interior. Hubo una oleada de incredulidad, mezclada con alivio e ira, y todo lo que podían hacer era abuchear y silbar mientras el helicóptero se alejaba.

El sustituto inmediato de De la Rúa solo duró una semana y Eduardo Duhalde, que le siguió, canceló la paridad peso/dólar y estableció un nuevo tipo de cambio oficial de 1,4 pesos por dólar, devaluando la moneda un 40 por ciento. Todos los depósitos en dólares fueron convertidos a pesos al tipo de cambio oficial, menguando por ende los ahorros. Aun así, la gente seguía sin poder retirar su dinero. Una cuarta parte del país estaba desempleada y la mitad vivía por debajo del umbral de la pobreza.

En ese momento no había muchas opciones para personas como Álvaro, pero la solución estaba en camino.

Los *cypherpunks* habían continuado mejorando sus trabajos anteriores hasta que se produjo un gran paso adelante en octubre de 2008, cuando una persona anónima, o varias, bajo el nombre de Satoshi Nakamoto, enviaron un correo electrónico al grupo. El correo comenzaba: «He estado trabajando en un nuevo sistema de dinero electrónico que es completamente entre particulares (P2P), sin la participación de un tercero de confianza», y contenía un archivo adjunto, un PDF de nueve páginas que exponía el modo en que funcionaba el sistema. Dijo que se proponía resolver el problema del doble gasto empleando una «red entre iguales en la que se realizasen transacciones con sellado de tiempo enlazándolas en una cadena de prueba-de-trabajo basada en *hash*».

En un documento titulado «Bitcoin: A Peer-to-Peer Electronic Cash System [Bitcoin: un sistema de dinero electrónico entre iguales]», Satoshi Nakamoto propuso una red de ordenadores en la que cada

uno mantenía una copia de todo el historial de transacciones de la red, un libro contable con todo lo que posee cada uno. Cualquiera es libre de descargarse el libro contable en su ordenador y unirse a la red. El historial completo de transacciones puede ser consultado por cualquiera, pero los usuarios que hay detrás de las transacciones son seudónimos, identificados únicamente por sus llaves públicas, que son un batiburrillo de letras y números. Solo los usuarios poseen las llaves privadas necesarias para acceder a los fondos vinculados a sus direcciones de Bitcoin, que son de su exclusivo control. Por primera vez, la gente podía ser realmente su propio banco.

Cuando se ejecuta una transacción, es comunicada a todos los ordenadores de la red para que actualicen sus libros contables. Las transacciones se agrupan para formar bloques de datos y una vez que el bloque se ha quedado sin espacio (1 megabyte en la actualidad), los ordenadores compiten por solucionar un complejo problema matemático con el fin de verificar las transacciones, sellar el bloque y registrarlo en sus libros contables.

Esto se hace empleando una función Hash de criptografía, que funciona como una máquina de codificación mágica en la que una entrada de datos de cualquier longitud es convertida en un grupo de letras y números de una longitud fija. Los ordenadores, o nodos, emplean todas las transacciones más recientes y sin confirmar como entradas en la función Hash y tratan de combinarlas con datos arbitrarios de tal forma que el resultado comience con cierto número específico de ceros. Se trata de un trabajo computacional muy intenso y requiere una gran cantidad de energía, pero una vez que los ordenadores hallan la respuesta, es fácil que el resto la verifique. Solo necesitan pasarla a través de la función Hash y verificar que ofrece la respuesta con el número requerido de ceros. Una vez que los nodos acuerdan que el sellado es válido, el bloque es registrado y vinculado a los bloques previos empleando el *hash* aceptado, formándose una *blockchain*, de ahí su nombre.

El ordenador que resuelve el problema en primer lugar recibe monedas y una comisión como recompensa. Las comisiones por transacción rara vez han superado la cantidad de 1 dólar —aunque se han precipitado hasta casi 40 dólares en máximos—. Este proceso, llamado

«minería», necesita unos diez minutos por bloque en la *blockchain* de Bitcoin.

«La adición paulatina de una cantidad constante de nuevas monedas es análoga a la de los mineros de oro que gastan sus recursos para poner oro en circulación. En nuestro caso, lo que se gasta es tiempo de computación y electricidad», escribió Satoshi Nakamoto en el documento.

Para modificar el libro contable, todos los mineros tendrían que estar de acuerdo y hacer el mismo cambio; esa es la razón por la que es muy difícil *hackear* la red.

La innovación tecnológica de la *blockchain* debía crear una red de participantes distribuidos a la que puede unirse cualquiera mediante el empleo de un sistema para la verificación de transacciones, conocido como algoritmo de consenso (prueba-de-trabajo en el caso de Bitcoin), que no requiere la participación de terceros de confianza. Un bloque de datos confirmados contendrá un *hash* criptográfico del bloque previo, que los vinculará y hará prácticamente imposible modificar la cadena.

Bitcoin fue su primera aplicación, pero los mismos principios pueden emplearse para crear diferentes tipos de redes. En el caso de Bitcoin, «Bitcoin» es el nombre tanto de la *blockchain* como de la propia criptomoneda (se utiliza la mayúscula «B» para la red y la minúscula «b» para la criptomoneda), mientras que el ether es la moneda que circula en la *blockchain* de Ethereum. Puede haber algunas cadenas de bloques que ni siquiera tengan su propia criptomoneda aparejada y no hay una única *blockchain*. Cada cadena tendrá sus propias características únicas, por lo que la expresión «en la *blockchain*» que se utiliza hasta la saciedad debería ir acompañada de la siguiente pregunta: «¿en cuál?».

De acuerdo con la filosofía del código abierto, Bitcoin es un protocolo público al que cualquiera puede unirse y que cualquiera puede modificar, o incluso copiar, para crear su propia versión independiente. No obstante, la modificación del protocolo es relativamente compleja y requiere que los desarrolladores del mismo añadan el cambio de *software* y su implantación, y que la mayoría de los nodos y mineros ejecuten esa nueva versión de *software*.

El primer bloque de la *blockchain* de Bitcoin fue minado en 2009 y la cadena ha continuado creciendo desde entonces, confirmando un nuevo bloque cada diez minutos y emitiendo un número decreciente de bitcoins a medida que aumenta la dificultad de minado. El número total de bitcoins que podrá crearse será de 21 millones. Hal Finney, que contribuyó a la investigación de proof-of-work y estaba en la lista de correo de los *cypherpunks*, recibió la primera transacción de Bitcoin de Satoshi Nakamoto. El programador Laszlo Hanyecz hizo la primera compra conocida con la moneda digital cuando compró dos pizzas por 10.000 bitcoins en 2010 (esas pizzas valdrían 85 millones de dólares en el momento de escribir este libro).

No fue una coincidencia que Bitcoin naciese en 2008, el año en que estalló la crisis financiera global. La confianza y la seguridad en el sistema financiero se resintieron después de que la economía estadounidense se sumiese en su mayor recesión desde la Gran Depresión. Los bancos habían concedido hipotecas a gente que no podía pagarlas y habían empaquetado esos préstamos en complicados derivados contra los que podían apostar, todo ello bajo la mirada de agencias de calificación corruptas y reguladores ineficaces; posteriormente, la gran mayoría tuvo que ser rescatada por el gobierno cuando todo se vino abajo.

Satoshi Nakamoto dejó un mensaje en el primer bloque de Bitcoin que se minó que decía:

> *The Times*, 3 de enero de 2009. Chancellor on brink of second bailout for Banks [Chancellor al borde de un segundo rescate bancario].

El texto hacía referencia al titular de la portada del *The Times* de Londres de ese día. Era una prueba de que el primer bloque fue minado ese día o con posterioridad a esa fecha, pero, sobre todo, también proporcionaba una pista de la principal fuente de inspiración de este dinero digital entre particulares. Era un acto de rebelión contra lo que los *cypherpunks* consideraban un sistema con profundos defectos.

Por primera vez en la historia, las personas podían transferir valor en minutos y a todos los continentes sin la necesidad de un intermediario y libres de censura. No había un banco central que emitiese las

monedas y dictase la política monetaria, no se requería una cuenta bancaria y ningún operario de procesos se llevaba grandes comisiones por el cambio de moneda. No había controles de moneda. Todo lo que se necesitaba era una conexión a Internet. El precio de las monedas estaba determinado por un mercado libre y abierto.

Entre tanto, los bancos tradicionales pueden tardar hasta una semana y aplicar comisiones de hasta 50 dólares en una transferencia internacional de dinero; pueden negarse a prestar servicio a negocios con los que no están de acuerdo o simplemente defraudar a los clientes, y los gobiernos pueden devaluar monedas locales mediante la impresión temeraria de dinero nuevo para financiar el gasto, o pueden prohibir compras en moneda extranjera y limitar las retiradas de efectivo.

En 2013 gobernaba en Argentina Cristina Fernández de Kirchner. Las cosas no estaban tan mal como durante el *corralito*, como llamaron a la crisis de 2001, cuando el gobierno prohibió las retiradas de dinero, pero el gobierno argentino volvía a restringir lo que la gente podía hacer con su dinero. Fernández había prohibido que los ciudadanos pudiesen comprar con moneda extranjera al objeto de detener la salida de dólares causada por los problemas recurrentes del país, como la inflación creciente y la devaluación del peso.

Fue entonces cuando Álvaro vio aparecer Bitcoin en las noticias, al haberse disparado en poco tiempo por encima de los 1.000 dólares por primera vez. De inmediato captó el valor de un dinero incensurable y googleó «cómo comprar Bitcoin en Argentina». No tenía muchos ahorros, pero consideró que sería mejor ponerlos en bitcoins que mantenerlos en pesos argentinos. Bitcoin se cotizaba en torno a los 600 dólares cuando hizo la compra y el peso argentino se cambiaba a seis por dólar. El peso se ha devaluado desde entonces un 90 por ciento, alrededor de 60 por dólar en el momento de escribir estas líneas, mientras que Bitcoin ha multiplicado su valor por ocho desde su máximo de 2013, alcanzando en la última cotización unos 8.500 dólares, con muchas oscilaciones intermedias.

Fue por entonces, entre 2011 y 2013, cuando desarrolladores de todo el mundo trataban de utilizar la tecnología de *blockchain* para hacer otras cosas aparte de «simplemente» transferir valor del punto A al

punto B. Estaban construyendo aplicaciones sobre la base de Bitcoin, empleando su código para crear cadenas de bloques separadas, e incluso iniciando sus propias redes de la nada. Exploraban otros usos como la negociación de valores descentralizada, los derechos de propiedad y la identidad. El entusiasmo en torno a estos proyectos y la adopción por parte de algunos operadores catapultó a Bitcoin por encima de los 100 dólares y luego de los 1.000 dólares por primera vez en 2013. Pero los usos prácticos eran todavía inauditos y Bitcoin no tardó en bajar hasta el nivel de los 500 dólares, dejando la mayoría de estos experimentos congelados en el primer invierno de las criptomonedas. Los auténticos convencidos siguieron trasteando y la comunidad Bitcoin continuó creciendo, integrada en su mayor parte por jóvenes con alguna formación en tecnología o económicas y con inclinaciones libertarias. Se reunieron en torno al foro online BitcoinTalk y en Reddit. No importaba que la mayoría de ellos no se hubiesen encontrado nunca en persona o que no supiesen los verdaderos nombres del resto. Para ellos, Bitcoin era algo más que dinero digital. Representaba un sistema de creencias y esos foros eran, a menudo, el único lugar en el que los *Bitcoiners* se sentían comprendidos.

En marzo de 2011, la comunidad ganó un nuevo miembro. Vitalik Buterin tenía diecisiete años y su primer mensaje en el foro de BitcoinTalk decía:

> En materia de economía podría escribir sobre conceptos como los tabúes sociales en torno al dinero y la inconveniencia práctica de pagar algo de menos de 5 dólares con herramientas convencionales como las tarjetas de crédito o PayPal (…) y cómo Bitcoin ofrece una manera de solucionar esto.

Continuaría adelante hasta conseguir el mayor impacto en el ámbito de la *blockchain* desde Satoshi Nakamoto, pero en ese momento solo pretendía escribir para el blog de *Bitcoin Weekly* a cambio de algunos bitcoins. No tenía ninguno y quería conseguirlos.