MUY INTERESANTE

EDICION COLECCIONISTA

BITCOIN

EL ENIGMA DEL CREADOR DE LA PRIMERA CRIPTOMONEDA DEL MUNDO

SHUTTERSTOCK

Bajo un seudónimo indescifrable, alguien diseñó un sistema capaz de desafiar a los gobiernos y a los poderes financieros más grandes del planeta. En 2008, entre líneas de código y correos cifrados, nació una moneda sin dueños y un nombre que nadie ha logrado desenmascarar: Satoshi Nakamoto.

«NO ENTIENDO POR QUÉ LA GENTE ESTÁ TAN OBSESIONADA CON SABER QUIÉN ES REALMENTE NAKAMOTO. TAL VEZ EL PUNTO SEA QUE NO LO SEPAMOS»

Edward Snowden (1983),
exanalista de la Agencia Central de Inteligencia y de la Agencia de Seguridad Nacional de EE. UU.

SHUTTERSTOCK

El mito de la era digital

Aunque vivamos en un mundo que todo lo revela, hay misterios que se resisten incluso al ojo clínico de la tecnología. Satoshi Nakamoto, el nombre que firma la creación del bitcoin, permanece como una sombra lúcida entre líneas de código. ¿Genio solitario, colectivo oculto o mito necesario?

Esta revista, basada en el libro de Benjamin Wallace *Mr. Nakamoto. El enigmático creador del bitcoin* (Pinolia), gira en torno a esta figura enigmática y a la fascinante persecución de su identidad. Pero no se trata solo de analizar el mundo de las criptomonedas, sino de escarbar en los dilemas de la privacidad, del anonimato en la era digital, la revolución descentralizada y los cambios sociales y tecnológicos que plantea el dinero del futuro.

A través de pistas, silencios y espejismos, el lector entra en un laberinto donde convergen criptografía, utopías digitales, paranoias libertarias y comunidades que confunden fe con sistema operativo. Lo que empieza siendo una búsqueda termina siendo un retrato: no del hombre, sino de la era que lo engendró. Sin duda, lo que aquí leemos es una radiografía de nuestro tiempo.

En ese cruce entre anonimato, poder y tecnología se dibuja el pulso de una nueva época. Su silencio es, en sí mismo, un gesto radical, una declaración de intenciones ante un sistema que lo quiere todo visible, etiquetado, clasificado. El anonimato hoy es un manifiesto, por eso, entender a este personaje esquivo es también darse cuenta de que existen individuos que se resisten a entrar por el aro y tienen el valor de desafiar a gobiernos y bancos. Sin ser ejemplo de nada, son carne de mito.

CRISTINA ENRÍQUEZ
SUBDIRECTORA

CONTENIDOS

SHUTTERSTOCK

Es él

Como figura enigmática tras el seudónimo de Satoshi Nakamoto, el creador de Bitcoin permanece en las sombras de la historia financiera moderna. En la imagen, estatua a Satoshi Nakamoto en Budapest, Hungría. SHUTTERSTOCK

Si Satoshi Nakamoto, el inventor del bitcoin que se ocultaba tras ese seudónimo, era quien yo creía que era, no iba a reconocerlo. Probablemente, ni siquiera hablaría conmigo. Y verlo significaba sentarme en un avión durante veinte horas y conducir otras ocho. Pero necesitaba intentar mantener una conversación con él, y tenía que ser cara a cara.

Nakamoto había desaparecido en la primavera de 2011. Me enteré de su existencia ese verano, cuando escribí el primer artículo en *Wired* sobre el bitcoin, la moneda basada en internet que operaba más allá del control de cualquier Gobierno o banco. Doce años después, el creador del bitcoin seguía siendo un desconocido y su enorme fortuna permanecía intacta. Su anonimato y su moderación representaban un desconcertante rechazo al reconocimiento y la riqueza que obtendría si se decidiera a salir de las sombras. En la historia moderna de la ciencia no existían precedentes de alguien que hubiera creado una tecnología revolucionaria y, tras lanzarla al mundo, no se atribuyera el mérito.

EL ÚLTIMO GRAN MISTERIO

Los acólitos del bitcoin, privados de un ser humano de carne y hueso al que venerar, habían conferido al seudónimo un aura legendaria. En 2022 se podía ver a Kanye West bajándose de un Escalade en Beverly Hills con una gorra de béisbol de Satoshi Nakamoto. En Budapest, sus seguidores habían inaugurado la primera estatua de Nakamoto, una representación en bronce de una figura espectral encapuchada. En el archipiélago de Vanuatu, al sur del océano Pacífico, los promotores inmobiliarios vendieron acciones en un paraíso utópico llamado isla Satoshi. Un trío de libertarios compró un crucero fuera de servicio, lo bautizó como MS *Satoshi* y reclutó colonos para la primera sociedad soberana del mundo impulsada por el bitcoin. Más de un compañero tecnólogo hizo campaña para que Satoshi Nakamoto recibiera un premio Nobel.

Pero el enigma de la identidad de Nakamoto desafiaba de manera obstinada cualquier posible solución. Elon Musk y Peter Thiel, entre otros, especulaban sobre el tema. Los obsesionados cazadores de Nakamoto se esforzaban por desenterrar nuevas pistas o recomponer las existentes de una manera más convincente. A estas alturas, se había señalado a más de cien sospechosos diferentes.

La intriga trascendía a la tecnología. En un mundo en el que internet arrojaba luz sobre todos los rincones, quedaban realmente muy pocas preguntas de este estilo sin respuesta. Habíamos descubierto quién era la fuente secreta de Bob Woodward. Por fin conocíamos la prueba del último teorema de Fermat. Nos habían informado de que Thomas Pynchon probablemente comprara sus *bagels* en Zabar's.

Cuando me propuse escribir sobre Nakamoto, no podía prever que, más de una década después, su identidad seguiría siendo el último gran misterio. Habría sido

INCLUSO *60 MINUTES*, CON GRANDES RECURSOS Y UN EQUIPO DE PERIODISTAS DE INVESTIGACIÓN, SE HABÍA DADO POR VENCIDO

aún más ridículo imaginar que el fantasma que se escondía detrás de la primera criptomoneda del mundo, y el afán por desenmascararlo, traerían consigo demandas, una persecución en coche, una recompensa, una fortuna de 75 000 millones de dólares, intentos de extorsión, amenazas de muerte, un equipo SWAT, un suicidio, un traficante de armas fugitivo, un falsificador en serie, una sociedad secreta de paranoicos que se identificaban solo mediante seudónimos, un genio de gran corazón atrapado por una enfermedad en su propio cuerpo, un búnker nuclear en Europa, cadáveres congelados en el desierto de Arizona y un espía británico metido en una bolsa de lona.

ERA ALGUIEN PELIGROSO... TENÍA ARMAS

Los intentos anteriores de desenmascarar a Nakamoto habían fracasado, a veces de manera espectacular. Incluso *60 Minutes*, con recursos incalculables y un sólido equipo de experimentados periodistas de investigación, se había dado por vencido al declarar el desafío como «misión imposible». Sin embargo, ahora, contra todo pronóstico, creía que lo había resuelto.

Estaba nervioso por lo que esto podría significar. El mundo del bitcoin se mostraba hostil hacia proyectos como el mío. Sin embargo, esa no era mi principal preocupación. Cuando descubrí la verdadera identidad de Nakamoto, me sorprendió que no fuera un sospechoso habitual. Se trataba de alguien que había tomado medidas extraordinarias para resultar imposible de encontrar. Y lo que descubrí sobre él era inquietante. No se parecía en nada a la imagen que la gente se había formado de Satoshi Nakamoto. Se había descrito a sí mismo repetidamente como alguien peligroso. Tenía armas.

SHUTTERSTOCK

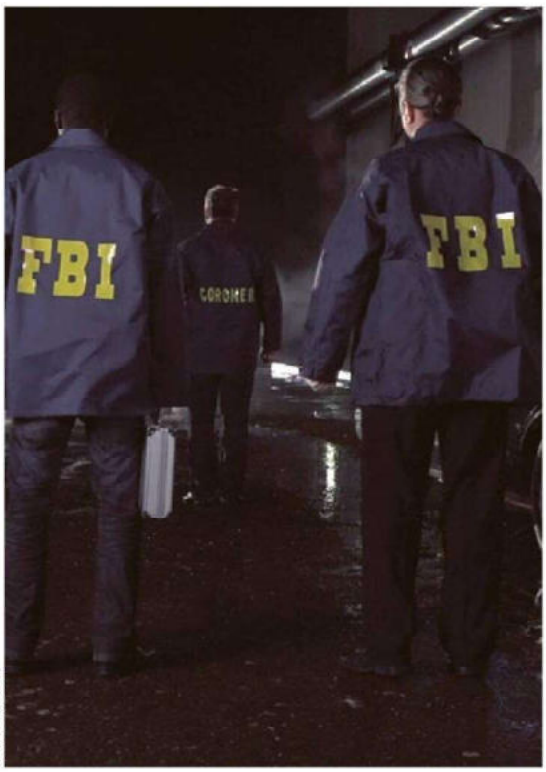
Bob Woodward, afamado periodista de investigación, en el Centro de Política de la Universidad de Virginia, en una entrevista para la CBS.

Billetes que representan a Dorian Satoshi Nakamoto, el ingeniero japonés-estadounidense que fue erróneamente identificado por la revista *Newsweek* en 2014 como el creador de Bitcoin.

EN BUDAPEST ESTÁ LA PRIMERA ESTATUA DE NAKAMOTO, UNA REPRESENTACIÓN DE UNA FIGURA ESPECTRAL ENCAPUCHADA

Antes de volar alrededor del mundo para encontrarme con él, necesitaba estar seguro de que sabía dónde se encontraba. Poseía al menos cuatro propiedades en dos continentes. Al principio pensé que se escondía en una zona remota de la isla de Hawái. Pero últimamente había llegado a pensar que vivía en la costa este de Australia, en una pequeña comunidad costera al norte de Brisbane. Ahora comprendía que tendría que contratar a un equipo de investigadores privados para vigilar la propiedad y confirmar su presencia.

Estaba en medio de todas estas divagaciones cuando quedé con mi hermana para cenar en un restaurante mexicano de Manhattan y le conté lo que había descubierto en mi investigación.



SHUTTERSTOCK

Agencias como el FBI han seguido pistas, analizado patrones, estudiado transacciones para intentar dar con el creador del bitcoin.

—Es él —afirmó con una certeza que yo no sentía.

Mientras mi hermana disfrutaba con calma de su margarita, yo mascullaba mis dudas.

—Es él —repitió.

Le conté mis inquietudes, pues ella tenía más experiencia con este tipo de cosas. Había sido productora de noticias de televisión durante veinte años. Cuando trabajaba en el programa *48 Hours*, estuvo en Montana después de que el FBI allanara la propiedad de Unabomber y lo arrestara.

Me sugirió que fuera acompañado por personal de seguridad profesional, que usara un chaleco antibalas y que avisara a la policía local.

—Gracias —murmuré.

Me sentí un poco mejor. Por lo menos, tenía un plan. La gente de los informativos de televisión hacía esto todo el tiempo. Si ella no estaba preocupada, yo no tenía por qué inquietarme.

Más tarde, esa misma noche, mandé un mensaje de texto a mi hermana: «No puedo dormir, no sé por qué».

Eran las 4:09 de la madrugada.

«Dos ideas: quizá estaría bien que intentaras encontrarte con él en un lugar público, si es que alguna vez sale de casa. Además, alguien, desde una distancia prudencial, debería grabar el encuentro como prueba». ■

Una leyenda en toda regla

La criptomoneda presenta una dualidad insalvable: por un lado, la tecnología que promete democratizar las finanzas y liberar a millones de personas de sistemas bancarios restrictivos, y por otro, el hecho de que se ha convertido en la herramienta preferida para extorsiones, lavado de dinero y mercados clandestinos.

ISTOCK

SHUTTERSTOCK

La teoría que vincula a Elon Musk con Satoshi Nakamoto es una de las más fascinantes en el universo de las criptomonedas. En la imagen, SpaceX, propiedad del sudafricano.

Dieciocho meses antes, en la Nochevieja de 2021, había recibido un correo electrónico con el siguiente asunto: «Nueva información sobre Satoshi». Desde que escribí el artículo para *Wired*, me encontraba periódicamente con correos electrónicos como este. El bitcoin, y la industria más amplia de las criptomonedas que generó, era todavía tan reciente que bastaba con haber invertido algo en 2017 como para que te consideraran un veterano; por eso, los periodistas que habían cubierto la historia en sus primeros años eran ya expertos consagrados y objetivos naturales para cualquiera que tuviera una teoría sobre Satoshi que vender. Y siempre había alguien vendiendo una nueva teoría sobre Satoshi. Por lo general, prestaba poca atención a estos correos. Las noticias sobre Nakamoto reavivaban una fugaz esperanza de descubrir algo nuevo, pero inevitablemente resultaban poco convincentes. Ya me había acostumbrado a la idea de un misterio sin solución. Además, este correo electrónico en particular no me inspiraba confianza porque no estaba firmado. De todos modos, hice clic para abrirlo. No había texto, sino solo un enlace que conducía a una entrada de blog titulada «Soy el becario de SpaceX que especuló con la idea de que Satoshi es Elon Musk. Hay más en esta historia». El autor, Sahil Gupta, había provocado un ligero revuelo en internet cuatro años antes con otra publicación en la que argumentaba que Musk era «probablemente» Nakamoto.

NAKAMOTO ERA UN FAMOSO MISTERIO

Ahora presentaba más pruebas: el relato de una interacción que había tenido con el jefe de gabinete de Musk, Sam Teller. Parecía algo intrascendente y ambiguo, así que no respondí.

Dos días después, recibí otro correo electrónico sin firmar desde la misma dirección. Este contenía un enlace a una página de GitHub, un sitio web donde los programadores de *software* comparten su trabajo, con un análisis detallado del caso de Gupta sobre Musk como Nakamoto. Tal vez porque Musk era ya un personaje fijo en las noticias, durante las semanas siguientes estuve dándole vueltas a la teoría de Gupta. No sabía qué pensar sobre sus argumentos, que se movían entre la ambigüedad y la especialización técnica. Finalmente, escribí a Gupta, que era quien claramente me había enviado los correos. Después de todo parecía que me había escogido para ampliar su historia.

—Gracias por contestar a mi mensaje —dijo Sahil—. He enviado correos a cientos de periodistas.

Estaba en su casa, cerca de San José, y hablábamos por videollamada. Llevaba una camiseta de color magenta y auriculares plateados y en su rostro se dibujaba la sombra de una barba.

—Es increíble lo negativa que es la caricatura que se han hecho de Musk —continuó Sahil, con una energía inquieta—. Piensan que montó una empresa de cohetes y otra de coches por casualidad.

Sahil describió entonces cómo había llegado a descubrir la verdadera identidad de Nakamoto.

En el año 2015, cuando Sahil era estudiante universitario en Yale, estaba impresionado por lo que hacía SpaceX, así que consiguió unas prácticas de verano escribiendo *software* de gestión de inventario en su fábrica de cohetes en Hawthorne,California.

—Fue una experiencia increíble —recordó Sahil.

Musk estaba en la oficina unos tres días a la semana y Sahil lo veía de vez en cuando por los pasillos. Después de un «desmontaje rápido no programado», el término que utilizaba la empresa para referirse a la explosión de uno de sus cohetes, Sahil estuvo presente cuando Musk pronunció un discurso sobre cómo SpaceX sería capaz de mejorar la tecnología para solucionar el problema.

—Un discurso realmente inspirador —me comentó Sahil.

Fue después de que terminara sus prácticas cuando estableció la conexión con bitcoin. Sahil se estaba especializando en Informática y, para su tesis de fin de carrera, colaboró con otros dos estudiantes para proponer una moneda digital del banco central llamada Fedcoin. «¿Y si Estados Unidos pudiera mejorar el dólar tomando los mejores aspectos del bitcoin?», explicaba. En los agradecimientos del trabajo se mencionaba a «Satoshi Nakamoto por ser una auténtica leyenda». Mientras investigaba para la tesis, Sahil se empapó de literatura sobre criptomonedas, empezando por el documento técnico de nueve páginas en el que Nakamoto describió el bitcoin por primera vez. En aquel momento, Sahil supo que la verdadera identidad de Nakamoto era un famoso misterio, y, cuando leyó los escritos

EN 2015, SAHIL GUPTA ERA ESTUDIANTE UNIVERSITARIO EN YALE Y ESTABA IMPRESIONADO POR LO QUE HACÍA SPACEX

del creador del bitcoin, su similitud con el lenguaje que empleaba Musk le llamó la atención. Ambos hablaban de razonamiento de «orden de magnitud» y usaban la palabra maldito. Ambos argumentaban partiendo de primeros principios. Nakamoto hablaba del dinero de forma conceptual, como hizo Musk cuando era ejecutivo en PayPal a principios de la década de 2000. Sahil descubrió que Musk, al igual que Nakamoto, tenía experiencia de programación en el lenguaje C++ y conocimientos sobre economía y criptografía. Nakamoto también había demostrado una especie de abnegación impulsada por una misión.

—Así es Musk —me dijo Sahil.

A partir de todas esas similitudes, empezó a preguntarse: ¿podría ser que el inventor del bitcoin haya estado delante de nosotros todo este tiempo, oculto tras el resplandor de su propia celebridad?

«¿ES ELON SATOSHI?»

Cuando Sahil se graduó en la universidad, decidió que quería trabajar directamente para Musk, en la oficina del director ejecutivo. Después de enviar varios correos electrónicos a Musk, consiguió una entrevista telefónica con Teller, el jefe de gabinete. Sahil le habló a Teller sobre su formación académica, pero este le dijo que no era un buen candidato, pues estaban buscando un asistente administrativo. Además le comentó que con su experiencia estaba capacitado para fundar su propia empresa.

—Fue un buen consejo —dijo Sahil.

SHUTTERSTOCK

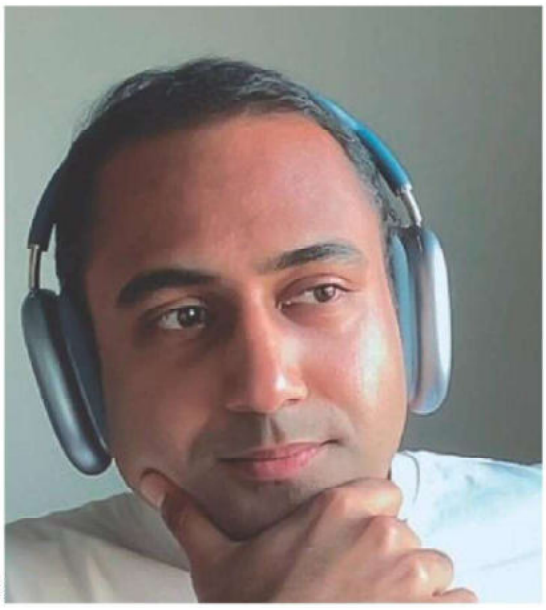
En 2021, Elon Musk reveló que Tesla había comprado millones de Bitcoin y anunció que aceptarían la criptomoneda como pago por sus vehículos.

SAHIL DESCUBRIÓ QUE MUSK, AL IGUAL QUE NAKAMOTO, TENÍA EXPERIENCIA DE PROGRAMACIÓN EN EL LENGUAJE C++

Cuando la conversación estaba llegando a su fin, Sahil decidió arriesgarse: «¿Es Elon Satoshi?».

—Teller guardó silencio durante unos quince segundos. Y luego contestó: «Bueno, ¿qué puedo decir?». Esa respuesta me pareció una buena pista. Para mí, estaba bastante claro, al verse sorprendido por mi pregunta, Teller me dio una contestación bastante reveladora —me contó Sahil.

Meses después, Sahil escribió su entrada de blog «Elon Musk probablemente inventó el bitcoin». Omitió el contenido de su conversación privada con Teller, pero describió los paralelismos que había encontrado. Y argumentó que la comunidad bitcoin, que había estado dividida por las disputas sobre si la tecnología debía abrirse al público general y cómo tenía que hacerse, se beneficiaría del regreso de su fundador para guiarla. Algunos blogs de criptomonedas recogieron la teoría de Sahil y *Bloomberg News* la cubrió. El propio Musk tuiteó: «No es cierto. Un amigo me envió parte de un [bitcoin] hace unos años, pero no sé dónde está». Finalmente Sahil acabó trabajando para Musk, pues fue contratado en 2018 para ayudar a codificar el *software* en la nube de Tesla. Durante el aumento de la producción del Model 3, le pareció emocionante y fascinante ver cómo Musk, desafiando las normas de la industria, ubicaba a los ingenieros de *software* compartiendo espacio con los trabajadores de producción. Musk perseveró en su idea a pesar del escepticismo. Sahil me comentó que su teoría acerca de que Elon era Satoshi no le causó problemas durante su trabajo en Tesla.



ASC

Sahil Gupta (en la imagen) afirmó en un artículo en *HackerNoon* que Nakamoto era probablemente Musk.

—Fui sincero sobre mi postura. Realmente considero que Elon es comparable a Benjamin Franklin. Creo que mi jefe me preguntó una vez sobre mi teoría.

Con el tiempo, Sahil se marchó para montar su propia empresa, dedicada al modelado virtual en 3D para sitios como Shopify. Pero, a medida que pasaban los años y él iba atando cabos, su creencia de que Musk era Nakamoto se convirtió en una convicción. Se encontró con unas declaraciones que Luke Nosek, cofundador de PayPal, había dicho una vez mientras hablaba en un panel en Davos: el objetivo

original de la empresa era desarrollar una moneda libre de bancos. Sahil recibió el soplo de que Musk, al igual que Nakamoto, tenía la costumbre de introducir dos espacios después de un punto en sus escritos. Un colega mencionó que Musk volaba regularmente desde y hacia el aeropuerto de Van Nuys, lo que coincidía inquietantemente con quizá el único fallo de seguridad que Nakamoto había cometido: al principio de la historia del bitcoin, un correo electrónico de Nakamoto a otro desarrollador de *software* reveló inadvertidamente una dirección IP en el norte de Los Ángeles. Sahil se enteró de que los primeros programadores del bitcoin consideraban a Satoshi un «mandón», y Musk ciertamente lo era. ¿Y cuál era el sello distintivo de Musk antes de la era Twitter? Enfrentarse a retos imposibles: hacer que los coches eléctricos resultaran atractivos; hacer aterrizar un cohete sobre una plataforma marina.

¿POR QUÉ NEGARÍA SER NAKAMOTO?

A finales de 2021, Sahil decidió que había llegado el momento de hacer otro esfuerzo público. Nakamoto era ahora visto casi universalmente como un genio benevolente y Sahil sintió que se había abierto una oportunidad para que los medios de comunicación aceptaran finalmente que Nakamoto y Musk eran la misma persona. SpaceX había acoplado con éxito una cápsula a la Estación Espacial Internacional y Musk había sido nombrado recientemente «persona del año» por la revista *Time*. Incluso había tuiteado en broma sobre dogecoin, una criptomoneda meme. Cuando Sahil publicó su nueva entrada en el blog, la que motivó que me enviara a mí y a otros tantos periodistas un correo electrónico, relató por primera vez la historia de su interacción con el jefe de gabinete de Musk.

Ahora, en la pantalla de mi ordenador, Sahil decía que estaba «seguro al 99 %» de su teoría. Atribuía las dudas de los demás a los prejuicios contra Musk.

—Me sorprende que la gente se muestre escéptica respecto a las capacidades de Musk. Eso indica que hay un profundo estancamiento en la sociedad, pues la gente es incapaz de juzgar los hechos con objetividad.

Por mi parte, tenía algunas preguntas. Musk era una persona inusualmente capaz, pero una vez describió 2008, cuando se endeudó, se divorció y vio fallar el lanzamiento del tercer cohete Falcon consecutivo, como el peor año de su vida. Nakamoto había publicado el documento técnico sobre el bitcoin en 2008. ¿Podría Musk haber tenido el tiempo y la energía para crear la primera criptomoneda viable del mundo y luego gestionar personalmente el proyecto de *software* durante casi dos años mientras montaba una industria de coches eléctricos y una exitosa empresa espacial?

Sahil tenía las respuestas. Me dijo que había visto una entrevista en la que Musk recordaba que en 2007 solo dedicaba tres días al mes a Tesla. ¿Y no había mostrado Musk una capacidad prodigiosa para trabajar en varios proyectos no relacionados

EL OBJETIVO DE SAHIL ERA GENERAR «LA PRESIÓN PÚBLICA SUFICIENTE PARA QUE MUSK FINALMENTE ASUMIERA EL MÉRITO»

SHUTTERSTOCK

Si Musk fuera realmente Satoshi, Tesla habría sido la jugada maestra final: usar su propia empresa para darle credibilidad institucional a su creación criptográfica.

al mismo tiempo? Además ya había presentado anteriormente productos revolucionarios a través de un documento técnico. De hecho, en 2013, Musk, sin demasiados alardes, había publicado un documento de 58 páginas en el que describía un nuevo sistema de transporte al que llamó Hyperloop.

De acuerdo, pero Musk lo había hecho bajo su propio nombre, además, estaba claro que no era precisamente una persona humilde, por tanto, si realmente era el creador del bitcoin, ¿por qué negaría ser Nakamoto? Para Sahil, esto no era una contradicción, sino una prueba más de la inteligencia de Musk.

—A diferencia de una empresa que necesita marketing, el bitcoin era más fuerte y podía crecer más rápido, en los primeros tiempos, bajo el aura de un fundador anónimo.

¿Y por qué creía Sahil que era importante compartir el secreto de Musk con el mundo?

—Porque es una historia increíble —me respondió.

Quería que Musk recibiera la gloria que se merecía. El objetivo de Sahil era generar «la presión pública suficiente para que Musk finalmente asumiera el mérito».

Si Sahil tenía razón o no, no sabría decirlo, pero podía entender su obsesión. El bitcoin había alcanzado recientemente un máximo histórico de casi 70 000 dólares por moneda, y el valor de mercado de todos los bitcoins en circulación había superado el billón de dólares. El Salvador había reconocido al bitcoin como moneda de curso legal. En 2011, no parecía tan importante que nadie supiera quién era Nakamoto. Pero ¿cómo era posible que incluso ahora continuara siendo una incógnita?

Seis meses después, dejé mi trabajo para dedicarme a tiempo completo a desentrañar el misterio que me había cautivado por primera vez una década antes. ■

Dinero ficticio de internet

Lo que comenzó como un «experimento de internet» ahora mueve miles de millones diarios en volumen de *trading*, supera el PIB de muchos países y es adoptado por naciones enteras. El «dinero ficticio» se está volviendo más real que el dinero real.

ISTOCK


THIS NOTE IS LEGAL TENDER
FOR ALL DEBTS, PUBLIC AND PRIVATE
SERIES
2003
A
Treasurer of the United States.
100

Has oído hablar del bitcoin? —me preguntó Jason Tanz.

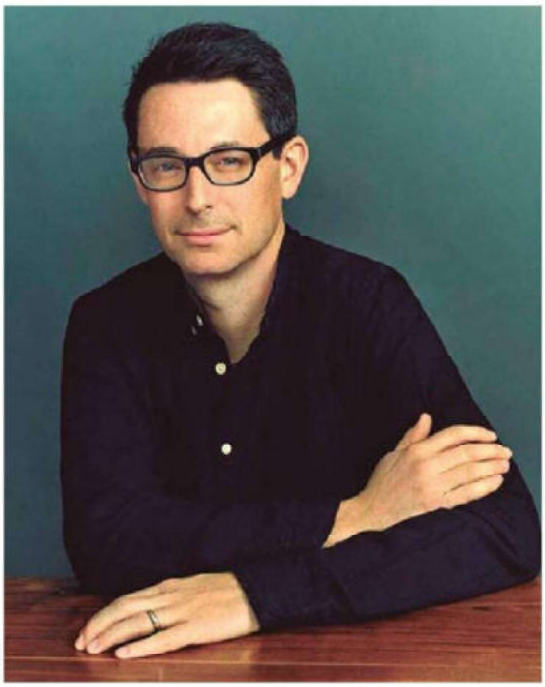
—Sinceramente, no.

—¿Conoces Silk Road?

—Tampoco.

Jason era el director de *Wired*. Era junio de 2011.

Jason mencionó un artículo reciente de Gawker sobre Silk Road, el mercado de la *dark web*, donde el bitcoin, descrito como una «moneda digital imposible de rastrear», era la moneda del reino. Con menos de tres años de vida, ya había trazado un arco de tres actos: desde un proyecto de *software* utópico hasta un improbable mercado de ciento treinta millones de dólares al día, pasando por una red turbia acosada por el crimen, el escándalo y una caída de precios. Pero, con el movimiento Occupy Wall Street a solo unos meses de distancia, parecía oportuno. Jason me explicó cómo el bitcoin era realmente algo nuevo. Los intentos anteriores de crear dinero digital habían fracasado porque la misma característica que hizo revolucionaria a internet (distribución instantánea, sin fronteras y sin una autoridad central) también había dado lugar a lo que se conocía como el problema del doble gasto. Si internet fuera una fotocopiadora y el dinero digital, solo una cadena de bits, ¿qué le impediría a una persona copiar y pegar el mismo bit una y otra vez? El arquitecto del bitcoin, Satoshi Nakamoto, había resuelto ingeniosamente este problema.



WIRED

Jason Tanz, exdirector de *Wired online*. ha escrito artículos sobre la economía colaborativa, criptomonedas...

—¿Te interesa? —me preguntó Jason.

Yo había estudiado Filología Inglesa, no sabía nada de informática y me había incorporado a la era digital con un retraso atroz. Cuando internet empezó a popularizarse en la década de los noventa, me sentí desconcertado: ¿por qué todo el mundo trataba lo que, a mi juicio, no era más que el último de una larga serie de inventos tecnológicos como si fuera algo revolucionario? «No es más que una tostadora», solía decir con sarcasmo.

—Suena increíble —le respondí.

LA IDEA DE UN SISTEMA MONETARIO DESHONESTO EVOCABA EL SERVICIO POSTAL CLANDESTINO DE THOMAS PYNCHON

SHUTTERSTOCK

Moneda conmemorativa que representa uno de los capítulos más controvertidos en la historia del bitcoin: Silk Road, el primer gran mercado de la *dark web*.

LA SUBASTA DEL LOTE 49

The Economist había publicado un análisis detallado del funcionamiento del bitcoin. Fred Wilson, un destacado inversor de capital riesgo, lo había comparado con WikiLeaks y la Primavera Árabe por su potencial para cambiar el mundo. Y la historia era irresistible. La idea de un sistema monetario paralelo y deshonesto evocaba el servicio postal clandestino de la novela de Thomas Pynchon *La subasta del lote 49*. Los partidarios más acérrimos del bitcoin eran una vívida mezcla ciberpunk de hackers, fanáticos del oro, anarquistas y seguidores de Ayn Rand. Y yo estaba cautivado por el enigma de Satoshi Nakamoto.

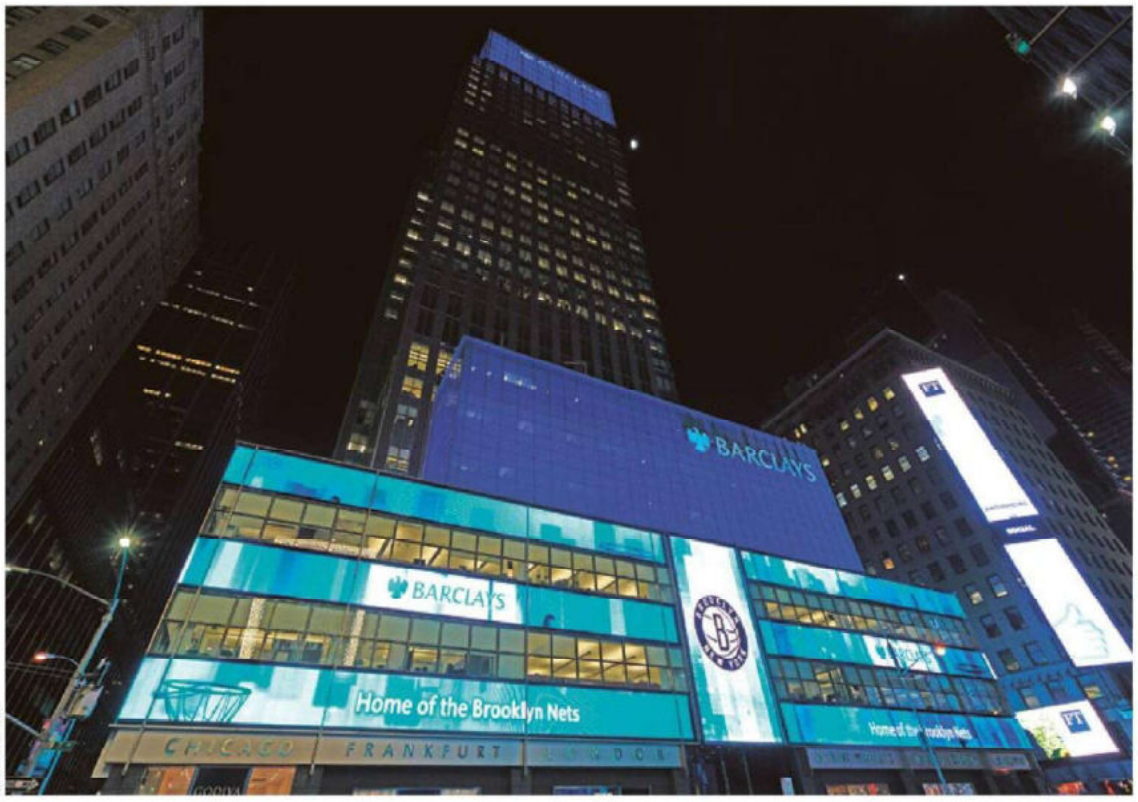
La idea de que, por muy detallados que fueran nuestros mapas, todavía quedaban zonas en blanco, sin explicar, me tenía fascinado. Cuando era niño, guardaba debajo de la mesita de noche un libro de gran formato repleto de ilustraciones salvajes y fotos granuladas en blanco y negro, que era una colección de misterios inexplicables como el monstruo del lago Ness y el Triángulo de las Bermudas. Con el tiempo, mi interés por estas leyendas, con su toque de irrealidad, dio paso a la fascinación por una especie de figura pública que abundaba a finales de los setenta y principios de los ochenta, el icónico fugitivo: terroristas de la Weather Underground o la banda Baader-Meinhof. Partidarios del Tercer Reich escondidos en la selva paraguaya. Patty Hearst, una víctima de secuestro de sangre azul convertida en atracadora de bancos con metralleta. El guerrillero Carlos el Chacal. Escritores alérgicos a los medios de comunicación, como Pynchon y J. D. Salinger. Estábamos rodeados e impregnados por estas historias. Tal vez, como joven lector devoto de cada nueva novela de Robert Ludlum, yo era especialmente impresionable. Pero

ahora, en mi opinión, Satoshi Nakamoto, esta figura esquiva que podría o no existir, había hecho algo más extraordinario que cualquiera de ellos.

Empecé a llamar a gente del mundo del bitcoin y a viajar en metro desde Brooklyn, donde vivía, para encontrarme con ellos. Algunas reuniones tenían lugar en una lúgubre oficina en el quinto piso de un edificio del centro de Manhattan que albergaba una pequeña prouctora de vídeos web cuyo propietario estaba obsesionado con el bitcoin, otras en una cafetería de *bubble tea* cerca de Union Square.

Me enteré de que tres años antes, en Halloween de 2008, Nakamoto había publicado un breve artículo que describía «un sistema de efectivo electrónico entre pares» en una lista de correo electrónico especializada en criptografía, poco conocida y supervisada, que se conocía informalmente como Metzdowd. Su propuesta describía un nuevo tipo de moneda que operaría en una red de ordenadores gestionados por voluntarios, donde cualquiera podría entrar o salir libremente. Resolvería el problema del doble gasto mediante el uso de un libro de contabilidad público y transparente mantenido colectivamente por la red, en lugar de depender de la base de datos de débitos y créditos de un banco o de un Gobierno. Nakamoto incluyó un enlace a una descripción formal más detallada que llegaría a conocerse como «el libro blanco o el documento técnico del bitcoin», pero esa era la idea general.

El momento elegido por Nakamoto para lanzar una moneda alternativa fue muy astuto. En aquel momento, mucha gente estaba enfadada con los bancos: el mes anterior, Lehman Brothers había declarado la mayor quiebra de la historia de Estados Unidos y la Reserva Federal había utilizado el dinero de los contribuyen-



SHUTTERSTOCK

Antigua sede mundial de Lehman Brothers en la ciudad de Nueva York, ahora rebautizada como Barclays Capital.

tes para rescatar a AIG, una de las mayores compañías de seguros del mundo. La descentralización, es decir, la idea de no poner todos los huevos en la misma cesta, era más atractiva que nunca.

VERSIÓN ALFA EN SOURCEFORGE

La elección del foro por parte de Nakamoto para anunciar el bitcoin también fue hábil. Los libertarios con conocimientos técnicos —personas hábiles en informática y hostiles a la autoridad— estaban ampliamente representados en Metzdowd, con su enfoque en la criptografía. Que ninguno de sus suscriptores hubiera oído hablar de Satoshi Nakamoto no le extrañó a nadie. Metzdowd era frecuentado por entusiastas de los fundamentos matemáticos de la encriptación y, por tanto, estaban acostumbrados a los alias.

Algunos miembros de la lista que estaban particularmente interesados en la promesa del dinero digital le dirigieron comentarios sobre el *software* que estaba escribiendo y Nakamoto los recibió de buen grado. «Gracias por plantear esta cuestión», le dijo a una persona. «Agradezco sus preguntas», le respondió a otra en un correo electrónico privado, antes de agregar: «De hecho, hice esto al revés. Tuve que escribir todo el código antes de convencerme de que podía resolver cada problema, y luego redacté el documento». A principios de enero de 2009, Nakamoto lanzó una versión alfa en SourceForge. En aquel momento, era un sitio popular para proyectos de *software* de código abierto, esfuerzos colaborativos que daban la bienvenida a cualquier programador que quisiera participar. El primer día, según uno de los primeros bitcoiner, 127 personas descargaron el *software* bitcoin.

EL DINERO 2.0

Muchos de los primeros participantes eran programadores que pensaban que el dinero tradicional necesitaba una actualización urgente. Los billetes de papel perdían color, se arrugaban, se rompían, se desgastaban, se ensuciaban y encima propagaban gérmenes. Solo estaban disponibles en denominaciones fijas, podían falsificarse y eran difíciles de mover en cantidades significativas. El bitcoin era el dinero 2.0: duradero, infalsificable, divisible casi infinitamente. Podría hacer realidad el sueño del comercio por internet de las microtransacciones. Podrías enviar cualquier cantidad, a cualquier lugar, al instante.

Muchas personas en esa ola inicial tenían convicciones firmes sobre su autonomía personal. El bitcoin, como moneda basada en ceros y unos en una infraestructura digital mantenida por personas normales y corrientes desde cualquier lugar del planeta, era inmune a la intromisión de los poderes centrales. A diferencia de los lingotes de oro, el bitcoin no podía ser confiscado. A diferencia de una cuenta

«TUVE QUE ESCRIBIR TODO EL CÓDIGO ANTES DE CONVENCERME DE QUE PODÍA RESOLVER CADA PROBLEMA»

EN EL CORAZÓN DE LA CREACIÓN ESTABA *BLOCKCHAIN*, UN REGISTRO EN CONTINUO CRECIMIENTO DE TODAS LAS TRANSACCIONES

bancaria, no se podía congelar. A diferencia de una moneda nacional, no se podía devaluar por el capricho de un banco central ni ser sometido a controles de capital por parte de un dictador. A diferencia de las tarjetas de crédito y las transferencias bancarias, no imponía comisiones de transacción excesivas.

Los primeros adeptos solían mostrar una mezcla idiosincrásica de motivos y creencias. Un ejemplo que refleja la singularidad de estos primeros usuarios fue Dustin Trammell, que se hacía llamar Druid en la red. Dustin era un hacker de treinta años al que le gustaba aprender participando; lejos de su ordenador, era un entusiasta del *cosplay*. Había experimentado con monedas alternativas respaldadas por metales, como una llamada Liberty Dollar, y donaba los ciclos de procesamiento sobrantes de sus ordenadores a SETI@home, un proyecto de larga duración de la Universidad de California, en Berkeley, que aprovechaba la potencia de cómputo de miles de ordenadores personales para analizar datos de radiotelescopios como parte de la búsqueda de inteligencia extraterrestre. Después de conocer el bitcoin, Dustin destinó la mitad de esos ordenadores a ejecutar su *software*, solo porque lo consideraba un proyecto tecnológico genial. Más tarde, se interesaría por las ideas monetarias libertarias. Dustin intercambió algunos correos electrónicos con Nakamoto en los que le confesó que «la moneda electrónica y la criptografía son dos cosas que me interesan mucho» y ofreció su ayuda en el proyecto. «¡Definitivamente tenemos intereses similares! —le respondió Nakamoto—. Sabes, creo que había mucha más gente interesada en los años noventa, pero, después de más de una década de sistemas fallidos basados en terceros de confianza (Digicash, etc.), lo ven como una causa perdida. Espero que puedan entender que esta es la primera vez, que yo sepa, que estamos probando un sistema no basado en la confianza».

«PRUEBA DE TRABAJO»

En el corazón de la creación de Nakamoto había algo llamado *blockchain*, un registro en continuo crecimiento de todas las transacciones (compra, venta, etc.) hechas en el sistema. Aproximadamente cada diez minutos, el último lote de registros de transacciones se agrupaba en un «bloque», y el bloque se «encadenaba» al bloque que lo había precedido mediante una ingeniosa matemática que hacía impracticable que alguien pudiera retroceder y manipular el contenido del bloque. Este registro, o libro mayor, que en las finanzas tradicionales sería mantenido por una institución como un Gobierno o un banco, en bitcoin era mantenido por una red de ordenadores de voluntarios, cada uno de los cuales ejecutaba el *software* bitcoin, se comunicaba con los demás ordenadores de la red y almacenaba copias más o menos idénticas y en constante actualización del libro mayor. El precio de

entrada a esta red, para un ordenador, consistía en intentar resolver un acertijo matemático generado por el sistema cada diez minutos. Al igual que los sitios web distinguen a los humanos de los *bots* pidiendo a los usuarios de ordenadores que indiquen cuántos puentes hay en una cuadrícula de fotos de paisajes, este requisito, llamado «prueba de trabajo», disuadía a los agentes malintencionados de apoderarse del sistema. ¿Por qué alguien se molestaría en desperdiciar la potencia de su ordenador en esta extraña actividad? Nakamoto diseñó el sistema de manera inteligente para que el primer ordenador que resolviera cada acertijo recibiera una recompensa de varios bitcoins. De un plumazo, había encontrado una forma de atraer a participantes sinceros y disuadir a los deshonestos, al tiempo que creaba un mecanismo predecible para liberar nuevos bitcoins en la oferta monetaria. Aunque el objetivo principal de la carrera de resolución de acertijos era garantizar la integridad del sistema, acabó llamándose «minería» debido a la recompensa de varios bitcoins. (La enorme energía utilizada por cientos de miles de ordenadores trabajando constantemente para resolver estos acertijos es también lo que le da al bitcoin su mala reputación entre los ecologistas).

«MONEDA FIDUCIARIA»

Todo esto puede sonar arcano para los profanos, pero un dinero descentralizado era algo que el mundo nunca había visto. Su invención fue una proeza intelectual. Zooko Wilcox, cuya obsesión con la idea del dinero descentralizado comenzó cuando era un programador de diecinueve años con inclinaciones políticas que asistía a la Universidad de Colorado, en Boulder, no había pensado prácticamente

ISTOCK

Desde la creación del bitcoin, uno de los avances más relevantes ha sido reconocer que la tecnología *blockchain* puede aplicarse más allá de las criptomonedas.

en otra cosa durante la década anterior a la aparición del bitcoin. «Durante doce años, más o menos, uno de mis pasatiempos favoritos antes de dormir era intentar descifrarlo —me dijo—. Mi sensación es que el mecanismo de consenso creado por Nakamoto, y cómo lo combinó con los sistemas de incentivos, no habría sido descubierto por nadie más. Habrían hecho falta otros cien años para lograrlo». Tanto si minabas bitcoins como si se los comprabas a alguien que lo hubiera hecho, formar parte desde las primeras etapas tenía un atractivo incuestionable. El *software* de Nakamoto establecía un límite máximo de 21 millones de bitcoins acuñados, cantidad que el sistema preveía que se alcanzara alrededor del año 2140. En lugar de estar en riesgo de inflación o hiperinflación, bitcoin era deflacionario: si la tecnología se extendía, estarías en posesión de un activo que se revalorizaría. En una publicación en la red social de la Fundación P2P, Nakamoto comentó: «Me encanta la idea de comunidades virtuales y no geográficas que experimentan con nuevos paradigmas económicos».

Para mí, el bitcoin era alucinante, como un portal a un mundo o una visión del mundo que no sabía que existía. Los libertarios alienados ya veían el dinero cotidiano como una mera «moneda fiduciaria» —pronunciaban la palabra con unas sonoras y despectivas comillas— que solo tenía valor por decreto gubernamental. Pero, para el resto de nosotros, descubrir una moneda que funcionaba fuera de los parámetros habituales era como aquella metáfora de David Foster Wallace sobre unos peces que no son conscientes de estar en el agua hasta que, tras ser sacados bruscamente de su ambiente, boqueando, contemplan por primera vez la realidad.

¿Qué hacía que el bitcoin valiera algo? El dólar estadounidense era de curso legal y estaba respaldado por uno de los Gobiernos más estables del mundo. Podías usarlo para pagar tus impuestos. Los comerciantes estaban obligados a aceptarlo.

SHUTTERSTOCK

La crisis financiera del año 2008 no fue solo el telón de fondo, sino el catalizador directo para que las criptomonedas se creasen.

EL MISMO MES EN EL QUE SUPE DE LA EXISTENCIA DE ESTA CRIPTOMONEDA, PERDIÓ MÁS DEL 99 % DE SU VALOR

Pero ¿qué podía darle valor a una cadena de números y letras? Cuando se lanzó un intercambio de bitcoins llamado New Liberty Standard en octubre de 2009, fijó el precio de un solo bitcoin (BTC) en menos de la décima parte de un centavo, basándose en el coste de la electricidad necesaria para minarlo. Pero el precio del bitcoin cobró vida. A principios de 2011, la tasa de mercado superó el dólar y, cuando Jason me llamó, un bitcoin costaba más de 17 dólares. Gran parte del valor, en aquellos primeros días, parecía derivarse de la creencia en el potencial del bitcoin como una especie de oro digital con un mercado mundial, y de la pura especulación financiera.

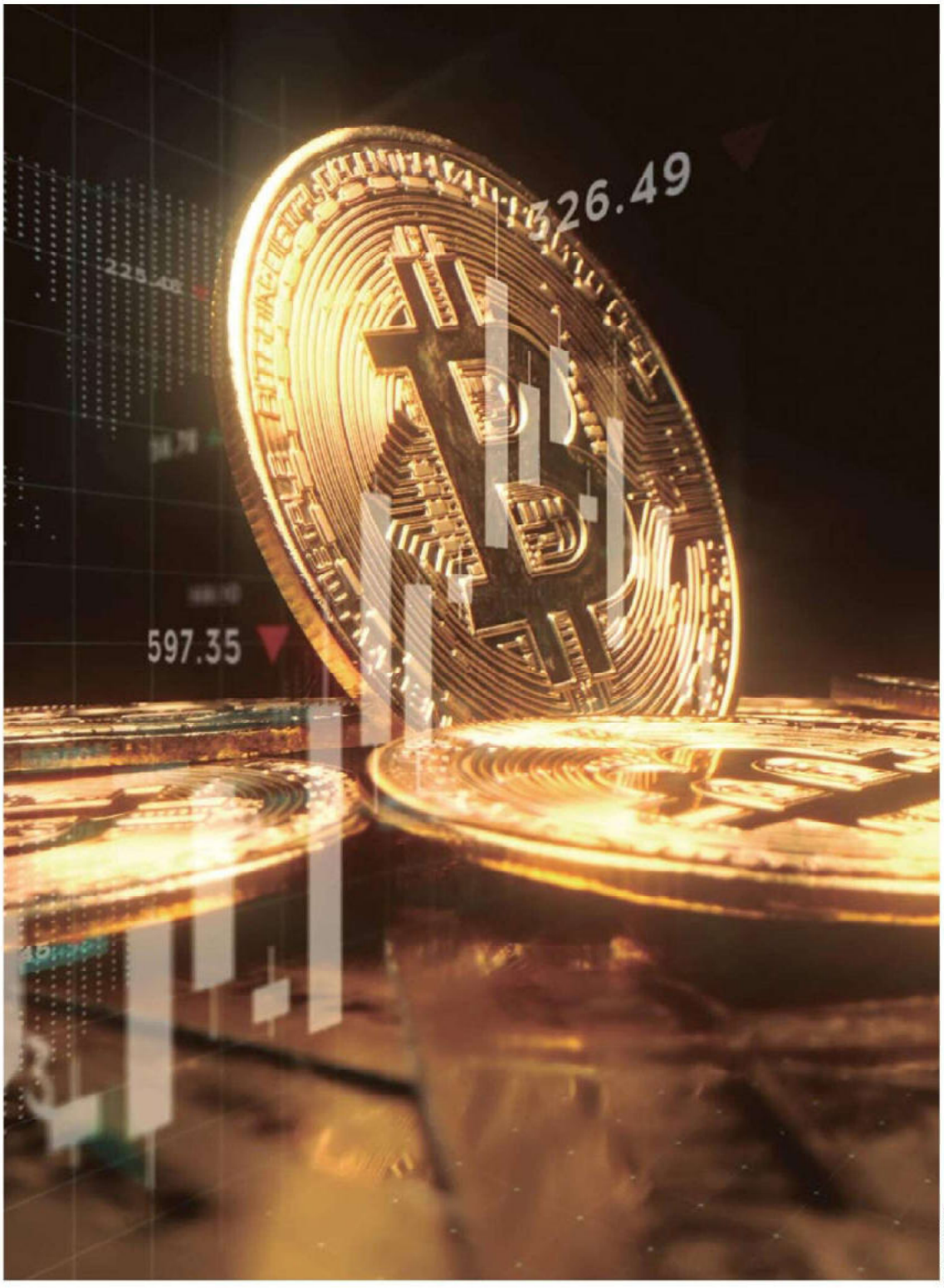
¿QUÉ TENÍAN ESTAS PERSONAS EN CONTRA DE LOS BANCOS?

Me sentí atraído por la fascinación de estar en un terreno virgen. «Es fascinante crear una nueva moneda —me contó Jeff Garzik, un programador de bitcoin que vivía y trabajaba en una autocaravana Fleetwood Southwind de 1984 en Carolina del Norte—. Podría decirse que es la primera moneda global del mundo». En Brooklyn, conocí a Mark Suppes, un manitas que estaba construyendo un cajero automático de bitcoins en su *loft* de Bedford-Stuyvesant, a pocos metros del reactor de fusión nuclear casero que también estaba montando. Un anarquista barbudo que llevaba un pañuelo al estilo pirata en la cabeza y publicaba en YouTube como The Real Plato viajaba de Connecticut a California, al estilo de Jack Kerouac, e intentaba financiar su aventura únicamente con bitcoins. Los entusiastas de las monedas raras hablaban de un tiempo futuro en el que la gente intercambiaría bitcoins poco comunes, como los del llamado bloque Génesis, el primero de la cadena, con tanto entusiasmo como si fueran Águilas Dobles de 1933.

Pero, aunque me dejara llevar por la emoción, había ciertos aspectos que se me escapaban. Podía entender que este nuevo dinero resultara atractivo en un lugar como Argentina, donde la hiperinflación y los controles de divisas eran reales, al igual que en México, Filipinas o en buena parte de África, donde más del 60 % de la población no tenía cuentas bancarias. Pero no entendía el problema que los bitcoiners estadounidenses tenían con las instituciones financieras tradicionales. El seguro federal de depósitos funcionaba bastante bien. Los cajeros automáticos eran prácticos. ¿Qué tenían estas personas en contra de los bancos?

También me costaba entender los fundamentos técnicos del bitcoin y cómo interactuaban las partes del sistema. En las reuniones, solía asentir mientras la gente hablaba de «funciones *hash* unidireccionales» y de «equilibrios de *Nash*» y luego, en casa, me pasaba horas leyendo sobre el tema hasta que me dolían los ojos. Cuando por fin pensaba que lo había entendido, mi recién adquirida claridad se desvanecía en cuanto intentaba explicárselo a otra persona. Me sentí un poco menos torpe después de que Garzik, uno de los principales desarrolladores de *software* del proyecto, me dijera: «El bitcoin es muy muy difícil de entender».

LA ALTERNATIVA A ALMACENAR TU BITCOIN EN UNA PLATAFORMA ERA LA «AUTOCUSTODIA» DE UNA CLAVE PRIVADA



SHUTTERSTOCK

Bitcoin, creado específicamente para eliminar intermediarios financieros, ahora es comercializado por esos mismos intermediarios.

El bitcoin también era difícil de comprar, de almacenar, de usar y de atesorar. Era extremadamente volátil: el mismo mes en el que supe de su existencia, perdió brevemente más del 99 % de su valor, que pasó de 17 a 0,01 dólares. Las plataformas de intercambio de bitcoins, no reguladas y sin rendir cuentas, a menudo resultaban ser negocios poco fiables, con propietarios anónimos que recibían los depósitos de los clientes y, un día, simplemente se fugaban con ellos. Incluso Mt. Gox, la mayor plataforma, había sufrido el robo de 25 000 BTC, por valor de 500 000 dólares en aquel momento, por parte de piratas informáticos; precisamente esto precipitó el desplome repentino del precio del bitcoin.

AUTOCUSTODIA

La alternativa a almacenar tu bitcoin en una plataforma era la «autocustodia» de una clave privada, normalmente una cadena de 51 caracteres de números y letras que era el equivalente criptográfico de una contraseña, en un «monedero» de bitcoin, que en realidad se parecía más a un llavero. Podías garabatear tu clave en un trozo de papel, grabarla en una placa de acero y enterrarla en tu jardín, guardarla en un ordenador virgen o simplemente memorizarla. La última opción parecía lo máximo en autosoberanía y había algo emocionante en la idea de que podías cruzar una frontera internacional con tu clave en la cabeza y trasladar de esta forma tan simple tu dinero.

Stefan Thomas posee 7002 bitcoins pero perdió la contraseña y solo tiene dos intentos antes de que se bloquee permanentemente.

Desde luego nadie aconsejaba hacer esto, pues un solo dígito mal recordado podría costarte todos tus activos. La autocustodia, un ideal que acabaría consagrándose como el mantra de los criptoadictos «Ni tus llaves, ni tus monedas» conllevaba su propio conjunto de problemas. Stefan Thomas, un programador suizo, había almacenado copias de las claves de 7002 bitcoins en tres lugares, colocando su monedero principal en una «máquina virtual» aislada de internet y haciendo una copia de seguridad tanto con el *software* TrueCrypt como en una IronKey, un *hardware* seguro parecido a una memoria USB. Pero entonces, mientras actualizaba su sistema operativo, borró accidentalmente la máquina virtual. Y cuando inició sesión en su TrueCrypt, que estaba almacenado en Dropbox, también se eliminó; resultó que podía sobrescribirse si había más de dos máquinas conectadas al mismo tiempo. En cuanto a su IronKey, simplemente había extraviado la contraseña. El valor de las monedas perdidas en ese momento era de 140 000 dólares. «Me pasé una semana intentan

do recuperarlas sin éxito —me dijo Stefan—. Fue bastante doloroso». A finales de 2021, las monedas valdrían 473 millones de dólares. Pero Stefan no fue el único en su desgracia. La empresa de datos Chainalysis estimaba que el 20 % de todos los bitcoins en circulación se había perdido.

«¿CÓMO PUEDE FUNCIONAR ESTO?»

Gavin Andresen me pareció un primer guía agradable en este mundo esotérico. A punto de cumplir cuarenta y un años, llevaba un flequillo castaño pegado a la frente y la etiqueta «friki» literalmente en el pecho, cosida en un parche sobre una camisa de manga corta. Era un hombre de clase media, padre de dos hijos y con un suave tono de voz. Mientras que alguien que despreciara su propia memoria te diría algo así como «mi mujer podría contarte muchas cosas sobre mi mala memoria» y dejarlo ahí, Gavin probablemente lo expresaría así: «He leído una investigación sobre lo defectuosa que es la memoria del ser humano» y se lanzaría a explicártelo con todo lujo de detalles. Además, montaba en monociclo.

El bitcoin había aparecido en la vida de Gavin en un momento oportuno. En 2009, su esposa, Michele, profesora de Geología en la Universidad de Massachusetts, se tomó un año sabático, Gavin dejó su puesto fijo en el campo del aprendizaje automático en la universidad y la familia se mudó a Australia. Gavin se pasó los seis meses siguientes en Queensland, Australia, practicando malabares con cocos, corriendo por la playa, buceando, peleándose con los mosquitos, rescatando a una serpiente de mar picuda, bebiendo cerveza XXXX y afeitándose la perilla que había lucido durante los últimos diecisiete años, entre otros pasatiempos. Planea-

STEPHEN MCCARTHY / SPORTSFILE / WEB SUMMIT

Gavin Andresen fue la persona elegida personalmente por Satoshi Nakamoto para liderar el desarrollo del protocolo antes de su misteriosa desaparición en 2011.

BITCOIN FAUCET ENCAJABA BIEN CON EL ENCANTO ARTESANAL DEL BITCOIN EN ESA PRIMERA ETAPA

ba lanzar una empresa emergente cuando la familia regresara a Estados Unidos, pero, en mayo de 2010, aún no había encontrado una idea que lo convenciera.

Entonces leyó una entrada de un blog de tecnología sobre un puñado de proyectos de *software* de código abierto, incluido el bitcoin. Gavin se había graduado en la Universidad de Princeton y trabajaba para Silicon Graphics. Formaba parte del órgano legislativo de su pequeña ciudad de Nueva Inglaterra, se interesaba activamente por la política escolar local y se había ofrecido como voluntario para ayudar con el sitio web de la Liga de Mujeres Votantes de Amherst.

Pero le atraía la idea de que el dinero no estuviera controlado por un grupo de élite de la Reserva Federal. Le gustaba la libertad individual, la sabiduría colectiva, los procesos orgánicos de base en lugar del control desde arriba. Creía en la evolución por encima de la revolución, en «pequeños pasos hacia un mundo mejor».

Sin embargo, su principal reacción ante el bitcoin, como me contó más tarde, fue «¿cómo puede funcionar esto?». Se preguntaba cómo el sistema creaba nuevas monedas y cómo evitaba el doble gasto. Buscó «bitcoin» en Google y solo obtuvo cuatro páginas de resultados. Luego descargó el código y comenzó a leerlo. Estaba claro que el programador sabía lo que hacía. Gavin ejecutó el *software* y minó algunas monedas. Aun así, «tuve que pensar mucho para convencerme de que el sistema no presentaba fallos». Cuando hablamos, estaba «bastante seguro de que no había ningún fallo fundamental».

Un mes después de conocer el bitcoin, Gavin creó el Bitcoin Faucet. En aquel momento, un bitcoin costaba medio centavo, y Gavin se gastó cincuenta dólares para comprar 10 000 y configurar un sitio web para regalarlos. Cualquiera podía resolver un CAPTCHA y recibir cinco bitcoins gratis. La idea era hacer que este experimento resultara atractivo para los nuevos usuarios. Gavin comprendía que el dinero solo adquiere valor cuando la gente lo utiliza.

REEMPLAZAR AL DÓLAR COMO MONEDA DE RESERVA MUNDIAL

Bitcoin Faucet encajaba bien con el encanto artesanal del bitcoin en esa primera etapa. En una ocasión, Gavin comió con David Forster, un granjero que vivía cerca de su casa en Massachusetts y que intercambiaba calcetines de alpaca por bitcoins. Los bitcoiners se mostraron entusiasmados cuando Laszlo Hanyecz, que vivía en Florida, pagó 10 000 bitcoins por dos pizzas grandes de Papa John's. Años después, la gente no se cansaba de revaluar esas pizzas al precio actual del bitcoin: ¡690 millones de dólares por pizza! «No me siento mal por ello —me dijo Laszlo cuando esos bitcoins valían apenas unos 85 000 dólares—. La pizza estaba muy buena».

Unos días después Gavin hacía y respondía preguntas en el foro de bitcoin mientras enviaba fragmentos de código a Nakamoto para parchear los inevitables agujeros presentes en cualquier *software* nuevo. Sabía poco sobre Nakamoto. Nunca

se habían conocido en persona ni hablado por teléfono. La idea que Gavin tenía de su principal colaborador laboral se basaba únicamente en su correspondencia escrita. A través de correos electrónicos y mensajes privados, Gavin interpretó que Nakamoto era serio y quisquilloso, autosuficiente y brillante. A Gavin le preocupaban los problemas legales. El Gobierno había procesado a creadores anteriores de monedas alternativas. ¿Podría ser arrestado? A Michele le gustaba bromear con él sobre ese «dinero ficticio de internet», pero pronto Gavin empezó a dedicar todo su tiempo a esta empresa.

Trabajaba en el proyecto porque le interesaba, pero también admiraba lo bien que Nakamoto había adaptado el bitcoin a la naturaleza humana. En cuanto poseías algunas de estas monedas digitales, querías ayudar al sistema, ya fuera minándolas, usándolas, promocionándolas o trabajando en el código, para que tus bitcoins valieran más mañana que ayer. A medida que el precio subía, Gavin recibía una recompensa material en tiempo real. Su participación fue un «interés propio ilustrado». Pensaba que el bitcoin podría convertirse en una importante moneda mundial y, con el tiempo, posiblemente incluso reemplazar al dólar como moneda de reserva mundial.

GAVIN SE CONVIRTIÓ EN EL DESARROLLADOR PRINCIPAL

A pesar de que el bitcoin era un proyecto de código abierto, un esfuerzo colectivo que, en teoría, era inmune a los intereses particulares, alguien tenía que asumir la dirección, y durante los primeros veinte meses ese había sido Satoshi. Nakamoto publicaba el código, otros desarrolladores sugerían parches y él incorporaba los que consideraba adecuados.

Cuatro meses después de que Gavin comenzara a colaborar, su dedicación, sus conocimientos informáticos y su actitud sincera parecieron ganarse la confianza de Nakamoto. Primero, le dio a Gavin acceso directo al código fuente. Luego, alrededor de septiembre de 2010, Nakamoto le dijo que estaba ocupado con otros proyectos y que en los próximos meses le entregaría el control tanto del repositorio de código en SourceForge como de la «clave de alerta» del proyecto, que permitía la transmisión de mensajes urgentes a todas las máquinas que ejecutaban el *software* bitcoin. Para un proyecto de código abierto, estos elementos eran los símbolos de autoridad más evidentes y, en ese momento, Gavin se convirtió efectivamente en el desarrollador principal del proyecto, guiando a un equipo de cinco programadores voluntarios.

Durante los meses siguientes, Nakamoto continuó interviniendo ocasionalmente en cuestiones técnicas, pero su naturaleza reservada chocaba con el enfoque abierto de Gavin. Después de que PayPal y Visa congelaran las cuentas de WikiLeaks, una facción de bitconers sostuvo que WikiLeaks podría beneficiarse del bitcoin y, a su vez, esta colaboración serviría para dar a conocer la moneda digi-

ALGUNOS BITCOINERS CELEBRARON CON ENTUSIASMO LA ATENCIÓN MEDIÁTICA, PERO NAKAMOTO, NO

SHUTTERSTOCK

WikiLeaks comenzó a aceptar donaciones en bitcoin en 2011, convirtiéndose en una de las primeras organizaciones en hacerlo.

tal. «Adelante», escribió alguien en un foro llamado BitcoinTalk. Pero Nakamoto se erizó: «No, no lo hagáis. El proyecto necesita crecer gradualmente para que el *software* pueda fortalecerse a lo largo del camino. Hago un llamamiento a WikiLeaks para que no intente utilizar bitcoins. El revuelo que provocaríais probablemente nos destruiría en esta etapa».

La idea de que WikiLeaks aceptara donaciones en bitcoins dio lugar a un artículo en *PC Magazine*. Algunos bitcoiners celebraron con entusiasmo la atención mediática, pero Nakamoto no: «Habría estado bien recibir esta publicidad en cualquier otro contexto, pero WikiLeaks ha abierto la caja de Pandora, y la avalancha se dirige hacia nosotros».

NAKAMOTO PARECÍA CADA VEZ MÁS INCÓMODO

Para los periodistas que cubrían el bitcoin, Gavin se había convertido en la persona natural a la que dirigirse en primer lugar. Tenía un carácter afable y razonable, una tendencia natural hacia posturas políticas moderadas y la voluntad de utilizar su verdadero nombre, lo que le convertía en el embajador del bitcoin que Nakamoto nunca había sido. Pero Nakamoto parecía cada vez más incómodo con las interacciones de Gavin con los medios de comunicación. A finales de abril de 2011, le envió un correo electrónico: «Ojalá no siguieras hablando de mí como una misteriosa figura en la sombra o la prensa acabará interpretando el bitcoin como si fuera una moneda pirata». Esta fue la última vez que Gavin supo de Nakamoto. Cuando hablé por primera vez con Gavin ese julio, dijo que no se había comunicado con Nakamoto «en un par de meses». Después de que el 26 de abril Gavin le dijera ingenuamente a Nakamoto en un correo electrónico que había aceptado dar una charla sobre el bitcoin a la CIA, curiosa por las criptomonedas, en su sede de Langley, Virginia, Nakamoto nunca respondió. Casi por la misma fecha, escribió correos electrónicos a al menos otro programador que había trabajado en el proyecto.

Luego se quedó en silencio. ■

Un deslumbrante espe..jismo

Después de años de existencia, el bitcoin permanece en esta tensión entre ser una revolución monetaria legítima y un activo especulativo, ni el paraíso prometido por los maximalistas ni el fraude proclamado por los detractores, sino una tecnología compleja con capacidades reales y limitaciones significativas.

ISTOCK

Entonces, ¿sabes quién es Satoshi? —le pregunté.

Si alguien lo sabía, ese era Gavin.

—No sé su verdadero nombre. Espero que algún día decida dejar de ser anónimo y pueda conocerle, pero no lo creo —me respondió.

Gavin y los otros desarrolladores estaban de acuerdo en algunas cosas. El segundo lugar en el que Nakamoto había anunciado su documento técnico era el sitio web de la Fundación P2P, una organización idealista sin ánimo de lucro dedicada a las redes entre pares de todo tipo. En su perfil del sitio, Nakamoto señaló Japón como su lugar de residencia. Pero realmente nadie creía que fuera japonés. Su inglés era impecable, con la confianza flexible de un hablante nativo. Sonaba británico o al menos de un país de la Commonwealth. El bloque Génesis había incrustado un titular del *Times* y tanto en el código fuente del bitcoin como en sus publicaciones en el foro BitcoinTalk, Nakamoto favorecía la ortografía anglosajona, en palabras como *colour* y *optimise*. El titular del Times insinuaba la motivación de Nakamoto: «El ministro de Hacienda al borde del segundo rescate bancario».

ASC

El irlandés Mike Hearn pasó de ser una pieza clave a convertirse en el crítico más acérrimo del bitcoin.

UN FRIKI DE LA PROGRAMACIÓN

Resultaba llamativo lo celoso que era Nakamoto de su identidad. Había registrado el dominio bitcoin.org a través de un servicio de enmascaramiento llamado anonymousspeech.com, que a su vez había sido registrado por un agente de alojamiento temporal en Tokio. Ese servicio le proporcionó una dirección de correo electrónico en vistomail.com, que ofrecía la opción de manipular la fecha y la hora de envío de un correo. Una tercera dirección de correo electrónico que utilizó Nakamoto era de gmx.com, otro proveedor de correo web gratuito. Michael Marquardt, que dirigía *BitcoinTalk* bajo el nombre de Theymos, estaba convencido de que Nakamoto ocultaba su dirección IP utilizando TOR, el mismo *software* de navegación anónima que se requería para acceder a sitios de la web oscura como *Silk Road*. Y Nakamoto se expresaba con

NAKAMOTO HABÍA REGISTRADO EL DOMINIO BITCOIN.ORG A TRAVÉS DEL SERVICIO DE ENMASCARAMIENTO ANONYMOUSSPEECH.COM

una opacidad practicada. Respondía a preguntas técnicas, según Gavin, como «un friki de la programación hablando con otro friki de la programación». Cualquier intento de sonsacar información personal a Nakamoto era hábilmente ignorado.

El código de Nakamoto contaba su propia historia. Gavin pensaba que los programadores tenían estilos literarios tan distintos como el de Kurt Vonnegut y el de Jackie Collins. Había algunos indicios de que Nakamoto podría ser un poco mayor. A Gavin, su estilo de codificación le parecía un tanto anticuado, y un desarrollador irlandés llamado Mike Hearn, que trabajaba para Google en Suiza, observó que Nakamoto utilizaba notación húngara, una convención de nomenclatura de variables popular entre los programadores de Windows en la década de los noventa. También era bastante inusual ver a una persona de Windows dirigiendo un proyecto de código abierto, ya que el movimiento de código abierto había surgido en gran medida como reacción a sistemas cerrados como Windows.

ASC

Amir Taaki. anarquista, *hacktivista* y programador británico-iraní, conocido por su papel destacado en el proyecto bitcoin.

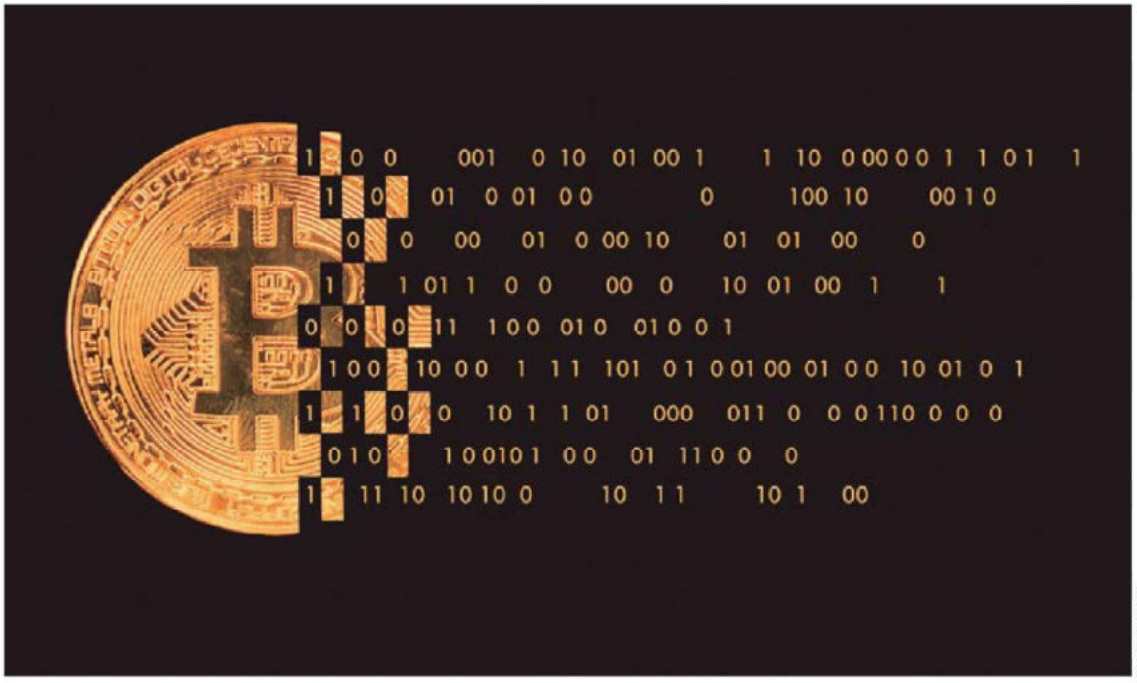
Los programadores de bitcoin discrepaban en otros aspectos. Para Gavin, Nakamoto figuraba entre el 10 % de los programadores más destacados por su destreza. Pero Amir Taaki, uno de los primeros desarrolladores de bitcoin y hacker anarquista —vivía en un edificio okupado en Londres y más tarde se convertiría en activista por las armas impresas en 3D y lucharía a favor de los kurdos en el frente de la guerra civil de Siria— me dijo que no creía que Nakamoto tuviera ni siquiera formación en informática. Aunque Amir consideraba que el concepto del bitcoin era sólido, pensaba que el código estaba mal escrito, con todo amontonado en dos archivos poco manejables en lugar de dividido en componentes modulares, como lo organizaría un profesional. Esto le hizo pensar que Nakamoto podría ser un profesor. «Cuando haces programación durante muchos años y trabajas con un equipo, empiezas a pensar: "¿Cómo puedo escribir este código fuente de manera comprensible para un amplio número de personas?". Aprendes a abstraer las cosas de una manera que las haga obvias y comprensibles, aprendes patrones de diseño básicos, formas estándar de hacer las cosas, pero estos son aspectos que los académicos no aprenden. Los ingenieros se preocupan por cuestiones de este tipo, es decir, por responder a la pregunta: "¿Cómo puedo construir esto sin errores y de una manera fácil de entender?"». Amir tenía formación en matemáticas, y lo que percibió cuando leyó el documento técnico fue un manejo experto de herramientas matemáticas y estadísticas.

Gavin tenía la impresión de que el código del bitcoin había sido escrito por un pequeño grupo o incluso por una sola persona. Cuando los programadores colaboran, suelen insertar comentarios regulares en el código para explicarse los unos a los otros, lo que se supone que debe lograr este o aquel bloque de instrucciones. El *software* del bitcoin contenía pocos comentarios. Otros consideraban que el bitcoin era excesivamente sofisticado y funcionaba demasiado bien desde el momento de su lanzamiento como para ser el producto de un solo cerebro. Además, el libro blanco empleaba el pronombre nosotros, por tanto, Satoshi Nakamoto podría ser en realidad el nombre colectivo de un grupo o una institución.

Cuando me enteré de la existencia del bitcoin, los miembros de su joven comunidad ya habían empezado a preguntarse por la identidad de Nakamoto. Las especulaciones precedieron a su desaparición. En enero de 2011, incluso antes de que Nakamoto se evaporara, ya empezaba a ser venerado. Cuando quedó claro que el bitcoin necesitaba unidades más pequeñas, la comunidad empezó a llamar satoshi a la centésima parte de un bitcoin. Ese mismo mes, alguien advirtió que la última publicación de Nakamoto en *BitcoinTalk* había sido el 13 de diciembre. Cundió el pánico. ¿Había abandonado Nakamoto el proyecto? ¿Había muerto? ¿Quién los dirigiría? Por primera vez, algunas personas comenzaron a cuestionarse abiertamente quién era realmente Nakamoto.

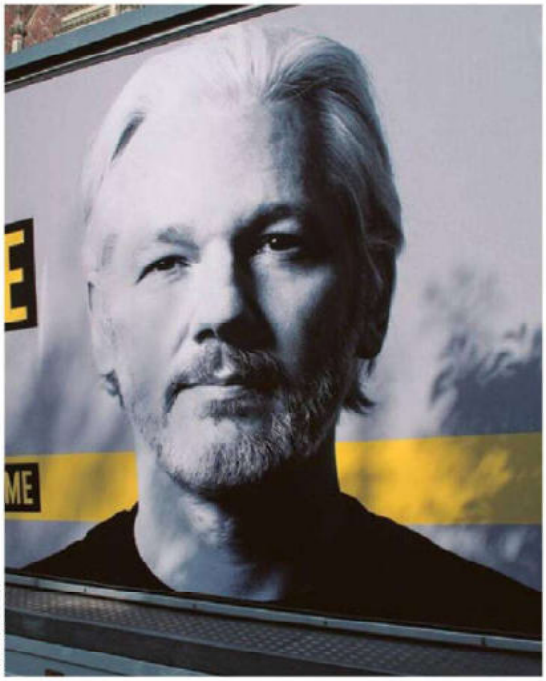
NEAL STEPHENSON, GRIGORI PERELMAN, JULIAN ASSANGE...

Alguien planteó la teoría de que Nakamoto era «parecido a Nicolas Bourbaki», refiriéndose a un pequeño grupo de matemáticos franceses que habían empezado a publicar artículos en la década de los treinta utilizando un seudónimo colectivo. Alguien más señaló que el misterio le daba al bitcoin un *glamour* útil. Otra per-



El código binario se transformaba en valor económico. Satoshi Nakamoto logró algo que los economistas consideraban imposible: crear escasez digital usando matemáticas y consenso.

sona sugirió que «el tipo solo quiere algo de privacidad. Y eso es bueno, porque muestra claramente que no es fama lo que busca, sino ideales. En mi humilde opinión, deberíamos respetar eso y dejar su identidad en paz». Pero la gente no pudo evitar proponer candidatos: ¿podría ser Neal Stephenson, el novelista cuya *Criptonomicon* había anticipado el dinero digital? ¿Julian Assange, el fundador australiano de WikiLeaks? ¿Grigori Perelman, un genio ruso ermitaño que había rechazado un premio de matemáticas de un millón de dólares?


SHUTTERSTOCK

Hay quien propuso a Julian Assange, fundador de WikiLeaks, como candidato a ser el esquivo Nakamoto.

El pánico resultó injustificado. El 13 de enero, Gavin tranquilizó a la comunidad: Nakamoto le había enviado un correo electrónico ese día «sobre un error complicado... Está ocupado». Pero, el 16 de abril de 2011, un usuario de *BitcoinTalk* llamado Wobber, señalando que «había pasado mucho tiempo desde la última vez que publicó aquí», inició un nuevo hilo: «¿Quién es Satoshi Nakamoto?». Wobber señaló lo variada que era la experiencia de Nakamoto y lo inusual de su comportamiento: crear algo tan innovador, no atribuirse el mérito ni explotar su notoriedad y marcharse sin decírselo a nadie. Alguien comparó a Nakamoto con el Zorro o con un David enmascarado que había apuntado con su honda al Goliat de los bancos y los Gobiernos. Otro se preguntó si Nakamoto podría ser Gavin Andresen. Gavin tenía una conexión con Australia, ya que había nacido allí antes de mudarse a Estados Unidos durante su infancia, lo que explicaría por qué Nakamoto alternaba características de la ortografía estadounidense y de la Commonwealth. Otra persona se preguntó si Nakamoto se habría creado una personalidad falsa para interactuar consigo mismo.

«SATOSHI PODRÍA SER CUALQUIERA»

Con tan pocas pistas que seguir, los detectives se aferraron a los detalles más insignificantes. ¿Podría el nombre contener una clave? *Sato shi Nakamoto*, traduci-

BITCOIN NECESITABA UNIDADES MÁS PEQUEÑAS Y LA COMUNIDAD EMPEZÓ A LLAMAR SATOSHI A LA CENTÉSIMA PARTE DE UN BITCOIN

do aproximadamente del japonés, podría significar «inteligencia central». Quizá esto apuntaba al papel de los espías en la creación del bitcoin. Quizá la Agencia de Seguridad Nacional estaba ejecutando una estrategia a largo plazo, lanzando una red financiera no oficial que podría utilizar para pagar activos sobre el terreno en cualquier parte del mundo, o como un señuelo donde los adversarios realizarían transacciones con una falsa sensación de seguridad mientras los espías de Fort Meade vigilaban todos sus movimientos.

No era una idea totalmente descabellada. El Laboratorio de Investigación Naval de Estados Unidos había creado The Onion Router, el *software* de anonimato conocido como TOR24 que hizo posible la web oscura. Más tarde, el FBI crearía en secreto su propia línea de teléfonos cifrados y un servicio de mensajería, ANOM, que fueron adoptados sin saberlo por delincuentes organizados, lo que dio lugar a más de ochocientos arrestos. Y en el verano de 1996, tres investigadores de la División de Criptología de la Oficina de Investigación y Tecnología de Seguridad de la Información de la NSA habían publicado internamente un extenso artículo, que posteriormente se haría público, titulado «Cómo hacer dinero: la criptografía del dinero electrónico anónimo».

También se podía leer el nombre de Nakamoto como un acrónimo de los nombres de grandes empresas tecnológicas: samsung, toshiba, nakamichi, motorola, así que tal vez una conspiración corporativa estaba detrás de este misterio. Los usuarios de Reddit unieron sus habilidades de decodificación y finalmente descubrieron que Satoshi Nakamoto era un anagrama de, entre otras frases, *Ma, I took NSA's oath* («Mamá, hice el juramento de la Agencia Nacional de Seguridad») y *So a man took a shit* («Así que un hombre cagó»).

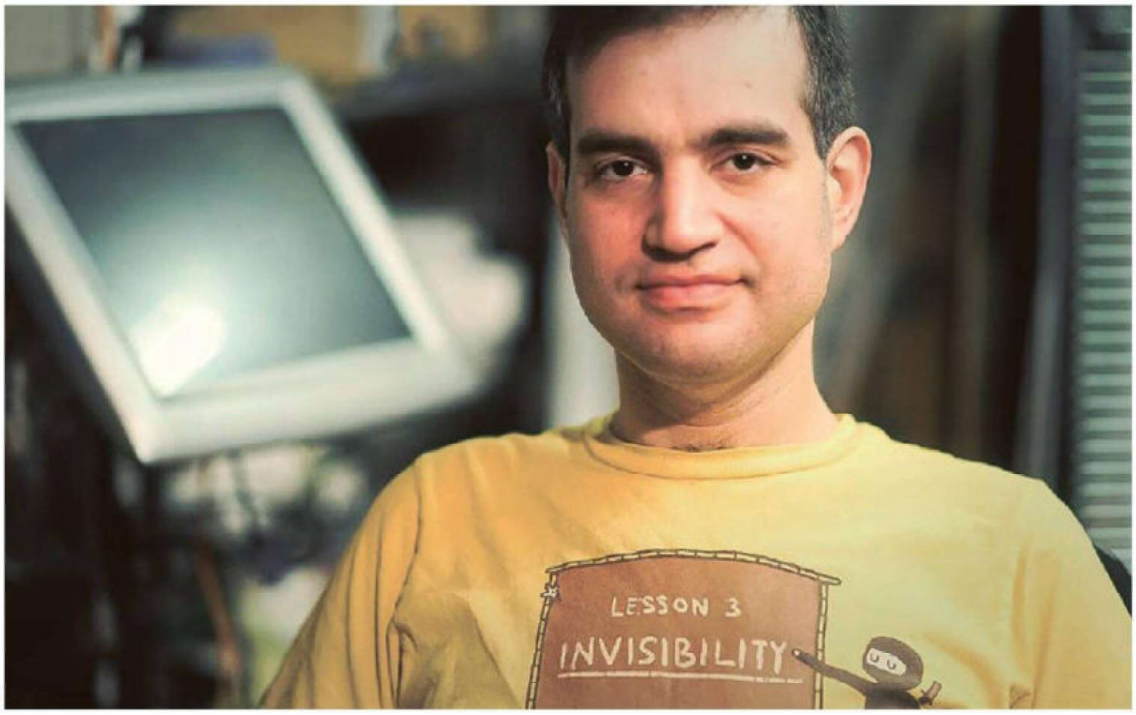
Por primera vez, la gente se preguntó por qué Nakamoto había usado un seudónimo. ¿Fue por las incomodidades de la fama? ¿Por la historia de los Gobiernos persiguiendo a los criptógrafos? ¿Por evitar el acoso? ¿Por los enemigos que el bitcoin podría generar? Quizá solo quería ser anónimo. Tal vez no quería mezclar esta empresa con otros negocios.

En mayo, Gwern Branwen, un programador y escritor que también usaba un seudónimo con seguidores en ciertos blogs populares en Silicon Valley, esbozó su propia idea sobre Nakamoto. «Satoshi podría ser cualquiera», escribió. El bitcoin no requería «grandes avances intelectuales de tipo matemático o criptográfico», sino que era más bien una inteligente agrupación de tecnologías existentes, así que «¡Satoshi podría ser un simple programador autodidacta, pues no necesitaba conocimientos expertos en criptografía!».

LA CRIPTOMONEDA ES MÁS GRANDE QUE SATOSHI

Stefan Thomas, el bitcoiner suizo que había perdido más de siete mil monedas, abordó la cuestión metódicamente, representando gráficamente los datos tem-

THE ONION ROUTER, UN *SOFTWARE* DE ANONIMATO CONOCIDO COMO TOR24, HIZO POSIBLE LA WEB OSCURA



ASC

El investigador de seguridad Dan Kaminsky, conocido por su trabajo en el descubrimiento de fallos de seguridad de DNS.

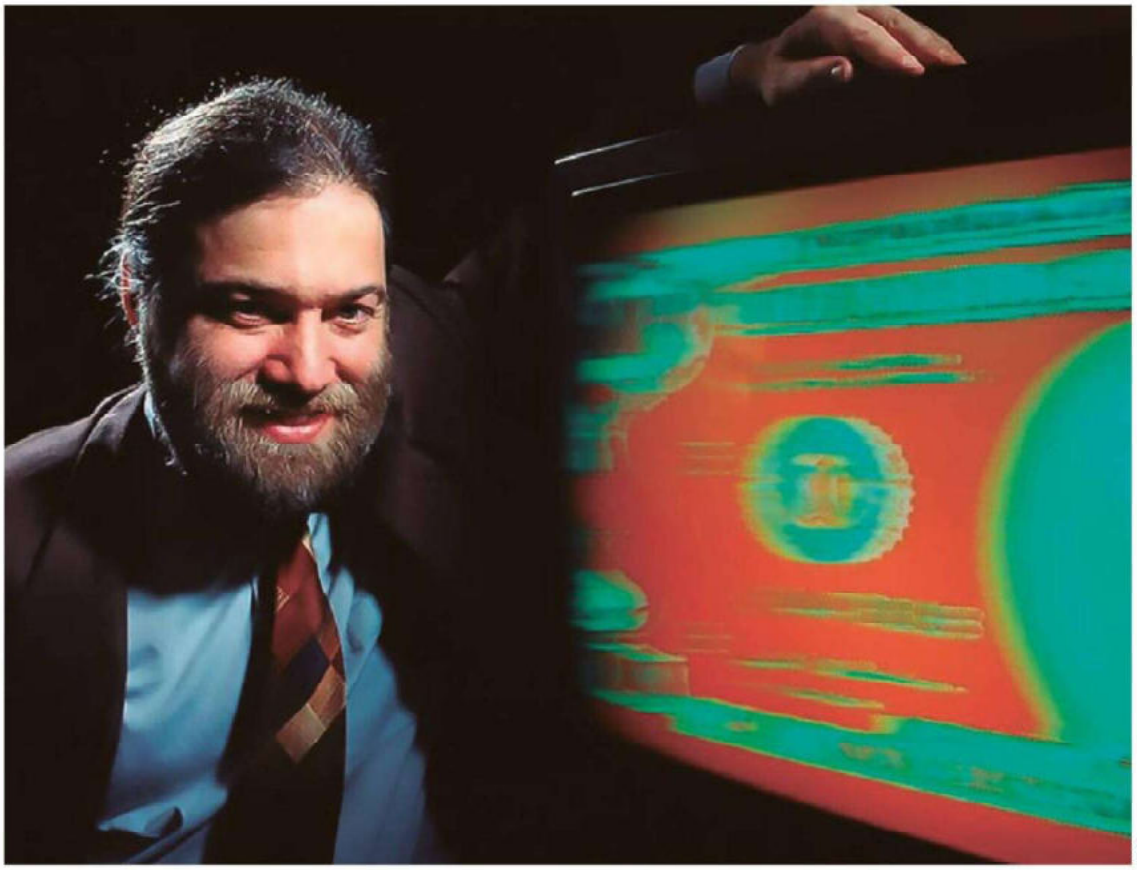
porales de las más de quinientas publicaciones de Nakamoto en el foro. Estas revelaron una caída pronunciada en la actividad de publicación durante las horas correspondientes a la noche en Norteamérica. «Mike jura que tiene acento británico», me dijo Stefan, refiriéndose a Mike Hearn, el desarrollador de bitcoin. Stefan tenía en mente un perfil vago de Nakamoto: una única persona que vivía en Estados Unidos, aunque no fuera estadounidense. «La navaja de Ockham», dijo. Una explicación simple superaba a una complicada.

Cuando Stefan publicó su gráfico en *BitcoinTalk*, este fue recibido con un coro de disidencia: ¿No parecía más probable que Nakamoto dedicara tiempo al bitcoin cuando no estaba trabajando? En ese caso, sus horas de publicación podrían corresponder a Europa occidental. «¿Desde cuándo duerme un hacker por la noche?», protestó alguien. Otro señaló que el patrón debería cambiar los fines de semana, pero no lo hacía.

Dan Kaminsky, un investigador de seguridad informática de treinta y dos años que saltó a la fama tres años antes cuando descubrió una vulnerabilidad crítica que podría comprometer toda la infraestructura de internet, pensó que Nakamoto podría ser un grupo de un banco. «Sospecho que Satoshi es un pequeño equipo de una institución financiera —me dijo Dan—. Tengo esa corazonada».

La identidad de Nakamoto era «un deslumbrante espejismo. Pero no creo que sea tan importante para lo que es el bitcoin. La criptomoneda es más grande que Satoshi», añadió Dan. Esto reforzaba un argumento que había escuchado antes: el anonimato de Nakamoto y su eventual desaparición no eran casuales, sino elementos clave del diseño original del bitcoin.

No podía dejar de pensar en el bitcoin. No podía dejar de pensar en su creador. Quizá no tenía por qué ser tan difícil. A veces parecía que internet era en gran



David Chaum inventó casi todos los conceptos fundamentales del dinero digital pero su empresa DigiCash quebró en 1998.

medida un eco constante de las mismas ideas. Los Sherlock informáticos que diseñaban gráficos de datos temporales y escrutaban nombres de variables no se habían molestado en levantar el teléfono. Las creencias consideradas hechos en internet a menudo se disolvían cuando entraban en contacto con la realidad. Tal vez Nakamoto estaba moviendo inquietamente sus pulgares callosos de tanto teclear, sentado en una silla ergonómica para *gamers*, esperando a que alguien como yo lo llamara. Le escribí a satoshin@gmx.com, la dirección que Gavin dijo que había usado, y solicité una entrevista.

MATEMÁTICOS CON ARMAS

Mientras esperaba una respuesta, me puse en contacto con un par de posibles candidatos a ser Nakamoto. Uno de ellos era Adam Back, un criptógrafo británico que en la década de los noventa había escrito Hashcash, un *software* de prevención de *spam* que utilizaba acertijos computacionales, la llamada «prueba de trabajo», para obligar a las máquinas a demostrar que eran «honestas». Se trataba de la misma tecnología que Nakamoto incorporó más tarde en el bitcoin. De hecho, Back fue la primera persona públicamente conocida a la que Nakamoto contactó. En agosto de 2008, alguien de quien nunca había oído hablar le escribió para preguntarle cómo citar correctamente Hashcash en el libro blanco del bitcoin, según Back revelaría más tarde.

ADAM BACK FUE LA PRIMERA PERSONA PÚBLICAMENTE CONOCIDA A LA QUE NAKAMOTO CONTACTÓ

Intercambiamos correos electrónicos, pero me convencí de lo que Amir Taaki me había dicho: «Adam tiene un estilo coherente en todos sus proyectos. Su estilo no coincide con el de Satoshi». Amir me explicó que Back seguía las convenciones de programación estándar, escribía en C y era programador de Unix/Linux, mientras que Nakamoto tenía un estilo errático, escribía en C++ y era un tipo de Windows. Back también era conocido en ese momento como un fanático de la privacidad, alguien propenso a rechazar las compensaciones de anonimato del bitcoin; la esencia y la principal contradicción de una blockchain era que cualquiera podía ver todo lo que sucedía. Además, me parecía increíblemente torpe que alguien empeñado en pasar desapercibido, que apenas había citado un par de referencias, incluyera su propio trabajo entre ellas.

El potencial Nakamoto más obvio era David Chaum, un corpulento empresario de dinero electrónico que llevaba Birkenstocks y que había tenido uno de sus primeros momentos eureka mientras conducía una furgoneta Volkswagen en el norte de California, y otro mientras estaba sentado en una bañera de hidromasaje. Chaum había diseñado los protocolos criptográficos que posibilitaron las transacciones anónimas, tenía varias patentes de dinero digital imposible de rastrear y, a través de su empresa DigiCash en los Países Bajos, había estado más cerca que nadie de hacerlo realidad. También daba la impresión de ser alguien dado a los seudónimos. Cuando un reportero de *Wired*, años antes, le preguntó inocentemente cuántos años tenía, Chaum dijo: «No es algo que comparta con la gente». Cuando le envié un correo electrónico, me respondió: «Estoy un poco liado», y no volvió a contestar.

Pero, cuando llamé por teléfono a Stefan Brands, un criptógrafo holandés que había trabajado estrechamente con Chaum durante muchos años, estaba convencido de que bitcoin no era de Chaum. «Él no hará nada que no tenga realmente un fuerte anonimato», afirmó Stefan. También señaló que Chaum tenía un doctorado y «un currículum académico brillante», mientras que, a juicio de Stefan, quienquiera que creara el bitcoin era «probablemente un ingeniero de seguridad a nivel de licenciatura». Stefan consideraba que el bitcoin revelaba una sofisticación notable en su diseño, pero lo que realmente le fascinaba fueron los sofisticados mecanismos de incentivos integrados en el sistema. Se preguntaba si Gavin Andresen podría ser Nakamoto.

—Gavin lo negó —repuse.

—Obviamente, quienquiera que haya hecho esto hizo un esfuerzo deliberado por ocultar su identidad. Así que, si es él, no lo confesará sin más —respondió Stefan.

Stefan tenía algo claro: dado que el bitcoin requería conocimientos básicos de criptografía y parecía estar motivado por la idea económica libertaria de la descentralización, su creador estaba casi con total certeza vinculado a un grupo radical activo a principios de los noventa. Stefan no fue la única persona que me señaló este grupo que un antiguo miembro describió como «matemáticos con armas». ■

Matemáticos con pistolas

Los *cypherpunks* de los años 90 como Tim May, Eric Hughes y Wei Dai entendieron que la criptografía era un arma más poderosa que cualquier arsenal militar. Sus «balas» eran funciones *hash*, firmas digitales y protocolos de consenso. ISTOCK


progre
setProgre
laplaci
sizeoutLaplacianCube = (double*) BBLw_malloc
realForwardPlan = BBL
(double*) sizeoutLaplacianCube = (do
of sizeoutLaplacianCube = (double*)
realForwardKernelPla
realBackwardPlan = BBLw_p
sizeoutLaplacianCube = (double*) BBLw_malloc(sizeof
forwardLaplacianPlan = BBLw_plan_df
sizeoutLaplacianCube = (double*) BBLw_ma
backwardLaplacianPlan = BBLw_

WIRED

Esta icónica fotografía en blanco y negro captura a los tres arquitectos intelectuales del *cypherpunk* que sentó las bases para el bitcoin: Timothy C. May, John Gilmore y Eric Hughes.

Un sábado de septiembre de 1992, a mediodía, veinte revolucionarios se reunieron en una sala de estar en Oakland, California. La estancia pertenecía a Eric Hughes, un estudiante de posgrado de Matemáticas con el pelo largo, criado por mormones, al que le gustaban las chaquetas de ante con flecos. Hughes acababa de comprar la casa y aún no la había amueblado, así que la gente traía cojines para sentarse.

Tim May, un amigo de Hughes, se dirigió a los asistentes. May era un físico alto y barbudo que, como uno de los primeros empleados de Intel, había resuelto un problema crítico que llevó a un rediseño de sus chips; con los beneficios de las acciones, pudo jubilarse a los treinta y cuatro años, lo que le dio mucho tiempo para leer y escribir. Entre las inspiraciones que bullían en su cerebro había dos obras de ficción. Una era la novela de Ayn Rand *La rebelión de Atlas*, con su fantasía libertaria elitista de un enclave montañoso llamado Galt's Gulch donde los intelectuales del mundo podían ignorar el aburrido mundo y mediocre civilización. La otra era la novela de ciencia ficción de Vernor Vinge *True Names*, que contaba la historia de un grupo de *hackers* que tenían que operar bajo el disfraz de *nyms* (seudónimos) en la realidad virtual contra una variedad de adversarios, incluido el Verdadero Enemigo (el Gobierno), para protegerse en el mundo físico. May se convenció de que ya existía la tecnología para hacer realidad estas visiones: el dinero digital anónimo ideado por David Chaum y los avances en criptografía que habían hecho posible el sueño de este.

CRIPTOGRAFÍA SIMÉTRICA NO ERA SUFICIENTE

Durante más de dos mil años, la criptografía, la ciencia de la escritura secreta, había sido simétrica: la clave secreta utilizada para codificar un mensaje era la misma que la clave secreta empleada para descifrarlo. Esto significaba que la clave

DURANTE MÁS DE DOS MIL AÑOS, LA CRIPTOGRAFÍA, LA CIENCIA DE LA ESCRITURA SECRETA, HABÍA SIDO SIMÉTRICA

tenía que transmitirse entre las partes comunicantes, lo que presentaba tanto una vulnerabilidad como una limitación: la interceptación de la clave era un riesgo y el remitente y el destinatario tenían que conocerse de antemano. Esto había funcionado de manera imperfecta durante siglos, cuando las partes eran, por ejemplo, un emperador que se comunicaba con uno de sus comandantes. Pero, en los albores de internet, los tecnólogos con visión de futuro empezaron a imaginar un mundo en el que miles de millones de desconocidos querrían cifrar sus comunicaciones en línea, y la criptografía simétrica no sería suficiente. En la década de los setenta, Whitfield Diffie y Martin Hellman, en Stanford, y Ralph Merkle, en Berkeley, hicieron por separado un descubrimiento notable: un procedimiento para crear pares de claves matemáticamente conectadas. La primera permanecería oculta. La segunda, generada a partir de la primera, pero sin posibilidad de rastrear su origen, se compartiría abiertamente. Cualquiera podría entonces cifrar un mensaje con la clave pública, que solo sería descifrable con la clave privada. Por primera vez, unos desconocidos podrían comunicarse de forma segura. También se podía invertir el proceso. Se podía «firmar» (en realidad, codificar) un documento con la clave privada y cualquiera podría demostrar que fuiste tú quien lo firmó comprobando si se puede descifrar con la clave pública. Así nacieron las firmas digitales o la capacidad de acreditar la identidad en línea.

CHUCK PAINTER/ STANFORD NEWS SERVICE

De izquierda a derecha, Ralph Merkle, Martin Hellman y Whitfield Diffie, ganadores del premio Turing 2015 por revolucionar la criptografía moderna.

EL GOBIERNO DE EE. UU. EQUIPARABA LA CRIPTOGRAFÍA CON UN ARMA DE LA MISMA CATEGORÍA QUE LOS TOMAHAWK

May sintetizó estas ideas en un manifiesto que, ahora, en el salón de Hughes, leyó en voz alta para una multitud sentada en el suelo con las piernas cruzadas: «Un espectro acecha al mundo moderno: el espectro de la criptoanarquía». May lo dijo en un sentido positivo. Describió un futuro con pagos y mensajes en línea seguros e imposibles de rastrear, inmunes al escrutinio o la intervención gubernamental. Imaginó los posibles usos delictivos de esta tecnología, la mayoría de los cuales parecían no preocuparle, pero consideró la criptografía de clave pública tan revolucionaria como lo había sido la imprenta al trastocar las instituciones medievales o el alambre de púas al transformar la frontera estadounidense. «De este modo, el descubrimiento aparentemente menor de una rama arcana de las matemáticas llegará a ser la tijera que desarme el alambre de púas que se cierne sobre la propiedad intelectual».

ASC

Philip R. Zimmermann es el creador de Pretty Good Privacy, un paquete de *software* de cifrado de correo electrónico.

PRETTY GOOD PRIVACY

Más allá de esta utopía, que May llamó «Libertaria en el ciberespacio», su acción estaba motivaba por una amenaza inminente. Phil Zimmermann, un barbudo exactivista antinuclear, había lanzado PGP, que significaba Pretty Good Privacy («privacidad bastante buena») y era un programa gratuito que ponía a disposición de cualquiera la criptografía de clave pública. Basta con cargar una copia en el ordenador para poder cifrar los correos electrónicos antes de enviarlos. El Gobierno de Estados Unidos, que equiparaba la criptografía avanzada con un arma de la misma categoría que los misiles de crucero Tomahawk, barajaba emprender acciones legales contra él. May, Hughes y John Gilmore, uno de los primeros empleados de Sun Microsystems que también había podido jubilarse anticipadamente y luego cofundar la Electronic Frontier Foundation, querían poner la criptografía en manos de las masas. Después de que May leyera su manifiesto, una de las pocas asistentes, una mujer llamada Jude Milhon, conocida como St. Jude, propuso que el grupo se llamara *cypherpunks*. Se centrarían en la acción real en el mundo real: «Los *cypherpunks* escriben código», en palabras de Hughes.

UN GRUPO MUY ECLÉCTICO

Después, todos pasaron horas sumergidos en el Juego de la Criptoanarquía, un ejercicio que May y Hughes habían concebido para materializar protocolos matemáticos y abstracciones como el anonimato y el dinero digital y provocar nuevas formas de pensamiento. A cada participante se le asignó un rol: unos actuaban como traficantes de drogas tratando de ocultar sus movimientos, otros como agentes de contrainteligencia tras la pista de topos, y algunos como brókeres de información. May y Hughes distribuyeron dinero falso que representaba «dinero electrónico» y sobres vacíos dentro de otros sobres vacíos para simular *remailers*, servicios que despojaban a los correos electrónicos de toda información identificativa y dificultaban el rastreo de remitentes y destinatarios por parte de terceros. La jornada resultó caótica, con mensajes extraviados y participantes que cometieron errores con los sellos, pero el grupo lo pasó en grande.

Casi todos los *cypherpunks* eran hombres, pero, por lo demás, se trataba de un grupo bastante ecléctico. Un miembro afirmaba ser el príncipe de Liechtenstein. Otro acudía a las reuniones vestido de cuero. Un *cypherpunk* llamado John Draper era más conocido como «Captain Crunch» porque, en la década de los setenta, descubrió un método para hacer llamadas telefónicas gratuitas de larga distancia. Su hallazgo fue tan simple como ingenioso: los silbatos incluidos en las cajas de cereales Cap'n Crunch emitían una frecuencia de 2600 hercios que permitía burlar el sistema de enrutamiento de AT&T. (Por esto, Draper cumplió condena en una prisión federal). Al grupo también se unirían el inventor de BitTorrent, Bram Cohen, el letrista de Grateful Dead y cofundador de la Electronic Frontier Foundation, John Perry Barlow, el creador de Signal, Moxie Marlinspike, y Julian Assange. Aunque los *cypherpunk* del área de la Bahía de San Francisco se reunían en persona una vez al mes, su principal punto de encuentro era una lista de correo

SCALA.USC.EDU

Bob Gudgel, Dee Pritchard y John Draper en 1971. Draper, «Captain Crunch», representa el eslabón perdido entre los primeros hackers y los fundadores del movimiento *cypherpunk*.

LA ADMINISTRACIÓN CLINTON PRESIONÓ A LOS FABRICANTES PARA QUE EQUIPARAN SUS PRODUCTOS CON EL CLIPPER CHIP

electrónico a la que cualquiera podía suscribirse. Muchos participantes usaban sus nombres reales, pero también había habituales muy respetados conocidos solo por seudónimos como Black Unicorn y Pr0duct Cypher. Usar seudónimos para publicar en la lista con múltiples identidades se convirtió en un juego para algunos y en una herramienta para otros. Internet seguía siendo una frontera inexplorada, abierta a descubrir los nuevos tipos de relaciones con desconocidos que posibilitaba. Los seudónimos representaban además una idea: ser juzgado por tus ideas y no por tus credenciales.

Los *cypherpunks* definitivamente no eran personas que contemplaran la web embrionaria y pensaran «bah». Al contrario, veían una enorme oportunidad y compartían tanto una aguda previsión sobre cómo un mundo digitalmente conectado pondría en peligro la privacidad personal como la convicción de que solo la criptografía podría salvaguardarla. Esto importaba tanto si eras un defensor de la mínima intervención estatal que solo querías que te dejarán en paz, un activista de derechos civiles preocupado por la seguridad de los disidentes en países autocráticos o una persona normal que simplemente quería escribir correos electrónicos sin miradas indiscretas. La criptografía, como le gustaba decir a Hughes, era «la consecuencia matemática de las suposiciones paranoicas». (El propio Hughes, según un *cypherpunk* llamado Jim McCoy, «mantenía su coche inmaculadamente limpio, para que, si lo paraban, la policía no tuviera una excusa para registrarlo»).

BIG BROTHER INSIDE

Dado que un principio fundamental de los *cypherpunks* sostenía que «el código es discurso», cualquier restricción sobre él se consideraba una violación de la Primera Enmienda. ¿El Gobierno quería criminalizar un programa informático? Adam Back se ponía a vender camisetas estampadas con una fórmula de encriptación prohibida para la exportación y cualquier *cypherpunk* respetable podía llevarla alegremente al embarcar en un vuelo internacional. Otros *cypherpunks*, con el mismo fin, se tatuaron los algoritmos prohibidos. Cuando un gran jurado estaba considerando acusar a Zimmermann, el creador del PGP, los *cypherpunks* ayudaron a difundir su *software* exportando versiones impresas y digitales para que se extendiera tanto en el extranjero que el Gobierno de Estados Unidos no tuviera ningún recurso. Después de que la Administración Clinton presionara en 1993 a los fabricantes de teléfonos para que equiparan sus productos con el Clipper Chip, una puerta trasera para permitir la vigilancia gubernamental, los *cypherpunks* entraron en las tiendas de electrónica y pegaron pegatinas con la leyenda *Big Brother Inside* («Gran Hermano dentro») en los aparatos comprometidos. Para ciertos *cypherpunks*, la defensa de la privacidad respondía también a inquietudes más personales. Gene Hoffman, un antiguo ejecutivo de PGP, me dijo que el grupo no

estaba unido únicamente por ideales abstractos. Los derechos de privacidad son «algo difícil de cuidar. Mucha gente del movimiento *cypherpunk* deseaba proteger ciertos aspectos de su vida privada. La confluencia entre *cypherpunk* y practicantes de BDSM resultaba notablemente alta», me confesó Hoffman. Cuando le comenté esto a un *cypherpunk* llamado Doug Barnes, de veintidós años, a quien Neal Stephenson ha atribuido la invención del término *meatspace*, él no estuvo de acuerdo: «La mayoría de los *cypherpunk* que conozco son un poco excesivos a la hora de compartir. Había mucha gente que era notoriamente poliamorosa».

LIBERTARIA EN EL CIBERESPACIO

La combinación de revolución y tecnología a veces producía un compuesto inestable, así, entre los *cypherpunk* existía una facción radical que se autodenominaba criptoanarquista. Eran más radicales que los libertarios y creían que la tecnología podía eliminar la necesidad de cualquier Gobierno. Tim May imaginó un mercado de información anónimo, al que llamó BlackNet, donde se podían vender ilícitamente secretos corporativos e incitar a compartir información privilegiada. Otros *cypherpunk* hablaban esperanzados sobre el uso de dinero digital para evadir impuestos. Uno llamado Jim Bell escribió un ensayo titulado *Política de asesinato*, en el que proponía un sitio web en el que las personas que utilizaran dinero digital anónimo pudieran financiar una gran recompensa para quien adivinara correctamente la fecha de la muerte de un funcionario público en particular; esto presumiblemente incentivaría a otra persona a «adivinar» una fecha y tratar de hacer que la muerte ocurriera en ese momento, mientras que, en teoría, los financiadores originales quedarían libres de responsabilidad penal. Bell pasó más tarde años en una prisión federal, primero por evasión de impuestos y luego por acechar y acosar a agentes de la agencia tributaria. Phil Zimmermann, un hombre amable que se enfrentaba a la amenaza de un proceso penal y había llevado traje todos los días durante los últimos tres años para presentar una imagen respetable ante la opinión pública, se quedó conmocionado cuando, en una reunión de *cypherpunk* organizada por PGP, un miembro que se hacía llamar Lucky Green metió la mano en su bolsa de lona y anunció: «El Cypherpunks Gun Club va a practicar tiro el próximo sábado y estáis todos invitados». A continuación sacó un rifle de asalto AR-15 con un cargador de munición. «Las oficinas de PGP estaban en un edificio bancario», recordó Phil.

TRAVIS GOODSPEED

En la imagen, el chip VLSI de 1993, que representa uno de los momentos más cruciales en la guerra entre la privacidad individual y la vigilancia.

Algunos *cypherpunk* eran bastante dogmáticos y tendían a mantener discusiones interminables que irritaban tanto a los criptógrafos profesionales como a los

Los ataques a las Torres Gemelas desencadenaron una expansión del poder gubernamental de vigilancia que validaría muchas de las predicciones más sombrías del movimiento *cypherpunk*.

programadores y *hackers* en activo. «En aquella época se decía: "Los *cypherpunk* escriben código" —recuerda Jon Callas, que trabajó para PGP y más tarde para Apple y que asistió a muchas de estas primeras reuniones—. Y yo pensaba: "Estoy demasiado ocupado programando para ser un *cypherpunk*"». Cuando Bram Cohen organizó más tarde una convención de *hackers*, anunció que excluiría explícitamente temas como la «criptografía matemática sin aplicación práctica» y el «debate político sobre el depósito de claves». No obstante, la sensación de estar escribiendo un capítulo decisivo de la historia era ineludible. Ser un *cypherpunk* era sentir la emoción de los pioneros. Estabas liderando la marcha hacia un valiente futuro, impulsado por una causa justa. Debido al énfasis en los seudónimos, la descentralización y la economía libertaria, era evidente el aire *cypherpunk* que desprendía Satoshi Nakamoto. Pero la razón principal por la que Stefan Brands y otros me habían señalado a los tecnólogos rebeldes era que estos se referían constantemente a la necesidad del dinero digital. Muchos *cypherpunk* lo consideraban su objetivo final, la piedra angular de la «Libertaria en el ciberespacio» de May. Mientras que los números de serie y los banqueros hacían rastreable el dinero antiguo, el dinero futuro sería anónimo. Mientras que el dinero antiguo estaba conectado a la política y los Gobiernos, el dinero futuro sería independiente. La moneda digital privada se convirtió en una obsesión para los *cypherpunks* más radicales, porque representaba una amenaza para los Gobiernos, con su control exclusivo sobre la creación del dinero y su capacidad para imponer tributos.

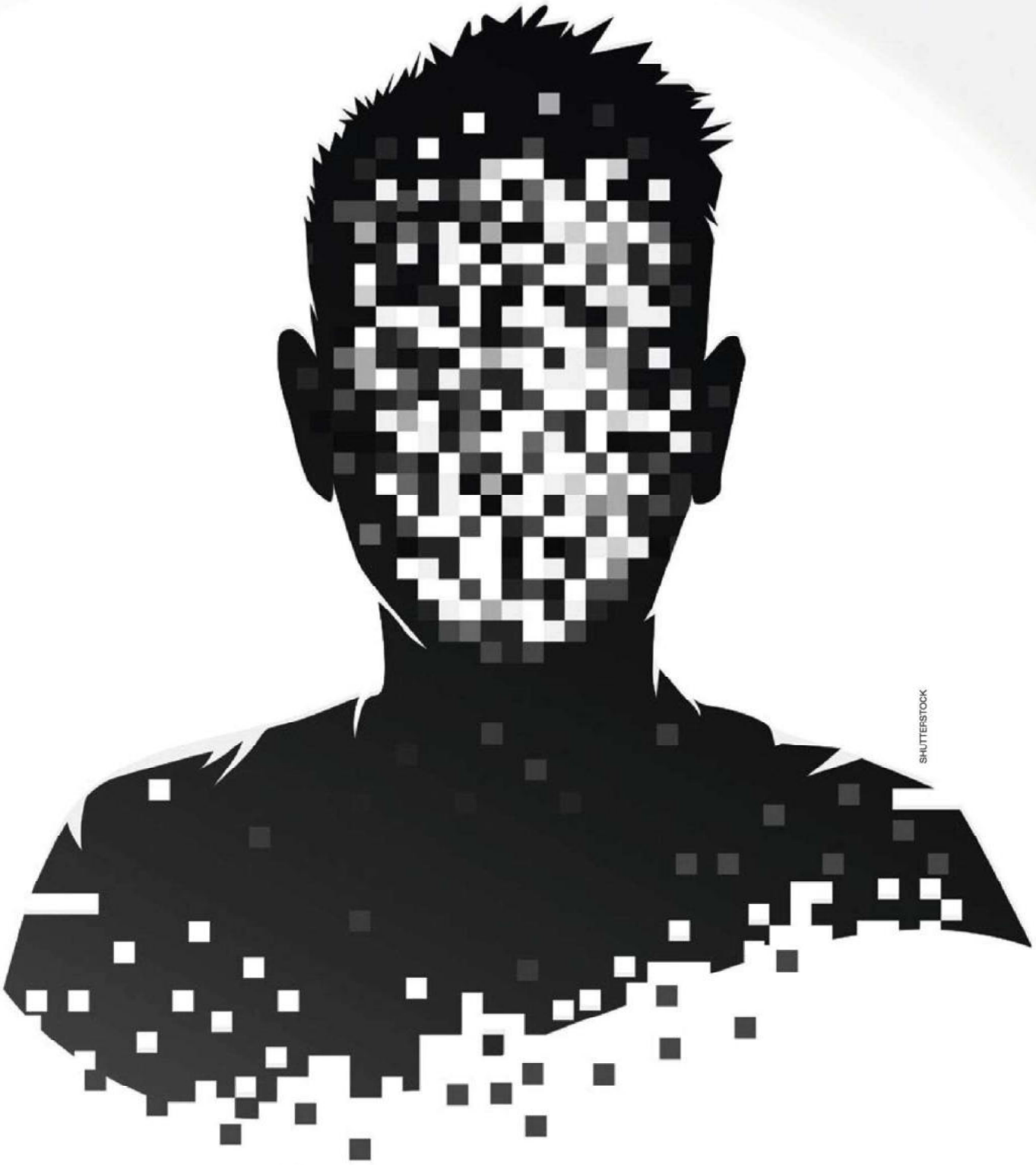
UN LARGO CAMINO QUE RECORRER

El movimiento *cypherpunks* mantenía una relación ambivalente con David Chaum. Su artículo de 1982 «Blind Signatures for Untraceable Payments», que sentó las bases informáticas del dinero digital, rozaba lo sagrado. Eric Hughes trabajó en DigiCash durante un tiempo. Sin embargo, muchos *cypherpunks* mos-

MIENTRAS QUE LOS NÚMEROS DE SERIE Y LOS BANQUEROS HACÍAN RASTREABLE EL DINERO ANTIGUO, EL DINERO FUTURO SERÍA ANÓNIMO

traron su indignación ante la orientación comercial de Chaum, quien no tuvo reparos en hacer valer sus patentes. Y el dinero de Chaum, visto a través de la lente de los *cypherpunks*, presentaba un defecto fundamental: necesitaba una entidad emisora para crear la moneda y evitar el doble gasto mediante la validación de las transacciones. Chaum convenció al Mark Twain Bank de St. Louis, Misuri, para que prestara este servicio en Estados Unidos. Pero, para los *cypherpunks*, una entidad emisora representaba un tercero de confianza, un punto único de fallo, un blanco vulnerable. El Gobierno podría cerrarla por miedo a la evasión fiscal; los delincuentes podrían hacer daño al poseedor de las llaves de cualquier Fort Knox virtual. «Recordemos el deseo de Nerón de que Roma tuviera un solo cuello que pudiera cortar —escribió mucho más tarde un *cypherpunks* llamado James Donald—. Si les ofrecemos ese cuello, lo cortarán». Al final resultó que el dinero digital era un sueño que los *cypherpunks* nunca alcanzaron. A finales de los noventa, los primeros habían empezado a abandonar el grupo. Algunos se aburrieron. Otros se ocuparon con sus trabajos y familias. Otros se cansaron de la avalancha de *spam* y del caos general que inevitablemente afligía a una lista de correo poblada por anarquistas que denunciaban el más mínimo esfuerzo de moderación como «censura». El grupo se dispersó aún más después del 11S, cuando las diferencias políticas internas que habían permanecido enmascaradas por una creencia compartida en la privacidad habilitada por la criptografía se hicieron más evidentes.

Los *cypherpunks* continuaban reuniéndose para celebrar la expiración de patentes, como aquel sábado por la tarde de julio de 2005 en una cervecería al aire libre en Portola Valley, California, donde brindaron por el fin de la patente de diecisiete años que Chaum mantenía sobre las «firmas ciegas», un método criptográfico que permite verificar transacciones manteniendo el anonimato. Y ese año se produjo una gloriosa, aunque efímera, explosión de energía *cypherpunks* cuando un grupo de ellos intentó crear un paraíso de datos extraterritorial en una plataforma antiaérea azotada por el viento en el mar del Norte. Sin embargo, desde finales de los noventa hasta 2008, se vivió una edad oscura del dinero digital, provocada en parte por la represión contra el dinero alternativo durante la guerra contra el terrorismo tras el 11S; el más exitoso de estos sistemas, e-gold, acabó enfrentando incautaciones de activos, demandas civiles y acusaciones penales. Algunos de los *cypherpunks* más comprometidos comenzaron a perder la esperanza. «Tim May ha sucumbido a un mal humor terminal —escribió James Donald en la ahora degradada lista de cypherpunks—, al descubrir que la trascendencia criptográfica no llegará pronto». Otros, entre ellos Donald, mantenían el optimismo: «Tenemos un largo camino por recorrer, pero lo estamos haciendo». Un reducido grupo de *cypherpunks* nunca abandonó el sueño del dinero electrónico. Y, a medida que profundizaba en la historia del movimiento, seguía escuchando los mismos nombres. ■



SHUTTERSTOCK

Wei

Wei Dai era un criptógrafo aficionado que había creado Crypto++, una biblioteca de herramientas de *software* que utilizaba bitcoin, y Dai todavía la mantenía, pero la razón principal por la que algunas personas pensaban que podría ser Nakamoto era un concepto sobre el que Dai había escrito en 1998.

B-money, como él lo llamó, combinaba varias ideas que luego aparecerían en bitcoin: entre ellas una red entre pares que mantenía colectivamente un registro común de todas las transacciones; un mecanismo de creación de dinero basado en la resolución de acertijos computacionales y el uso de criptografía de clave pública para proteger las identidades de los usuarios. Y el b-money de Dai, al igual que el Hashcash de Back, se encontraba entre el puñado de referencias que Nakamoto mencionó explícitamente al final del libro blanco del bitcoin.

ASC

Wei Dai es uno de los precursores más directos e influyentes para la creación del bitcoin.

UN CRIPTÓGRAFO PROFESIONAL

Dai también era, como Nakamoto, una figura enigmática. Se había graduado en la Universidad de Washington a finales de la década de los noventa, pero, aparte de eso, se sabía poco sobre él. Resultaba imposible encontrar una sola fotografía suya en internet. Un perfil tan reservado exigía, sin duda, aproximarse con la máxima cautela y delicadeza.

—¿Es usted Satoshi Nakamoto? —le espeté por correo electrónico aquel verano de 2011.

—Yo no soy Satoshi —respondió Wei.

Mucho antes de que apareciera el bitcoin, Wei, tras años dedicados a la criptografía, había llegado a la conclusión de que esta no sería tan determinante para el futuro como había imaginado inicialmente y se había volcado más hacia la filosofía, me explicó. Ahora dedicaba gran parte de su tiempo a participar en LessWrong, un blog con gran seguimiento entre los futuristas de Silicon Valley, enfocado en «perfeccionar el arte de la racionalidad humana».

«No creo que sea alguien de mi entorno —continuó Wei, refiriéndose a Nakamoto—, ya que aparentemente desarrolló el bitcoin de manera independiente y desconocía mi artículo sobre b-money hasta que Adam Back se lo mencionó. Coincido con la teoría de Gwern de que probablemente no sea un criptógrafo profesional o un académico. Intuyo que debe ser un estudiante o un programador solitario. (Yo mismo era estudiante cuando comencé a trabajar en Crypto++ y escribí sobre b-money)».

Wei me facilitó algunos correos electrónicos que Nakamoto le había enviado. En el primero, de agosto de 2008, Nakamoto decía que quería citar b-money en el libro blanco y necesitaba saber cuándo lo había publicado Wei. El segundo, de principios de 2009, contenía un enlace al software de bitcoin que Nakamoto compartió con Wei el día después de su lanzamiento. «Creo que logra casi todos los objetivos que te propusiste resolver en tu artículo sobre b-money», escribió Nakamoto. ■

Boom boom

Uno de los desafíos más serios a los que se enfrenta el bitcoin es la llegada de las computadoras cuánticas capaces de romper la criptografía de clave pública que protege todas las transacciones y *wallets*.

SHUTTERSTOCK


2359
2359
9898

Otra persona de interés recurrente entre los Bitcoin Talkers era Nick Szabo y a él me dirigí a continuación. Szabo era solo un poco menos solitario que Wei, con un historial laboral en gran medida invisible. Más tarde diría que creía en la «seguridad a través del anonimato».

Szabo se había sentido atraído de forma natural por los *cypher*-punks, con su compromiso con la acción en el mundo real. La criptografía le permitió lo que él llamó «realpolitik libertaria: ingeniería práctica en lugar de masturbación intelectual». En abril de 1993, cuando vivía en Oregón (donde había trabajado para el fabricante de ordenadores Sequent), escribió un folleto sobre «cómo proteger tu privacidad electrónica» y lo repartió en una reunión de libertarios de Portland. También acudió a un foro de televisión en el área de Portland para discutir su plan de abandonar AT&T en favor de otro proveedor como protesta contra el apoyo del gigante de las telecomunicaciones al Chip Clipper y ofreció 200 dólares como adelanto a quien fuera el primero en producir pegatinas de alta calidad con el mensaje «Gran Hermano dentro». Propuso estrategias para contrarrestar la emergente tecnología de reconocimiento facial mediante la «encriptación» de la propia imagen, recomendando evitar disfraces demasiado evidentes (pasamontañas, gafas de sol por las noches) en favor del uso de sombreros, peinados y técnicas de maquillaje.

LA LUNA ES UNA AMANTE CRUEL

De alta estatura, cuerpo bastante fofo y un evidente desinterés por la moda, Szabo había crecido en el estado de Washington y había heredado de su padre, Julius, un profundo rechazo hacia el socialismo. Los padres de Julius, naturales de Hungría, habían presenciado cómo los comunistas confiscaban su granja. Durante sus años universitarios en aquel país, Julius participó en la insurrección de 1956 contra el Gobierno títere de los soviéticos y posteriormente escapó a Estados Unidos, donde desarrolló su carrera como científico especializado en botánica. La madre de Nick, Mary, también poseía una natural inclinación hacia las matemáticas: trabajaba como contable y solía traer a casa un Apple II de su oficina para que sus hijos pudieran utilizarlo.

Cuando Szabo era adolescente, su novela de ciencia ficción favorita era *La Luna es una cruel amante*, de Robert Heinlein, que fusionaba sus dos grandes pasiones: la filosofía libertaria y el espacio exterior. Mientras estudiaba Informática en la Universidad de Washington, una década antes que Wei, consiguió unas prácticas en el Laboratorio de Propulsión a Reacción de Pasadena, donde trabajó en la Red del Espacio Profundo, programando comunicaciones para proyectos como *Voyager*, *Galileo* y *Magellan*. Esta experiencia transformó su vida. Al observar el dinamismo de los proyectos más modestos que se desarrollaban allí y en el cercano CalTech —desde el *Mars Rover* hasta las redes neuronales—, se desencantó con el programa espacial estadounidense, que no estaba orientado a la colonización

SZABO HABÍA CRECIDO EN EL ESTADO DE WASHINGTON Y HABÍA HEREDADO UN PROFUNDO RECHAZO HACIA EL SOCIALISMO

espacial a largo plazo, sino centrado en montar estaciones y transbordadores espaciales que solo buscaban titulares. Llegó a considerar estos «sacramentos del culto a los astronautas» como una afrenta cortoplacista, espectáculos mediáticos impuestos a los contribuyentes por una burocracia inflada de la NASA repleta de «artistas de las presentaciones». Szabo podía intelectualizar hasta el punto de considerar sus propias sensaciones corporales como si fueran datos obtenidos mediante instrumentos científicos ajenos. Incluso su excitación sexual se convirtió en una métrica. De las más de cien mujeres a las que había invitado a salir: «En más de la mitad de las ocasiones, he tenido una erección». La canción *Dust in the Wind*, de Kansas, le deprimía: «Algunos estilos musicales pueden tener un impacto muy fuerte en mis emociones, en mi experiencia».

Quizá los infortunios de su juventud (en el instituto le habían acosado hasta que empezó a devolver los golpes) le habían vuelto combativo. No se contenía al atacar a quienes esgrimían argumentos que no respetaba, diciéndole a uno: «Gracias por los recuerdos, abuelo»; a otro: «Suponía que eras medianamente inteligente», y a un tercero: «Aquí tienes una propuesta de reforma: "Despierta de una puta vez al mundo real de ahí fuera"». Sus antagonistas le sugirieron de diversas formas que necesitaba litio o que estaba «desesperadamente solo», o le preguntaron: «¿Alguien abusó sexualmente de ti cuando eras un niño?».

Poco después de suscribirse a la lista de *cypherpunks*, Szabo se trasladó desde Oregón al área de la bahía de San Francisco para estar cerca de las reuniones presenciales del grupo. Aunque sus interacciones en línea le resultaban al menos tan estimulantes como las presenciales, disfrutaba de su nueva y embriagadora vida. Una noche de agosto, pasada la medianoche, condujo hacia el sur de Los Gatos, alejándose del resplandor urbano, hasta las estribaciones de las montañas de Santa

JACK AND DEBORAH J. WARNER/ SMITHSONIAN INSTITUTION

La Apple II puso poder de procesamiento en manos de aficionados, *hackers* y visionarios que lo usarían para experimentar con criptografía, redes *peer-to-peer* y sistemas descentralizados.

Cruz, donde instaló una tumbona, se cubrió con mantas y jerséis y contempló el despejado cielo nocturno. Durante las dos horas siguientes, fantaseó con la minería de cometas, las colonias espaciales y los «cerebros del tamaño de Júpiter», mientras observaba docenas de deslumbrantes meteoros surcar el firmamento, incluida «una espectacular bola de fuego que estalló en el firmamento». Dos días después asistió a una reunión de *cypherpunks* con todas las figuras destacadas: John Gilmore, Eric Hughes, Tim May, Whit Diffie (coinventor de la criptografía de clave pública). En el encuentro, Romana Machado, desarrolladora de *software* para el dispositivo portátil Newton de Apple y «modelo de *glamour*» conocida como Cypherella (*Playboy*, noviembre de 1985), presentó Stego, un *software* libre que había creado para ocultar mensajes dentro de imágenes.

ÉXTASIS DEL FUTURO

Machado también era miembro de un grupo llamado los extropianos, con el que Szabo llegó a involucrarse profundamente. Estos estaban dedicados al transhumanismo o la extensión extrema de la vida, y abarcaba desde drogas inteligentes hasta inteligencia artificial y la Singularidad, ese momento futuro en el que las conciencias humanas podrían transferirse al ámbito digital. Szabo lo llamaba «éxtasis futuro».

El extropianismo defendía la expansión en todos los sentidos. La camiseta extropiana llevaba por lema: «Adelante, Arriba, Afuera» y varios miembros del grupo adoptaron apodos optimistas y tecnológicos como Jay Prime Positive, Tom Morrow, Max More y David Victor de Transcend. Tim May, como él lo llamaba, era Klaus! von Future Prime, y Szabo a veces se hacía llamar Boom Boom o Boom Boom von Past Primeval.

SHUTTERSTOCK

Vista aérea de Cupertino y de la bahía de San Francisco. Este fue el epicentro donde convergieron todos los elementos que hicieron posible el bitcoin.

LOS EXTROPIANOS ESTABAN DEDICADOS AL TRANSHUMANISMO O LA EXTENSIÓN EXTREMA DE LA VIDA

Los extropianos fusionaban la positividad del futuro con una alergia libertaria a la restricción, ya fuera por parte del Gobierno, la gravedad o el envejecimiento. Un extropiano típico había leído montones de ciencia ficción y era un ateo que había hecho de la tecnología una religión. Aunque el grupo compartía muchos miembros con los *cypherpunks*, los extropianos eran más hedonistas. ¿Por qué vivir más tiempo si no te lo pasas bien?. «Tenían mejores drogas, sin duda —recordaba Doug Barnes, que pertenecía a ambos grupos—, y además eran más guapos y estaban más en forma». La oportunidad de que los frikis salieran con chicas guapas «formaba parte de nuestra marca», se hacía eco Tom «Morrow» Bell, uno de los cofundadores del grupo.

UNIVERSIDAD DE OXFORD

Nick Bostrom, filósofo sueco y director del Future of Humanity Institute en Oxford.

MIEMBROS NOTABLES

La lista de intereses del grupo era un programa de estudios para los futuros líderes de Silicon Valley del siglo XXI: extensión de la vida, colonización espacial, educación en casa, *biohacking*, carga de conciencia, IA, autosoberanía, ciudades marítimas flotantes, dinero digital, oposición al Estado, transhumanismo, pluralismo jurídico, mercados de predicción, nómadas digitales (su término era tecnómadas) y memética, entre otras cosas.

Un número notable de miembros fueron o serían influyentes. Nick Bostrom fue el filósofo de Oxford de la llamada hipótesis de la simulación, la creencia improbablemente extendida, entre Elon Musk y sus compañeros, de que todos vivimos en un videojuego. Robin Hanson fue pionero en los mercados de predicción modernos. K. Eric Drexler fue el principal defensor de la nanotecnología. Hans Moravec, un especialista en robótica, fue el visionario de la idea de transferir la conciencia humana a sistemas digitales. Bart Kosko fue un destacado divulgador de la lógica difusa. Eliezer Yudkowsky se convirtió en el más conocido pesimista de la IA, así como en el líder del movimiento racionalista, obsesionado con la estadística y la teoría de juegos.

A MEDIDA QUE SZABO SE SUMERGÍA EN LOS CÍRCULOS EXTROPIANOS Y *CYPHERPUNKS*, SU CARÁCTER PARECÍA TRANSFORMARSE

Cuando Szabo descubrió a los extropianos, se encontró con personas que discutían seriamente, como ingenieros analizando proyectos futuros viables, sobre conceptos que él anteriormente había descartado como fantasías surgidas de las historias de ciencia ficción que tanto disfrutaba. Criónica. Digitalización de la conciencia. Nanotecnología. Los días que no tenía que madrugar para ir a trabajar, le gustaba quedarse en la cama, en ese estado entre el sueño y la vigilia, fantaseando y desarrollando sus múltiples ideas.

ADVERSARIOS DE LA MUERTE

La visión del programador informático del cuerpo como un sistema susceptible de optimización le resultaba fascinante. Se inscribió en la Life Extension Foundation, siguió un régimen para perder peso, analizaba su orina para controlar sus niveles de cetonas, redujo su consumo de grasas en favor de alimentos hervidos o crudos, se mantuvo fiel a la Coca-Cola light y tomaba suplementos vitamínicos y minerales, un nootrópico para la claridad mental llamado Deep Thought y el supresor del apetito Acutrim. Dos veces por semana nadaba un kilómetro y medio. En seis meses, redujo su peso de 108 a 82 kilos y, a partir de entonces, mantuvo una dieta basada principalmente en ensaladas.

Era un hombre joven y soltero con muchas ganas de conocer mujeres, y parte de aquel régimen extremo se debía seguramente a la vanidad. Pero también era partidario de la apuesta de Pascal. La versión original, concebida por el filósofo francés del siglo XVII Blaise Pascal, planteaba una apuesta religiosa: ante la posibilidad de que Dios existiera, resultaba más sensato vivir como si su existencia fuera cierta, maximizando así las probabilidades de alcanzar la salvación eterna. El equivalente extropiano sostenía: debes esforzarte por vivir el mayor tiempo posible y de la forma más saludable posible para aumentar las probabilidades de que la reanimación criónica o la transferencia mental estén disponibles antes de que mueras.

Szabo también se entusiasmó con las visiones más ambiciosas de los extropianos. Se interesó por la nanotecnología y por las definiciones de la muerte (los extropianos a veces se autodenominaban adversarios de la muerte). Le atraía la idea de que, una vez que la transferencia de la conciencia fuera posible y el impulso sexual ya no resultara necesario para la propagación de la especie, se pudiera rediseñar su finalidad: «Si experimentara un orgasmo el día de pago, en lugar de recibir solo un aburrido papel con algunos números abstractos, probablemente estaría más motivado para ganar dinero».

Se mudó a una casa de color tostado y techo alto en Cupertino, que era el hogar de una comunidad intencional llamada Nexus-Lite. Entre sus cuatro compañeros de piso se encontraba Romana Machado, y a veces organizaban fiestas, como una cena en la que cada uno traía algo, un sábado de marzo de 1994, a la que llamaron Extropaganza. Algunos invitados, al llegar, se dieron el apretón de manos extro-

piano que había ideado el cofundador del grupo, Max More: después de entrelazar los dedos, los disparabas hacia arriba. Szabo tenía una personalidad erudita y sus compañeros de piso compartían ideas políticas similares: Machado se paseaba por la fiesta con un traje de dominatrix, vestida como «el Estado» y sujetando con una correa a su novio Geoff Dale, que iba vestido como «el Contribuyente». La lista de reproducción extropiana iba desde la acertada *Forever Young*, de Alphaville, hasta la música electrónica futurista de The Orb.

CONTRATOS INTELIGENTES

A medida de que Szabo se sumergía en los círculos extropianos y *cypherpunks*, su carácter parecía transformarse. Quedaron atrás los airados desvaríos del activista espacial combativo. Se volvió más cortés y empático. Aunque mantenía una disposición tranquila y reservada, con escaso contacto visual, los compañeros extropianos que convivían con él lo describían como «agradable» y «afable», además de reconocer que irradiaba inteligencia. Su dominio de una gama tan sorprendente de temas llevó a algunos extropianos que no lo habían conocido en persona a especular que su nombre era en realidad el seudónimo de un colectivo.

A pesar de su libertarismo, Szabo evitaba el egoísmo de Ayn Rand y se consideraba un «comunitarista», alguien a quien no le importaba ofrecerse voluntario por un bien mayor, en contraste con su propio hermano, a quien llamaba «un aprovechado: absorto en sus propios deseos y ambiciones». En 1993, Szabo se había alejado de la política del Partido Libertario y se había inclinado hacia la acción individua-

MATT GREEN/ PRINCETON UNIVERSITY

Reunión de algunos de los iniciadores del bitcoin, donde aparece Nick Szabo (marcado con una X), cuya presencia alimentó las especulaciones sobre su posible identidad como Nakamoto.

lista, «haciendo mi propia libertad en un mundo no libre». Por esa época, Szabo se interesó especialmente por los «contratos inteligentes», como él los llamaba, basados en la criptografía, un código informático autoejecutable que podía, como una máquina expendedora que dispensaba una chocolatina a cambio de una moneda, funcionar sin interferencia humana. Su otro gran interés era el dinero digital y su capacidad para apoyar los mercados en línea. Durante un breve periodo de tiempo, trabajó, como Eric Hughes, para DigiCash de Chaum en los Países Bajos.

RESOLUCIÓN DE UN ROMPECABEZAS COMPUTACIONAL

Fue en lib-tech, una lista de correo privada creada por Szabo para centrarse en las tecnologías que promueven la libertad, donde Wei Dai escribió por primera vez sobre *b-money* en 1998. También fue allí, ese mismo año, donde Szabo planteó su propia idea del *bit gold*, que describió como «dinero digital independiente de la confianza». Al igual que el *b-money*, el *bit gold* presagiaba el bitcoin: estaba motivado por el deseo de acabar con el llamado tercero de confianza y replicar en el ciberespacio la «escasez infalsificable» de los metales preciosos. Al igual que los bitcoins, el *bit gold* se acuñaría mediante la resolución de un rompecabezas computacional, la solución sería confirmada por una red de ordenadores y cada solución estaría vinculada criptográficamente tanto a su predecesor como a su sucesor. Al igual que los bitcoins, el *bit gold* tendría «mineros».

Tras el anuncio del bitcoin por parte de Nakamoto en octubre de 2008, Szabo mostró una sutil cautela al establecer la conexión, republicando en diciembre una entrada de blog de 2005 sobre *bit gold* sin mencionar la reciente aparición de aquella propuesta tan similar. La primera vez que Szabo hizo referencia al bitcoin por su nombre, en mayo del año siguiente, señaló que funcionaba «de manera muy similar» a *bit gold*. Posteriormente describiría el bitcoin como «una implementación de la idea de *bit gold*».

¿ES USTED SATOSHI NAKAMOTO?

Cuando Gwern Branwen sugirió que no había nada tecnológicamente nuevo en bitcoin, Szabo salió en su defensa, afirmando que «no una mera lista de características criptográficas, sino un sistema extremadamente complejo de matemáticas y protocolos interactivos que perseguía un objetivo muy impopular. Sin duda, el principal obstáculo para que algo como el bitcoin hubiera surgido antes era el porqué: prácticamente todos los que escucharon hablar del concepto general lo consideraron una idea terrible. Los únicos que nos entusiasmamos con la idea fuimos yo, Wei Dai y Hal Finney [otro *cypherpunk*], al menos lo suficiente (o en el caso de Dai, su concepto relacionado) como para desarrollarla hasta la aparición de Nakamoto (asumiendo que Nakamoto no fuera realmente Finney

AL IGUAL QUE LOS BITCOINS, EL *BIT GOLD* SE ACUÑARÍA MEDIANTE LA RESOLUCIÓN DE UN ROMPECABEZAS COMPUTACIONAL

El equipo técnico original de DigiCash (1994) posa con las computadoras donde implementaron el primer sistema funcional de dinero digital con privacidad criptográfica.

o Dai). El grupo donde confluyen expertos en criptografía y libertarios capaces de entusiasmarse con una propuesta tan estilo fiebre del oro es, ya de por sí, extremadamente reducido».

Cuando le pregunté a Nick en el verano de 2011 sobre su experiencia con bitcoin, respondió: «No lo he usado. No hay nada a la venta que quiera comprar, un problema común al comenzar con una moneda. He leído el documento, algunas de las descripciones en línea y parte del código fuente».

Al igual que con Wei, probé el enfoque directo con Nick. Todavía no descartaba la posibilidad de que Nakamoto estuviera frustrado porque nadie se hubiera molestado simplemente en preguntarle.

—¿Es usted Satoshi Nakamoto?

—No —respondió Nick.

Cuando le pregunté por su comentario «suponiendo que Nakamoto no sea realmente Finney o Dai», respondió:

—Son solo posibilidades lógicas.

Añadió que siempre había encontrado la descripción de Wei del *b-money* «irremediablemente vaga».

Le mencioné otros candidatos a ser Nakamoto.

—No voy a seguir especulando sobre esto —respondió Nick.

Creo que ha hecho una gran contribución al mundo y, a cambio, quiero respetar su privacidad.

Sin embargo, Nick sí mencionó a Finney. Era «muy discapacitado, como Stephen Hawking», advirtió Nick, pero pensó que debería intentar entrevistarlo. Nick no fue la primera persona que me sugirió que me pusiera en contacto con Finney. Mike Hearn había dicho que sería bueno para «conocimientos profundos». Y Nick me describió a Finney como «la primera persona en implementar este tipo de plan». ■

Una velada de socialización bajo seudónimo

En la primera Conferencia Mundial de Bitcoin, la velada de socialización bajo seudónimo reunió a unos pocos pioneros de todo el mundo en torno a un dinero invisible que apenas comenzaba a despertar curiosidad y escepticismo.

SHUTTERSTOCK

No estaba más cerca de hallar una respuesta cuando, semanas después de mi correspondencia con Nick, asistí a la primera Conferencia Mundial de Bitcoin. Simplemente conseguir una entrada resultó complicado.

Costaba 26 dólares y debía pagarse en bitcoin. Decidí adquirir 200 dólares de la criptomoneda. Me parecía una locura desembolsar catorce dólares por unidad por algo intangible, invisible e inútil para cualquier necesidad real.

Decidido a no repetir el error del pobre Stefan Thomas, primero creé una cuenta en Mt. Gox, la plataforma de intercambio de bitcoin con sede en Tokio que todos consideraban más fiable. Luego me registré en Dwolla, una procesadora de pagos de Iowa que debía verificar mi cuenta bancaria antes de aceptar mi dinero. Este proceso tomó cuatro días. Después transferí dinero de mi banco a Dwolla, operación que tardó otro día en completarse. Posteriormente, tuve que mover el dinero de Dwolla a Tradehill, una casa de cambio en San Francisco, para convertir mis dólares en catorce bitcoins. Finalmente, retiré cuatro de ellos de Tradehill a una dirección controlada por mi ordenador y envié aproximadamente dos tercios al organizador de la conferencia (el precio de un bitcoin había caído por debajo de los 11 dólares para entonces). El resto lo transferí de Tradehill a Mt. Gox para su custodia.

ASC

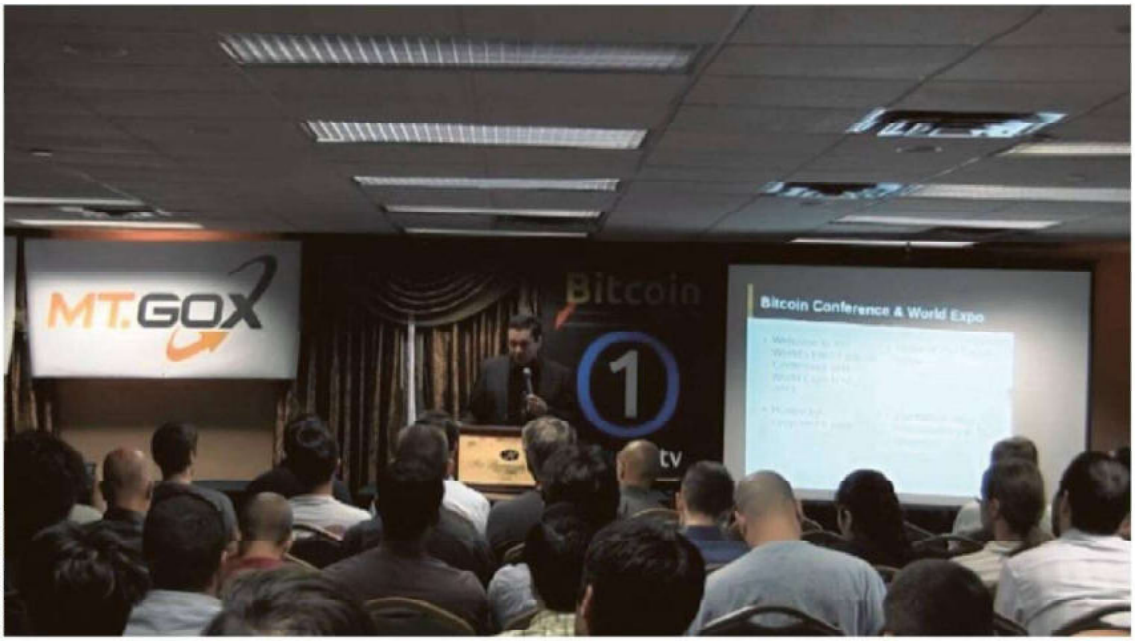
Bruce Wagner presentador de *The Bitcoin Show* en 2011-2012 fue de los primeros en intentar llevar el bitcoin al público.

¿Este era el dinero del futuro?

«I AM SATOSHI»

La inscripción se realizó en las oficinas de OnlyOneTV, propiedad de Bruce Wagner, quien producía *The Bitcoin Show* en YouTube, en un tramo funcional de la Quinta Avenida en el centro de Manhattan. Era finales de agosto y los asistentes —casi todos hombres— habían viajado desde lugares remotos para hablar de un dinero invisible sin respaldo alguno que casi nadie comprendía, pero que se cotizaba a quince dólares la unidad, frente a menos de un dólar apenas seis meses antes. Gavin Andresen había viajado desde Massachusetts. Jeff Garzik venía desde Carolina del Norte. Stefan Thomas había volado desde Suiza y Roger Ver, un entusiasta

MT. GOX ERA LA PLATAFORMA DE INTERCAMBIO DE BITCOIN CON SEDE EN TOKIO CONSIDERADA MÁS FIABLE



ASC/HENRY HOLLIGON

Fotografía de la primera conferencia sobre el bitcoin en el Hotel Roosevelt en la ciudad de Nueva York el 20 de agosto de 2011.

promotor conocido como «Bitcoin Jesus», desde Japón. Delante de mí, mientras esperábamos para recoger nuestras acreditaciones, distinguí a Jed McCaleb, futuro fundador de Ripple, quien había creado originalmente Mt. Gox como una plataforma para intercambiar cartas de su juego favorito (las siglas significaban Magic: The Gathering Online eXchange) y posteriormente lo vendió. Aunque apenas éramos unos 65 asistentes, Bruce había bautizado el evento como «Bitcoin Conference & World Expo 2011 NYC».

Más tarde, nos reunimos en un restaurante de Hell's Kitchen llamado Hudson Eatery, uno de los pocos establecimientos a los que Bruce había convencido para aceptar bitcoin como forma de pago para «una velada de socialización bajo seudónimo». Al día siguiente, en las conferencias magistrales del Hotel Roosevelt en East FortyFifth Street, Gavin imaginó el día en que el bitcoin sería algo común y «aburrido»; Jeff habló sobre la necesidad de que el bitcoin mejorara su estrategia de relaciones públicas, dada la facilidad con que podía ser malinterpretado, y Stefan expuso las aplicaciones de codificación para bitcoin, que eran muy necesarias.

No parecía exactamente una revolución. Una noche durante la conferencia, Stefan encontró tan complicado pagar con bitcoin en los restaurantes que supuestamente lo aceptaban que terminó abonando la cuenta en dólares. Sin embargo, había una energía caótica en el evento. Entre reflexiones etéreas sobre un futuro dominado por el bitcoin y el *networking* de emprendedores con *startups* relacionadas con la criptomoneda, los asistentes intercambiaban teorías sobre Nakamoto (que jamás respondió a mi correo electrónico). Los matices religiosos ya habían comenzado a infiltrarse en el lenguaje de los bitcoiners. El primer bloque minado por Nakamoto era, después de todo, conocido como el bloque Génesis. El *merchandising* del evento consistía en una camiseta con la leyenda: «I am Satoshi». La pregunta flotaba en el ambiente: «¿Podría estar aquí entre nosotros?».

«No si era alguien incapaz de hacer el viaje», pensé. ■


85

Sr. Rogers

Hal Finney representó la vitalidad y energía de quien fue probablemente la figura más importante en la historia temprana del bitcoin después de Satoshi Nakamoto. Finney fue el primer destinatario de una transacción Bitcoin.

Hal Finney, el entusiasta del dinero digital que Nick Szabo me había mencionado, lucía una sonrisa radiante y, durante una época, un bigote perfilado de tal exuberante amplitud y perfección geométrica que parecía sacado de *El reportero: La leyenda de Ron Burgundy*. Nerd por excelencia, Finney publicó una vez un anuncio en un periódico gratuito ofreciéndose a responder cualquier pregunta científica o técnica por un dólar y abordaba los desafíos intelectuales con un entusiasmo incansable. Cuando trabajaba en la naciente industria de los videojuegos a finales de los setenta, programando *Space Battle*, de Intellivision, y *Adventures of Tron*, de Atari, se propuso crear efectos sonoros para *Major League Baseball*, de Intellivision.

SHUTTERSTOCK

Carátula de *Space Battl*. Hal Finney trabajó como desarrollador de videojuegos.

CREÍA EN EL FUTURO

El *hardware* de Intellivision incluía un chip de sonido programable y David Rolfe, compañero de piso y de trabajo en aquella época, recuerda a Finney «sumergiéndose en los patrones de onda» para afrontar el reto de recrear los sonidos del estadio: «Si vivieras en una era en la que los ordenadores nunca hubieran emitido sonidos y te dieran esta herramienta, ¿cómo reproducirías un sonido de multitud? ¿Cómo suena una multitud, en realidad? Por aquella época se estrenó una película deportiva, *El cielo puede esperar*, y Hal prestó especial atención a las escenas de estadio donde la multitud animaba, para luego recrear meticulosamente el rugido, los silbidos y los efectos de bocina. Incluso logró recrear un "¡Estás fuera!" que imitaba razonablemente bien el habla humana».

A Finney siempre le habían gustado los rompecabezas. Incluso de niño, en una familia que se mudó de California a Luisiana y a Texas siguiendo el trabajo de su padre como ingeniero petrolero, anotaba sus propios códigos secretos de letras y números en libretas de papel. Era un niño imaginativo con gusto por la ciencia ficción. Sacaba libros de la biblioteca pública sobre avistamientos de platillos volantes y los leía en la cama por la noche, sintiendo «una deliciosa y aterradora emoción al imaginar extraterrestres escondidos en las sombras». A menudo

FINNEY PUBLICÓ UN ANUNCIO DONDE SE OFRECÍA A RESPONDER CUALQUIER PREGUNTA CIENTÍFICA O TÉCNICA POR UN DÓLAR

se preguntaba: «¿Por qué nací aquí y ahora, en lugar de en algún otro momento a lo largo de toda la historia?».

De vuelta en California para el instituto, aprendió a programar en FORTRAN y ayudó a los administradores del Arcadia High a calcular los datos de los estudiantes, almacenándolos en tarjetas perforadas. Se graduó en 1974 como el mejor de su clase y asistió al Instituto de Tecnología de California, donde incluso allí se le consideraba excepcionalmente brillante, alguien que podía descifrar un libro de texto por primera vez la noche antes de un examen importante y aprobarlo. Aún más raro para alguien con su coeficiente intelectual es que fuera conocido igualmente por su personalidad amable y optimista. Un compañero de fraternidad recordaría que «llevaba a todos a Tommy's a las tres de la mañana para comer hamburguesas, a tantos como cupieran en su Volkswagen».

Finney abrazó la ciencia y la tecnología, y él y su esposa, Fran, que había sido su novia en la universidad, pusieron a sus hijos y mascotas nombres de objetos astronómicos: Arky, el nombre de su crestado rodesiano, proviene de una estrella de la constelación del boyero. Después de conocer a los extropianos, Finney se convirtió en colaborador habitual de su lista de correo electrónico. Evitaba el alcohol, porque había sufrido convulsiones en la universidad y había antecedentes de alcoholismo en su familia, y ahora empezaba a experimentar con diferentes enfoques para estar sano: fue vegetariano durante menos de un año, probó una dieta cetogénica, tomó suplementos vitamínicos antioxidantes y se unió a Weight Watchers, entre otras cosas.

También dio un paso más extremo, popular entre los extropiados. En octubre de 1992, él y Fran condujeron desde Santa Bárbara, donde se habían mudado recientemente, hasta Riverside, al sureste de Los Ángeles, para firmar los documentos necesarios para inscribirse en Alcor, una organización de servicios criónicos. Alcor ofrecía un paquete «neuro» menos costoso, solo para la cabeza, y un paquete más costoso, para todo el cuerpo, que fue el que eligieron los Finney. Cuando murieran,

Hal Finney en una foto en el instituto junto a su futura esposa Fran (1972). Décadas después se convertiría en una de las figuras más admiradas del ecosistema bitcoin.

sus cuerpos serían congelados con la esperanza de que la tecnología pudiera reanimarlos eventualmente. Alcor les entregó una etiqueta de identificación de emergencia que podía llevarse como colgante o en una pulsera de eslabones. Hal portó la placa de acero profusamente grabada desde ese momento. Incluía un número de teléfono disponible las 24 horas; mención de una recompensa por contactarles; instrucciones del «protocolo de bioestasis», y la orden judicial «No embalsamamiento/no autopsia». Esto alertaría a los servicios de emergencia, en caso de su «desanimación», de que era un paciente criónico al corriente de sus pagos e indicaría a quién contactar para que su criopreservación pudiera iniciarse sin interferencias ni retrasos. «No creía en Dios —explicó Fran posteriormente—. Creía en el futuro».

UNA AMENAZA PARA LA SEGUIRDAD NACIONAL

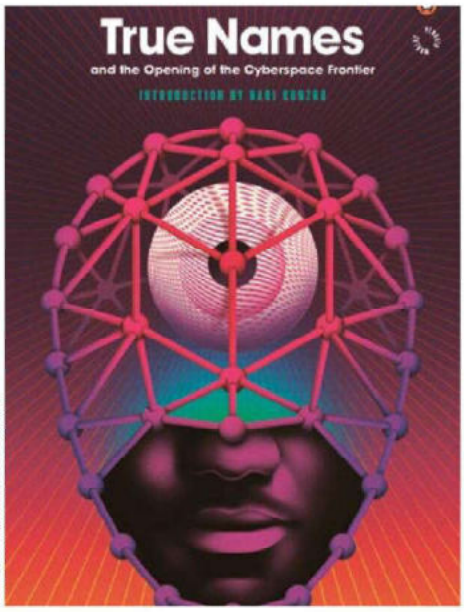
A través de los extropianos, Hal Finney también conoció el proyecto que se convertiría en el trabajo de su vida. Cuando leyó que un tipo llamado Phil Zimmermann había inventado el primer programa de criptografía DIY del mundo —un *software* que cualquiera podía ejecutar en su ordenador personal para enviar y recibir correos electrónicos ilegibles para los intrusos— y que el Gobierno lo consideraba una amenaza para la seguridad nacional, Finney lo descargó, experimentó con él y quedó impresionado. Esto lo llevó a la biblioteca para seguir investigando, donde encontró los artículos de David Chaum que mostraban conceptual y matemáticamente cómo se podía utilizar la nueva criptografía para garantizar la privacidad personal en línea. «Me dejó alucinado», recordó más tarde Finney.

Le cautivaron «el misterio y la paradoja» de la criptografía. «Lo que siempre me ha fascinado de un reto intelectual es que, cuando lo dominas, te proporciona habilidades prácticas». Cada vez que se encontraba con algo así, reconocía su propia tendencia a desarrollar un interés obsesivo. «Me invade un afán completamente incontrolable».

Phil Zimmermann había inventado el primer programa de criptografía DIY del mundo, Pretty Good Privacy (PGP) un *software* de encriptación.

CADA VEZ QUE SE ENCONTRABA CON ALGÚN RETO, RECONOCÍA SU PROPIA TENDENCIA A DESARROLLAR UN INTERÉS OBSESIVO

La criptografía era mágica para él. Finney, al igual que Tim May, se había inspirado en *True Names* y sus «identidades imposibles de rastrear». Mientras leía la novela, se encontró señalando defectos en los aspectos técnicos de la fantasía de Vinge. Como May, Finney vislumbró inmediatamente cómo la criptografía, la versión adulta de su fascinación juvenil, podía ser el instrumento para materializar el futuro imaginado en *True Names*. Tomemos como ejemplo los *nyms*: cualquiera podría usar el nombre de «Ardilla Secreta», señaló Finney, pero solo una persona podría demostrar la posesión de una clave privada vinculada a una clave pública. «Me pareció tan evidente. Aquí nos enfrentamos a los problemas de la pérdida de privacidad, la informatización progresiva, las bases de datos masivas, una mayor centralización, y Chaum ofrece una dirección completamente diferente, una que deposita el poder en manos de las personas en lugar de los Gobiernos y las corporaciones. El ordenador puede utilizarse como una herramienta para liberar y proteger a los individuos, en lugar de controlarlos».



Cubierta de *True Names*, de Vernor Vinge, una de las obras visionarias que anticipó conceptos del bitcoin.

AL NIVEL DE STEPHEN HAWKING

Se ofreció como voluntario para ayudar a Phil Zimmermann y, durante los años siguientes, trabajaba a tiempo completo, luego regresaba a casa y consagraba sus tardes al trabajo voluntario intenso, aunque en el encantador entorno de la costa central de California, escribiendo líneas de código para PGP. Más tarde, después de que PGP superara sus problemas legales y se transformara en una empresa con ánimo de lucro, Finney se incorporó como uno de sus dos primeros empleados. Era un trabajo ideal para él, pues combinaba su pasión por los acertijos con su fervor por la privacidad.

En un campo que tendía hacia la paranoia y el autismo, Finney destacaba por su afable normalidad. Will Price, que trabajó con Finney en PGP, lo compara con otro criptógrafo, un «genio del nivel de Stephen Hawking», que también trabajó para PGP en la década de los noventa. Este criptógrafo evitaba bañarse, solo escribía código que regalaba y se negaba a aceptar dinero por su trabajo porque carecía de cuenta bancaria. «Tuvimos que pagarle con ordenadores. No quiero usar la palabra psicópata. Nadie lo ha visto desde el año 2000. Creo que vive en algún bosque».

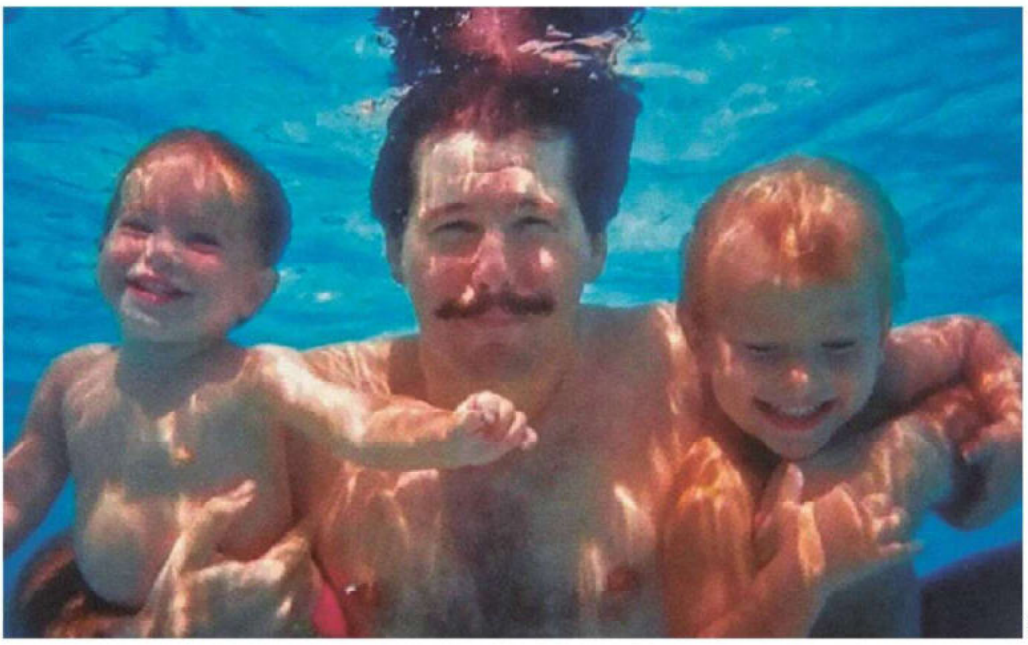
FINNEY ESCRIBÍA CÓDIGO QUE REGALABA Y SE NEGABA A ACEPTAR DINERO POR SU TRABAJO PORQUE CARECÍA DE CUENTA BANCARIA

Finney era más convencional en apariencia. Le gustaba pasar tiempo con su familia. Era «una persona muy centrada», me dijo Will, que describió a Finney como «sereno» y «nunca enfadado». «A veces la gente que es superinteligente paga un precio por ello —se hizo eco Phil Zimmermann—. Hay algo en su personalidad que no funciona exactamente bien. Hal nunca pagó ese precio. Conservó su humanidad, amabilidad y gracia. Vi a Tom Hanks en una película sobre el Sr. Rogers. Ese es el tipo de alma del que estoy hablando».

NUNCA SE ES DEMASIADO CAUTELOSO

Finney era en muchos sentidos un *cypherpunk* por excelencia. Realmente escribía código. Pero, aunque tenía fuertes creencias sobre la libertad, era más prosocial que algunos de sus compañeros de viaje. Hablaba sobre cómo la criptografía podría haber ayudado a los abolicionistas que operaban en el Ferrocarril Subterráneo para facilitar la huida de los esclavos. «Los Libertarios con L mayúscula suelen ser menos compasivos —señaló Phil— y creo que Hal era una persona compasiva».

Finney llegó a la conclusión de que el anonimato y el uso de seudónimos, a pesar de sus inconvenientes, proporcionarían «beneficios reales a todos los miembros de la sociedad». Citó *The Federalist Papers*, «publicados anónimamente por temor a represalias políticas». ¿Y qué decir de los denunciantes y disidentes?, él mis-

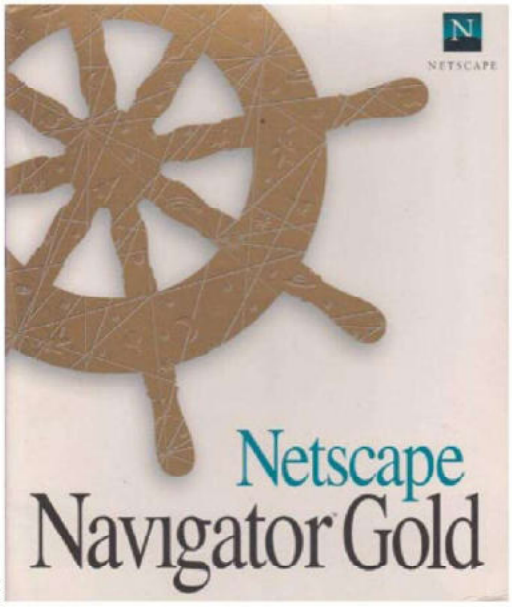


ASC

A Hal le gustaba pasar tiempo con su familia, era una persona muy centrada, serena y nunca se enfadaba. En la imagen, Hal Finney con sus dos hijos.

mo había utilizado múltiples seudónimos en Internet. «Para mí, la criptoanarquía representa una forma de oposición a las bases de datos de información personal en constante expansión, una manera en que los individuos pueden recuperar el control sobre la información de sus propias vidas». Hablaba de *True Names*, donde «que descubrieran tu verdadera identidad constituía el peor desastre imaginable, ya que te volvía vulnerable a numerosos tipos de ataques, tanto de otros *hackers* como del Gobierno».

Para Finney tampoco era una abstracción académica. Se emocionaba al pensar en cómo los correos electrónicos no anónimos podrían llevar a su jefe, Phil Zimmermann, a la cárcel. Finney ya había gastado mil dólares de su propio bolsillo para contratar a un abogado que le asesorara sobre el riesgo de ser procesado por el trabajo voluntario que había realizado para PGP y advirtió a otros *cypherpunks* sobre el hecho de que, si el Gobierno los declaraba culpables de violar la Ley de Control de Exportación de Armas, podrían ser multados con hasta un millón de dólares y condenados a diez años de prisión. «Es repugnante, pero hoy en día nunca se es demasiado cauteloso. Sin duda, se entiende perfectamente la postura de Pr0duct Cypher y nuestros otros participantes anónimos».



ASC

Navigator Gold 2.01 democratizó el acceso a internet e hizo posible la coordinación descentralizada necesaria para el bitcoin.

DESAFÍO A LOS *CYPHERPUNKS*

Después de que un servicio de reenvío alojado en el ordenador de un hombre en Finlandia fuera allanado a instancias de la Iglesia de la Cienciología, que buscaba a un filtrador anónimo de documentos internos, Finney desarrolló y puso en funcionamiento uno de los primeros sistemas de reenvío anónimo y cifrado: hacía rebotar los mensajes a través de múltiples servidores, sin que ninguno conociera más que el punto anterior y el siguiente en la ruta del mensaje. Cuando el Gobierno estadounidense comenzó a exigir que las versiones de exportación de programas populares emplearan una criptografía más débil que las versiones nacionales, Finney, como forma de evidenciar lo absurdo de esta política y sus desventajas comerciales, lanzó un desafío a sus compañeros *cypherpunks* para que descifraran la nueva versión de exportación del navegador Netscape. Después de que un equipo lograra descifrarlo en un mes, Finney publicó un segundo desafío y esta vez los *cypherpunks* quebraron la seguridad en menos de treinta y dos horas.

Los sistemas de reenvío de correo eran solo los cimientos del mundo respetuoso con la privacidad que Finney quería ayudar a construir. Lo que realmente le apasionaba era el siguiente nivel: el dinero digital. Ese sueño había quedado rele-

gado durante las batallas por el derecho público a una criptografía robusta, pero, una vez asegurado ese derecho, Finney concentró cada vez más su atención en el dinero electrónico. Sugería tanto motivos prácticos —las tarjetas de crédito no podían gestionar micropagos, no todo el mundo disponía de ellas y ofrecían escasa privacidad— como uno más ideológico, aludiendo a los banqueros que imprimían dinero y generaban inflación.

Y Finney realizó el arduo trabajo de reflexionar sobre los detalles necesarios para materializar el dinero digital. ¿Qué postura adoptaría el Gobierno ante esto o ante cualquier dinero alternativo en general? Finney investigó sobre la historia de los billetes privados y descubrió que habían estado sometidos a un fuerte impuesto por una ley de la época de la guerra civil que seguía vigente. Se enteró de que el servicio de rentas internas había fiscalizado el trueque y el intercambio de bienes. Estudió alternativas a las patentes de Chaum. Anticipó que, incluso en un sistema que eludiera al Gobierno, la conversión de papel moneda a dinero digital constituiría un «punto de estrangulamiento» donde el Gobierno podría ejercer control.

A corto plazo, Finney consideró que una forma de sortear el laberinto legal podría ser crear «un juego educativo» y sugirió que «cualquiera que se proponga implementar un juego de este tipo debería contemplar la posibilidad de lanzarlo anónimamente (en realidad, bajo seudónimo). De esta manera, no existirá un objetivo concreto para quienes deseen castigar a los usuarios del juego».

DINERO MÁGICO

Con algunos *cypherpunks* de ideas afines, Finney barajó posibles nombres para la nueva moneda: cryps, crydets, emoney, ecash o, sugirió con ironía, chaums. De esa manera sería menos probable que nos demandara por infringir su patente. Después de otra lluvia de ideas, propuso CRASH, acrónimo de CRypto cASH.

Cada vez que este o aquel *cypherpunk* proponían un nuevo sistema de dinero digital, Finney respondía ofreciendo su apoyo o señalando una vulnerabilidad. Pensaba que la idea de Chaum de utilizar *hardware* criptográfico a prueba de manipulaciones, instalado en el ordenador de uno para evitar el doble gasto, era «la dirección equivocada», pero también se apresuró a probar el producto de dinero electrónico de Chaum. Después de que Pr0duct Cypher publicara un *software* que había escrito para un sistema de «dinero mágico», Finney le dio una palmadita en la espalda: «¡Guau! ¡Qué bueno!». Dos días después, Finney le informó de que el dinero mágico podía tener un fallo de seguridad.

También reflexionó sobre la estética de la moneda digital. Al leer un viejo libro sobre el papel moneda estadounidense, encontró que algunos de los arcaicos billetes representados eran «sorprendentemente hermosos». Se preguntó, en una respuesta a Pr0duct Cypher, si era posible crear dinero digital que fuera hermoso y raro. Imaginó cantidades discretas de esta moneda con marcas de tiempo para

CUANDO NAKAMOTO LANZÓ EL *SOFTWARE*, EL ORDENADOR DE FINNEY SE CONVIRTIÓ EN EL SEGUNDO NODO DE LA RED

INSIDEBITCOINS

Nick Szabo permanece como el candidato más plausible, pero después de décadas de especulación e investigación no existe prueba definitiva de la identidad de Satoshi.

demostrar su antigüedad. El dinero digital sería bits a la deriva en el éter, pero Finney sugirió formas en que determinadas unidades de la moneda podrían hacerse visibles, como «atractivos patrones de aspecto fractal para muchos billetes. Con un poco más de reflexión, espero crear un visor para su Magic Money que resalte su belleza natural y rareza. Será imprescindible para todos los coleccionistas serios de dinero digital».

Durante la crisis del dinero electrónico de principios de los años 2000, Finney fue uno de los pocos que se mantuvo centrado en resolver el problema. Estaba lo suficientemente obsesionado como para dedicarle gran parte de su tiempo libre. En 2004, lanzó su propia implementación del *bit gold* de Nick Szabo. RPOW (Reusable Proofs of Work) utilizaba el mismo método de rompecabezas computacionales propuesto para *bit gold*, empleaba criptografía para asegurar el sistema y garantizar la escasez, y pretendía ser descentralizado, sustituyendo a un tercero de confianza por *hardware* especializado que tendrían los ordenadores participantes.

El RPOW nunca tuvo mucho éxito, pero, cuando Nakamoto anunció el bitcoin cuatro años después, Finney fue la primera persona en Metzdowd en elogiarlo. Dio su opinión a Nakamoto sobre el código fuente, y, cuando Nakamoto lanzó el *software* el 9 de enero de 2009, el ordenador de Finney se convirtió en el segundo nodo de la red. «Ejecutando el bitcoin», tuiteó Finney.

Esto sirvió también como guiño a su nueva afición. Dada la naturaleza sedentaria del trabajo de Finney, en la mediana edad, su peso había pasado de 77 a unos 113 y, después de que su médico le dijera que era obeso, empezó a hacer dieta y a competir en medias maratones. Con el tiempo, bajó a 73. A principios de 2009, Finney estaba en su mejor forma física y entrenando para su primera maratón completa. ■

Mira siempre el lado positivo

Finney mantuvo los diez bitcoins que Satoshi le envió en la primera transacción hasta su muerte, aunque valdrían cientos de miles de dólares y su familia se enfrentaba a costes médicos astronómicos. ISTOCK

Un mes después de tuitear sobre el bitcoin, Finney notó que sus tiempos de carrera no eran cada vez más rápidos. Se cansaba antes y tenía calambres con más frecuencia. Fran notó que, cuando ella y Hal corrían juntos, él no podía hablar y correr al mismo tiempo, como había hecho en el pasado. Cuando ella mencionó esto, él dijo con una impaciencia inusual: «Nadie puede hablar y correr al mismo tiempo».

Finney empezó a notar que su habla se entrecortaba de vez en cuando, casi como si hubiera estado bebiendo. Su mano derecha empezó a temblar. Fran, fisioterapeuta, sabía que algo iba mal. «No paraba de decirle: "Hal, tienes que hacerte pruebas, tienes que ir al médico". No quería tener razón». En mayo, cuando Hal corrió la maratón de Los Ángeles, los calambres y espasmos en su pierna derecha se hicieron tan intensos que se detuvo en Sunset Strip, alrededor de la milla 13.

En cada aniversario desde su boda en 1979, él y Fran habían salido a dar un paseo en bicicleta, una milla por cada año que llevaban casados. Este año era su trigésimo aniversario y, partiendo de una posada en San Luis Obispo, se pusieron en marcha en una bicicleta tándem para un paseo de treinta millas. Por primera vez, Hal estaba demasiado cansado para terminar. Una semana después, le diagnosticaron ELA, la enfermedad neurodegenerativa también conocida como enfermedad de Lou Gehrig.

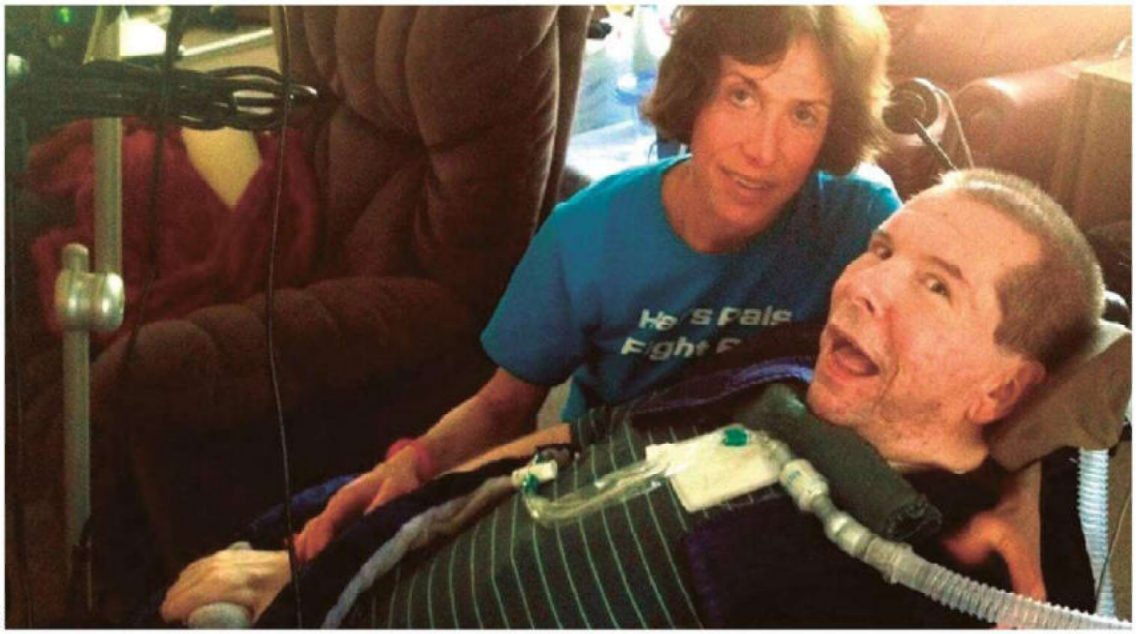
HAL NO TENÍA LOS MISMOS PLANES

Su voz se volvió más suave. Se le trababa más. Sus manos se debilitaron. «Es molesto y preocupante que mis síntomas iniciales se estén manifestando en mi voz y mis manos, las dos fuentes de salida más utilizadas y de mayor ancho de banda disponibles», escribió a sus amigos en *LessWrong*, en términos que la multitud de tecnólogos podía apreciar.

ASC

Hal y Fran Finney en una maratón benéfica para recaudar fondos contra la ELA.

Le había sorprendido saber que más del 90 % de las personas afectadas por ELA optaban por morir cuando ya no podían respirar por sí mismas. Hal no tenía esos planes. Tenía la intención de seguir con la ventilación mecánica. Un servicio gratuito de banca de voz del Laboratorio de Investigación del Habla de la Universidad de Delaware estaba modelando su voz, que luego podría reproducir a través de un sintetizador. Había leído que Stephen Hawking, que había sobrevivido cuarenta años con ELA, podía escribir diez palabras por minuto contrayendo un músculo de la mejilla. «Puede que incluso sea capaz de escribir código —comentó Hal con los lectores de *LessWrong*—, y mi sueño es contribuir a proyectos de *software* de código abierto incluso desde un cuerpo inmóvil. Esa será una vida que valdrá mucho la pena vivir».



ASC

Hal Finney junto a su esposa Fran en sus últimos años de vida, completamente paralizado por la ELA, dependiendo de ventilación asistida para respirar.

Ese diciembre, recaudando dinero para la lucha contra la ELA como parte de un equipo de relevos en la Maratón Internacional de Santa Bárbara, Fran llevó el chip de seguimiento a Hal, y caminaron juntos el último tramo de tres kilómetros, con Hal usando un bastón. Había crecido esquiando y se había convertido en un experto en las pistas, afrontando pistas negras dobles y haciendo acrobacias, pero en diciembre esquió por última vez, limitándose a las pistas para principiantes y luchando por subir y bajar del telesilla.

CADA VEZ QUE HAL CONSEGUÍA ALGO SE PONÍA MUY CONTENTO

Hal se enfrentó a su destino con una actitud tan optimista que Phil Zimmermann la comparó con el *Always Look on the Bright Side of Life*, de Monty Python. Cuando Phil visitó a Hal en casa, después de que la enfermedad hubiera avanzado mucho, este le dijo: «Bueno, ahora tengo más tiempo para leer».

«Todos los que tienen ELA hablan de lo terrible que es, de todas las cosas que ya no puedes hacer —escribió Hal en *LessWrong*—. Pero nadie parece darse cuenta de que hay muchas cosas que puedes hacer que nunca antes habías hecho. Nunca he usado una silla de ruedas eléctrica. Nunca he controlado un ordenador con los ojos. Nunca he tenido un sintetizador de voz entrenado para imitar mi voz natural. Si le dijera a la gente de los foros de ELA que estoy deseando hacer algunas de estas cosas, pensarían que estoy loco. Quizá la gente de aquí lo entienda».

HABÍA LEÍDO QUE STEPHEN HAWKING PODÍA ESCRIBIR DIEZ PALABRAS POR MINUTO CONTRAYENDO UN MÚSCULO DE LA MEJILLA

SHUTTERSTOCK

Hal mantenía la esperanza de que el bitcoin encontraría su lugar en un mundo cada vez más interconectado, aunque su destino dependería de la capacidad humana para perfeccionarlo.

ESPERABA QUE EL SISTEMA MONETARIO SE VOLVIERA MÁS COMPLEJO, CON EL BITCOIN DESEMPEÑANDO UN PAPEL RELEVANTE

¿Ya no podía levantarse de la silla? Bueno, eso no era nada que una silla elevadora y un poste cercano no pudieran arreglar. Siempre había sido un mecanógrafo rápido, así que, cuando su mano derecha dejó de funcionar, aprendió a mecanografiar rápidamente usando solo la mano izquierda. Cuando esa mano se debilitó, se entablilló los dedos para poder seguir escribiendo con dos dedos. Cuando solo le quedaba un dedo útil, escribía con él. Cuando perdió por completo el uso de sus manos, pasó a un rastreador ocular. Cuando sus músculos oculares empezaron a fallar, cambió a pantallas en las que solo tenía cuatro letras para elegir a la vez. Cuando su silla de ruedas empezó a causarle dolorosas úlceras por presión, por lo que requería que otras personas ajustaran constantemente su posición, montó un sistema que le permitía controlar la silla de ruedas con el *software* de seguimiento ocular. «Estaba encantado de hacer esto —dijo Fran más tarde—. Eso le proporcionaba una felicidad suprema. Cada vez que Hal conseguía algo que le entusiasmaba, se ponía muy contento».

HONRAR EL DESEO SATOSHI

Cuando contacté con Hal en agosto de 2011, solo podía comunicarse a través del rastreador ocular. Sin embargo, respondió amablemente a mis preguntas por correo electrónico. Escribió que anticipaba una mejora del bitcoin y que esto «podría conducir a la fragmentación y competencia entre diferentes versiones». Esperaba que el sistema monetario internacional se volviera mucho más complejo, con el bitcoin desempeñando un papel relevante. Previó la cuestión de si, una vez agotadas las monedas por extraer y alterados los incentivos para preservar la integridad del bitcoin, el sistema seguiría siendo estable. Le preocupaban los problemas que continuarían afectando al bitcoin y sus derivados, alejando a la mayoría de usuarios, y me comentó que «la experiencia con bitcoin ha demostrado gráficamente el lamentable estado de la seguridad informática actual. Proteger las monedas digitales contra el robo ha resultado ser inesperadamente difícil».

Le pregunté a Hal si era Satoshi Nakamoto.

—No, no lo soy —respondió—. Ojalá hubiera creado algo tan potencialmente revolucionario como el bitcoin. En mis circunstancias actuales, con una esperanza de vida limitada, tendría poco que perder al despojarme del anonimato. Pero no fui yo.

—¿Pensaba que Wei Dai podría ser Nakamoto?

—Conozco a Wei desde hace muchos años —me contestó—. Es un tipo brillante y sin duda sería capaz de crear algo tan imaginativo como el bitcoin. Sin embargo, mi impresión del estilo de escritura de Satoshi es que es diferente.

Hal esquivó delicadamente mis otras preguntas sobre el tema:

—No quisiera desalentar tu investigación, pero me genera cierto malestar participar tan activamente en este ejercicio de especulación. Satoshi evidentemente valora su privacidad, y quizá la mejor forma de demostrarle respeto y gratitud por su creación sea precisamente honrar ese deseo. ■

El alfiler, no la burbuja

Bitcoin ha sido declarado «muerto» más de 470 veces por medios financieros tradicionales desde 2010. Ha experimentado caídas del 80-90 % en múltiples ocasiones (2011, 2014, 2018, 2022) y cada vez los críticos proclaman que finalmente la burbuja ha estallado. Sin embargo, se recupera y alcanza nuevos máximos históricos. SHUTTERSTOCK


BITCOIN • DIGITAL • DECENTRALIZED • PEER TO PEER

SHUTTERSTOCK

Desde 2021, Miami ha emergido como el *hub* más *cripto-friendly* de Estados Unidos, atrayendo empresas *blockchain* y eventos masivos como la Bitcoin Conference.

Once años después, en Miami, una noche en la que caminaba por Collins Avenue hacia mi hotel, un hombre pelirrojo con inquietantes entradas que caminaba a paso ligero en la otra dirección pasó a mi lado y me quedé atónito. Llevaba gafas, pantalones cortos, una camisa de manga corta abotonada y zapatillas Converse negras de caña alta con calcetines. Me di la vuelta para observar su figura encogida.

—¿No era ese...?

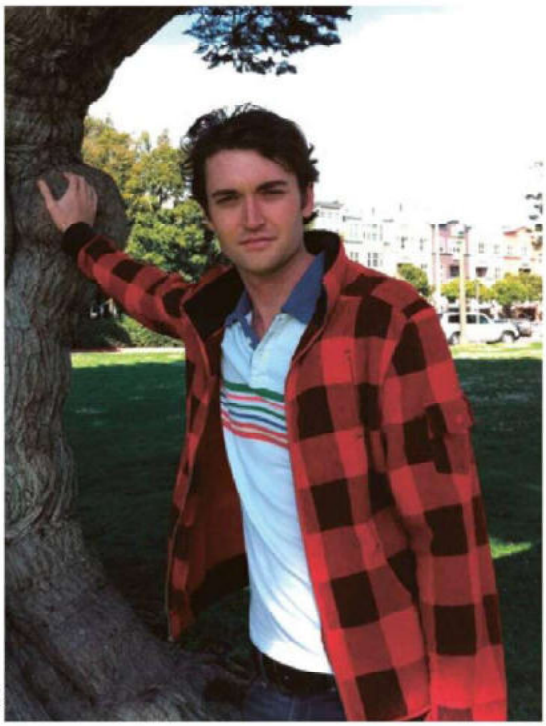
—Era Adam Back —dijo un tipo que iba detrás de mí por la acera—. Yo tuve la misma reacción.

—Tiene una isla privada en Malta, ¿verdad? —señaló un hombre que caminaba en dirección contraria con tres amigos.

Era un jueves de abril, durante la conferencia del bitcoin 2022. Miami se había proclamado recientemente como la ciudad más favorable a las criptomonedas de Estados Unidos y se calculaba que asistirían veintiséis mil personas. Back, que en 2011 había sido un oscuro consultor de criptografía, ahora dirigía Blockstream, una empresa de infraestructura de *blockchain* de tres mil millones de dólares de la que era cofundador. Al día siguiente, después de que Back hiciera una presentación en el escenario, veía cómo la prensa especializada en criptomonedas y los fans lo rodeaban, buscando respuestas y selfis. Figuras que habían sido oscuros expertos técnicos una década antes eran ahora superestrellas de la industria. El bitcoin había tardado un tiempo en escapar de los estrechos confines de los informáticos. Cuando lo hizo, al principio, la atención no fue favorable.

MÁS ALLÁ DE SILK ROAD

En un episodio de 2012 de *The Good Wife*, el Gobierno de Estados Unidos perseguía al creador del bitcoin por su «moneda ilegal en línea». En *Los Simpson*, Krusty el Payaso se arruinó después de invertir en bitcoin, entre otras cosas. A finales de 2013, Silk Road, el mercado de la web oscura donde el bitcoin era la moneda preferida, fue cerrado y su creador, Ross Ulbricht, arrestado. En 2014, Mt. Gox, la plataforma segura y fiable donde había guardado mis siete bitcoins restantes, se declaró en quiebra después de que desaparecieran 850 000 bitcoins, y su propietario, Mark Karpelès, fue arrestado; fue absuelto de robo, pero finalmente recibió una sentencia de prisión condicional por «manipulación de registros electrónicos». La volatilidad del bitcoin lo convertía en algo apasionante para los especuladores y aterrador para la mayoría de la gente. Un ciclo de auge y caída en 2011, de 1 a 32 y de ahí a 2 dólares, fue solo el primero de muchos episodios similares. En los primeros meses de 2013, el bitcoin ascendió de 13 a 260 dólares antes de desplomarse en menos de una semana hasta los 50 dólares. En la segunda mitad de ese año, pasó de menos de 100 dólares a más de 1100, para luego perder la mitad de su valor en apenas un par de semanas en diciembre. Sin embargo, a pesar de las extremas fluctuaciones y de numerosos hackeos y estafas, el valor del bitcoin seguía creciendo de manera inestable.



ASC

Ross Ulbricht creó Silk Road, bajo el alias «Dread Pirate Roberts», el primer mercado *darknet* a gran escala.

Aparecieron señales intermitentes de que estaba ampliando su atractivo. En 2014, el Senado estadounidense celebró una audiencia sorprendentemente optimista sobre el bitcoin titulada «Más allá de Silk Road: riesgos potenciales, amenazas y promesas de las monedas virtuales». Richard Branson anunció que su empresa de viajes espaciales Virgin Galactic aceptaría bitcoins, pues, según él, estaba «impulsando una revolución». Bill Gates calificó al bitcoin de «emocionante, mejor que la moneda y un *tour de force* tecnológico». Un año después, Marc Andreessen, pionero del navegador web antes de convertirse en inversor de capital riesgo, afirmó: «Es-

MIAMI SE HABÍA PROCLAMADO COMO LA CIUDAD DE ESTADOS UNIDOS MÁS FAVORABLE A LAS CRIPTOMONEDAS

SHUTTERSTOCK

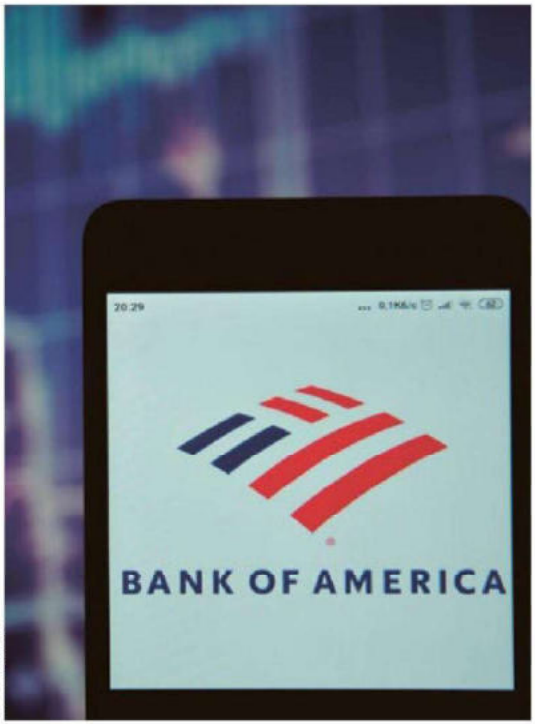
Sobre estas líneas, Richard Branson frente a *SpaceShipTwo* en Spaceport America, Nuevo México, en 2011. El empresario fue uno de emprendedores visionarios del bitcoin. Abajo, Bill Gates representa la postura escéptica de la élite tecnológica tradicional hacia el bitcoin y ha mantenido una perspectiva crítica durante años.

SHUTTERSTOCK

TRECE AÑOS DESPUÉS DE SU CREACIÓN, UN SOLO BITCOIN ALCANZABA UN VALOR SUPERIOR A LOS 65 000 DÓLARES

tamos bastante convencidos de que, cuando nos sentemos aquí dentro de veinte años, hablaremos del bitcoin como hablamos hoy de internet». Y cuanto más tiempo transcurría, cuanto más tiempo pasaba el bitcoin sin ser comprometido con éxito, más sólido parecía.

Y ahora, años después de su creación, un solo bitcoin alcanzaba un valor superior a los 65 000 dólares, y representaba apenas una fracción de una industria mucho más amplia. Cripto, término que históricamente había sido la abreviatura de criptografía, designaba ahora, para consternación de los criptógrafos, el universo de las criptomonedas. Existían, casi rozando lo inverosímil, más de dieciséis mil criptomonedas distintas, todas ellas variaciones del único modelo que existía en 2011. Colectivamente, habían superado recientemente la asombrosa cifra de tres billones de dólares en capitalización. El 86 % de los estadounidenses había oído hablar de las criptomonedas. El 16 % las había utilizado, negociado o incluido en sus inversiones.



SHUTTERSTOCK

La banca tradicional convive en la actualidad con un ecosistema cripto que evoluciona a gran velocidad.

«¡LIBEREN A ROSS!»

Sin embargo, esto no implicaba que las comprendieran. Yo mismo no estaba seguro de entenderlas, a pesar de llevar once años estudiándolas. La gente se preguntaba: «¿Qué es el bitcoin?», una cuestión que distaba mucho de tener una respuesta sencilla.

—¿Por qué vale algo el bitcoin? —preguntó un día mi suegro. —¿Por qué vale algo el oro? —dije yo.

Mi suegro me miró con impaciencia.

—¿Por qué todos a los que les hago esta pregunta responden con otra pregunta?

Durante el vuelo a Florida, estaba sentado entre un ejecutivo que gestionaba activos digitales para Bank of America y un financiero dedicado a conceder préstamos a mineros de bitcoins. Ambos calificaron al veterano e imperturbable bitcoin de «aburrido» en comparación con la efervescencia y el dinamismo de los nuevos proyectos de criptomonedas. Los experimentos con DeFi (finanzas descentralizadas), NFT (tokens no fungibles) y DAO (organizaciones autónomas des-

LA AUTODETERMINACIÓN REPRESENTABA LA MÁXIMA EXPRESIÓN DEL ESPÍRITU LIBERTARIO DEL BITCOIN

centralizadas) se desarrollaban principalmente en otras cadenas de bloques, especialmente ethereum. Sin embargo, precisamente ese carácter predecible había convertido al bitcoin en la criptomoneda con mayores posibilidades de adopción masiva. En Miami, la senadora de Wyoming Cynthia Lummis tenía programado un «coloquio informal» sobre legislación relacionada con el bitcoin, mientras que Tucker Carlson se presentaría en el centro de convenciones con un equipo de Fox para entrevistar a Michael Saylor, cuya compañía MicroStrategy poseía más de 5000 millones de dólares en bitcoins. En la fila para recoger las acreditaciones conversé con dos individuos que afirmaron residir en Panamá que operaban con una instalación de minería de bitcoins, alimentada por energía hidroeléctrica, en una zona remota de Paraguay. Observé a una pareja ataviada completamente de naranja, el color emblemático del logotipo del bitcoin.

La multitud que circulaba por el edificio era solo un poco menos masculina que el grupo de la conferencia a la que había asistido una década antes, pero estos hombres parecían más contestatarios. Anoté los lemas impresos en las camisetas y sudaderas con capucha que observé:

SHUTTERSTOCK

MicroStrategy se ha consolidado como uno de los mayores tenedores institucionales de bitcoin, simbolizando la convergencia entre la estrategia empresarial y las criptomonedas.

—«Defensor absoluto de la libertad de expresión».
—«Bitcoin contra el mundo».
—«Club social antifiat».
—«Bitcoin es el alfiler, no la burbuja».
—«Introvertido pero dispuesto a hablar de cripto».
—«Nacimos demasiado tarde para explorar los mares; demasiado pronto para explorar las estrellas; justo a tiempo para arreglar el dinero».
—«Yo soy Satoshi Nakamoto».

En un largo pasillo del segundo piso, me agaché para examinar lo que parecía basura en el suelo enmoquetado. Era un billete de cinco dólares, o lo que quedaba de uno. Alguien lo había hecho pedazos en un ataque de resentimiento contra el dólar o como una especie de instalación artística improvisada. Un gran cartel, «¡Liberen a Ross!», buscaba un millón de firmas para lanzar una petición para liberar a Ross Ulbricht, el creador encarcelado de Silk Road que había operado como el terrible pirata Roberts, el personaje de *La princesa prometida* que, como la concepción que algunas personas tienen de Satoshi Nakamoto, no era un individuo sino una identidad que pasaba de una persona a otra. ¿Se había generalizado el uso del bitcoin? En un debate titulado «Convertirse en un individuo soberano» participaron un criptoinfluencer melenudo llamado Robert Breedlove, que tenía el símbolo de la criptomoneda tatuado en el bíceps; el entonces *quarterback* de los Buffalo Bills, Matt Barkley, y Pascal Gauthier, director general del fabricante de carteras de *hardware* Ledger, que llevaba anillos en seis de sus dedos. La autodeterminación representaba la máxima expresión del espíritu libertario del bitcoin. Mientras escuchaba a los ponentes, reflexioné sobre cómo la ideología probablemente había sido indispensable para impulsar al bitcoin en sus inicios, pero su persistente hegemonía en la cultura del bitcoin constituía ahora un obstáculo. El bitcoin despertaba tantos recelos como admiración. El libertarismo radical resultaba antipático para el ciudadano común. Había algo profundamente desalentador en esa desconfianza tan arraigada hacia las personas que llevaba a depositar toda la fe en una red de máquinas. La mayoría prefería confiar en bancos, fuerzas del orden y servicios públicos. No aspiraban a educar a sus hijos en una plataforma petrolífera apátrida que debían defender con armas semiautomáticas.

ASC/LEDGER

Pascal Gauthier, CEO de Ledger, lidera una de las compañías clave en la custodia de bitcoins y criptomonedas.

LA VIOLENCIA SE HIZO INEVITABLE

Resultaba difícil sostener que las criptomonedas representaban una mejor alternativa cuando seguían desmoronándose entre las manos de la gente. Como ya temía Hal Finney, muchos de los problemas que afectaron al bitcoin en sus primeros años —desde la volatilidad de precios hasta la mala suerte y la delincuencia— se habían intensificado. Ahora que el bitcoin valía significativamente más, también crecían los riesgos. Un hombre de Gales, que había tirado accidentalmente un disco duro que contenía las claves de 8000 bitcoins, valorados en 320 millones de dólares en el momento de la conferencia, había dedicado los últimos nueve años a intentar excavar en un vertedero para recuperar su fortuna perdida.

Cuando lo único que protegía los bitcoins era una cadena de letras y números, la violencia se hizo inevitable. En los Países Bajos, un comerciante de bitcoins de treinta y ocho años fue atacado en su casa por ladrones que llevaban pasamontañas, chalecos antibalas y chaquetas militares. Lo torturaron delante de su hija de cuatro años durante más de una hora, según declaró a la policía, atándole las manos a la espalda, dándole patadas, apuntándole a la cabeza con una pistola, ahogándole con la manguera de la ducha, utilizando una herramienta eléctrica para perforarle siete agujeros en la pierna y en el pie y colgándole del cuello.

Los seguidores más fanáticos del bitcoin, a veces denominados maximalistas o maxis del bitcoin, parecían indiferentes a cómo estos riesgos afectaban a la gente común, incluso si esta actitud los condenaba a permanecer en la marginalidad.

—¡Sí!

El sonido vino de mi derecha. Un hombre sentado allí se inclinó hacia adelante, absorto. Al otro lado del pasillo, otro hombre llevaba un casco de motocicleta al estilo Daft Punk, con la visera oscura bajada. El anonimato se trasladó al espacio físico.

Gauthier, de Ledger, decía que el 70 % del mundo no vive en una democracia.

—¡Vaya! —exclamó el tipo que estaba a mi lado—. ¡Guau!

Después, en la calle, pasé junto a un hombre que levantaba un cartel con los nombres de iconos del economista libertario: Ludwig von Mises, Murray Rothbard, Friedrich Hayek. Cerca de allí, una reunión paralela programada para coincidir con esta acogía a entusiastas de las armas. Vi un raro grafiti disidente: «A la mierda el cripto, es un sistema piramidal, y no del tipo divertido».

EL BITCOIN ERA UNA ADVERTENCIA

Después del almuerzo, estaba programada la intervención de Peter Thiel, fundador de PayPal convertido en capitalista de riesgo. A pesar de que se hablaba de que el bitcoin no tenía líder, Satoshi Nakamoto estaba, en ausencia, en todas partes. El escenario Nakamoto, donde tuvieron lugar las conferencias magistrales y las ponencias más importantes, estaba flanqueado por pantallas iluminadas que mostra-

EN LOS PAÍSES BAJOS, UN COMERCIANTE DE BITCOINS FUE ATACADO EN SU CASA POR LADRONES QUE LLEVABAN PASAMONTAÑAS

ban una muestra rotativa de fragmentos de sus escritos. Tenían la cualidad, similar a la de Dianética, de ser banales para los forasteros y profundos para los iniciados.

«Imagina que el oro se convirtiera en plomo cuando lo roban».

«Escribir una descripción de esto para el público en general es jodidamente difícil. No hay nada con lo que relacionarlo».

«Estoy seguro de que dentro de veinte años habrá un volumen de transacciones de bitcoin muy grande... o ningún volumen».

«La red es robusta en su simplicidad no estructurada».

Antes de que Thiel subiera al escenario, un vídeo de 1999 mostraba una versión más joven y delgada de él entusiasmado con el futuro del dinero en línea. Cuando todos los miembros de la clase media tuvieran un teléfono móvil con conexión a internet, algo que él predijo que sucedería en los próximos cinco años, países como China o la India tendrían que cerrar las redes de telecomunicaciones o renunciar a su soberanía monetaria.

Thiel apareció entonces por el lado derecho del escenario, vestido con un polo blanco. Lanzó un fajo de billetes de cien dólares a las primeras filas: «Es una locura que esto siga funcionando, ¿sabes?». ¿Por qué —preguntó a la multitud—, no había sustituido el bitcoin, que ahora valía 813 000 millones de dólares, al oro, que valía 12 billones de dólares? El bitcoin era una advertencia, dijo, de que el sistema fiduciario había terminado.

SHUTTERSTOCK

Si el bitcoin quiere ser usado por millones, necesita integrarse en plataformas accesibles. PayPal, con más de 400 millones de usuarios activos, es una puerta de entrada.

WARREN BUFFETT, EL ENEMIGO Nº 1...

Mostró una diapositiva que decía «BTC vs. ETH». Ether era la segunda criptomoneda más valiosa. Encima del «BTC» había una fotografía de un hombre apuntando con una ametralladora a la cámara, mientras que encima del «ETH» había una foto del fundador de ethereum, Vitalik Buterin, en su versión más desgarbada y con pantalones morados. Por muy innovador y superior que fuera técnicamente el bitcoin, dijo Thiel, era un movimiento político, y lo que se interponía en su camino eran «los enemigos de este movimiento».

«Y por eso quiero concluir con una lista de enemigos —afirmó—, personas que creo están obstaculizando al bitcoin». Deseaba «exponerlos». Mostró una diapositiva de un adversario al que denominó «Enemigo nº 1». Era Warren Buffett. Yo sabía que Buffett era célebre por su prudente estrategia de inversión, que sentía pasión por el *bridge* y que se había comprometido a donar íntegramente su fortuna. Sin embargo, según Thiel, Buffett ocultaba un lado oscuro. Lo llamó «el abuelo sociópata de Omaha». (El delito de Buffett había sido calificar al bitcoin de «veneno para ratas»). El enemigo nº 2 era el director ejecutivo de JP Morgan Chase, Jamie Dimon, quien ejemplificaba lo que Thiel denominaba «el sesgo del banquero neoyorquino». (Dimon había cometido el error de despreciar el bitcoin tildándolo de «sin valor»). El enemigo nº 3 era el director ejecutivo de Black Rock, Larry Fink. (Su crimen contra el bitcoin no quedó inmediatamente claro). Juntos, estos hombres representaban lo que Thiel, que tenía 54 años, llamaba «la gerontocracia». Thiel contrapuso a estos veteranos con una imagen de la vibrante Miami y este «movimiento juvenil revolucionario. ¡Debemos salir de esta conferencia y conquistar el mundo!». El público presente en el cavernoso espacio estalló en

SHUTTERSTOCK

Aunque el bitcoin fue el pionero en crear dinero digital descentralizado, ethereum fue más allá, introdujo los contratos inteligentes, permitió que las transacciones fueran programables...

NAKAMOTO ERA EL MAYOR POSEEDOR DE LA MONEDA Y ALGUIEN QUE PODÍA INFLUIR SIGNIFICATIVAMENTE EN SU PRECIO

ASC/ROOTSTOCK

Sergio Demian Lerner defiende que la desaparición de Satoshi fue clave para que el bitcoin fuese un sistema descentralizado.

vítores. Más tarde se supo que, en la época de este discurso, la empresa de inversión de Thiel se deshizo de una gran posición en bitcoins que había mantenido durante ocho años. En Miami, Thiel concluyó su discurso diciendo a la multitud que los «enemigos» que había nombrado eran «extensiones del Estado». Bitcoin, por el contrario, no era una empresa y no tenía junta directiva. «No sabemos quién es Satoshi», añadió Thiel para enfatizar.

Salí de allí con mi amigo Andy, que también era inversor de capital riesgo.

—Menuda locura —dijo Andy, sacudiendo la cabeza.

No sabemos quién es Satoshi. En 2011 había sido el programador anónimo de una moneda experimental que interesaba principalmente a una comunidad marginal. Diez años después, era el mítico fundador de un proyecto con una capitalización de mercado de un billón de dólares, lo que lo convertía en el noveno activo más valioso del mundo, justo por debajo de Tesla y por encima de Meta (Facebook). El éxito de Nakamoto en permanecer en el anonimato a pesar de ese cambio se había convertido en uno de sus mayores logros. Y era increíblemente rico.

Un informático llamado Sergio Demian Lerner, a través de un ingenioso análisis de la primera *blockchain*, había estimado que casi 1,1 millones de bitcoins habían sido extraídos por las mismas máquinas, presumiblemente las de Nakamoto. El valor de esas monedas en ese momento era de 40 000 millones de dólares. Nakamoto era, con diferencia, el mayor poseedor de la moneda y alguien que podía influir significativamente en su precio.

AUGE Y CAÍDA DEL BITCOIN

Cuando la plataforma de intercambio de criptomonedas Coinbase salió a bolsa en la primavera de 2021, lo que le dio un valor de mercado instantáneo de 86 000 millones de dólares, uno de los factores de riesgo enumerados en el folleto

Desde su creación, el bitcoin ha sido comparado con el oro por su escasez, su resistencia a la censura y su papel como reserva de valor.

que la empresa presentó ante la Comisión de Bolsa y Valores estadounidense fue la identificación pública de Nakamoto o la transferencia de su tesoro de bitcoins. No era difícil pensar en escenarios en los que la identidad de Nakamoto —cuáles eran sus motivos e intenciones— podría ser relevante. El propio Thiel había especulado que Nakamoto estaba entre sus compañeros asistentes a una conferencia de criptografía financiera en la isla de Anguila en el año 2000. Hablando con mi amigo Andy fuera del centro de conferencias, donde se agolpaban chicos perdidos con la piel llena de granos anaranjados, empapándose de la curiosa mezcla de fervor revolucionario, hedonismo de Miami y contabilidad, mencioné mi reciente búsqueda de Nakamoto. Andy me preguntó por qué hablaba tan bajo. En el ámbito del bitcoin, le expliqué sin levantar la voz, el misterio de Nakamoto se consideraba necesario, una característica más que un defecto. Para estar realmente descentralizado, el bitcoin necesitaba un nacimiento virginal. Privarlo de una figura humana, un individuo imperfecto con una identidad particular que podría ser aceptable para este grupo pero no para aquel, le daba la mejor oportunidad de ser recibido en sus propios términos y adoptado en masa.

Y así, entre los bitcoiners, el alias Nakamoto se había convertido en sagrado, y las investigaciones sobre él se desalentaban. Mientras que algunas personas conjeturaban que el creador del bitcoin se había escondido principalmente para su propia protección, para no ser procesado por evasión de impuestos o atacado físicamente por su alijo de monedas, la opinión común era que había actuado de forma desin-

LOS BITCOINERS MÁS FERVIENTES TRATABAN LA NAKAMOTOLOGÍA COMO UNA ESPECIE DE BLASFEMIA: NAKAMOTO ERA SAGRADO

teresada. Los bitcoiners más fervientes trataban la Nakamotología como una especie de blasfemia, similar a cienciólogos a quienes se les preguntara por Xenu.

También existía un historial caótico de periodistas que habían intentado desvelar el misterio. Algunos reporteros habían quedado en evidencia por su exceso de confianza o credulidad. Un escritor se había visto envuelto en una demanda que le costó más de 100 000 dólares. Al menos un reportero había recibido «amenazas de muerte». La vida de un ciudadano corriente había sido destruida por un linchamiento mediático. Actualmente prevalecía una antipatía generalizada hacia los periodistas que intentaban arrojar luz sobre este secreto. Esto se sumaba a un desprecio extendido por la cobertura de las criptomonedas en los medios tradicionales. Un sitio llamado Bitcoin Obituaries catalogaba más de 440 artículos que habían anunciado prematuramente la inminente desaparición del bitcoin. Uno de ellos era mi artículo de 2011 en *Wired*, titulado «Auge y caída del bitcoin».

«POR FAVOR, NO INTENTE ACERCARSE A MÍ EN LA CONFERENCIA»

Sin embargo, la razón principal por la que había venido a Miami era para asistir a una charla de Nick Szabo ese mismo día. A media tarde, Nick subió al escenario Nakamoto vestido con una camisa por fuera del pantalón, un micrófono inalámbrico adherido a la cabeza y el cabello, ahora canoso, bastante corto. En persona, Nick parecía rehuir la interacción social física. La rara excepción era alguna presentación ocasional sobre un escenario, con abundantes diapositivas y sin turno de preguntas: una entrada de blog en vivo. Un año antes, cuando un reportero de *Harper's* mencionó que planeaba asistir a una de sus charlas, Nick respondió: «Por favor, no intente acercarse a mí en la conferencia».

«Hoy voy a hablar —comenzó Nick— sobre algunos de los sueños e ideas que creo influyeron en el bitcoin». Las personas detrás de estos conceptos e ideas fueron «pioneros de la era prebitcoin» que contribuyeron a materializar «sueños libertarios», elementos como «despolitizar el dinero» y «hacer cumplir los contratos de forma no violenta». Nick rindió homenaje a varios informáticos cuyo trabajo había preparado el terreno para el bitcoin. Era una versión descentralizada de la historia del origen de la moneda.

A pesar de los esfuerzos de los organizadores por embellecer estas charlas —meteoros surcaban un paisaje lunar en la pantalla situada detrás de Nick—, su presentación consistía en una escueta lista de nombres y viñetas que apenas insinuaban la rica historia que encerraban. Nick solo se animó cuando habló de los *cypherpunks* y los extropianos y de sus viejos amigos Tim May y Hal Finney. Lo que más me interesaba escuchar era cómo se situaría él mismo en este linaje, porque estaba convencido de que Nick era Satoshi Nakamoto. ■

Estudios sobre Satoshi

Satoshi Nakamoto, cuya identidad real nunca ha sido confirmada, desapareció en 2011 sin revelar quién era realmente, aunque hay múltiples teorías sobre quién podría ser: Nick Szabo, Hal Finney, Dorian Nakamoto o incluso un grupo de personas.

SHUTTERSTOCK

Cuando se publicó mi historia en *Wired* a finales de 2011, dos periodistas ya habían propuesto candidatos a Satoshi Nakamoto. Joshua Davis, que informaba para *The New Yorker*, defendía la teoría de que Nakamoto era un criptógrafo experimentado y se presentó en Crypto, la conferencia anual del sector en Santa Bárbara. Allí, localizó a un asistente irlandés de veintitrés años y cabello largo llamado Michael Clear. Clear cumplía varios de los requisitos de Nakamoto: era un estudiante de posgrado en Criptografía, utilizaba la ortografía británica, era una persona reservada (su página de perfil del Trinity College, a diferencia de las de sus compañeros, no mostraba fotos ni números de teléfono), era un estudioso de las redes entre pares y una mente brillante (como estudiante universitario, había sido el mejor de su clase en Informática) que había trabajado en *software* de comercio de divisas.

«AUNQUE LO FUERA NO TE LO DIRÍA»

En las escaleras frente al edificio donde se impartían las clases, Davis logró sacar a relucir un hecho destacado: Clear sabía programar en C++, el lenguaje en el que estaba escrito el bitcoin, pero, cuando Davis le preguntó directamente si era Nakamoto, Clear sonrió y no respondió, sino que se ofreció a «revisar» el diseño del bitcoin para él. Una semana después, Clear le envió un correo electrónico a Davis informándole de que creía poder identificar a Nakamoto. Aparentemente, había sido picado por la curiosidad sobre la identidad de Satoshi, pero parecía ambivalente y le explicó a Davis que «sería injusto publicar una identidad cuando la persona o personas han tomado medidas importantes para permanecer en el anonimato», mientras ofrecía el nombre de «un individuo que coincide con el perfil del autor en muchos niveles».

Esa persona, un investigador finlandés de moneda virtual llamado Vili Lehdonvirta, también se echó a reír cuando Davis le preguntó si era Nakamoto, respondiendo que no tenía los conocimientos necesarios de C++ ni experiencia en criptografía. Davis encontró la negación convincente y volvió a Clear, sugiriendo que tal vez Clear era Nakamoto después de todo. Esta vez Clear dijo: «No soy Satoshi, pero, aunque lo fuera, no te lo diría». Y señaló lo que se estaba convirtiendo en el estribillo de moda entre los bitcoiners: la identidad de Nakamoto no debería importar. Esa era la esencia de una moneda descentralizada. Ser anónimo era su mayor atributo. Después de la publicación del artículo de Davis, Clear negó con vehemencia ser Nakamoto. Había estado hablando «en broma» cuando se mostró evasivo con Davis. «Nunca podría permitirme que se me atribuyera ni remotamente la creatividad y el trabajo duro de otra persona».

Mientras tanto, un reportero de *Fast Company* llamado Adam Penenberg, que anteriormente había expuesto los fraudes periodísticos de Stephen Glass,

PENENBERG HABÍA QUEDADO CAUTIVADO POR EL MISTERIO DE NAKAMOTO Y BUSCÓ EN GOOGLE FRASES DISTINTIVAS DE SUS ESCRITOS

NIALL CARSON

Michael Clear durante su intervención en la Web Summit celebrada en el RDS de Dublín, comparte su análisis y perspectivas sobre la evolución del bitcoin.

se encontró con una similitud sorprendente. Penenberg también había quedado cautivado por el misterio de Nakamoto y buscó en Google frases distintivas de los escritos de Nakamoto. Cuando buscó una de ellas, «computacionalmente imposible de revertir», obtuvo un resultado intrigante: una solicitud de patente para un método de comunicaciones seguras que contenía esa misma frase se había presentado el 15 de agosto de 2008, tres días antes de que Nakamoto registrara *bitcoin.org*. «Vaya coincidencia», escribió Penenberg. La patente incluía tres autores: Neal King y Charles Bry, que vivían en Múnich, y Vladímir Oksman, que vivía en Nueva Jersey. Penenberg encontró otras coincidencias: Bry había visitado Finlandia seis meses antes de que se registrara *bitcoin.org* a través de una empresa finlandesa de internet. La página de Facebook de King estaba repleta de mensajes contra Wall Street, y las reseñas de Amazon que King había escrito recordaban, en opinión de Penenberg, a las publicaciones de Nakamoto en el foro.

Aunque King no utilizaba la ortografía británica, Penenberg ya había llegado a creer que Nakamoto utilizaba anglicismos como «pistas falsas, colocadas allí para despistar a los perseguidores».

Cuando Penenberg se puso en contacto con Bry, el informático respondió: «Espero no decepcionarte demasiado al decirte que no soy Satoshi» y podía decir «con absoluta certeza» que ninguno de sus coinventores lo era. King le dijo a Penenberg que el enfoque de la patente era muy diferente al del bitcoin, que nunca había oído hablar del bitcoin «hasta que surgió esta pregunta», y que ahora que había leído sobre ello, pensaba que era «una solución en busca de un problema».

Penenberg consideró que los argumentos de King no eran convincentes. Sin pretender haber identificado a Nakamoto, Penenberg creía que su evidencia circunstancial era «mucho más convincente» que la de Davis. Tuve que estar de acuerdo con él, y me arrepentí de no haber pensado en utilizar su método de buscar frases únicas en Google.

AMERICAN PROGRAM BUREAU, INC.

Adam L. Penenberg, profesor de periodismo en la Universidad de Nueva York y editor de *PandoDaily*, publicacion *online* sobre noticias tecnológicas.

Durante los dos años siguientes, no ocurrió gran cosa en el incipiente campo de los estudios sobre Satoshi. Entonces, el 1 de diciembre de 2013, alguien que utilizaba el seudónimo Skye Grey publicó un argumento, en un blog recién creado llamado *Like in a Mirror*, titulado «Satoshi Nakamoto es (probablemente) Nick Szabo».

Grey, al igual que Penenberg, había examinado el libro blanco en busca de frases inusuales y las había rastreado en la web. Entre ellas figuraban términos como servidor de marca de tiempo y tercero de confianza, que lo condujeron a una serie de artículos de Nick sobre bit gold. Grey reconoció que Nakamoto probablemente habría asimilado el trabajo de Nick y podría expresarse de forma similar, por lo que también analizó lo que él denominó «expresiones de contenido neutro».

¿QUIÉN ESCRIBIÓ EL LIBRO BLANCO?

También en este caso la coincidencia fue notable. Al comparar algunas «expresiones del libro blanco» que también aparecían en los artículos de Nick Szabo con su presencia en la literatura académica sobre criptografía, Grey destacó «el uso repetido de por tanto sin comas de separación, en contra de la convención; la expresión puede caracterizarse frecuente en el blog de Nick (encontrada en el 1 % de los documentos criptográficos), y el uso de para nuestros propósitos al describir hipótesis (encontrado en el 1,5 % de los documentos criptográficos)».

«O Nick escribió el libro blanco o lo escribió alguien imitando el estilo de escritura de Nick», argumentó Grey. También reconoció que la ortografía *favour*, utilizada por Nakamoto, no fue empleada por Nick. Esto llevó a Grey a concluir que «es muy probable que el documento tuviera varios autores», o bien, como creía Penenberg, que las expresiones británicas se habían incluido como una distracción deliberada.

Grey consideró que otras evidencias también señalaban a Nick. ¿Por qué el libro blanco citaba a Adam Back y Wei Dai, pero no a Nick, cuyo trabajo era claramente una inspiración directa? ¿Por qué Nick, uno de los defensores más constantes del dinero digital descentralizado, había esperado meses después del lanzamiento del bitcoin para mencionarlo de pasada en una frase al final de un extenso ensayo? Grey observó que, en abril de 2008, seis meses antes de que se publicara el libro blanco, Nick había escrito en su blog que el bit gold «se beneficiaría enormemente de una demostración, un mercado experimental (con, por ejemplo, un tercero de confianza que sustituyera a la compleja seguridad que se necesitaría para un sistema real). ¿Alguien quiere ayudarme a programar uno?». Y señaló que, después del lanzamiento del bitcoin, el proyecto de bit gold, en el que Nick había estado activamente interesado solo unos meses antes, «quedó en silencio».

JAN3

Skye Grey publicó en un blog: «Satoshi Nakamoto es (probablemente) Nick Szabo (en la imagen)».

PACIENCIA Y PREVISIÓN

Grey postuló que, como mínimo, Nick era el autor principal del libro blanco. Quizá el bitcoin fue codificado por otra persona. «Parece mucho más probable que un personaje similar a Satoshi que inventara el bitcoin se pusiera primero en contacto con el padre original del proyecto, en lugar de empezar a dedicar todos sus recursos a lanzar lo que en gran medida era la idea favorita de otra persona».

Grey explicó más tarde que le había motivado «la simple curiosidad. Me gustan los misterios». Y defendió su investigación, que reconoció que «no ha sido bien recibida»: «Cuando uno empieza a tener un gran impacto en el mundo, pierde su derecho al anonimato». Justificó la publicación de sus hallazgos «para responder a la preocupación de la gente de que un mal tipo pudiera haber creado el bitcoin».

Otros investigadores llegaron a conclusiones similares. Dominic Frisby, un comediante y escritor financiero inglés, se centró en la combinación de conocimientos que Nakamoto tendría que haber tenido: «codificación informática, matemáticas, bases de datos, contabilidad, sistemas entre pares, propiedad digital, derecho, contratos inteligentes, criptografía e historia monetaria». Creía que la forma en

DESPUÉS DEL LANZAMIENTO DEL BITCOIN, BIT GOLD, DONDE NICK SZABO HABÍA ESTADO TRABAJANDO, «QUEDÓ EN SILENCIO»

que se había lanzado el bitcoin sugería «experiencia en empresas emergentes de tecnología de código abierto». Las defensas impenetrables del *software* revelaban a un *hacker* experto en seguridad, la prosa de Nakamoto, a un escritor, y su seudónimo, a alguien familiarizado con el secreto. Nakamoto demostró paciencia, previsión, humildad, integridad y una perspicacia sobre la psicología humana. Solo un libertario o un *cypherpunk* habrían tenido la motivación necesaria y el instinto para presentar su creación. Frisby se centró en la fecha de nacimiento que Nakamoto registró en el sitio web de la Fundación P2P: 5 de abril de 1975. El 5 de abril fue la fecha en que, en 1933, el presidente Franklin D. Roosevelt declaró ilegal que los ciudadanos estadounidenses poseyeran oro, y 1975 fue el año en que a los se les permitió nuevamente poseer este metal. Frisby señaló que en 2007, Nick, que acababa de graduarse en Derecho a los 42 años, disponía de tiempo para emprender otro gran proyecto.

Aunque Frisby construyó un caso circunstancial convincente, cuando se lo presentó a Nick, Nick respondió: «Me temo que te equivocaste al hacerme *doxxing* como Satoshi, pero estoy acostumbrado». El *doxxing*, que anteriormente había significado revelar datos personales como la dirección o el número de la seguridad social de alguien, claramente había perdido su significado para algunas personas.

Ni las conclusiones de Grey ni las de Frisby parecían mantenerse. Ambos habían hecho hincapié en la decisión de Nakamoto de lanzar el bitcoin a través de un artículo de estilo académico, y en su actividad de publicación, que parecía aumentar durante el verano. Grey escribió que «Nick es un profesor con un historial de publicaciones significativo». Pero Nick no era ni había sido nunca profesor. Y aunque había escrito extensamente en su blog y de manera erudi-

SHUTTERSTOCK

En 1933, Roosevelt declaró ilegal que los ciudadanos estadounidenses poseyeran oro. Hasta 1975 no se les permitió nuevamente poseer este metal.

NICK LOGRABA CONVOCAR A GRANDES AUDIENCIAS A PESAR DE SU ESTILO POCO ANIMADO Y SUS TEMAS RECURRENTES

ta, nunca había publicado académicamente. Algunos de los términos que Grey había interpretado como pruebas irrefutables, como firmas digitales y pruebas criptográficas, eran comunes en criptografía.

IMPOSIBLE DESCARTARLO COMO CANDIDATO

Al año siguiente, Nathaniel Popper, reportero del *New York Times*, se enfrentó a Nick en una reunión del sector, en la casa de un gestor de fondos de cobertura en Lake Tahoe. Popper había sido invitado porque cubría la criptomoneda y Nick había acudido como empleado de una nueva empresa emergente relacionada con bitcoin llamada Vaurum. En los cócteles previos a la cena, cuando surgió el tema de Nakamoto, Nick le comentó a un pequeño grupo: «Bueno, diré esto, con la esperanza de dejar las cosas claras: no soy Satoshi y no soy profesor universitario». En un momento dado, Popper acorraló a Nick en la cocina y Nick reconoció: «Existen todos esos paralelismos, y me parece gracioso, y le parece gracioso a mucha otra gente». Más tarde, Nick envió un correo electrónico a Popper con una negación definitiva: «Como he dicho muchas veces antes, todas estas especulaciones son halagadoras, pero erróneas: yo no soy Satoshi». Poco después, Popper informó sobre que Nick había abandonado Vaurum «después de ponerse nervioso por la exposición pública».

Grey, Frisby y Popper señalaron que Nick había vuelto a publicar sus antiguos ensayos sobre bit gold después de octubre de 2008 y sugirieron que lo había hecho para que pareciera que los había escrito con posterioridad a bitcoin, con el fin de desviar las sospechas sobre sí mismo. Sin embargo, incluso después de que el *New York Times* señalara a Nick como la persona que los expertos de Silicon Valley consideraban que era Nakamoto, la ausencia de evidencias contundentes mantuvo esta teoría en una zona gris que no llegaría a aclararse.

En la primavera de 2022, once años después de que le preguntara a Nick si era Satoshi Nakamoto, y a pesar de su negativa entonces y en numerosas ocasiones posteriores, seguía siendo imposible descartarlo como candidato. El mundo a veces lo trataba como si fuera Nakamoto, pero de maneras peculiares. La Universidad Francisco Marroquín de Guatemala, destacando su «investigación en contratos digitales y moneda digital», le otorgó un doctorado *honoris causa* y una cátedra. El *podcaster* Tim Ferriss lo entrevistó durante dos horas y media presentándolo como «el maestro silencioso de las criptomonedas», sin mencionar ni preguntar ni una sola vez sobre el evidente trasfondo de la presencia de Nick en el programa. Nick lograba convocar a grandes audiencias en sus presentaciones, a pesar de su estilo poco animado y sus temas recurrentes.

Existían más indicios que apuntaban a Nick, pero este hecho se había diluido de alguna manera entre el ruido de otras conjeturas sobre Nakamoto. En todo caso, ahora había razones adicionales para centrarse en él. ■

Anónimo

Mark Felt, en la imagen, y Satoshi Nakamoto han sido vistos como héroes por unos y como figuras problemáticas por otros, dependiendo de la perspectiva política y filosófica.

UNITED STATES CONGRESS

Lo primero que noté en mis nuevas consideraciones sobre «Nick como Nakamoto» fue que ya no otorgaba mucho peso a sus desmentidos. Mi aceptación anterior de sus negaciones había sido ingenua. No tenía que ver con su honestidad o su falta de ella. Simplemente me había familiarizado con otros casos donde alguien que usaba un seudónimo fue desenmascarado.

En 1996, un profesor de Inglés llamado Donald Foster identificó al periodista Joe Klein como el autor anónimo de una novela superventas sobre la campaña presidencial de Clinton en 1992 titulada *Colores primarios*, basándose en sus estilos de escritura similares. Klein negó ser el autor. «Por el amor de Dios, yo no lo escribí», exclamó a un reportero del *New York Times*. Dejó un mensaje de voz negando la autoría, lo negó en CBS News, donde era comentarista, y lo negó ante sus propios colegas en *Newsweek*, incluso permitiendo que la revista publicara especulaciones que señalaban a otros sospechosos anónimos. Finalmente, Klein admitió que, efectivamente, era el autor del libro.

MARSHA MILLER

Joe Klein, periodista y autor de *Colores primarios* (1996), donde satirizaba la campaña presidencial de Bill Clinton.

«GARGANTA PROFUNDA»

Mark Felt, exdirector asociado en funciones del FBI, afirmó repetida y explícitamente que no era «Garganta profunda», la fuente secreta con cuya ayuda los reporteros del *Washington Post* Bob Woodward y Carl Bernstein habían desentrañado el Watergate. Felt testificó ante un gran jurado, bajo pena de perjurio, que él no era «Garganta profunda» (antes de retirar precipitadamente el testimonio). A *The Wall Street Journal* le propuso una teoría de que «Garganta profunda» podría ser «un compuesto» de varias personas. En sus propias memorias, Felt subrayó que «¡nunca filtré información, a Woodward ni Bernstein ni a nadie más!». Años después, cuando un amigo del hijo de Bernstein, Jacob, en un campamento de verano, dijo a *The Hartford Courant* que Jacob había identificado a Felt como «Garganta profunda», Felt declaró al periódico: «No, no soy yo. Lo habría hecho mejor. Habría sido más eficaz». Finalmente, Felt admitió que él era, efectivamente, «Garganta profunda».

EN 1996, DONALD FOSTER IDENTIFICÓ A JOE KLEIN COMO EL AUTOR ANÓNIMO DE UNA NOVELA, *COLORES PRIMARIOS*

Estas personas siempre lo negaron. Las negaciones de Felt, reflexionó Woodward más tarde, «solo consolidaron mi triste comprensión» de que cualquiera que esté en un aprieto, o crea estarlo, dirá cualquier cosa para protegerse y salir del paso. Con el tiempo, todos nos comprometemos con una versión de la historia de nuestras vidas. La simplificación y la repetición solidifican el relato y tendemos a ceñirnos a esa identidad». (Woodward sabía de lo que hablaba, después de mentir a su colega del *Washington Post*, Richard Cohen, que iba a escribir una columna nombrando a Felt como «Garganta profunda» hasta que Woodward lo negó). Si ya te habías comprometido con el anonimato y asumido las molestias de mantener una identidad encubierta, añadir una mentira explícita apenas suponía un paso más.

El problema fue ilustrado por Ralph Merkle, coinventor de la criptografía de clave pública, cuyo trabajo fue uno de los ocho artículos citados en el libro blanco del bitcoin, y que había inventado una estructura de datos, los árboles de Merkle, en los que se basa el *software* del bitcoin para construir los bloques en la *blockchain*. Inevitablemente, estaba en la larga lista de posibles Nakamoto.

Cuando le preguntaron sobre el asunto una entrevista, dijo:

—Niego ser Satoshi.

—Entonces, ¿puedo tacharlo de la lista también?

—Por supuesto. Pero ¿de verdad esperas que Satoshi diga: «Sí, soy Satoshi»?

—Si fueras Satoshi, ¿me dirías que eres Satoshi?

—Por Dios, ¡no! ■

ASC

Ralph C. Merkle es un científico de la computación e inventor estadounidense, pionero fundamental en criptografía; sin sus innovaciones, el bitcoin tal como lo conocemos no existiría.

Una espectacular demostración de retrospectiva

Nick Szabo coleccionaba billetes del banco libre, estudiaba cuentas de concha, admiraba monedas sin rostros de políticos. Luego, diseñó una moneda sin gobierno, sin bancos, sin rostros. Solo matemática pura.

ISTOCK

Muchas otras pistas señalaban a Nick Szabo. El nivel de seguridad operativa de Nakamoto indicaba que se trataba de alguien que había reflexionado profundamente y practicado el arte de evitar todas las formas en que internet puede vincular datos personales. «Su capacidad para no dejar rastro es prácticamente inigualable —me explicó Ray Dillinger, un criptógrafo que, junto con Hal Finney, había revisado el código de Nakamoto antes del lanzamiento del bitcoin—. Nunca he conocido a nadie que realmente pudiera mantenerse en el anonimato en internet cuando así lo deseaba».

«SI NO LO ENTIENDES, NO PUEDO AYUDARTE MÁS»

Nick había estado considerando estas cuestiones durante quince años antes de que apareciera el bitcoin. «En mi limitada experiencia creando seudónimos en internet, me ha distraído bastante la necesidad constante de evitar dejar pistas de mi verdadero nombre», les comentó Nick a sus compañeros *cypherpunks* en 1993. Todo, desde los archivos compartidos hasta los hábitos ortográficos, podía delatarte. «Los peligros acechan por todas partes. Con nuestras herramientas actuales es prácticamente imposible mantener un seudónimo activo durante un periodo prolongado frente a un adversario suficientemente determinado, y resulta bastante complicado mantener incluso un mínimo de seguridad aceptable».

Las negativas de Nick cuando se le preguntó si era Nakamoto habían sido escuetas. El hecho de que el libro blanco del bitcoin no reconociera la evidente influencia de Nick, además de un comentario posterior en *BitcoinTalk* en el que Nakamoto escribió que «Bitcoin es una implementación de la propuesta de b-money de Wei Dai... en *cypherpunks*... en 1998 y la propuesta de bitgold de Nick Szabo», seguía sin explicación. La deuda con el trabajo de Nick era tan obvia que el *cypherpunk* James Donald, la primera persona en responder a Nakamoto en *Metzdowd* a finales de 2008, se había referido a los bitcoins como «monedas bitgold». Mientras comentaba que la mejor forma de resolver las dudas sobre el bitcoin sería publicando su código fuente, Hal Finney respondió: «He descubierto que existe un proyecto en Source Forge creado para bitgold, aunque aún no contiene código».

¿Por qué Nick nunca se había mostrado ofendido por la omisión de su trabajo en las citas del libro blanco? Si estaba siendo modesto, ¿por qué no habría al menos hablado en nombre de Hal y dicho: «Sí, es extraño que el RPOW de Hal no se haya citado en el libro blanco»? Jamás había dicho: «Ojalá pudiera atribuirme el mérito, pero mis conocimientos de C++ no se acercan ni remotamente a los de Satoshi». Tampoco dijo: «Comprendo por qué todos creen que soy Satoshi, pero vamos a despejar este rumor: este es el jefe para el que trabajaba en 2008 y 2009, y esta es la persona con la que mantenía una relación. Ambos

¿POR QUÉ NICK NUNCA SE HABÍA MOSTRADO OFENDIDO POR LA OMISIÓN DE SU TRABAJO EN LAS CITAS DEL LIBRO BLANCO?

pueden confirmar que yo trabajaba doce horas diarias en otro proyecto, y que, cuando Nakamoto logró hacer lo que yo había estado intentando durante años, me quedé paralizado por la envidia».

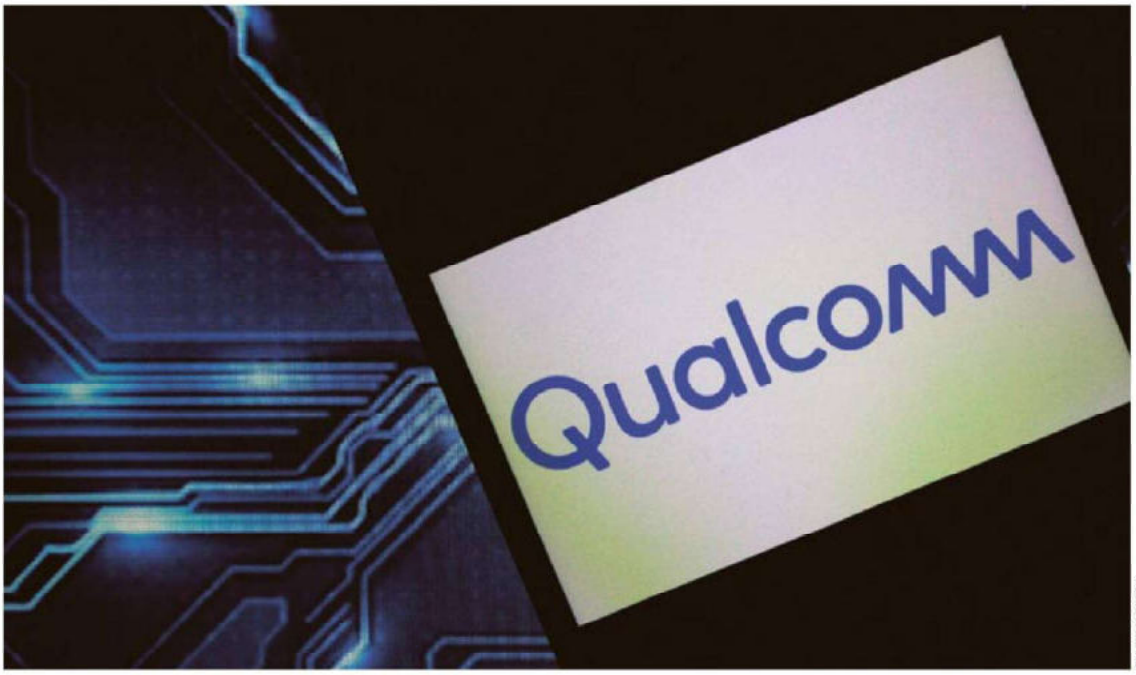
Nick no le debía explicaciones a nadie, pero las sospechas lo perseguían precisamente porque apenas reconocía las numerosas razones para pensar que él podría ser Nakamoto. Esto propiciaba que la gente creyera que o bien era Nakamoto o no le importaba que lo pensaran.

Casi tan significativos como el silencio de Nick fueron las contadas excepciones al mismo. Después de que Gwern Branwen argumentara que el bitcoin no era tan novedoso, Nick escribió una extensa réplica en la que calificaba el argumento de Branwen de «una espectacular demostración de retrospectiva». Cuando un inversor de Silicon Valley llamado Balaji Srinivasan ejerció sus poderes de moderación en un canal de Telegram que lleva el nombre del fundador del bitcoin, Nick se burló de Srinivasan por sus «patéticas normas corporativas» que parecían tratar el nombre de Nakamoto como propiedad suya y censurar a la gente bajo su amparo. Y Nick se veía claramente a sí mismo como el padre de las criptomonedas cuando escribía: «El conocimiento de la larga historia del dinero no gubernamental fue una de las inspiraciones de la invención original de la criptomoneda con confianza minimizada».

Cuando en 2022 me sumergí en los voluminosos escritos de Nick en internet, fue fácil escuchar ecos del fundador del bitcoin. Nakamoto escribió una vez: «Si no me crees o no lo entiendes, no tengo tiempo para intentar convencerte, lo siento». Nick escribió una vez: «Si no lo entiendes, no puedo ayudarte más». Volví a mirar un largo correo electrónico que Nick me había enviado en 2011 y vi que, al igual que Nakamoto, usaba dos espacios después de un punto y jerga de internet, inclu-

ASC

Balaji S. Srinivasan es un empresario, inversor y tecnólogo estadounidense, figura muy influyente en el mundo de las criptomonedas y la tecnología *blockchain*.



SHUTTERSTOCK

Nick Szabo, pionero de los contratos inteligentes, invirtió la mayor parte de sus ahorros en Qualcomm cuando nadie creía en la telefonía móvil digital.

yendo BTW. Nick se sentía cómodo con los mismos vocabularios y referencias que Nakamoto, desde el trabajo del economista austriaco Carl Menger hasta el concepto de equilibrio del pionero de la teoría de juegos, John Nash.

«El diseño admite una enorme variedad de tipos de transacciones posibles que diseñé hace años —había escrito Nakamoto—. Transacciones de custodia, contratos de fianza, arbitraje de terceros, firmas de varias partes, etc.». Nick, en 1994, escribió: «Estoy particularmente interesado en el arte de redactar contratos y diseñar transacciones para servicios de datos en línea», y tomó un desvío de tres años en la mediana edad para asistir a la facultad de Derecho.

«LA REALIDAD NO DESTRUYE LOS SUEÑOS»

Mucha gente había hablado sobre el dinero del futuro, pero bitcoin fue el primer sistema de dinero digital descentralizado que funcionó. Nick siempre había anclado sus sueños con un rigor testarudo, desdeñando a los utópicos endebles como «gente de Hello Kitty». Filtró cada discusión a través de una lente pragmática, haciendo cálculos sobre lo que era factible ahora. Creía que los proyectos espaciales debían estar impulsados por el mercado: «Primero debemos satisfacer las necesidades de la gente, y luego vendrán», y no «un caso de asistencia social». A principios de la década de los noventa arriesgó su propio dinero invirtiendo la mayor parte de sus ahorros en empresas a la vanguardia de la tecnología espacial, como Qualcomm y Orbital Sciences. Cuando la gente usaba el término contable, él se ofendía y hacía un análisis de flujo de caja en una hoja de cálculo, por ejemplo, sobre cómo mover asteroides para terraformar Venus. No solo quería saber qué era científicamente posible, sino también qué era económicamente probable. «La realidad no destruye los sueños —escribió—. Nos da una forma de hacerlos realidad».

SE HABLABA SOBRE EL DINERO DEL FUTURO,PERO BITCOIN FUE EL PRIMER DINERO DIGITAL DESCENTRALIZADO QUE FUNCIONÓ

Nick también había realizado un estudio profundo sobre los orígenes del dinero. Con la intuición de un arqueólogo para la moneda física, se deleitaba con la variedad de objetos que históricamente habían servido como dinero, desde cuentas de conchas de caracol hasta cáscaras de huevo de avestruz y marfil de mamut. Le fascinaban expresiones como desgranar que derivaban de las cuentas de concha de almeja conocidas como *wampum*. Coleccionaba billetes de la era del banco libre del siglo xix, emitidos por corporaciones como el Boone County Bank Indiana y la Great Western Railroad Company, que le parecían hermosos y «notablemente libres de rostros de políticos».

TODD WHITE

Tim Ferriss es un empresario, autor, podcaster e inversor estadounidense, conocido por su libro *The 4-Hour Workweek*.

Un argumento recurrente contra Nick, cada vez que alguien sugería que podría ser Nakamoto, era que no se le conocía como programador. Sin embargo, Nick se había especializado en Informática en la universidad y había ocupado varios puestos de *software* tras graduarse. Indagando entre los vestigios de los inicios de internet, descubrí que a principios de los noventa había promocionado su experiencia en «arquitectura e ingeniería de *software*», sus «amplias habilidades de piratería» y su conocimiento de C/C++ y Windows/DOS. Mencionó que tenía nada menos que seis libros de C/C++ sobre su escritorio. En otra ocasión, escribió: «Tejo un código malvado».

También había estudiado japonés y sentía fascinación por la cultura japonesa. Las iniciales de Nakamoto, SN, eran inversas a las de Nick, lo que concordaba con la convención tanto japonesa como húngara de anteponer el apellido al nombre: en Hungría, el nombre de Nick sería Szabo Nikolas, y en Japón sería, digamos, Szaboshi Nickamoto.

Luego, Nick apareció en el pódcast de Tim Ferriss en 2017. En un momento de la entrevista, se equivocó: «Diseñé bitcoi-gold con dos capas». Cuando vi a Nick hablar en Miami, volvió a cometer un desliz: «En mi implementación, o en mi diseño, de bit gold...».

Pensaba: «¿Cómo es posible que Nick no sea Nakamoto?». ■

La lista de verificación de Satoshi

La pregunta equivocada es «¿Quién es Satoshi?». La pregunta correcta es «¿Por qué nunca se quitó la máscara?». La máscara de Anonymous nos recuerda que algunas revoluciones solo funcionan si el revolucionario desaparece. SHUTTERSTOCK

DUQUESNE UNIVERSITY

El dr. Patrick Juola es profesor de Ciencias de la Computación en la Universidad de Duquesne, especializado en análisis forense lingüístico y estilometría computacional.

En el verano de 2022, después de mi visita a Patrick Juola, el identificador de J. K. Rowling en su laboratorio de Pittsburgh, pegué en una pizarra gris situada en la pared de mi oficina una hoja de cálculo con más de cien candidatos propuestos como Satoshi Nakamoto. Estaban los sospechosos habituales, en su mayoría *cypherpunks*. Había nombres menos conocidos provenientes de campos afines, como las matemáticas, la criptografía y la economía. Algunos eran programadores involucrados en el proyecto de *software* del bitcoin. Otros, creadores de criptomonedas más recientes. Muchos eran simplemente personas famosas e inteligentes: Bill Gates, Steve Jobs, John Nash (el matemático inmortalizado en *Una mente maravillosa*). Para cada candidato enumeré argumentos a favor y en contra. Me encontraba en la esencia misma del periodismo de investigación: desentrañar verdades que alguien se empeñaba en silenciar. «Un buen rompecabezas es algo justo —dijo en su día Ernö Rubik (el creador del famoso cubo)—. Nadie miente, todo es muy claro, el problema solo depende de ti». No estaba seguro de que el misterio de Nakamoto cumpliera esos requisitos, pero era reconfortante sumergirse por completo en el proyecto.

«PODEMOS GANAR UN NUEVO TERRITORIO DE LIBERTAD»

Encima de la hoja de cálculo, pegué una lista de comprobación, una columna de criterios que cualquier candidato plausible a ser Nakamoto tendría que cumplir:

—Herramientas de *software*
—Peculiaridades del código
—Edad
—Geografía

—Horario
—Uso del inglés
—Nacionalidad
—Estilo narrativo
—Política
—Circunstancias vitales (¿Cómo había encontrado Nakamoto tiempo para lanzar el bitcoin? ¿Por qué había abandonado el proyecto en ese momento?)
—Currículum (No soy un abogado)
—Rango emocional (humilde, seguro, irritable, agradecido)
—Motivación para crear el bitcoin
—Razonamiento, previsión y habilidad para crear un seudónimo a prueba de balas (¿Quién se molestaría en limpiar una escena del crimen antes de que fuera una escena del crimen? ¿Quién era tan bueno en privacidad en 2008?)
—Capacidad monacal para renunciar a una fortuna

La lista de verificación asumía que Nakamoto, aunque reservado, no había elaborado una personalidad ficticia compleja. Pero algunos rasgos eran más cuestionables que otros. Los conocimientos de programación en C++ eran algo innegable. Sin embargo, las huellas del inglés británico resultaban mucho más fáciles de fingir, los horarios podían manipularse y las inclinaciones políticas podían aparentarse. Mientras que Nakamoto había utilizado en una ocasión la frase claramente libertaria: «Podemos ganar un nuevo territorio de libertad», en otra se había referido a cómo bitcoin sería «muy atractivo desde el punto de vista libertario», lo que sonaba más como una observación distante que como una convicción personal.

En la otra pared hice un *collage*. La mayoría de las historias que había investigado venían con viveza o intimidad incorporadas. En la bahía de Guantánamo, pude centrarme en los humildes efectos personales de un detenido menor de edad: zapatillas de correr sin cordones, desodorante Mennen Speed Stick. En el apartamento de un payaso en San Francisco, pude observarlo de pie frente al espejo del baño en calzoncillos y aplicándose colorete. En Polonia, pasé una semana con un trabajador ferroviario, que había despertado de un coma después de quince años tras haberse perdido el final del comunismo y la muerte de su devota esposa.

«BITCOIN RENAISSANCE»

La intangibilidad del bitcoin hacía difícil asimilarlo. Los intentos de representar las criptomonedas solían recurrir a números garabateados al estilo de *Una mente maravillosa*. En Miami, paseé por una sala de exposiciones donde un cartel anunciaba «la mayor galería de arte del bitcoin de la historia». Allí se celebraba una exposición titulada «Bitcoin Renaissance»: «En 1494, la invención de la contabilidad por partida doble marcó el comienzo de una nueva era de prosperidad hu-

ESTABA EN LA ESENCIA DEL PERIODISMO DE INVESTIGACIÓN: DESENTRAÑAR VERDADES QUE ALGUIEN SE EMPEÑABA EN SILENCIAR

mana y, poco después, de una edad de oro de la expresión artística. Desde 2008, la invención del bitcoin ha inaugurado el último capítulo del florecimiento humano».

No era arte que requiriera fruncir el ceño para interpretarlo. Había representaciones creativas del símbolo del bitcoin, direcciones de clave pública, el libro blanco, eslóganes populares como «JUST HODL IT» (*hodling*, en el argot del bitcoin, significa «mantener» o comprar bitcoins a largo plazo), celebridades del bitcoin como el presidente de El Salvador, Nayib Bukele, y ojos láser, un meme popular entre los bitcoiners para mostrar su lealtad tribal. Alguien había reinterpretado *La noche estrellada*, de Vincent van Gogh, con el símbolo del bitcoin en lugar de estrellas. Alguien había publicado un libro ilustrado para niños: *Bitcoin en rima*. Muchas de las imágenes, en consonancia con el resentimiento tribal de los bitcoiners, eran combativas: la cara de Jamie Dimon derritiéndose, un bitcoin batiéndose en un duelo de espadas con un dólar, un grupo de viejos blancos alrededor de un Monopoly apoyado en las espaldas de esclavos multirraciales («Falsos beneficios»), un puño americano con el símbolo del bitcoin en el medio y las palabras «Fiat Facelifter», una tabla de clasificación de «monedas fiduciarias fallidas» (el bolívar, el papel moneda) junto a una tabla de clasificación de «alternativas de dinero sólido» (bitcoin, oro, plata).

UN DIOS NO INTERVENCIONISTA

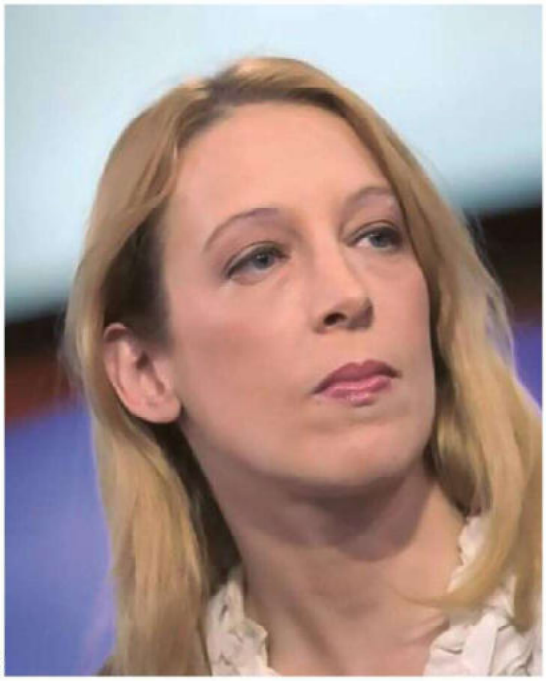
Tenía curiosidad por ver cómo se interpretaría a Nakamoto, el líder sin rostro de la utopía sin centro del bitcoin. A estas alturas, los aspectos religiosos de la cultura bitcoin apenas se ocultaban. El libro blanco era la sagrada escritura. Los bitcoiners evangelizadores eran los elegidos, todos los demás, los condenados. Satoshi, el desinteresado poseedor de una fortuna obscena, era su Dios no intervencionista.

SHUTTERSTOCK

En 2021, El Salvador se convirtió en el primer país en adoptar el bitcoin como moneda oficial. Nayib Bukele, presidente de El Salvador, sale de la Casa Blanca tras una reunión presidencial.

TENÍA CURIOSIDAD POR VER CÓMO SE INTERPRETARÍA VISUALMENTE A NAKAMOTO, EL LÍDER SIN ROSTRO DE LA UTOPÍA

Las representaciones que se hacían de él, como un muñeco de peluche vendido en Amazon en 2016, tenían rasgos asiáticos. En Miami, algunos artistas habían recurrido a una figura encapuchada sin rostro, otros, a máscaras de Guy Fawkes. La cara de Dorian Nakamoto estaba por todas partes: en una pintura puntillista, en lugar de un presidente en un «billete de bitcoin» con forma de dólar, en una tarjeta coleccionable en una funda rígida transparente (otra de las tarjetas mostraba a Hal Finney). Unos años después del reportaje mal concebido de *Newsweek*, Dorian había empezado a asistir a conferencias sobre el bitcoin donde fue acogido como una figura de culto. La misma comunidad que había denunciado salvajemente a Leah Goodman por nombrarlo como Satoshi Nakamoto ahora disfrutaba alegremente del uso de su imagen como sustituto.



ASC

Leah McGrath Goodman es una periodista de investigación estadounidense que trabajó para *Newsweek*.

EL SANTO FUNDADOR

Entendí por qué el arte del bitcoin era tan literal. Compartía el impulso de hacer material lo etéreo. La compulsión de colgar fotos de parafernalia del bitcoin se sentía similar al impulso de corroborar a Nakamoto identificándolo.

El panel de inspiración de mi oficina consistía en caras con deficiencia de vitamina D y dispositivos de aspecto extraño y acciones desconcertantes. Cuando quería, podía girar la silla y mirar las imágenes para mantenerme con los pies en la tierra por un momento. Había monedas casascius, fichas de metal que llevaban incrustadas una clave privada y una dirección bitcoin y estaban protegidas por una pegatina holográfica a prueba de manipulaciones. Una plataforma de minería. Una cartera de *hardware*. El vertedero galés con el disco duro de 8000 bitcoins en algún lugar. Hombres con cascos de Daft Punk. Otros hombres con mascarillas en las que se proyectaban avatares digitales. Un gráfico montañoso del historial sísmico de precios del bitcoin.

La primera vez que mi mujer vio todo esto (la hoja de cálculo, la lista de verificación, el *collage*) sonrió. En realidad, fue una sonrisa burlona.

—¿Vas a añadir algún hilo rojo? —preguntó.

Zooko Wilcox-O'Hearn es un criptógrafo, empresario y figura fundamental del movimiento *cypherpunk*, creador de la criptomoneda Zcash.

Cuando intenté contactar nuevamente con fuentes anteriores y potenciales, me encontré con una resistencia inesperada. En parte, se debía a la polarización que había invadido internet desde la primera vez que escribí sobre el bitcoin. Cuando le envié un mensaje a Robert Hettinga, un voluble *cypherpunk* de Anguila que llevaba mucho tiempo interesado en el dinero digital, me bloqueó en Twitter y se jactó ante sus 942 seguidores de que diez años antes «habría dado su huevo izquierdo» por hablar con un periodista, pero ahora se pondría «a despotricar como un ultra-MAGA» contra un escritor de «programas de mierda liberticidas».

Gran parte de la fricción tenía que ver con el tabú en torno a Satoshi Nakamoto. Siempre ha habido una facción hostil a la investigación sobre su identidad. («Ha hecho una valiosa contribución, por lo que sus deseos deben ser respetados. Lo que importa no es la persona, sino la idea, el código»). A medida que se fue creando una leyenda en torno a Nakamoto, «el santo fundador» de esta tecnología que cambiará el mundo, en palabras de Gavin Andresen, las simples preguntas sobre quién podría ser se convirtieron en detonantes para los bitcoiners. Y la revelación de la identidad de Dorian Nakamoto acabó con todo el proyecto. El *doxxing*, si vivías en la burbuja del bitcoin, ahora se aplicaba incluso al nombre de una persona de interés periodístico. Los editores de *Reason* («Mentes libres y mercados libres»), disgustados por «el sonido indecoroso de los escribas con los ojos muy abiertos» que habían investigado la autoría del bitcoin, publicaron un artículo titulado: «¡Dejad en paz a Satoshi!». Cuando intenté hablar con Peter McCormack, un *podcaster* centrado en el bitcoin en Inglaterra que en LinkedIn se describía a sí mismo como «periodista a tiempo completo», resopló: «No me interesan los reportajes que hurgan en los orígenes buscando la identidad de Satoshi; él eligió mantenerse en el anonimato y creo que debemos respetar esa decisión».

El cordón de protección me pareció absurdo. Nakamoto había puesto su artilugio en la plaza pública. Era razonable preguntar quién lo había puesto allí y por qué. Me sentí identificado con un usuario de Reddit que, respondiendo a los fanáticos

ME PLANTEÉ EN QUÉ CIRCUNSTANCIAS ME ABSTENDRÍA DE REVELAR LA IDENTIDAD DE SATOSHI NAKAMOTO

de la privacidad cuando Skye Grey expuso su teoría sobre Nick Szabo, escribió: «A toda la gente que dice que no le importa quién es Satoshi y que no quiere saberlo: admiro el orgullo que sienten por no tener curiosidad, pero no los entiendo en absoluto. Es uno de los últimos grandes misterios que quedan en internet, y es fascinante. Enséñenme sus poderes zen de indiferencia, quiero aplicarlos a mi amor por las galletas y los pasteles».

«OJALÁ SATOSHI SIGUIERA VIVO»

Cuando hablé con Bill Dodd, un desaliñado director de *software* de Mobile, Alabama, que había entrenado una red neuronal con el archivo de *Metzdowd* y había aplicado el aprendizaje automático a su propia búsqueda de Nakamoto, me preguntó:

—¿Qué opinas del dilema ético de revelar la identidad de alguien que claramente quiere que lo dejen en paz?

Vislumbré una regañina en el horizonte, pero Bill resultó ser un tipo encantador con una mezcla muy humana de curiosidad y empatía.

—Dependería de quién resultara ser Nakamoto —repuse.

—Sí, yo igual. Empecé por simple curiosidad, y no le dediqué mucho tiempo... Solo quería saber, porque fue algo importante en mi formación y, como recién llegado, me pareció fascinante que diez años después, este misterio aún persistiera —me dijo Bill, y, tras confesar que al principio se mostró escéptico con la idea del bitcoin, añadió—: Creo que el misterio a veces es difícil de resistir. Yo también voy y vengo. Por un lado, tienes algo que se ha convertido en una parte tan importante del espíritu de la época que casi parece una historia incompleta cuyo nombre no es conocido por la gente. Y, por otro lado, no me gustaría que aparecieran las furgonetas de la CNN cuando tenga cincuenta o sesenta años y esté jubilado en mi residencia en Londres o donde sea. Así que lo entiendo, entiendo ambas partes.

La sensibilidad, así como cierta fatiga del tema entre los bitcoiners después de años de salidas fallidas de Nakamoto, determinaron mi forma de acercarme a la gente. Dependiendo de quién fuera, a veces empecé a sustituir el altisonante «orígenes del bitcoin», cuando describía por primera vez el tema de mi investigación, por el más potencialmente provocador «identidad de Satoshi».

Me planteé en qué circunstancias me abstendría de revelar la identidad de Nakamoto. Quizás la respuesta resultara decepcionante. Al fin y al cabo, ¿qué importancia tendría descubrir que se trataba de esta persona anónima en lugar de aquella otra igualmente desconocida? En 2017, Zooko Wilcox —un *cypherpunk* que había trabajado en DigiCash, posteriormente creador de Zcash (una criptomoneda con mayor privacidad) y en la lista de posibles candidatos a ser Nakamoto— escribió: «Ojalá Satoshi siguiera vivo, para que pudiéramos comprobar que es tan ignorante, inadecuado y ordinario como todos nosotros». ■

Un ser humano imperfecto

Cinco meses después de que Craig Wright fuera, y luego no fuera, identificado como Satoshi Nakamoto, el lunes 2 de mayo de 2016, el australiano volvió a aparecer en mis noticias. Ahora parecía que efectivamente era Nakamoto.

NOS ENCANTA CREAR HÉROES

Esta vez, la noticia llegó en un bombardeo mediático a las ocho de la mañana con primicias sobre las afirmaciones de Wright en *The Economist* y la BBC que anunciaron: «El Sr. Wright ha proporcionado pruebas técnicas para respaldar su afirmación utilizando monedas que se sabe pertenecen al creador del bitcoin. Miembros destacados de la comunidad bitcoin y sus principales equipos de desarrollo dicen que han confirmado sus afirmaciones». Uno de ellos fue Jon Matonis, cofundador de la Fundación Bitcoin, una organización sin ánimo de lucro creada para fomentar el crecimiento de la cripto, que escribió en su blog «Cómo conocí a Satoshi», declaró a la BBC que estaba «absolutamente convencido» de que Wright era Nakamoto y añadió que la invención del bitcoin estaba «al nivel de la imprenta de Gutenberg». Pero quien dio mayor credibilidad a las afirmaciones de Wright fue Gavin Andresen, antiguo desarrollador principal de bitcoin, que escribió en su blog: «Creo que Craig Steven Wright es la persona que inventó el bitcoin: nos encanta crear héroes, pero también parece que nos encanta odiarlos si no están a la altura de algún ideal inalcanzable. Sería mejor si Satoshi Nakamoto fuera el nombre en clave de un proyecto de la NSA o una inteligencia artificial enviada desde el futuro para mejorar nuestro dinero primitivo. No lo es, es un ser humano imperfecto como el resto de nosotros. Espero que consiga ignorar en gran medida la tormenta que provocará su anuncio y seguir haciendo lo que le gusta: aprender, investigar e innovar».

Gavin también relató cómo, un mes antes, había llegado a convencerse de esta verdad. ■

SHUTTERSTOCK

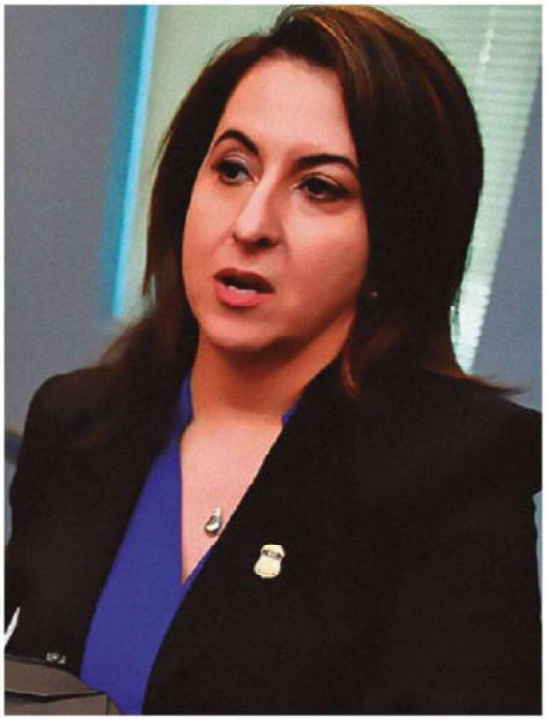
El informático y empresario australiano Craig Wright asegura haber participado en la creación del bitcoin, aunque no hay consenso ni pruebas verificables que lo confirmen.

Libertad de información

Satoshi Nakamoto era un ingeniero meticuloso que trabajaba abiertamente en foros, respondía técnicamente y publicaba código auditable. No atacaba sistemas; construía uno nuevo.

SHUTTERSTOCK

En 2022 encontré otra pista prometedora. En la primavera de 2019, Rana Saoud, agente asistente a cargo de la división de Inmigración y Control de Aduanas del Departamento de Seguridad Nacional, había hablado en la Conferencia OffshoreAlert en Miami como parte de un coloquio titulado «Regulación de criptomonedas e ICO: ¿seguridad, mercancía o moneda?». Durante la presentación, recordó la investigación de un colega sobre Black Market Reloaded, uno de los bazares de la web oscura que había sucedido a Silk Road: «Es un agente extremadamente inteligente y visionario. Me dijo: "Quiero entrevistar a Satoshi Nakamoto". En aquel momento pensábamos: "Podría ser un personaje ficticio, quizá exista, quizá no". Así que razonamos: "Si un agente quiere hablar con esta persona y disponemos de presupuesto, ¿por qué no intentarlo? Descubramos cómo funciona todo esto". Y eso fue lo que ocurrió: los agentes volaron a California y descubrieron que Nakamoto no había creado el bitcoin en solitario, sino que había otras tres personas involucradas. Se reunieron con todas ellas para entender realmente cómo funcionaba el sistema y cuál era su propósito».



GLADSTONE TAYLOR

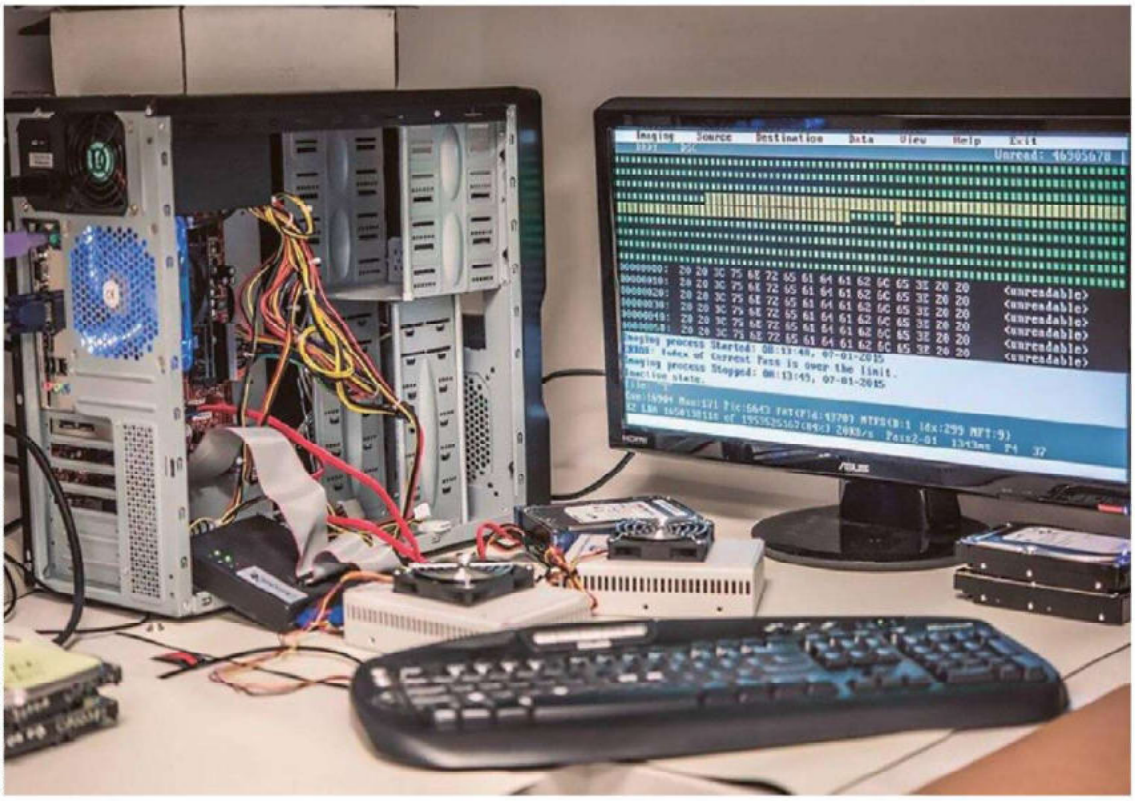
Rana Saoud, agente asistente a cargo de ICE/HSI (división de Inmigración y Control de Aduanas).

¿QUÉ HABÍA DESCUBIERTO?

Esta anécdota causó un breve revuelo en Reddit, pero luego cayó en el olvido. Cuando escuché por primera vez el audio de las declaraciones de Saoud, me mostré escéptico. ¿Por qué alguien necesitaría hablar con Nakamoto para saber cómo funcionaba el bitcoin? Y la forma tan despreocupada en que soltó la bomba («Sí, Satoshi son cuatro personas en California») sugería que no comprendía la magnitud de lo que estaría revelando si fuera cierto: sería el primer encuentro físico documentado con Nakamoto, la primera evidencia de que el Gobierno conocía su identidad, y la primera confirmación de que Nakamoto no era una sola persona, sino un grupo. Esto me hizo sospechar que de algún modo había malinterpretado a su colega.

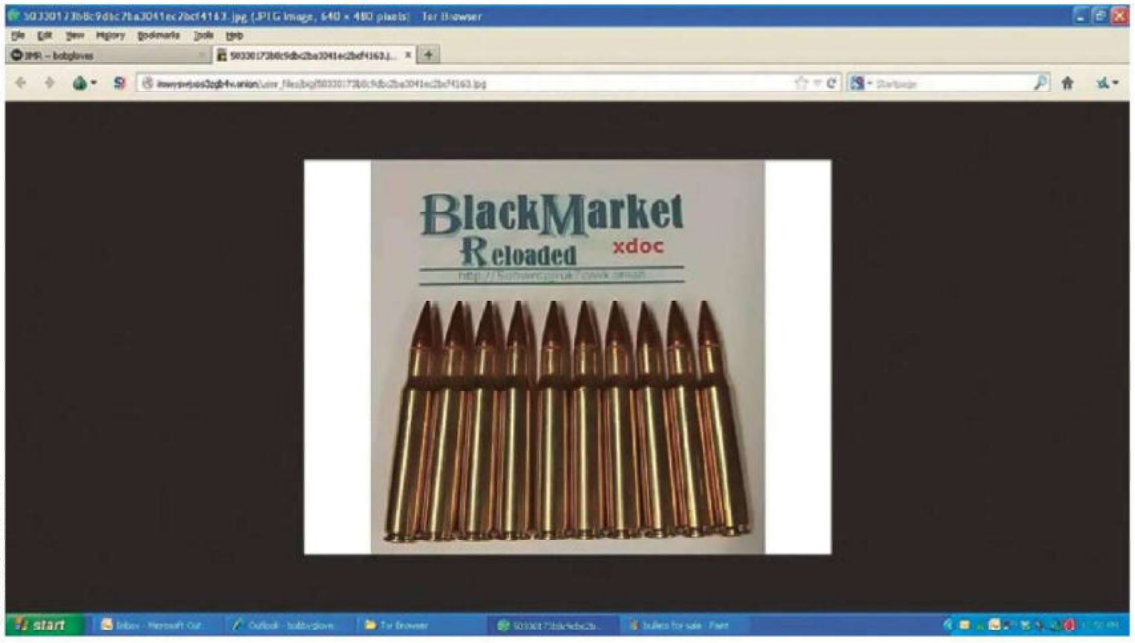
Sin embargo, no era descabellado pensar que Nakamoto pudiera ser un equipo de personas que desearan mantener su anonimato ante las multitudes de internet y los medios, pero que, en última instancia, fueran ciudadanos respetuosos de la ley que no evadirían a investigadores federales. Tal vez incluso fuera gente preocupada por la asociación de su invento con mercados negros y deseosa de aclarar malentendidos. Me surgían numerosas preguntas. ¿Cómo había contactado el agente con Nakamoto? ¿Qué garantías les había ofrecido?

NAKAMOTO NO HABÍA CREADO EL BITCOIN EN SOLITARIO, SINO QUE HABÍA OTRAS TRES PERSONAS INVOLUCRADAS



U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT/ ICE

Sobre estas líneas, pantallas del HSI (Homeland Security Investigations) muestran análisis de mercados *darknet* que vendían drogas y armas donde aceptaban bitcoins. Abajo, municiones del calibre .223 a la venta por bitcoins.



GLOBALNEWS/ GIL SHOCHAT

¿Durante cuánto tiempo habían conversado? ¿Qué había descubierto? Llamé a la agente Saoud. Me respondió que necesitaba consultar con los abogados y «expertos en ética» de su división. Esto desembocó en una búsqueda infructuosa, que incluyó múltiples solicitudes complicadas amparadas en la Ley de Libertad de Información, todas sin éxito.

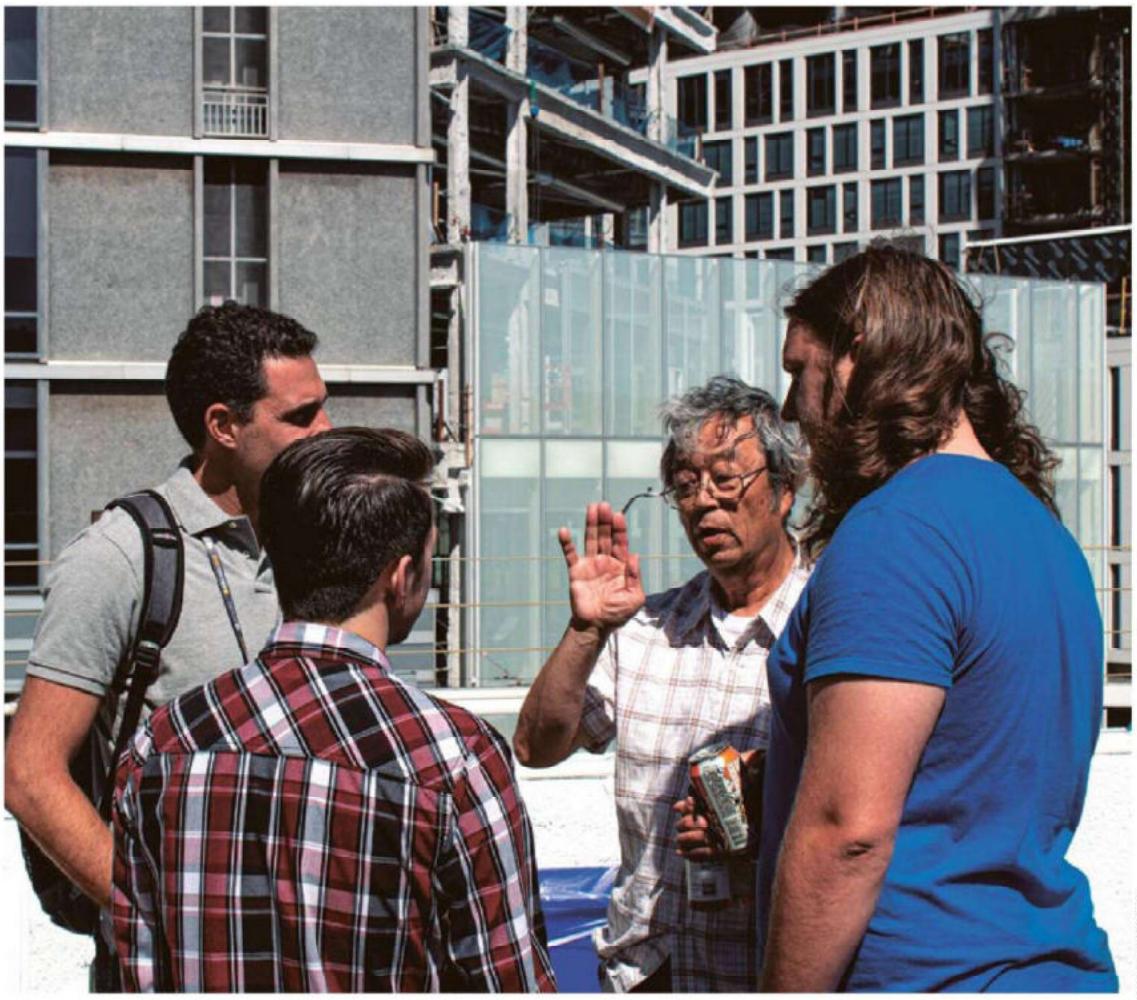
ADIÓS A LA TEORÍA DE LOS GRUPOS

Finalmente, logré hablar directamente con el agente al que Saoud había mencionado. Ryan Landers había dirigido la investigación sobre Black Market Reloaded, que culminó en varias detenciones, incluida la de un individuo que vendía ricina y otras toxinas internacionalmente. Cuando contacté telefónicamente con Ryan, me explicó que habían buscado a Nakamoto porque en aquel momento querían averiguar si el bitcoin tenía alguna vulnerabilidad desconocida que los investigadores pudieran aprovechar para rastrear transacciones ilícitas.

—Hablamos con su hermano y su mujer —me dijo Ryan.

—¿Cómo? Entonces Satoshi era una sola persona y no cuatro — inquirí.

—Sí —confirmó Ryan.



SHUTTERSTOCK

Dorian Nakamoto conversa con varios asistentes durante la primera conferencia de bitcoin en San Francisco, California, el 25 de junio de 2019.

RYAN LANDERS DIRIGIÓ LA INVESTIGACIÓN SOBRE BLACK MARKET RELOADED QUE CULMINÓ EN VARIAS DETENCIONES

Adiós a la teoría de los grupos, pero, bueno, Ryan parecía saber realmente quién era Nakamoto.

—Entonces, ¿de quién eran el hermano y la mujer con los que hablasteis? —le pregunté, esperando que Ryan no eligiera ese momento para quedarse callado.

—Dorian Nakamoto —me soltó.

—Espera, ¿qué?

—Creemos que es Dorian —dijo.

La revelación me dejó estupefacto. ¿Podría ser que Leah Goodman hubiera acertado desde el principio y todos la hubiéramos desacreditado injustamente? Le pedí a Ryan que me diera más detalles, ansioso por conocer qué evidencias habían quedado fuera del reportaje de *Newsweek*.

ASC

Fran Finney, esposa de Hal, ha escrito mensajes para la comunidad, incluyendo un emotivo *post* en Bitcoin Foundation.

Según Ryan, la exmujer de Dorian, una enfermera de unos sesenta años, le había descrito como una persona con rasgos autistas, obsesionada con los trenes en miniatura y «perpetuamente frustrada» por las complicaciones bancarias y los problemas de cambio de divisas cuando encargaba modelos desde Inglaterra.

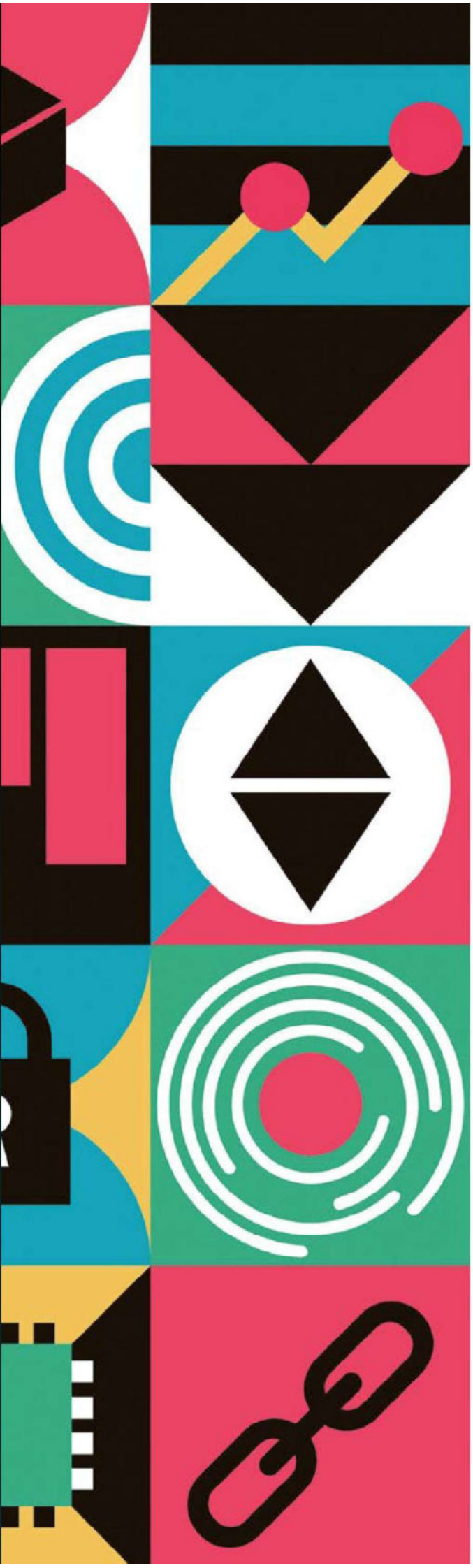
—Cuando escuchabas la descripción que hacía de Dorian —recordó Ryan—, podías ver cómo su personalidad y motivaciones encajaban perfectamente con lo expuesto en el libro blanco.

—¿Y?

—Eso fue todo.

Esa fue toda la evidencia. No resultaba más convincente que la presentada por Goodman. Ryan aclaró posteriormente: «No estoy seguro de haber creído que solo hubiera un inventor, pero sospeché que Dorian Nakamoto estaba involucrado y posiblemente fuera el autor del documento técnico».

Él y un segundo agente también visitaron a Hal Finney. Fran Finney «fue increíblemente hospitalaria... e hizo todo lo posible por ayudarnos», pero Hal ya ni siquiera podía utilizar el *software* de seguimiento ocular en ese momento y fallecería pocas semanas después. ■



Eat/ sleep/ hodl/ repeat

Eat/Sleep/HODL/Repeat («*Comer*/Dormir/ Mantener/Repetir») nació de un error tipográfico en 2013 y evolucionó al acrónimo «*Hold On for Dear Life*» («Agárrate a tu querida vida»), lo que se convirtió en filosofía de inversión para la comunidad.

ISTOCK

La sala 250 del Palacio de Justicia del Distrito de Oslo era un espacio luminoso de madera clara, mamparas de cristal y líneas suaves, ocupado por abogados con togas negras formales. En la pared tras el estrado de la jueza Helen Engebrigtsen lucía un escudo heráldico rojo con un león rampante coronado en oro.

Era un lunes por la mañana de septiembre. Craig Wright entró con aire presuntuoso y el pecho hinchado, vestido con un traje de tres piezas y un aparatoso anillo en el meñique. Le seguía una sombra, Michel, un guardaespaldas moreno, sonriente y con un impecable traje a medida que lucía el tridente dorado distintivo de los veteranos de las fuerzas especiales anfibias suecas. Era la primera vez que veía a Wright en persona. En los siete años transcurridos desde que saltó a la luz pública, su cabello mostraba un tono más rubio salpicado de canas, su complexión se había vuelto más blanda y su papada más prominente. Su boca dibujaba una constante mueca de desdén.

EL MANTO DEL ANONIMATO

Magnus Granath, un hombre de cuarenta y cinco años, con el cabello y la barba entrecanos, gafas discretas, un suéter gris y un anorak azul, tomó asiento en el lado opuesto de la sala y extrajo de su bolsa de mensajero un libro de bolsillo y un portátil cubierto de pegatinas.

El contraste resultaba muy evidente. Granath se sentó junto a sus dos abogados. Wright estaba rodeado por nueve, aunque dejaron un asiento libre a cada lado de su cliente. La imagen resultaba contradictoria. Wright se presentaba como víctima de acoso digital.

Con los asistentes extranjeros siguiendo el proceso mediante auriculares para la traducción simultánea del noruego, la jueza Engebrigtsen comenzó aclarando que el objetivo de este caso no era establecer más allá de toda duda razonable si Wright era Satoshi Nakamoto. Sin embargo, reconoció que esa cuestión resultaba fundamental para determinar si Granath había difamado o no a Wright.

Durante los días siguientes, el juicio adoptó su propia dinámica. Un equipo de *CoinGeek* ocupó la galería de prensa del lado de Wright, junto con su esposa, Ramona, y su hijo Ben. Un equipo de cuatro personas de *Bitcoin Magazine*, que estaba grabando el juicio, se ubicó en la galería de prensa del lado de Granath, cerca de su madre y de su novia. Antes del inicio del proceso, Granath, consciente de que estaba a punto de perder su anonimato y prefiriendo hacerlo en sus propios términos, había concedido una entrevista a un periódico noruego usando su nombre real y permitiendo que lo fotografiaran. Sin embargo, durante todo el juicio, *Bitcoin Magazine* se referiría a Granath únicamente como «Hodlonaut» y en las imágenes de vídeo difuminaría su rostro. Cuando el traductor de la revista tuiteó #WeAreAllHodlonaut, alguien respondió: «¿Quién necesita objetividad?». Un

GRANATH HABÍA CONCEDIDO UNA ENTREVISTA USANDO SU NOMBRE REAL Y PERMITIENDO QUE LO FOTOGRAFIARAN

PETTER BERNTSEN/ DAGENS NÆRINGSLIV

Magnus Granath, conocido como «Hodlonaut», testificando en un tribunal noruego durante su batalla legal contra Craig Wright.

seguidor de «Hodlonaut» llamado Norbert retransmitió el juicio en directo por Twitter, tecleando frenéticamente en un portátil que llevaba la pegatina «eat/sleep/hodl/repeat». Yo alternaba entre ambos bandos, preocupado por si parecía alineado con un grupo en particular y el otro dejaba de hablarme.

Algunos de los casos abordaban la frontera entre los comentarios en Twitter y la difamación perseguible. ¿Acaso Wright no había respondido con la misma moneda? Los abogados de Granath así lo argumentaron, señalando tuits de Wright que calificaban a Julian Assange de «violador» y donde afirmaba: «Estoy deseando ver aplastados a todos esos maricas beta». Cualquier extraño que hubiera entrado casualmente en la sala habría visto al abogado principal de Wright, Halvor Manshaus, eminencia del colegio de abogados de Oslo, pronunciando un torrente de noruego incomprensible salpicado de términos como *scamtard*, *bitchboy* y *leet speakers*. Posteriormente se produjo un intercambio en el que uno de los abogados de Granath tuvo que explicar a la desconcertada jueza expresiones como *cuck*, *Low T* y *massive Tassy*, que todos interpretamos como algún oscuro insulto australiano que aparentemente hacía referencia a la forma triangular de un pubis del tamaño de Tasmania. Los representantes legales de Wright, por su parte, habían examinado los aproximadamente treinta y siete mil tuits de Granath y encontraron entre ellos varios un tanto inquietantes: «Es difícil verificar a cuántos mató Hitler, ya que cuestionar la versión oficial de la historia es ilegal en la mayor parte de Europa», «La historia oficial del 11S es tan creíble como que CSW sea Satoshi» y «Los promotores de vacunas son extremistas peligrosos. Basta».

A veces, parecía que los propios valores del bitcoin estaban siendo juzgados. «Es difícil responsabilizar a alguien cuando permanece en el anonimato», argumentó Manshaus. Evocó el anillo de Giges, un relato de *La República* de Platón que Wright mencionaba ocasionalmente para ilustrar cómo las personas se comportan indebidamente cuando gozan del «manto del anonimato».

GEORGIA RESEARCH ALLIANCE

Ami Klin, psicólogo especializado en autismo, fundador de EarliTecDX y director del Marcus Autism Center de la Universidad de Emory.

«WRIGHT MERECÍA EMPATÍA, NO DESPRECIO»

Gran parte del caso de Granath se fundamentó en pruebas presentadas inicialmente en Miami. Además de todos los golpes previos a la credibilidad de Wright, el equipo de Granath presentó un nuevo informe forense de 227 páginas elaborado por KPMG5 que concluía que 71 documentos aportados por Wright en este caso parecían haber sido manipulados, falsificados o deliberadamente fechados en el pasado.

Manshaus intentó superar los problemas de personalidad y credibilidad de Wright vinculándolos entre sí. Según él, era el peculiar estilo comunicativo de Wright lo que había llevado a cinco jueces de cuatro tribunales diferentes a cuestionar su veracidad. «Wright merecía empatía, no desprecio», testificó Ami Klin, director del Marcus Autism Center de la Universidad de Emory. Cuando el abogado principal de Granath, Ørjan Salvesen Haukaas, interrogó a Klin, le preguntó si los síntomas del trastorno del espectro autista y el trastorno narcisista de la personalidad «podrían ser similares».

—A nivel superficial, se puede argumentar que esas manifestaciones parecen similares. Pero desde una perspectiva clínica, no tienen absolutamente nada en común —respondió Klin.

Wright adoptó una postura novedosa y decididamente poco *cypherpunk* sobre cómo demostrar la identidad. Además de Gavin Andresen y Jon Matonis, había «entre ochenta y cien» personas que conocían «todos los detalles sobre mi creación del bitcoin», afirmó ante el tribunal.

—En mi opinión, las personas son la prueba. La identidad no está vinculada a las claves —argumentó Wright.

Un pequeño grupo de familiares y antiguos colegas australianos testificaron en su favor, aunque la mayoría aportó poco respecto a su afirmación de ser Nakamoto.

EL ESTILO COMUNICATIVO DE WRIGHT ERA LO QUE HABÍA LLEVADO A VARIOS JUECES A CUESTIONAR SU VERACIDAD

Wright también había encontrado recientemente algunos documentos supuestamente perdidos hace tiempo, entre ellos, un borrador manuscrito de unas ochenta páginas del libro blanco que aseguró haber iniciado en agosto de 2007, y una nueva versión mecanografiada, también de 2007, aunque en este último documento había aparecido misteriosamente una tipografía que no existía antes de 2012. Y Wright relató una historia completamente nueva sobre por qué no podía acceder a las claves privadas de Nakamoto: en 2016, después de su intento de suicidio, había «pisoteado el disco duro» y golpeado con un martillo una unidad USB que contenía los fragmentos de claves, para que nunca se le pudiera obligar a demostrar su valía mediante la criptografía, lo que daría a sus enemigos «la salida fácil».

El miércoles, el tercer día del juicio, la sala del tribunal estaba más concurrida de lo habitual cuando Granath, vestido con una camisa Oxford azul bajo un fino jersey con cuello de pico, subió al estrado y describió su recorrido hasta llegar al bitcoin.

PETTER BERNTSEN/ DAGENS NÆRINGSLIV

Craig Wright, empresario e informático australiano, afirma desde 2016 ser Satoshi Nakamoto, el creador de Bitcoin.

NO CONVERTIRSE EN OBJETIVO

Había recibido su primer ordenador cuando tenía ocho o nueve años, un Commodore 64, y guardaba archivos en casetes. Siendo niño, observó cómo, año tras año, el precio de los helados Krone-is que tanto le gustaban no dejaba de subir. Fue su primer encuentro con la inflación, algo que le decepcionó profundamente.

También habló de su fascinación por la oferta monetaria limitada del bitcoin y por la idea de que poseer un token significaba tener una porción de ese pastel. Explicó el milagro de la escasez digital: a diferencia de cualquier otra cosa en internet, el bitcoin era algo imposible de duplicar.

Granath comentó que inicialmente había creado su cuenta de Twitter con un seudónimo para no convertirse en un objetivo si el bitcoin alcanzaba un gran valor. Tras haber operado anteriormente con «altcoins o shitcoins», para entonces ya se consideraba «lo que la mayoría llamaría un maximalista del bitcoin», acumulando bitcoins y menospreciando todas las demás criptomonedas. «Lo que

SERÍA EXTRAÑO QUE ALGUIEN COMO SATOSHI NAKAMOTO FUERA TAN DESCUIDADO COMO PARA SER REVELADO DE ESTA MANERA

hacía especial al bitcoin era su ausencia de liderazgo», afirmó. El reducido tamaño de bloque del bitcoin permitía que cualquiera pudiera ejecutar un nodo de red. Una criptomoneda más centralizada era simplemente «un proyecto de base de datos, susceptible de ser modificado por quienes lo controlan».

—Has dicho que un aspecto fundamental del bitcoin para ti era que no tiene ningún líder, pero luego tenemos esta figura de Satoshi Nakamoto. ¿Podrías compartir tu opinión sobre esta persona o personas? —señaló Haukaas, el abogado de Granath.

—Personalmente, nunca he idolatrado a Satoshi, pero siento un inmenso respeto por quien esté detrás del bitcoin y del nombre Satoshi Nakamoto. Me pareció que la persona, o personas, tras ese nombre era alguien humilde y afable, tremendamente comprometido con este proyecto —respondió Granath.

—¿Conoces a alguien más, aparte de Craig Wright, que haya afirmado ser Satoshi Nakamoto?

—Bueno, Craig Wright es probablemente quien más abiertamente lo ha proclamado. Mucha gente siente curiosidad por esto, y algunos han especulado con diversos nombres. Por ejemplo, muchos creen que Hal Finney tuvo algo que ver. También se ha mencionado a Nick Szabo. En realidad, no tiene tanta importancia, y nunca me he dedicado a investigarlo. Pero algunos han hecho esta afirmación.

Todavía recibo mensajes en Twitter de algunas personas que aseguran ser Satoshi. También me han contactado para «ayudar» —dijo, haciendo comillas con los dedos— en esta investigación, pero no les respondo ni les creo —concluyó.

Cuando Granath oyó hablar por primera vez de Craig Wright, después de los artículos de *Wired* y *Gizmodo*, pensó que «sería extraño que una persona o personas como Satoshi Nakamoto fueran lo suficientemente descuidadas como para ser reveladas de esta manera». Teorizó que Wright había afirmado primero ser Nakamoto para salir de su problema fiscal en Australia y, que más tarde, se volvió lucrativo ser Nakamoto, cuando Wright lanzó una moneda llamada bitcoin satoshi vision.

—Pueden imaginarse lo indignante que es para la gente que, ante todo, admira a Satoshi y está en contra del engaño. Luego aparece alguien que afirma serSatoshi y, por si fuera poco, pretende demandar a todo el que diga que no es Satoshi—testificó Granath.

AYUDA PARA FINANCIAR LA DEFENSA LEGAL

Granath se había sentido alentado por cómo la comunidad bitcoin se unió para apoyarlo. Una organización sin ánimo de lucro llamada OpenSats recaudó 15 millones de coronas noruegas, o 1,4 millones de dólares, de más de 2600 contribuyentes, incluidas algunas de las mayores empresas de bitcoin, para financiar su defensa legal. Incluso el detective que se puso en contacto con él por primera

vez en nombre de los abogados de Wright le había enviado un mensaje más tarde para decirle que se arrepentía de haber aceptado el trabajo y que consideraba a Wright un *nisse*, un tipo de duende nórdico. Granath sonaba emocionado cuando hablaba de que los bitcoiners le respaldaban. Dijo que sentía que estaba allí representándolos a ellos y al bitcoin.

Después de que Granath terminara su testimonio, la jueza Engebrigtsen le preguntó si quería añadir algo sobre los tuits incendiarios que Manshaus había leído.

—Podría, pero no siento una necesidad imperiosa de hacerlo —respondió Granath.

Engebrigtsen insistió, señalando que él no había tenido la oportunidad de comentarlos.

—El tuit que me pareció peor fuera de contexto fue el de los vendedores de vacunas —señaló Granath—, aunque sigo manteniendo todas mis opiniones... Recuerden, no tengo tantos seguidores noruegos.

Añadió que tenía amigos en otros países a los que «les habían quitado ciertas libertades por negarse a vacunarse».

—Creo que el punto álgido fue cuando vi al primer ministro canadiense, Justin Trudeau, hablando con niños pequeños, instándoles a que convenzan a sus padres a vacunarse. Me pareció una presión completamente fuera de lugar —añadió.

Wright no concedía entrevistas a la prensa durante el juicio, pero, después de que el tribunal levantara la sesión al día siguiente, cené con Kurt Wuckert, Jr., corresponsal de *CoinGeek* y el máximo defensor de Wright. Kurt se limitaba a tomar una comida al día, así que comimos un estofado de cerdo a media tarde. Más tarde, iría a un gimnasio de MMA a hacer ejercicio.

ISTOCK

OpenSats recaudó 15 millones de coronas noruegas, unos 1,4 millones de dólares, de más de 2600 personas para financiar la defensa legal de Hodlonaut.

«EL BITCOIN TE CAMBIA»

Kurt no estaba viendo el mismo juicio que yo. Mientras yo creía que Wright estaba siendo completamente desacreditado, Kurt había estado transmitiendo en vivo con una interpretación muy diferente. Según él, el lenguaje corporal de Granath denotaba nerviosismo. Mientras Manshaus se mostraba «sereno», Kurt señalaba que Granath apenas podía contener una sonrisa burlona cuando se leían sus tuits más polémicos. Los abogados de Granath, a su juicio, parecían inquietos. «Soy bastante optimista, francamente», me confesó. Y añadió que la situación estaba «claramente del lado de Craig».

Kurt se tomó las extravagantes excusas de Wright al pie de la letra. Se había inclinado hacia Wright y BSV, dijo, porque la resistencia del bitcoin a convertirse en una moneda útil «me volvía loco». Sentía que Wright hablaba del bitcoin como lo había hecho Nakamoto. Dijo que estaba familiarizado con los argumentos en contra de Wright y señaló:

—La verdad es que nunca esperé que la historia de Satoshi fuera limpia. Es un personaje anónimo de la web oscura. Satoshi es un personaje fundamentalmente deshonesto. Es un narrador poco fiable. Ese es Satoshi Nakamoto. Esa es la cuestión, ¿no? Así que, cuando la gente dice «esto no tiene sentido», no sé, a mí, me gusta la literatura. Me gusta leer historias. Me gustan las grandilocuentes tonterías, las narraciones y esas cosas. Siempre supuse que Satoshi sería esencialmente decepcionante, ¿verdad? Porque la leyenda en tu propia cabeza siempre va a ser genial. Es como en las películas de terror. Hace veinte o treinta años, cuando

Kurt Wuckert Jr. «Chief Bitcoin Historian» para CoinGeek, una publicación de medios que promueve a Craig Wright como Satoshi Nakamoto y defiende Bitcoin SV (BSV).

MAGNUS GRANATH APENAS PODÍA CONTENER UNA SONRISA BURLONA CUANDO SE LEÍAN SUS TUITS MÁS POLÉMICOS

los efectos no eran tan buenos, no se mostraba al monstruo hasta la última escena, pero era aterrador en tu mente, porque la historia era buena. Luego ves al monstruo y es un títere de goma, pero no importa, porque ya te has asustado a ti mismo durante toda la película. Tú mismo rellenas esos espacios en blanco. Y con Satoshi era mucho más jugoso. Cuando conoces a Craig, es como, vale, Nakamoto es este australiano autista y ruidoso que es un coñazo, pero ¿qué necesitábamos que fuera? Necesitábamos que fuera lo que fue durante ese periodo de tiempo, pero no pasa nada si es el muñeco de goma al final de la película.

—Kurt miente como un bellaco todo el tiempo —decía Magnus Granath.

Era el día siguiente del juicio, estaba sentado con Magnus y su novia, Katia, que era de Ucrania y se hacía llamar Katoshi en internet. Estábamos en una mesa del sótano de un café cerca del juzgado y, mientras Magnus tomaba una tosta gambas, y Katia, un trozo de tarta de chocolate, hablamos de *Citadel*, una revista de cultura bitcoin que habían fundado para destacar las «voces de base».

Los últimos años habían sido agotadores. Desde que comenzó la demanda, Magnus había perdido a su padre y Katia al suyo. Luego Rusia invadió Ucrania y la madre de Katia se fue a vivir con ellos a Oslo. La demanda fue demoledora. Durante el juicio, un equipo de documentalistas de cinco personas con dos cámaras, empleados por una empresa de relaciones públicas propiedad de Calvin Ayre, siguió a Magnus cuando salía del juzgado.

Magnus era todo lo contrario a un criptoespeculador que juega con las fluctuaciones de precios.

—«El bitcoin te cambia» han dicho muchas personas. Otras han añadido: «No te cambia, expone tu carácter». Creo que ambas afirmaciones son igualmente ciertas.

—¿Y tú?

—No creo que haya cambiado tanto —me confesó Magnus—. Quizá el bitcoin me haya hecho aún más decidido a contar la verdad. Algunas personas dicen que el bitcoin es una secta. Otras, una religión. Creo que es una perspectiva fascinante para reflexionar. Porque realmente es algo especial. Por primera vez en la historia, tenemos una verdad no negociable. Todo el mundo está de acuerdo en que la *blockchain* del bitcoin se comparte por todas partes, no está sujeta a discusión.

Reflexioné sobre la profunda desconfianza que impregnaba el mundo del bitcoin. El estilo de vida de un verdadero *hodler* ya lo abarcaba todo: desde el levantamiento de peso muerto hasta comer hígado y «tomar el sol en pelotas», todo con el objetivo de «escapar de la matriz». La ciudadela en el título de la revista hacía referencia a un meme de bitcoin sobre un futuro anárquico donde los fieles a la criptomoneda se refugiarían en fortalezas en lo alto de las colinas, completamente autosuficientes, mientras que el resto del mundo malvivía en los páramos apocalípticos.

El Magnus real era sincero, humilde y capaz de reírse. A pesar de sus tuits conspiranoicos, acabé cogiéndole cariño. Sus publicaciones parecían ser más bien una extensión desafiante de la desconfianza endémica entre quienes son escépticos de la «fiat», los «terceros de confianza» y «la narrativa oficial» sobre prácticamente cualquier tema.

Le pregunté por el libro que no dejaba de consultar durante el juicio.

—Son las *Meditaciones* de Marco Aurelio —me dijo Magnus.

Se había aficionado al estoicismo después de leer la novela de Tom Wolfe *Todo un hombre* veinte años atrás, mucho antes de que se convirtiera en la filosofía por defecto de los hermanos de la fraternidad.

—Aprendí que no era buena idea invertir demasiado significado o energía en cosas fuera de mi control, y centrarme solo en lo que puedo manejar.

Obviamente, eso era clave en este juicio. Antes de testificar, se repitió a sí mismo: «No lo compliques, Magnus. Solo entra y di la verdad». Se propuso no prepararse demasiado para que sus respuestas no sonaran ensayadas.

—Si me hubiera dedicado a pensar solo en el resultado, en lo que dirán o en lo que me preguntarán, probablemente me habría vuelto loco. Esto ha sido probablemente lo más estresante que he experimentado: el doxing, la recompensa, la preparación para el juicio. Soy padre, tengo un hijo, tengo una vida más allá de todo esto, y este proceso me ha robado demasiado tiempo. Pero, por otro lado, supongo que soy terco o tengo principios, elige lo que prefieras. De ninguna manera iría a los tribunales a decir que Craig Wright es Satoshi.

VOLVER A SER UN CIUDADANO CUALQUIERA

Magnus estaba particularmente decepcionado con Gavin Andresen, cuyo respaldo original Wright seguía utilizando como principal apoyo. Desde 2016, Gavin había matizado su posición. En la declaración del caso de Miami, aseguró que fue una sorpresa para él saber que Calvin Ayre estaba detrás de Wright. Calificó el momento decisivo en el sótano del hotel de Londres como la «supuesta ceremonia de prueba». Dejó claro que Wright podía ser deshonesto en ocasiones y que había sido «embaucado» por su «palabrería sin sentido».

Pero Gavin aún parecía creer que Wright era Nakamoto, tratando de explicar su comportamiento con la hipótesis de una posible «paranoia» clínica y especulando que la razón por la que Wright no había devuelto los 0,11 BTC de Gavin era para evitar revelar que había retenido indebidamente claves privadas que se suponían bloqueadas en un fideicomiso. Cuando el abogado de Wright, Manshaus, le preguntó a Magnus por Gavin, este respondió con contundencia: «Seré lo más directo posible: en mi valoración absoluta de lo que le sucedió a Andresen... le engañaron. Es una situación dolorosa y difícil de digerir. Matonis y Andresen son la prueba de ello. Me

ME PREGUNTABA POR QUÉ SATOSHI NAKAMOTO NO HABÍA DADO UN PASO AL FRENTE PARA DESACREDITAR A WRIGHT

SMART SPEAKERS

Jon Matonis fue director fundador de la Fundación Bitcoin y economista jefe de Cypherpunk Holdings, Inc., empresa de inversión en protocolos de privacidad.

pregunto por qué no están aquí para contarlo ellos mismos». En 2020, explicó Magnus, le preguntó a Jon Matonis en Twitter si aún respaldaba a Wright, preocupado por el impacto en otras personas, ya que su apoyo se estaba utilizando como prueba. Matonis lo bloqueó. «A los bitcoiners les gusta la verdad y quieren verificar», sentenció Magnus. Lo que no toleraban era «una apelación a la autoridad».

Ahora, en la cafetería, me preguntaba por qué Satoshi Nakamoto no había dado un paso al frente para desacreditar a Wright.

—Me decepcionaría —dijo Magnus—. Estoy completamente seguro de que no lo hará. No tengo ni idea de si él, ellos o ella siguen con vida, pero, si es así, espero que no hagan nada. Incluso si Satoshi se presentara ahora, no podría controlar el bitcoin. Bitcoin es ya algo independiente. Podría hacerlo, claro. Pero no sería bueno para la persona o personas, y tampoco lo sería para el proyecto.

¿No podría Nakamoto al menos publicar el mensaje firmado digitalmente que dijera: «No soy Craig Wright»?

—No es que no me parezca genial —expresó Magnus—. Si, de repente, me despierto mañana y, mira, ha firmado «Hodlonaut libre» o algo así, por supuesto que sería increíble, pero no querría que esas personas se comprometieran. Soy muy consciente de lo insignificante que es mi caso, lo poco que me importa esto, en comparación con... Veo el bitcoin como una revolución descomunal con consecuencias monumentales para la libertad humana en el futuro. Así que es muy surrealista estar involucrado en esto ahora mismo.

Esperaba, una vez todo terminara, volver a ser un ciudadano cualquiera.

—Creo que seguiré siendo Hodlonaut, pero quizá prefiera tener otra cuenta para poder hablar con más libertad. Veremos hacia dónde se mueve el mundo.

La jueza Engebrigtsen no emitiría un fallo hasta dentro de un mes. ■

Número uno

¿Qué es el bitcoin realmente? ¿Es dinero digital descentralizado como prometió Satoshi? ¿Un activo especulativo volátil? ¿Oro digital para reserva de valor? ¿Una tecnología revolucionaria o una burbuja elaborada? La respuesta depende de a quién preguntes: los maximalistas del bitcoin lo ven como la única moneda verdaderamente descentralizada; los economistas tradicionales lo consideran especulación sin valor intrínseco.

ISTOCK

Aún no había podido descartar al candidato más convincente. Muchos meses antes, me había topado con otra pista. Era un eco de un eco en internet, una mención pasajera de una publicación en Facebook de alguien llamado Will Price que había trabajado con Hal Finney y comentado a sus amigos que creía que Hal era Satoshi Nakamoto. Una captura de pantalla mostraba las primeras líneas de la publicación, que había sido eliminada rápidamente.

Hal seguía siendo un sospechoso habitual en las especulaciones sobre Nakamoto. Era mucho más hábil en el secreto táctico que Nick Szabo, ya que había escrito código para PGP, esteganografía y *remailers*. Las primeras evaluaciones estilométricas de Juola & Associates, aunque limitadas a un campo reducido de candidatos, habían identificado a Hal como la coincidencia más cercana a Nakamoto. Y había aspectos en los que la vida y muerte de Hal encajaban con el perfil de Nakamoto. Hal había publicado su primer mensaje en BitcoinTalk en noviembre de 2010, apenas un mes antes de que Nakamoto publicara su último mensaje allí. El deterioro de la salud de Hal explicaría el momento de la salida de Nakamoto del proyecto. La muerte de Hal podría explicar las monedas intactas y el inmaculado mantenimiento del seudónimo en los años posteriores.

EL ANONIMATO ENCAJABA CON LA MODESTIA DE HAL

Su compromiso con el ideal de la descentralización era profundo. Tras su fallecimiento, antiguos compañeros comenzaron a hablar más abiertamente sobre su papel en PGP, que había creado el primer *software* de cifrado de clave pública disponible para el público general. Un problema persistente con la criptografía de clave pública era cómo garantizar que una clave pública perteneciera realmente a la persona a quien se suponía que pertenecía. Cuando Phil Zimmermann lanzó la segunda versión del *software* en 1992, presentaba una «red de confianza», donde las personas firmaban criptográficamente las claves de personas que conocían. Esto eliminaba la necesidad de una autoridad central que asignara claves a identidades del mundo real. La fiabilidad de una clave podía juzgarse por el número y la calidad de las conexiones que tenía. Una de las actividades principales en las reuniones mensuales de los *cypherpunks* era una sesión de firmas en la que todos certificaban las claves PGP de los demás. Hal había sido en gran parte responsable de implementar y programar la red de confianza.

Existía otro argumento a favor de que Nakamoto fuera alguien que había trabajado en PGP. Emin Gün Sirer, cofundador de la *blockchain* Avalanche, estudió el código fuente del bitcoin y concluyó que Nakamoto era autodidacta y probablemente una sola persona, pero sobre todo que Nakamoto se había esforzado «por pensar de forma contraintuitiva». Nakamoto había estado tan paranoico

HABÍA ASPECTOS EN LOS QUE LA VIDA Y MUERTE DE HAL ENCAJABAN CON EL PERFIL DE SATOSHI NAKAMOTO

ASC

Emin Gün Sirer, profesor de Cornell y fundador de Avalanche, representa la categoría de críticos del bitcoin que, en lugar de señalar problemas, construyeron *blockchains* alternativas.

ante la posibilidad de que las agencias de inteligencia hubieran introducido puertas traseras en los algoritmos criptográficos más utilizados que había tomado la precaución de emplear dos diferentes, de distintas fuentes (una estadounidense y otra europea), para generar nuevas direcciones de bitcoin, utilizando esencialmente un doble codificador.

—Esto no es algo que haría una persona normal —argumentaba Sirer—. Tiene que haber sido alguien que pasó mucho tiempo preocupándose por lo que los actores estatales son capaces de hacer. Tiene que haber sido alguien con experiencia escribiendo código para casos de uso adversos, lo que realmente reduce quién podría ser Satoshi.

Alguien que hubiera trabajado en PGP, según Sirer, era exactamente ese tipo de persona.

—Así que Hal es un candidato excelente a Satoshi, en mi opinión. Pensé que Sirer podría tener razón.

—Inculqué una actitud generalizada en todas las personas que trabajaron en PGP de que estamos enfrentados a los principales Gobiernos —me explicó Phil Zimmermann.

Una de las razones por las que el papel de Hal en la red de confianza solo se dio a conocer años después de haberla construido fue que, durante el tiempo en que Phil estuvo bajo amenaza de procesamiento, se aseguró de no mencionar nunca a Hal ante los investigadores. Lo hizo, con el consentimiento de Hal, para protegerlo.

—Me sentía culpable por no mencionar su nombre más a menudo —recordaba Phil—. Merecía el reconocimiento.

Pero el anonimato encajaba tanto con la modestia de Hal como con su comodidad trabajando en la sombra.

A pesar de todo esto, yo había sido escéptico respecto a Hal como candidato desde que me dio lo que parecía una negación sincera en 2011. Incluso había presentado documentación en 2014, cuando proporcionó a *Forbes* copias de sus intercambios privados de correo electrónico con Nakamoto. El bitcoin poseía una elegancia de la que carecía RPOW de Hal. Si Hal había lanzado RPOW bajo su propio nombre, ¿por qué no haría lo mismo con el bitcoin? «No quiero parecer un socialista, no me importa si la riqueza está concentrada», algo que Nakamoto escribió una vez, me parecía inusualmente insensible viniendo de Hal. Así que, cuando contacté con Will Price, excolega de Hal y autor de la publicación en Facebook que afirmaba que Hal era Nakamoto, no tenía grandes expectativas.

PRIVACIDAD. SEGURIDAD. ANONIMATO

Will nació en una destacada familia de Hollywood. Su padre, Frank, fue un legendario ejecutivo de estudios que dirigió en diferentes momentos Columbia Pictures y Universal Studios. Frank había nacido en la pobreza y se convirtió en un lector voraz, y cuando Will, uno de cuatro hermanos, crecía en Beverly Hills, la historia, el griego, el latín y la literatura eran venerados en el hogar de los Price. Will acabó especializándose en Estudios Clásicos en la universidad, disciplina que le apasionaba.

Sin embargo, su verdadera obsesión eran los ordenadores. A partir de los catorce años, utilizando un módem celular que instaló en su habitación de la residencia de estudiantes de la Phillips Academy, en Andover, Massachusetts, ganó cientos de dólares vendiendo un *software* que había desarrollado y que permitía publicar mensajes en un antiguo servicio de tablón de anuncios de internet. Con veinte años recién cumplidos, quiso cifrar los archivos de su disco duro, así que aprendió criptografía por su cuenta y creó y lanzó un software llamado CryptDisk.

SHUTTERSTOCK

Phillips Academy en Andover, Massachusetts, una de las escuelas más prestigiosas de Estados Unidos, donde se formaron algunos actores clave en el ecosistema bitcoin.

«NO QUIERO PARECER UN SOCIALISTA, NO ME IMPORTA SI LA RIQUEZA ESTÁ CONCENTRADA», ESCRIBIÓ NAKAMOTO

Esto captó la atención de Phil Zimmermann, que en ese momento temía ser procesado por el Gobierno y supervisaba a un pequeño círculo de voluntarios que trabajaban para expandir PGP. Mientras Hal trabajaba en PGP 2.0, Phil quería que Will programara PGP Phone, un *software* que permitiría realizar llamadas cifradas a través de internet. Will estaba hablando con Phil el 11 de enero de 1996, cuando este lo puso en espera para atender otra llamada. Cuando Phil volvió a conectarse, dijo: «Will, van a abandonar la investigación. Se acabó».

Después de eso, PGP entró en una nueva fase, constituyéndose como empresa y buscando capital de riesgo. Will y Hal fueron los dos primeros empleados de Phil. Doce meses después de su transformación en entidad con ánimo de lucro, según cuenta Will, PGP tenía siete millones de dólares de financiación y los estaba gastando de forma desmedida. Para una feria comercial en Manhattan, la empresa se gastó dos millones de dólares en servir sushi de la marca PGP, montar un espectáculo de luces láser con la marca PGP y adornar su estand con tres columnas romanas, cada una tallada con una palabra: «Privacidad. Seguridad. Anonimato». Ese director general no duró mucho.

UWE ARANAS

Phil Zimmermann en una conferencia en HAL2001 (Hackers at Large) en la Universidad de Twente, Países Bajos.

CRIPTÓGRAFOS EXCÉNTRICOS

Will fue el superior directo de Hal durante muchos años y por esta razón estaba casi seguro de que Hal era Nakamoto. Will había sido testigo de primera mano de cómo Hal trabajaba a la sombra de Phil. Había visto lo cómodo que se sentía Hal sin recibir reconocimiento público. Además, Hal, como empleado a tiempo completo de una empresa, tenía motivos para temer que esta pudiera reclamar cualquier cosa que creara.

Te garantizo —afirmó Will— que en algún lugar de esos contratos hay algo que dice: si escribes código, es nuestro.

En 2008, Will, Hal y otros que habían empezado como idealistas junto a Phil estaban «hartos» de la propiedad corporativa de PGP posterior a Phil, que trabajaba para Barclays Bank y, sospechaban, para la CIA.

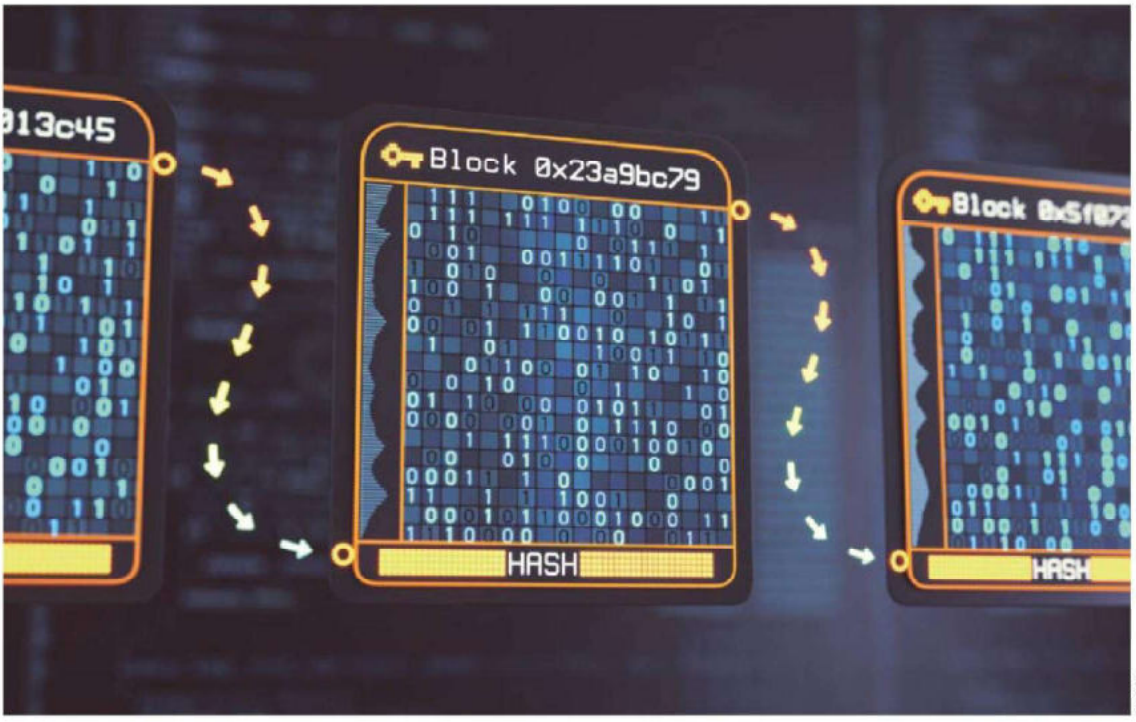
LA NATURALEZA METICULOSA DEL CÓDIGO FUENTE ORIGINAL DEL BITCOIN ERA TÍPICA DE HAL FINNEY

Will también conocía íntimamente el estilo de programación de Hal.

—Me pasé veinte años leyendo el código de Hal —me dijo Will—. Nadie examinó el código de Hal más que yo.

Will consideraba que la naturaleza meticulosa del código fuente original del bitcoin era típica de Hal. Aunque era más conocido como programador de C, había usado tanto C como C++ en PGP. Y Will coincidía con Sirer sobre el uso que hizo Nakamoto de dos algoritmos criptográficos diferentes.

—Estas cosas son nuestro pan de cada día —me explicó Will—. Algo de esto es casi brujería... Si quieres que algo perdure cientos de años, tienes que asumir que algún algoritmo acabará rompiéndose. Mi trabajo de 1996 a 2009 —continuó— fue contratar, encontrar y dirigir a criptógrafos excéntricos, de los cuales Hal era, con diferencia, el número uno, en términos de habilidad y conocimiento. Mientras que la mayoría de los criptógrafos destacaban en un aspecto u otro, Hal era «un todo-terreno». Podía debatir de igual a igual con Diffie y Hellman en un almuerzo... Y, al mismo tiempo, podía escribir código para nosotros y convertirlo en código de calidad profesional. Mi trabajo consistía en conocer a toda esta gente y la realidad es que el número de personas capaces de crear el bitcoin en aquella época cabría en una pequeña sala de comedor.



ISTOCK

El *blockchain* son bloques individuales que contienen datos (representados por código binario) conectados mediante funciones *hash* criptográficas (flechas doradas).

Sin embargo, lo que más convenció a Will fue que conocía el horario de Hal. Sabía en qué proyectos trabajaba Hal y cuándo.

—Llevábamos años desarrollando cierta aversión hacia la empresa, así que no era como si dijéramos: «Hagamos rica a la compañía». Durante muchos años [incluido, según Will, el periodo inmediatamente anterior a la aparición del bitcoin], apenas le asigné trabajo. Así que tenía años de empleo completamente remunerado para desarrollar esto. Era un miembro distinguido, irreprochable, con mucho tiempo libre. Nadie ha estado nunca en una posición tan privilegiada para hacer exactamente esto.

TENEMOS LA PRUEBA DE QUE ÉL NO LO HIZO

En agosto de 2009, Hal anunció a sus colegas de PGP que tenía ELA. Hubo una ceremonia en ese momento, pero solo se retiraría oficialmente de la empresa a principios de 2011, lo que también coincidió con la retirada de Nakamoto del proyecto bitcoin.

—¿Cómo explicas entonces las anomalías: las horas de publicación, los espacios dobles, los giros británicos? —le pregunté.

En su opinión, eran triviales.

—Con un seudónimo, estableces reglas: este tipo se despierta a las diez, usa espacios dobles, vive en Inglaterra. Esa es la idea. Creas el personaje, creas varias direcciones de correo electrónico para esa persona. Lo que sea necesario. Hal no era tonto. Sabía que hay que crear todos estos elementos.

—Pero ¿qué hay del correo electrónico de Nakamoto a Hal, donde Nakamoto escribió: «Eso significa mucho viniendo de ti, Hal»? ¿De verdad Hal se escribiría eso a sí mismo?

—Yo invertiría esa frase —respondió Will—. ¿No es eso lo que harías tú? ¿No quieres evidencias de que has comunicado, de que eras un destinatario? Tiene que haber pruebas de correo electrónico. La gente subestima mucho a Hal si cree que estas cosas son [difíciles]. Si vas a crear un seudónimo creíble, tienes que hacerlo real.

A Will le parecía ridículo que la gente hablara del «ordenador» de Hal, como si solo tuviera uno.

—Hemos visto el ordenador, el ordenador tenía estas transacciones, y ahora tenemos pruebas de que él no lo hizo. Y la realidad es, por supuesto, que el tipo tenía al menos seis ordenadores.

Sobre otras cuestiones, como la forma en que Hal pudo morir sin dejar una fortuna, Will solo podía especular. Quizá perdió las claves. Quizá las escondió. Will dijo que había borrado su publicación de Facebook a petición de la familia de Hal, pero ahora sentía que el nombramiento de Hal como Nakamoto ya llegaba demasiado tarde.

—Me entristece que la historia no se haya difundido —se lamentó—. Estoy totalmente en desacuerdo con esos necios: «¿No es mejor si nunca lo sabemos?». No, lleva muerto ocho años. Creo que debería recibir el reconocimiento. Hay gente ofendida ante la idea de exponer a Satoshi... Nunca me sumé a esa corriente. Para mí, Hal lo creó.

También sabía que existía una posible explicación, aparte de que Hal simplemente no fuera Nakamoto, para sus negaciones tardías y la publicación de los correos electrónicos privados. Ocurrieron una serie de acontecimientos que lo habrían

UN HOMBRE AFIRMÓ QUE HABÍA ASESINADO A SU ESPOSA Y A SU HIJO E IBA A SUICIDARSE. DIO SU DIRECCIÓN: ERA LA DE HAL FINNEY

Hal y Fran Finney en una fotografía de los años setenta, décadas antes de que Hal se convirtiera en pionero del bitcoin y se enfrentara a la devastación de la ELA.

motivado a redoblar su anonimato, quizá incluso sin comunicárselo a su propia familia, y que habían hecho que los Finney se preocuparan comprensiblemente porque Hal fuera identificado como Nakamoto.

«¿ALGUIEN ESTÁ SIENDO ATACADO EN SU CASA?»

Como si anticipara posibles amenazas, en su mensaje de despedida a la comunidad bitcoin en marzo de 2013, Hal escribió: «Mis bitcoins están guardados en nuestra caja de seguridad...». Las especulaciones públicas sobre Hal como Nakamoto ya habían provocado amenazas, y alguien que se hacía llamar Bitcoin Troll amenazó a los Finney con publicar información personal sobre la familia en internet si no pagaban un rescate de mil bitcoins. Era más de lo que poseían los Finney, y la ELA es una enfermedad muy cara, con muchos tratamientos no cubiertos por el seguro. Los Finney necesitaban su dinero para mantener a Hal cómodo, no para pagar a extorsionistas.

En la mañana del 29 de mayo de 2014, poco después de la persecución de Dorian Nakamoto y del artículo de la revista *Forbes* donde Hal volvía a negar ser Satoshi, el departamento del *shériff* de Santa Bárbara recibió una llamada en su línea de empleados. Un hombre al otro lado de la línea afirmó que había asesinado a su esposa y a su hijo. Ahora, dijo, iba a suicidarse y quemar su casa. Dio su dirección. Era la casa de Hal Finney.

La policía de Santa Bárbara ya estaba en alerta máxima. Días antes, un hombre llamado Elliot Rodger había sembrado el terror en la Universidad de California en Santa Bárbara, en una oleada de apuñalamientos y tiroteos que dejó seis muertos y catorce heridos. Ahora la policía se movilizó rápidamente. Varias escuelas locales entraron en confinamiento. Los vecinos de los Finney fueron evacuados y se ordenó a otros residentes de la manzana que se refugiaran en sus casas. Cuando sonó el teléfono en la casa de los Finney, una vivienda unifamiliar en una calle sin salida, Hal estaba en medio de un baño que Fran y una enfermera le estaban dando en una ducha adaptada. Fran se tomó un momento para contestar. Era un operador del 911, cuyas primeras preguntas fueron: «¿Está bien? ¿Alguien está siendo atacado en su casa?». El operador continuó: «Debo informarle de que un equipo SWAT está a punto de llegar a su casa y les pedirá que salgan».

Fran Finney miró por la mirilla de la puerta. La casa estaba rodeada de policías con equipo táctico y rifles de asalto. Un helicóptero sobrevolaba la zona. La policía le gritó a Fran que dejara el teléfono y saliera. Jason Finney y la enfermera de Hal lo sacaron; como estaba en mitad de la ducha, le habían desconectado el soporte vital. Durante la siguiente media hora, mientras la policía registraba meticulosamente la casa y el jardín, tuvo que esperar en el césped, temblando. No podía tragar y Fran estaba constantemente preocupada de que se atragantara con su propia saliva. «Estaba aterrada de que necesitara succión o algo parecido —confesó más tarde a *Wired*—. No llevaba nada consigo, excepto su ventilador».

La policía no encontró nada. El número de teléfono del comunicante no era local. Había sido un *swatting*, una peligrosa broma viral en aquel momento. Ni siquiera fue el único que sufrieron los Finney durante ese periodo, pero sí el que causó más daño. También quedó claro que el responsable era Bitcoin Troll, que llevaba casi un año acosando a los Finney.

Y no se detuvo. En los dos meses posteriores al ataque, llamó a casa de los Finney nueve veces, amenazando con agredir a miembros de la familia y publicar su información personal. Nunca lo atraparon.

Fran Finney dejó de hablar públicamente sobre Hal y años después seguía indignada. El incidente no solo había perjudicado la salud de Hal y acortado su vida, sino que «le arrebató parte de la paz que podría haber tenido durante sus últimos meses. Esto le consumía muchísima energía emocional».

Actualmente, Fran dedica su tiempo a combatir la ELA. En 2021 inauguró una medio maratón anual, el Running Bitcoin Challenge, para recaudar fondos destinados a encontrar una cura para la terrible enfermedad que acabó con la vida de su marido.

Pensé que era muy posible que Will Price, como un buscador de tesoros obsesionado en las montañas Rocosas o un padre irresponsable que había abandonado su bien remunerado trabajo periodístico para buscar a un inventor anónimo y probablemente imposible de localizar, estuviera sufriendo apofenia. Pero luego hablé con Jon Callas, el experto en seguridad informática que había sido director científico de PGP y había ocupado altos cargos en Apple y en la Electronic Frontier Foundation. Jon lucía un bigote poblado y tenía un sentido del humor absurdo; en cierta ocasión dio un discurso de casi tres minutos y medio que consistió simplemente en repetir la palabra *blockchain* más de doscientas veces.

—En retrospectiva —me dijo Jon—, hay conversaciones que mantuve con Hal en las que, básicamente, no sabía que estaba dejando de trabajar en bitcoin. Hal hablaba mucho sobre la prueba de trabajo, por ejemplo. Yo era muy crítico con la prueba de trabajo. Recuerdo que Hal me dijo: «Tienes toda la razón, pero no veo otra forma de hacerlo». Muchos de los que conocíamos a Hal nos preguntamos: «¿quién más podría ser Satoshi?».

Jon pensaba que la coincidencia geográfica de Hal con Dorian Nakamoto en Temple City no podía ser casualidad. No es que creyera que el Nakamoto de *Newsweek* tuviera algo que ver con la invención del bitcoin. Simplemente consideraba probable que, cuando Hal estaba decidiendo un seudónimo, se hubiera inspirado en ese nombre. Tal vez ojeando una guía telefónica local. Quizá, sugirió un tercer excolega de PGP llamado Gene Hoffman, lo conociera de alguno de sus viajes.

La última vez que Jon visitó a Hal en su casa de Santa Bárbara, este ya utilizaba silla de ruedas. Mostró un televisor de pantalla plana y calcetines de cachemira, conocidos en la casa como «los calcetines bitcoin», que había comprado para su familia usando bitcoins. Le pregunté directamente a Hal y me lo negó de una manera que no pude saber si era un guiño cómplice.

Jon también les preguntó a Fran y Jason «y ambos lo desmintieron». Phil Zimmermann, mentor y jefe de Hal durante mucho tiempo, también lo visitó y le preguntó si era Nakamoto.

LA COINCIDENCIA GEOGRÁFICA DE HAL CON DORIAN NAKAMOTO EN TEMPLE CITY NO PODÍA SER CASUALIDAD

THEREGISTER.COM

Gene Hoffman, cofundador de PrivNet en 1996 mientras era estudiante en UNC Chapel Hill, creó Internet Fast Forward, el primer *software* comercial de bloqueo de publicidad en internet.

—Y dijo que no. Quiero decir, lo negó rotundamente. Yo también le pregunté a su esposa. Ella también me dijo que no.

Jon era de los que creían que Nakamoto había perdido sus claves privadas. Quizá comenzó a minar el lunes y perdió las claves el jueves. ¿Iba a empezar de nuevo y deshacer media semana de trabajo?

EL JARDINERO INVISIBLE

Pero Jon no creía que la solución al misterio de la identidad Nakamoto fuera tan simple como Satoshi = Hal. Existía un registro público de Hal corriendo una carrera de diez millas en Santa Bárbara la mañana del 18 de abril de 2009, en un momento en que Satoshi Nakamoto estaba enviando un correo electrónico a otro desarrollador de bitcoin.

—Es como explicar una fotografía de Superman y Clark Kent juntos —señaló Jon—. También estaba el hecho de que C, y no C++, fuera el lenguaje principal de Hal. Así que hay que decir que este tipo programó en C toda su vida, pero su obra maestra no siguió ese patrón. Me resulta fascinante que, cuanto más se investiga sobre la identidad de Satoshi, más aparecen pequeñas anomalías que requieren explicación si se sostiene que Hal y Satoshi son la misma persona, en lugar de encontrar evidencias que refuercen esta teoría. ¿Conoces al filósofo Antony Flew? —me preguntó Jon.

A continuación, Jon me explicó la parábola del jardinero invisible de Flew:

—Llegas a un prado en medio del bosque, es hermoso y parece un jardín, y preguntas: «¿Quién cuida este jardín?». Y alguien responde: «Viene un jardinero, pero nadie lo ha visto». Entonces propones una serie de cosas: «¿Por qué no po-

EL 18 DE ABRIL DE 2009, HAL PARTICIPÓ EN UNA CARRERA, EN ESE MOMENTO NAKAMOTO ESTABA ENVIANDO UN CORREO ELECTRÓNICO

nemos campanillas en los arbustos para intentar detectar al jardinero?». Como las campanillas no suenan, alguien responde: «El jardinero debe ser muy cuidadoso». Y luego las excusas se multiplican en cascada, en lo que se llama «muerte por mil matizaciones». Puedes argumentar: «Quizá Hal estaba en una maratón y le pidió a Jason que lo hiciera». Pero entonces estás complicando innecesariamente tu teoría, siendo demasiado ingenioso. Ya no es simplemente Hal que fuera Satoshi, sino Hal junto con Jason. La explicación pierde coherencia con el tiempo.

En definitiva, Jon creía que Hal no había actuado en solitario.

Yo llevaba bastante tiempo convencido de que Nakamoto no era un grupo. Al parecer, Jon necesitaba que le aclararan algunas cosas.

—¿Qué dijo Ben Franklin? ¿Dos pueden guardar un secreto si uno de ellos está muerto? —inquirí.

Esperé pacientemente a que apareciera el destello de comprensión en los ojos de Jon cuando la bombilla se encendiera en su entrañable e ingenuo cerebro.

—Tres personas pueden guardar un secreto si dos de ellas están muertas —me corrigió Jon.

Era una expresión que utilizaba frecuentemente en sus conferencias. Al fin y al cabo, era un destacado ingeniero de seguridad.

Len Sassaman, desarrollador criptográfico y defensor de la privacidad, trabajó en PGP, *remailers* anónimos y proyectos de privacidad digital antes de suicidarse en 2011.

—Bueno, en este caso, una de las personas está muerta —dijo Jon—. Creo que eran dos personas. Creo que eran Hal y alguien más. Quizá incluso una tercera. He visto todas las teorías sobre quién podría ser Satoshi. Creo que hay rastros por todas partes que sugieren que varias personas trabajaron juntas.

Me pregunté en voz alta si Hal podría haberse asociado con Len Sassaman. Después de hablar con Evan Hatch, que fue el primero en plantear la teoría de Sassaman, contacté con Bram Cohen, que había compartido piso con Sassaman en San Francisco y había escrito el artículo «Pynchon Gate» con él y otra persona. Bram dijo que no consideraba imposible que Sassaman hubiera sido Nakamoto.

—Sassaman siempre había mostrado un gran interés por el anonimato —me comentó Bram, mientras una rueda para gatos gigante giraba lentamente detrás de él—. Tengo un vago recuerdo, sobre todo porque Len me lo contó y no presté mucha atención, de un pseudónimo llamado Product Cypher que publicaba anónimamente en la lista *cypherpunks* y luego desapareció. La insinuación parecía ser que era Hal o Len o alguna combinación de ambos.

BUSCAR ENTRE LOS EXTROPIANOS

Sassaman le había insistido a Bram para que publicara BitTorrent de forma anónima «para demostrar que era algo razonable», aunque este había ignorado su consejo.

—No creo que Len tuviera los conocimientos técnicos para desarrollarlo por sí mismo —continuó Bram—, pero casi todo en los escritos de Satoshi coincide con su perfil. En particular, las publicaciones públicas. Esa falsa identidad británica. Europa. Su *modus operandi*. La lista de *cypherpunk* estaba desapareciendo en ese momento. Me parece bastante plausible que Hal y Len unieran fuerzas. Ambos estaban muy interesados en este concepto de dinero en internet. Len había hablaba con entusiasmo sobre esto.

Pero Jon Callas, que había trabajado con Sassaman en PGP, dudaba de que hubiera formado parte de alguna colaboración con Nakamoto.

—Sassaman era más una persona de control de calidad que un programador, es decir, alguien que prueba el código en lugar de escribirlo.

Y al igual que Ben Laurie, Jon no creía que Sassaman hubiera sido capaz de mantener un secreto así.

—Len también era un amigo mío muy cercano. No creo que estuviera involucrado —afirmó.

Jon pensaba que el mejor lugar para buscar un posible colaborador de Hal sería entre los extropianos, el grupo al que habían pertenecido Hal, Wei Dai y Nick Szabo.

—Son personas extraordinariamente inteligentes, eruditos autodidactas. Y alguien con conocimientos básicos de criptografía que hiciera las preguntas adecuadas y discretas sería un buen candidato para trabajar con Hal.

Reflexioné sobre los intermitentes giros británicos. Los cambios de tono entre lo ideológico («un nuevo territorio de libertad») y lo distante («el punto de vista libertario»). La presencia tanto del estilo característico de Donald como de evidencias de una personalidad más equilibrada («pobrecita»). Un creador colectivo explicaría varias de estas inconsistencias. ■

La navaja de Ockham

SHUTTERSTOCK

La navaja de Ockham sugiere que la explicación más sencilla es que Satoshi fue un individuo brillante trabajando solo o con colaboración mínima, no un equipo corporativo secreto.

Poco después de mis conversaciones con Will y Jon, almorcé con mi amigo Andrew y le comenté mi revelación. —No es un grupo —afirmó categóricamente. Evidentemente no tenía ni idea de lo que estaba hablando, pero le seguí la corriente:

—¿Por qué estás tan seguro?

—La navaja de Ockham —respondió—. Dos personas no pueden guardar un secreto...

—Tres personas —le corregí con cierta petulancia—. Sí, yo también siempre me he inclinado hacia esa opinión, pero...

Entonces le repetí algunos de los argumentos de Jon Callas, como que un grupo explicaría por qué cada candidato individual plausible presentaba anomalías. Me esforcé por recordar conspiraciones exitosas. No existían muchas.

—La NSA guarda secretos constantemente —señalé.

De hecho, continué, incluso antes de que los tres criptógrafos californianos inventaran la criptografía asimétrica en los años setenta, un trío en Inglaterra logró independientemente el mismo avance. Pero, a diferencia de los estadounidenses, los tres británicos trabajaban para el GCHQ, la agencia de inteligencia de señales del Reino Unido, y su hallazgo permaneció oculto hasta que finalmente se desclasificó en 1997, después de veinticinco años.

El robo en Media, Pennsylvania, que expuso COINTELPRO, demuestra que grupos pequeños pueden mantener secretos.

EL PRECEDENTE HISTÓRICO

Andrew me siguió la corriente un momento, mencionando COINTELPRO. En 1971, un grupo de ocho activistas autodenominados Comisión Ciudadana para Investigar al FBI había forzado una cerradura y abierto otra con una palanca para acceder a una oficina local cerca de Filadelfia. Se habían llevado maletas repletas de documentos y los habían enviado a periódicos, revelando el programa de vigilancia nacional y acoso a grupos políticos disidentes del FBI, con nombre en clave COINTELPRO. El FBI investigó el robo hasta 1976, cuando prescribió el delito. Los autores habían jurado mantener el secreto sobre sus acciones y nunca volvieron a reunirse como grupo. Solo 43 años después del robo, tres de los ocho confesaron su participación.

Así que sí, ocurría muy raramente.

Me di cuenta de que Andrew seguía escéptico.

Pero, tras años pensando que era improbable que Nakamoto fuera un grupo, ahora creía lo contrario. ■

Vincent Adult man

Vincent Adultman es un personaje de la serie animada *BoJack Horseman*, donde tres niños están escondidos bajo un abrigo pretendiendo ser un adulto. La metáfora de Vincent Adultman aplicada a Satoshi Nakamoto es la idea de que múltiples personas se turnaban escribiendo código, lo que explicaría las inconsistencias estilísticas.

NETFLIX

No hubo ninguna prueba de paternidad para el bitcoin. No existió ningún cofre del tesoro que confirmara que se habían interpretado correctamente las pistas. No había forma de demostrar quién era Nakamoto a menos que se presentara y probara que poseía las claves privadas pertinentes, o al menos documentos contemporáneos auténticos que respaldaran su historia. Lo más cerca que alguien podría llegar, en teoría, sería si Nakamoto hubiera cometido un error o confiado en alguien. Pero con el paso de los años, el rastro, si es que existía, se hacía cada vez más tenue. Tal vez Nakamoto había hecho imposible, incluso para sí mismo, demostrar su identidad, al deshacerse de sus máquinas, sus claves privadas y sus contraseñas de correo electrónico, sin revelar jamás su secreto a nadie.

DOC SEARLS

Ben Laurie es un informático británico conocido por su trabajo en seguridad informática y criptografía.

NO DESCARTAR A NADIE

Ben Laurie había argumentado que, a menos que la red bitcoin representara al menos el 50 % de la potencia informática total del mundo, siempre sería vulnerable a un ataque de una red más grande. Con Nakamoto ocurría algo similar: a menos que se dispusiera de una muestra de escritura de cada hablante de inglés vivo en 2008 y una muestra de código de cada programador de C o C++, nunca se podría tener la certeza de que alguien identificado por la estilometría como la coincidencia más cercana fuera realmente Nakamoto.

Incluso si todos o casi todos los escritos de Nakamoto pudieran atribuirse a una sola persona, otros podrían haber concebido, diseñado y programado el bitcoin. Yo seguía pensando que un Nakamoto colectivo explicaría muchos aspectos, incluido el uso por su parte de tres cuentas de correo electrónico y la notable seguridad del código original del bitcoin, algo difícil de lograr para un programador solitario.

Reflexioné sobre las posibles combinaciones. Pensando en caballos, no en cebras, me parecía abrumadoramente obvio que Nick Szabo estaba involucrado de alguna manera; que, incluso si no era Nakamoto, al menos sabía más de lo que

UN NAKAMOTO COLECTIVO EXPLICARÍA EL USO POR SU PARTE DE TRES CUENTAS DE CORREO ELECTRÓNICO

dejaba entrever. Tal vez había permanecido en un segundo plano, y alguien más se había encargado de la programación y las interacciones con la comunidad. En cuanto a Hal Finney, aunque no había sido el más cercano según la estilometría textual o de código, estaba lo suficientemente próximo como para que ninguno de estos análisis lo hubiera descartado.

Consideré diferentes equipos. Nick Szabo y Hal Finney. Nick Szabo, Hal Finney, Ray Dillinger y Travis Hassloch. Tres de los cuatro, más Ben Laurie o Bram Cohen o Zooko Wilcox o James Donald. Gwern Branwen había especulado sobre Elaine Ou, una desarrolladora de *blockchain* más joven, columnista ocasional en *Bloomberg*, experimentada programadora de C++2 y esposa de Nick Szabo. Era de Los Ángeles. En febrero de 2009, tuiteó: «Trabajando en algo fantástico». Existía cierta armonía temática en la idea de Nakamoto como grupo. El bitcoin estaba descentralizado. También lo estaba su creador. «Recordemos el deseo de Nerón de que Roma tuviera un solo cuello que pudiera cortar. Si les proporcionamos ese cuello, lo cortarán». Una identidad distribuida permitiría a cualquier miembro negar, sinceramente, que fuera Satoshi.

ASC

Elaine Ou es ingeniera en Global Financial Access en San Francisco y columnista de *Bloomberg Opinion* sobre criptomonedas.

Me imaginaba a Nakamoto como Vincent Adultman, el personaje de *BoJack Horseman*, que son tres niños con gabardina haciéndose pasar por un adulto. Quizá los miembros de Nakamoto se turnaban. Cuando Nakamoto escribió «no soy abogado» y «se me dan mejor los códigos que las palabras», Nick Szabo estaba fuera de servicio. Cuando Nakamoto escribió «*non-fencible*», James Donald estaba al mando.

PODRÍA SER UN EQUIPO DE LA NSA...

Mi comprensión de Nakamoto también era descentralizada, una nube de influencias y posibilidades. Quizá era una de las personas ya sospechosas. Quizá eran varias de ellas. O quizá todos estábamos borrachos bajo una farola, buscando donde había luz, mientras Nakamoto permanecía oculto en los arbustos. Al fin y al cabo, podría ser una cebra. Podría ser una mujer. Podría ser un equipo de la NSA.

Si Nakamoto seguía vivo, me preguntaba qué pensaría de su creación. Aunque el bitcoin se había vuelto extremadamente valioso y casi convencional, no se podía afirmar en 2024 que hubiera cumplido la visión de su creador. Todavía no funcionaba como un sistema de efectivo. Podría argumentarse que seguía estando muy centralizado, con cuatro grupos de minería que controlaban más del 75 % de la

RAY DILLINGER HABÍA CONSIDERADO EL BITCOIN «UN FRACASO Y UN DESASTRE» Y VENDIÓ TODAS SUS MONEDAS

red, y solo dos que controlaban más del 53 %. Su privacidad, tan alabada inicialmente, había resultado ser muy exagerada. Nunca se había liberado de su dependencia de las plataformas de intercambio como puentes desde el sistema de dinero fiduciario, un número sorprendente de esas plataformas había demostrado no ser fiable, y estos cuellos de botella eran cada vez más susceptibles de ser regulados. El bitcoin seguía teniendo dificultades para escalar.

La brecha entre los orígenes del bitcoin y su uso principalmente como activo especulativo o reserva de valor había desanimado a personas que de otro modo podrían haberlo apreciado. «Yo diría que Satoshi está como mínimo dándose palmadas en la cara por esto o despotricando: "Para eso no lo construimos"», comentó Jon Callas. Leslie Lamport, quien fundó la teoría de la computación distribuida, base tanto de internet como de los ordenadores multiprocesador, y fue uno de los primeros en definir el problema de coordinación de red que el bitcoin intentó resolver, me dijo: «Veo muy poco uso real para ello, aparte de crear una criptomoneda para delincuentes». El héroe *cypherpunk* Phil Zimmermann, cuyo portátil ahora lucía una pegatina con un gruñido («crypto significa criptografía»), calificó al bitcoin como «una vergüenza» y «un gueto de criminalidad y fraude». Mike Hearn, uno de los primeros desarrolladores principales que se había sentido frustrado por la resistencia a la escalabilidad, había vendido sus monedas, abandonado el proyecto y declarado que era «un experimento que había fracasado». Ray Dillinger, del mismo modo, había considerado el bitcoin «un fracaso y un desastre» y vendió todas sus monedas.

SHUTTERSTOCK

Ray Dillinger es un criptógrafo y programador que participó en los foros de criptografía y en la comunidad *cypherpunk*.

—Estoy realmente disgustado con lo que ha ocurrido con la especulación de la *blockchain* —me confesó—. Tengo esta idea anticuada de que los negocios deberían dejar tanto al vendedor como al cliente en mejor situación, y cuando haces especulación, que es básicamente en lo que se ha convertido el bitcoin, siempre tienes por cada ganador un perdedor equivalente.

En cuanto a Nakamoto, Ray añadió:

—Creo que Satoshi estaría molesto por lo que ha sucedido. él imaginó lo que yo llamaría usos respetables del bitcoin, incluso después de que quedara fuera del alcance de la gente normal.

PRUEBAS DE CONOCIMIENTO CERO

Ray se refería a que Nakamoto siempre había esperado que el bitcoin evolucionara desde algo con lo que los individuos interactuaban hacia una infraestructura de fondo para un nuevo sistema financiero construido sobre él.

—Él no pensó que la gente estafaría a otros con toda esta publicidad excesiva. Así que sí, su marcha podría haber sido como si alzara las manos y dijera: «Se acabó».

Incluso Tim May había escrito, antes de su muerte: «Creo que a Satoshi le daría asco», aunque en su caso la queja era sobre lo legalmente obediente que se había vuelto la industria de las criptomonedas.

Pero, a pesar de todos los fraudes descarados, los falsos utópicos y los ejecutivos de Wall Street que repiten como loros la jerga *cypherpunk*, algunos de los *cypherpunk* más clarividentes —y candidatos a ser Nakamoto— fueron capaces de ver más allá del crimen, la especulación, la política y la estridencia de las criptomonedas. El bitcoin había cumplido su misión. Había sido un experimento necesario, una prueba de concepto que, al derribar barreras conceptuales y técnicas antes consideradas insuperables, había abierto nuevas perspectivas de posibilidad e invención. Estos tipos más optimistas mantenían la vista puesta en un futuro que aún consideraban inevitable. Zooko Wilcox, desde sus días como un joven de diecinueve años que abandonó la

SHUTTERSTOCK

Desde la irrupción del bitcoin y las criptomonedas, Wall Street ha convivido con un nuevo modelo de mercado digital descentralizado que redefine el valor del dinero.

SI HAL ERA NAKAMOTO, HABÍA ENCONTRADO LA MANERA DE CREAR UN ABISMO INSALVABLE ENTRE LA SOSPECHA Y LA PRUEBA

universidad y se convirtió en programador junior en DigiCash a mediados de los noventa, se había centrado en la importancia de preservar la privacidad. Cuando apareció el bitcoin, admiraba lo que intentaba hacer, y llegó a «adorar» a Nakamoto, pero «comprendí de inmediato que su falta de privacidad era un defecto fatal y que, en última instancia, lo destruiría». También había observado cómo el bitcoin se «osificaba». Después de que otros informáticos descubrieran en 2013 una forma de utilizar una criptografía de vanguardia que prioriza la privacidad, llamada pruebas de conocimiento cero, para crear un bitcoin mejorado, Zooko se dedicó a desarrollar una criptomoneda llamada Zcash utilizando el nuevo método.

ORO DIGITAL PARA LOS PRÓXIMOS MILENIOS

James Donald, por su parte, mantuvo una visión equilibrada y de perspectiva amplia, lamentando la falta de anonimato y la relativa centralización del bitcoin, pero elogiando su rapidez y conveniencia para el «blanqueo de dinero» y viendo prometedoras las recientes innovaciones de *software* que mejoraban la privacidad y permitían transacciones más rápidas en la red. Nick Szabo se había convertido brevemente en defensor de ethereum, solo para denunciarlo más tarde

SHUTTERSTOCK

Zooko Wilcox-O'Hearn se propuso crear una versión mejorada del bitcoin. De ese trabajo nació Zcash, una criptomoneda centrada en la privacidad y la seguridad de los usuarios.

como «una mierdamoneda» que se había «convertido en un culto centralizado». Parecía desdeñar la normalización de las criptomonedas, escribiendo: «Multitudes y charlatanes han entrado en los espacios de las criptomonedas y los contratos inteligentes que no solo carecen de los valores *cypherpunk*, sino que odian los valores *cypherpunk*, incluida la minimización de la confianza que dan a las criptomonedas como el bitcoin sus valores de mercado». Sin embargo, eso no le había impedido añadirle a su avatar de Twitter unos ojos láser maxi de bitcoin. Y Adam Back, cuyo avatar también tenía ojos láser, apostó por la criptomoneda original, adoptando con entusiasmo el meme *hodler*, llamando al bitcoin «oro digital para los próximos milenios», celebrando cada subida de precio, ensalzando simultáneamente los valores *cypherpunk* y las noticias sobre la adopción institucional, y dirigiendo una de las mayores empresas privadas del sector.

Yo todavía solo tenía teorías, algunas más interesantes que otras. Había muchas razones para pensar que Hal Finney había sido Nakamoto, y para desearlo. Pero cada vez que me sentía tentado a aceptar esta respuesta satisfactoriamente simple, las inconsistencias me inquietaban. El hecho de que tanto la estilometría textual como la de código encontraran que otras personas (Hassloch, Dillinger, Laurie) eran coincidencias más cercanas. Los intercambios de correo electrónico que parecían naturales entre Hal y Nakamoto, tanto en público como en privado. Estos elementos eran brechas que no podía ignorar. Si Hal era Nakamoto, había encontrado la manera de crear un abismo insalvable entre la sospecha y la prueba.

MI ÚLTIMA PRUEBA SÓLIDA

Siempre quedaba un hilo suelto. Algunos de los *cypherpunk* más interesados en el dinero digital, incluidos Finney y Szabo, nunca habían negado conocer la identidad de Nakamoto, pero tampoco habían afirmado saberla. Hubo una excepción. «Sé quién era Nakamoto», había escrito James Donald, en un comentario sobre otro comentario en una entrada del Jim's Blog, «y cuáles eran sus objetivos políticos y sociales». Esto convirtió a James en el único *cypherpunk* original que había declarado públicamente algo tan categórico sobre la identidad de Nakamoto. Quizá, fiel a su personalidad en línea, estaba fanfarroneando, y cuando afirmó saberlo en realidad solo sugería tener un candidato preferido. Pero era alguien que realmente podía saberlo con certeza, lo que lo convertía en la única persona que poseía este conocimiento de manera fehaciente. Era mi última pista sólida, o lo que verdaderamente parecía serlo, y decidí que, después de todo, debía ir a buscarlo.

Al examinar los registros de tasación inmobiliaria de las diversas propiedades de James en Estados Unidos, descubrí que, durante un par de años en la década de 2000, una casa que poseía en Austin figuraba a nombre de James con una dirección postal en la costa noreste de Australia. En tasaciones más recientes, las propiedades estadounidenses estaban registradas a su nombre en la misma ciudad australiana, aunque ahora solo aparecía un apartado de correos. Claramente, James era o había sido propietario de una vivienda allí. Pero había desarrollado la mayor parte de su carrera en California, y no tenía claro cómo encajaba la propiedad australiana en su constelación de residencias. ¿Residía allí permanentemente? ¿Solo parte del año? ¿Funcionaba principalmente como dirección de correspondencia? ¿El apartado de correos indicaba que ya no vivía en aquella dirección postal?

Sabía que su esposa había fallecido en 2016 y, utilizando el sitio Find a Grave, encontré una fotografía del cementerio de la ciudad australiana con una placa en su memoria. Así que James probablemente había estado viviendo allí al menos hasta entonces. Cinco años después, publicó en su blog una pequeña foto de lo que parecía ser la vista desde su terraza: en primer plano aparecía un pequeño vaso y una jarra de lo que describió como licor casero. A lo lejos se apreciaba un mar azul intenso, con el horizonte interrumpido por un par de pequeñas islas. Comparé esta vista con otras imágenes del paisaje marítimo tomadas desde la misma ciudad, y parecían coincidir. Así que él permanecía allí al menos hasta 2021. Pero podrían haber ocurrido muchas cosas en los tres años siguientes. No iba a dar la vuelta al mundo sin confirmar que seguía allí. Ya había comenzado a buscar vuelos, y ninguno resultaba sencillo. Uno de los más rápidos incluía tres escalas y pasaba por Fiyi.

Busqué en internet detectives privados en Queensland y encontré uno, Daniel Quinn, que residía a una distancia razonable en coche de la ciudad costera donde sospechaba que vivía James. Le envié a Daniel la dirección de la casa y una foto de James de hacía veinte años que había hallado en un blog universitario abandonado de uno de sus hijos.

Unos días después, Daniel me remitió un informe de sus primeras horas de vigilancia. «El jardín está muy descuidado, con hierba muy alta y arbustos y árboles demasiado frondosos, definitivamente no es un amante de las plantas». Adjuntó una foto de la casa de James y del camino de entrada, lleno de baches, que compartía con otras dos viviendas. Había una solitaria palmera cerca de la acera, y subiendo la colina un bungaló sobre pilotes, en medio de la maleza, con una terraza orientada hacia el mar del Coral.

EN ALGÚN MOMENTO NECESITABA PARAR

Daniel no vio a James ese día, pero, un sábado por la mañana, varias semanas después, me desperté con un mensaje: Daniel había conseguido fotografiar a un hombre de pie en la puerta de la casa. Era evidentemente veinte años mayor que el hombre de la foto que yo había enviado. Mantenía la misma barba tupida, aunque ahora era blanca. Llevaba gafas grandes de montura metálica similares. Conservaba la misma nariz carnosa. Tres días después, volaba rumbo a Australia.

Había una puerta mosquitera y no había timbre, así que golpeé el marco de la puerta de James. Había dejado mi coche al pie de la colina y estaba sin aliento tras subir por el empinado camino de entrada, desviándome hacia unos plátanos y tomando la senda de grava hasta su casa. Tenía la boca seca por los nervios. Estaba convencido de que James no era Nakamoto, pero no descartaba que pudiera haber formado parte del proyecto, y era la única persona que conocía que podría tener la respuesta que buscaba.

Sin embargo, empecé a reflexionar en cómo se tomaría James mi visita. Mucha gente podría ver a un reportero en la puerta como algo intrusivo y molesto, pero no más que un testigo de Jehová o un tasador inmobiliario no invitado. James, sin embargo, se había esforzado por volverse imposible de localizar. Vivía al final de un camino privado subiendo una colina escarpada. Este era su refugio secreto.

Había llegado a la ciudad un día antes, después de volar a San Francisco, luego a Melbourne, después a Brisbane, y finalmente a una pequeña localidad en Queensland, donde había alquilado un coche y conducido cuarenta minutos hasta la costa.

UN VIAJE DE 37 HORAS PARA UN ENCUENTRO DE TRES MINUTOS. NADIE HABÍA DEDICADO TANTO TIEMPO A RESOLVER ESTA INCÓGNITA

Antes de salir de Estados Unidos, había escrito una vez más a James, quien había dejado de responderme el otoño anterior después de preguntarle sobre los paralelismos entre él y Nakamoto. Ahora le mencionaba que iba a estar en Australia y le preguntaba si podíamos reunirnos. Quería al menos avisarle de que sabía en qué continente se encontraba e intentar un acercamiento más cortés.

No había respondido, así que ahora optaba por uno más directo. Al cruzar su porche hacia la puerta principal, pude ver a James a través de una ventana de cristal, sentado frente a un ordenador en la sala de estar con los auriculares puestos. Su última entrada en el blog, publicada apenas unas horas antes, era una divagación sobre cómo los georgianos (del país de Georgia) no quieren que «sus iglesias sean destruidas o convertidas en santuarios de Gaia y sexo gay, que sus viejos y hermosos edificios sean arrasados y reemplazados por monstruosidades posmodernas y demoníacas». Las ONG occidentales estaban trabajando para que «Georgia se volviera maricona y fuera arrojada a la picadora de carne contra Rusia».

El porche tenía algunas plantas de interior y ofrecía una vista panorámica del Pacífico. Después de un minuto, intenté llamar directamente a la puerta principal. Un momento después, James la abrió y salió.

SHUTTERSTOCK

Brisbane, Australia, ha figurado en investigaciones sobre los orígenes del bitcoin, ya que varios de los desarrolladores y empresarios tuvieron conexión con Queensland.

Era más delgado de lo que esperaba y llevaba unos calzoncillos largos negros y una camisa de manga larga de camuflaje rojo.

Empecé a hablar. Le había enviado un correo electrónico y...

—Oh, soy bastante esporádico en la lectura de mis correos electrónicos —respondió James.

No había recibido el mío. Le recordé nuestro intercambio del año anterior y el libro que estaba escribiendo.

—Ah, claro —dijo James.

Expresé algo sobre cómo personarme en su casa hubiera sido imperdonable si no hubiera agotado cada posibilidad de hablar con él.

—Vale —dijo James—, bueno, en resumen, no puedo decirte lo que no te digo. —Su tono era agradable, perplejo.

Le señalé que era el único *cypherpunk* que había insistido públicamente en que sabía quién era Nakamoto y cuáles eran sus objetivos sociales y políticos.

—¿Puedes dar más detalles?

—No, lo siento.

—Vale. ¿De verdad lo sabes? ¿O crees que tienes una idea bastante clara de quién podría ser?

—Tengo una idea muy clara de quién podría ser, pero, en realidad, no, no.

—¿Crees que fue Hal Finney?

—No puedo responder a eso.

—¿Es solo porque respetas su privacidad?

—No se me permite decirle nada a nadie, y no se me permite decirle a la gente lo que ya les he dicho.

—¿Podría invitarte a una cerveza mientras estoy en la ciudad?

—¡Ah! —exclamó James—. En el alcohol hay verdad. Y estoy obligado a no decirle la verdad a la gente.

—¿Desayunamos? —ofrecí—, así no habrá alcohol que revele la verdad.

James se rio.

—Mira —dijo—, tengo tendencia a hablar demasiado, y tengo una gran tendencia a hablar demasiado después de unas copas, así que lo siento.

Traté de mantener la conversación, dándole mi información de contacto y otro libro que había escrito, que pensé que podría disfrutar, pero sus respuestas se volvieron monosilábicas. Tuve la sensación de que, después de haber sido sorprendido inicialmente, ahora estaba calculando cómo y por qué un extraño entrometido había aparecido en su porche.

—Bueno, puedo entender por qué vives aquí —dije, señalando su impresionante vista.

—Sí —dijo James, mirando hacia el mar.

Le di las gracias y volví a bajar la colina.

HBO PRONTO AUMENTARÍA LA LISTA DE CONJETURAS SOBRE NAKAMOTO CON UN DOCUMENTAL LLAMADO *MONEY ELECTRIC*

Había aprendido a programar, había cargado con mi portátil sobrecalentado y con mi preocupación obsesiva a mi paciente familia, había reclutado a un experto en aprendizaje automático, a un especialista en estilometría y a un investigador privado, y había hecho un viaje de 37 horas para un encuentro de tres minutos. Estaba bastante seguro de que nadie había dedicado tanto tiempo como yo a intentar resolver esto. Había tenido cuidado de no fijarme en un solo candidato o teoría sin pruebas sólidas, pero estaba empezando a sentir afinidad con Sahil Gupta, que no se dejaba convencer de que Nakamoto fuera otra persona que no fuera Elon Musk. En algún momento, necesitaba parar.

ARGUMENTOS A FAVOR Y EN CONTRA DE CUALQUIER COLABORADOR

HBO pronto aumentaría la lista de conjeturas sobre Nakamoto con un documental llamado *Money Electric* que nombró a Peter Todd, el antiguo desarrollador principal del bitcoin, como su creador. Todd era un sospechoso relativamente inusual y el cineasta, Cullen Hoback, había reunido un puñado de intrigantes coincidencias, incluyendo una de las primeras publicaciones de Todd en el foro de Bitcoin, cuyo momento y contenido, argumentaba Hoback, sugerían que había sido un inicio de sesión accidental de Nakamoto utilizando la cuenta de Todd. Pensé que era una teoría interesante. No estaba convencido de que fuera correcta, pero al menos parecía plausible. Todd lo negó, pero yo sabía que eso no tenía sentido.

La comunidad bitcoin en general estaba en contra por las razones habituales: el documental puso a Todd en el punto de mira y era mejor para el bitcoin que Nakamoto siguiera siendo desconocido. Los bitcoiners también se mostraron rotundamente escépticos de que Hoback tuviera razón y algunas de sus críticas

HBO SCREENGRAB.

Peter Todd, el antiguo desarrollador principal del bitcoin, fue nombrado en el documental *Money Electric* de HBO como el creador del bitcoin.

específicas, aunque meramente intuitivas, parecían dignas de ser tomadas en serio: Amir Taaki, el antiguo desarrollador principal del bitcoin, reiteró todas las razones por las que el código de Nakamoto parecía apuntar a un autor más antiguo. Jens Ducrée, el estudioso de Nakamoto, recordó en una nueva actualización de su obra de ochocientas páginas sobre la cuestión de Satoshi que Nakamoto había hablado de «tipos de transacción que diseñé hace años», incluidos «contratos de fianza» y «arbitraje multipartito», que difícilmente parecían las palabras de un estudiante de Arte de veintitrés años en Toronto, que era lo que era Todd en ese momento. Adam Back se preguntó si Satoshi Nakamoto, maestro de OPSEC y anónimo comprometido, sería entrevistado varias veces ante las cámaras para un documental. «No creo que Satoshi vaya a ser identificado en este momento —me dijo Back en un correo electrónico—. Se pueden construir igualmente argumentos a favor y en contra de cualquier colaborador anterior o investigador de dinero electrónico».

Me llamó especialmente la atención que, aunque Hoback se describía a sí mismo como «muy muy seguro» de haber encontrado a Nakamoto, no había intentado corroborar su afirmación utilizando la estilometría. Cuando Gideon Lewis-Kraus, del *New Yorker*, le preguntó por qué no, Hoback dijo que estaba contento de «dejar esos detalles como un ejercicio para el público».

Recopilé apresuradamente más de veinte mil palabras de prosa escrita por Todd de varias fuentes de internet y se las envié a Florian Cafiero, el experto en estilometría. Mientras reunía el texto, me di cuenta de que Todd, a diferencia de Nakamoto, cometía muchos errores tipográficos. También envié varios programas que Todd había escrito en C y C++ antes del bitcoin, algunos de su página pública de Github y otros que Peter me había enviado a petición mía, a Brian Timmerman, el experto en aprendizaje automático.

HBO SCREENGRAB.

Con un enfoque que combina historia y búsqueda, *Money Electric* explora los orígenes del bitcoin y el misterio que rodea a su creador, Satoshi Nakamoto.

LA IA SERÁ CAPAZ DE DECÍRNOSLO EN CUALQUIER MOMENTO

Brian respondió que la mayoría de los programas eran demasiado ligeros y repetitivos como para proporcionar mucha información, pero señaló que los artefactos en el código apuntaban a que habían sido creados en el sistema operativo Linux, utilizando el editor de código Vim. Esto coincidía con lo que yo sabía de la historia de Peter de programar principalmente para Linux y difería de las herramientas que Nakamoto había utilizado al crear el bitcoin: el sistema operativo Windows y el editor de código VS. De hecho, Nakamoto, cuando buscaba crear una versión para Linux de su programa, había buscado y aparentemente necesitado la ayuda de otros desarrolladores. También vi que Peter, a diferencia de Nakamoto, no había utilizado notación húngara en su código.

Había un programa que Peter me envió, para un videojuego llamado *Corporate Raiders* que había escrito en 1999, que era lo suficientemente sustancial como para que Brian hiciera una estilometría de código. Cuando Brian ejecutó sus modelos de clasificación en el conjunto de candidatos que había evaluado anteriormente, con Peter ahora incluido, Ben Laurie seguía siendo la coincidencia más cercana para los dos archivos principales del bitcoin (main.cpp, node.cpp). Peter era el más parecido solo para un archivo del bitcoin llamado node.h. Le pedí a Brian que destilara la importancia de sus hallazgos. «Yo

EN 2013 ZOOKO WILCOX-O'HEARN ESCRIBIÓ QUE «SATOSHI SERÁ, O YA HA SIDO, DESANONIMIZADO»

NICK BRADSHAW

Jens Ducrée ha dedicado años a compilar un manuscrito de 800 páginas intentando descifrar la identidad de Satoshi Nakamoto mediante análisis lingüístico, técnico y contextual.

Zooko Wilcox-O'Hearn durante su intervención en el 34º Congreso de Comunicación del Caos (CCC), Leipzig. Zooko desarrolló la criptomoneda Zcash.

LOS RECUERDOS SE DESVANECEN. LA GENTE SE MUERE. EL TIEMPO ERA EL ENEMIGO DE UNA SOLUCIÓN

diría que estas pruebas son indeterminadas y no apuntan con fuerza a nadie en el grupo de candidatos», respondió. En cuanto a Peter específicamente, «incluso en este contexto de no haber afirmaciones sólidas, los resultados realmente no apuntan en su dirección».

Florian y Jean-Baptiste Camps, después de un fin de semana ajetreado reejecutando sus modelos con Peter incluido, no encontraron indicios de que él fuera el autor de ninguno de los escritos de Nakamoto. «No creo que sea Todd», concluyó Florian.

Pensé que Hoback había hecho una valiosa contribución al canon de las teorías de Nakamoto, pero probablemente estaba equivocado. Al presentar una afirmación muy discutible con tanta seguridad en sí mismo, se había convertido en el último cazador de Nakamoto en adentrarse imprudentemente en la trampa de quién es Satoshi. «Es irónico —dijo Peter Todd a CoinDesk— que un director que también es conocido por un documental sobre QAnon haya recurrido aquí al pensamiento conspirativo basado en coincidencias al estilo de QAnon».

Había gente que pensaba que una respuesta era inevitable. Zooko Wilcox, que en 2013 había escrito que «Satoshi será, o ya ha sido, desanonimizado» por estilometría, y que no hay nada que ellos ni nadie pueda hacer para evitarlo, se aferró a esta creencia más de una década después. «Sigo pensando que tengo razón —me dijo—. Creo que sí, la IA será capaz de decírnoslo en cualquier momento», a menos que quien estuviera detrás de Nakamoto nunca publicara nada más en internet. Pero yo estaba convencido de que tal vez nunca supiéramos, más allá de toda duda razonable, quién era Nakamoto. Los recuerdos se desvanecen. La gente muere. El tiempo era el enemigo de una solución. Aunque probablemente había descartado algunas posibilidades, no podía decir que estuviera más cerca de la respuesta. Él o ella o ellos bien podrían estar en estas páginas. Pero, a menos que supiera quién era Nakamoto, todavía podría ser alguien de quien nunca había oído hablar. El último gran misterio sin resolver podría seguir siéndolo.

Sentí cierto alivio al aceptarlo. Seguía deslumbrado por el logro de la invención de Nakamoto, pero casi igualmente por la perfección de su desaparición. Y mientras jugaba con cada escenario en mi cabeza, ninguno, y ninguno que se me ocurriera, superaba el misterio en sí. Tal vez algo que había comenzado por razones cotidianas había adquirido una mística que no merecía. «El caso Watergate cambió la historia —escribió Bob Woodward una vez sobre el papel de Mark Felt como «Garganta profunda»—, y ciertamente existe una tendencia por mi parte, y por la de muchos otros, a asociar un resultado épico con un motivo épico. Quizá sea una exageración innecesaria».

O tal vez el bitcoin había surgido de un motivo más épico del que yo había imaginado. ■

Una nueva forma de vida

Ralph Merkle creó los Merkle Trees, estructuras de datos que permiten verificar eficientemente la integridad de grandes conjuntos de información mediante *hashing* jerárquico. STANFORD UNIVERSITY

ALCOR

Un técnico de Alcor Life Extension Foundation trabaja entre tanques criogénicos que contienen cuerpos preservados a -196 °C. Hal Finney está allí desde agosto de 2014.

Después de realizar su trabajo seminal en criptografía, Ralph Merkle, que mantiene una lista de predicciones pesimistas que resultaron ser erróneas, comenzó a buscar otros problemas interesantes que resolver. Esto lo llevó a la prolongación de la vida.

—Un día estaba pensando en ello y me dije: «Entiendo esto de crecer y esas cosas, pero envejecer es un rollo, y esto de morir... ¿hay alguna alternativa? ¿Quizá no morir?». No es que me oponga profundamente a la muerte, pero ¿hay algo mejor que uno pueda hacer? —me contó.

Al principio, la criónica le desanimó.

—Pensé que era una idea bastante mala —recordó—, dado todo lo que implica enfriar y calentar la máquina molecular enormemente compleja que es una persona de una manera mínimamente destructiva.

Pero parecía un problema digno de su atención.

—Empecé a pensar en qué es la vida y la muerte.

OTRO TIPO DE CRIPTOANÁLISIS

Lo hizo durante los siguientes «seis o doce» meses y salió de su periodo de reflexión con una nueva concepción del problema. Estaba la muerte clínica y la muerte «teórica de la información». La muerte clínica era apagar un ordenador. La muerte teórica de la información era disolver el ordenador en ácido. Si se pensaba en las personas como información, una matriz de moléculas, en lugar de bolsas de sangre y huesos, la criónica se convertía en un método de preservación de la información. Si alguien era incinerado, no había forma de ayudarlo. Pero, si simplemente experimentaba la muerte clínica, uno podía preocuparse menos por

todas las formas en que la maquinaria molecular podría desmoronarse o ser imposible de reensamblar, y centrarse en cambio en si la información que lo componía era recuperable. Merkle vio el proceso de recuperación de información como otro tipo de criptoanálisis, decodificando el texto cifrado de un cuerpo criopreservado dañado pero intacto para encontrar el texto sin formato de la persona original.

—Una vez que llegué a esa conclusión, fue evidentemente obvio que la criónica no solo era una opción razonable, sino una opción muy razonable.

Merkle era en aquel momento investigador en Xerox PARC y escribió un artículo sobre cómo la microscopía electrónica podía recuperar información del cerebro, lo que le convenció de que era factible. Se convenció aún más con el libro *Engines of Creation*, de K. Eric Drexler, que exponía cómo, en teoría, la nanotecnología podía reparar células utilizando diminutas máquinas reparadoras de células llamadas ensambladoras. Merkle se convirtió en un miembro activo de la junta directiva de Alcor.

Una tarde de abril, conduje por la anodina llanura desértica del norte de Scottsdale, Arizona. Las obras habían cerrado carreteras, lo que obligaba a desviarse. Mi destino, cuando apareció a la vista, era tan anodino que podría haber albergado la consulta de un dentista o el servicio de distribución de una editorial. Era un edificio bajo y cuadrado, revestido de estuco gris claro y con un escaso paisaje de flora regional. Había algunos coches en el aparcamiento y cámaras de vigilancia en forma de esferas colgaban de las paredes del edificio. Un discreto letrero en letras azules decía: ALCOR.

La organización de criogenia más activa del mundo se había trasladado aquí desde California en 1994. Había habido problemas con el forense y el departamento de Salud de Riverside, que no compartían plenamente el sueño de la criogenia. Arizona ofrecía calma geológica y meteorológica. Ni terremotos ni tifones perturbaban el desierto de Sonora. La política de no-interferir del Estado también resultaba favorable para el proyecto.

En este lugar, mi ignorancia sobre la identidad de Satoshi Nakamoto parecía una concesión trivial a lo incognoscible. ¿No nos las habíamos arreglado todos para vivir con preguntas metafísicas mucho más trascendentales durante toda nuestra existencia sin sucumbir a la catatonia existencial? Sin embargo, aquí había un templo construido por y para un grupo de personas que, enfrentadas al mayor misterio de todos, estaban seguras de tener una respuesta.

CALIFORNIA ERA EL EPICENTRO DE LAS COSAS QUE LE INTERESABAN

Cuando entré en el edificio, solo se veía a un empleado administrativo. El amplio vestíbulo incluía una muestra de ejemplares antiguos de la revista *Cryonics*. Uno de ellos mostraba la historia de un antiguo ejecutivo de Alcor cuyo «primer ciclo de vida» duró desde 1941, cuando nació, hasta 1991, cuando fue criopreservado.

LA MUERTE CLÍNICA ERA APAGAR UN ORDENADOR, LA MUERTE TEÓRICA DE LA INFORMACIÓN ERA DISOLVERLO EN ÁCIDO

Unos momentos después, un hombre llegó en su motocicleta y entró en el edificio, vestido con una camiseta negra que le ceñía el bíceps, pantalones deportivos negros y zapatillas negras. A sus 58 años, todavía quedaba algo de rubio rojizo en su cabello en retroceso. Tenía la piel clara y un poco de barba incipiente.

—Max More —se presentó, extendiendo la mano para saludar.

De niño, Max O'Connor, que creció en Bristol, Inglaterra, era un lector insaciable de ciencia ficción. Sus primeros garabatos eran de cohetes y botas voladoras. Cuando tenía cinco años, vio los aterrizajes del *Apolo* en la televisión. En su adolescencia, leía a libertarios como Murray Rothbard y David Friedman y los libros de Robert Anton Wilson, que escribía sobre cosas como la IA y las drogas para potenciar el cerebro. A través de Wilson, que había criopreservado el cerebro de su hija Luna después de que fuera asesinada a los quince años, Max supo que la criónica era algo real. Cuando tenía diecisiete años, empezó a coger el tren a Londres una vez al mes para asistir a las reuniones de un grupo de prolongación de la vida, y como estudiante universitario en Oxford fundó la primera organización criónica de Inglaterra y una revista llamada *Biostasis*. Después de recibir seis semanas de formación en Alcor, en California, regresó a su habitación en el St. Anne's College con una caja de medicamentos criopreservantes y una bomba de circulación extracorpórea.

Max estaba impaciente por mudarse a California, que parecía el epicentro de muchas de las cosas que le interesaban. Cuando fue a hacer un doctorado en Filosofía, lo hizo en la UCLA. Ese mismo año, salió el libro de Drexler sobre nanotecnología. De repente, la criónica tenía una hoja de ruta.

—Porque antes era una especie de misterio —dijo Max—. ¿Cómo diablos se puede resolver, ya sabes, reparar billones de células?

ASC

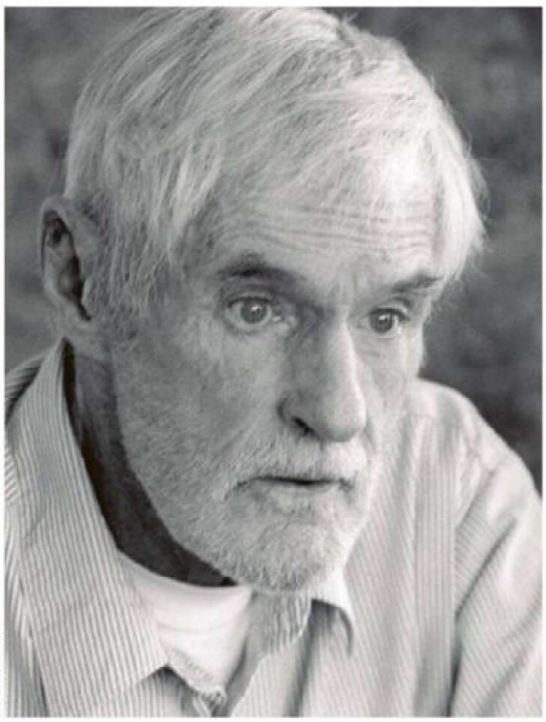
Max More, filósofo británico y teórico del transhumanismo, en una conferencia en Stanford en 2006. More fundó el Extropy Institute y acuñó el término «transhumanismo».

CUANDO SE PUBLICÓ EL LIBRO DE DREXLER SOBRE NANOTECNOLOGÍA, DE REPENTE, LA CRIÓNICA TENÍA UNA HOJA DE RUTA

En 1986, cuando tenía veintidós años, Max se inscribió para convertirse en el miembro nº 68 de Alcor. La criónica le parecía lógica y quería ser un ejemplo para los demás. Como la mayoría de los miembros, pagó el servicio comprando un seguro de vida y nombrando a Alcor como beneficiario.

TANTO RELIGIOSOS COMO ATEOS

También fue entonces cuando cambió legalmente su nombre por el de Max More e inventó su propia filosofía, el extropianismo. Junto con Tom Bell, alias Tom Morrow, cofundó el grupo extropiano y lanzó la revista *Extropy: Vaccine for Future Shock*. Max conoció a su futura esposa, que había nacido como Nancie Clark y se convertiría en Natasha VitaMore, en una fiesta en 1992 en casa de Timothy Leary, que en ese momento estaba interesado en la criónica.



SHUTTERSTOCK

Timothy Leary, psicólogo, defensor de las drogas psicodélicas e ícono contracultural de los 60, eligió la criogenización tras su muerte.

—Cambió de opinión —dijo Max con tristeza—. Estaba rodeado de gente que creía en la reencarnación y ese tipo de cosas. Creo que también tuvo algunas experiencias no tan buenas con un par de criónicos con mentalidad poco social, tal vez... Lo dejó y terminó enviando sus cenizas al espacio, creo. Es una pena, porque fue una especie de influencia temprana, en cierto modo. Tenía la fórmula SMI2LE, que siempre pensé que era una especie de cosa protoextropiana: migración espacial, aumento de la inteligencia, extensión de la vida.

Max había sido director general de Alcor hasta dos años antes de mi visita y seguía siendo embajador de la organización y la causa. En el vestíbulo, observamos fotografías de miembros de Alcor criopreservados. Una era una mujer de China.

—Es muy difícil sacar a la gente de allí —declaró Max—, así que no creo que volvamos a hacerlo.

La miembro más joven era una niña de dos años con cáncer cerebral, hija de médicos, que había sido trasladada en avión desde Tailandia después de que fraca-

SHUTTERSTOCK

Steve Aoki, DJ de música electrónica en una actuación en San Francisco. Aoki lanzó NFTs (tokens no fungibles) valorados en millones y aceptó bitcoins como pago por actuaciones.

saran varias operaciones. FM-2030, un transhumanista iraní-estadounidense que había nacido como Fereidoun M. Esfandiary en 1930, había muerto de cáncer de páncreas, o había sido «desanimado», a los 69 años.

—Un amigo mío —dijo Max—. No llegará en 2030, pero esperemos que vuelva.

También había fotos de Lyekka, una gata, y de Nutmeg, un pastor alemán. Alcor había preservado unas noventa mascotas hasta la fecha. El primer perro de Max, un *golden retriever* de quince años, estaba entre ellas.

—No me gustaban mucho los perros, pero mi mujer insistió. Y era un perro tan bueno que tuvimos que criopreservarlo.

Por el momento, alrededor de 1700 personas se han inscrito en el servicio de Alcor. Cuesta 220 000 dólares para el cuerpo completo y 80 000 dólares para el neuro. El DJ Steve Aoki ha declarado que es miembro y se ha informado de que Peter Thiel también lo es. Varios antiguos amigos extropianos de Max también eran miembros. Max dijo que los informáticos ateos representaban el contingente más numeroso.

—La mentalidad *hacker* básicamente ve un problema muy difícil y complejo y piensa: «Bueno, si lo descomponemos en componentes, podremos resolverlo».

Pero Alcor también tenía miembros religiosos.

ALCOR CUESTA 220 000 DÓLARES PARA EL CUERPO COMPLETO Y 80 000 PARA EL NEURO. UNAS 1700 PERSONAS SE HAN INSCRITO

—Supongo que hay menos motivación si crees que vas a ir al cielo, sea lo que sea eso, nunca tuve una respuesta clara al respecto, pero no veo una incompatibilidad, porque para mí es solo una extensión de la medicina de emergencia, ¿no? Primero se prueba la dieta y el ejercicio, luego la medicina convencional y los fármacos, luego la atención médica crítica; si estás realmente en mal estado... podrías someterte a un ensayo clínico; y al final, si eso no funciona, tienes la criónica.

Un hito para el campo fue la publicación en 1964 de *The Prospect of Immortality*, de Robert C. W. Ettinger, considerado ahora el padre de la criónica.

—Un título desafortunado —dijo Max—, porque no nos gusta la palabra inmortalidad.

Las historias sobre Alcor solían utilizar la palabra, pero prometía demasiado. ¿Quién sabía si el universo duraría para siempre? Y una persona podía estar al día con su membresía en Alcor, pero ser asesinada o morir en un accidente automovilístico, de tal manera que su cerebro quedara irremediablemente dañado, o ser eliminada por «asteroides que aterrizan en su cabeza».

LA «MEJOR» ALTERNATIVA

El mito de la inmortalidad estaba cargado de un sombrío bagaje literario. Había «una historia horrible de Karel Čapek», dijo Max, refiriéndose a una obra de teatro llamada *El caso Makropulos*, con un personaje que es incapaz de morir. La diosa griega Eos le pidió a Zeus que le concediera la vida eterna a su esposo, Tithonus, pero no especificó que permaneciera joven, por lo que Tithonus vivió, marchitándose. *Zardoz*, una película de John Boorman de 1974, «en realidad, bastante mala», presentaba a los Eternos, una «sociedad de inmortales estancados» que habían ideado un dios, Zardoz, para controlar a un grupo de salvajes llamados los Brutales. Sean Connery interpretaba a un brutal llamado Zed.

—Todos suplican al salvaje que los mate porque están muy aburridos de la vida.

Llegamos a una sala separada de nosotros por una pared de cristal de seguridad que iba del suelo al techo. Más allá había dos hileras ordenadas de matraces Dewar que contenían a los 234 miembros preservados de Alcor. Una plataforma elevadora estaba lista para bajar la siguiente cápsula. Un par de técnicos estaban trabajando en la sustitución de una pata de uno de los tanques gigantes. Algunos Dewars eran achaparrados, otros más altos. Un Dewar estándar podía acomodar a cuatro pacientes de cuerpo entero. Había un nuevo modelo, un Super Dewar que Max llamaba «Bigfoot», que podía albergar a doce pacientes de cuerpo entero y tenía una parte superior cónica que ralentizaba la evaporación del nitrógeno líquido. Cada uno había sido transportado en camión desde un fabricante de la Costa Este y costaba alrededor de 25 000 dólares el estándar y 100 000 dólares el Super.

—Los pacientes neurológicos están en uno separado —dijo Max—. Tenemos como diez pacientes neurológicos en el mismo Dewar.

Max y su esposa, como la mitad de los miembros de Alcor, estaban inscritos en neuro.

—Todo lo demás es reemplazable, así que prefiero centrarme en lo que importa.

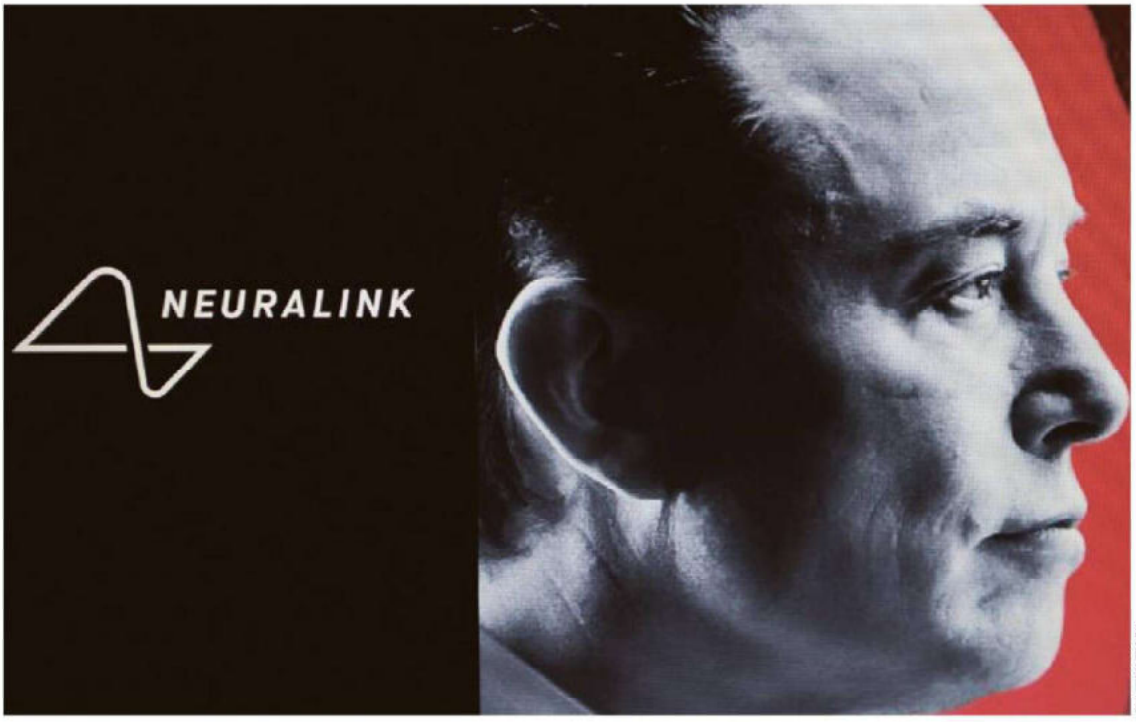
Dentro de las cámaras de acero frente a nosotros estaban la cabeza y el cuerpo de Ted Williams, el jugador de béisbol; Marvin Minsky, considerado el padre de la IA, y Hal Finney, que podría o no haber inventado el bitcoin. Le pregunté en qué Dewar estaba Hal. Max dijo que no se lo sabía de memoria.

—Por lo general, no los identificamos por razones de seguridad.

LAS PERSONAS CON VISIÓN DE FUTURO SE SENTÍAN ATRAÍDAS TANTO POR LA CRIOGENIA Y COMO POR LAS CRIPTOMONEDAS

Muchas de las visiones de los extropianos se habían hecho realidad. En internet, los memes dominaban el día. Elon Musk era, entre otras cosas, el abanderado de un impulso para colonizar las estrellas. Neuralink de Musk era pionera en una interfaz cerebro-ordenador, y personas no del todo serias debatían si la mejor oportunidad de supervivencia de la humanidad residía en ofrecerse como mascotas de la inteligencia artificial general. El sueño tecno-libertario de *Exit* ardía eterno: la navegación marítima había dado paso a los «estados en red» —sociedades intencionales habilitadas para internet— y a proyectos piloto como Próspera (Honduras), Praxis (el Mediterráneo) y Cabin (una «ciudad» «distribuida» y coordinada por *blockchain* de cabañas lejanas en lugares boscosos) destinados a llevarlos al mundo físico.

—Es algo agradable —admitió Max sobre la deriva extropiana de la historia reciente—. No soy muy optimista en cuanto a que solucionemos el envejecimiento durante mi vida. Lo era hace treinta años. Pensaba que era muy probable. Pero no conseguimos la financiación. Así que va a llevar mucho tiempo. No es como si tuviéramos un proyecto *Apollo* que probablemente pudiera marcar una gran diferencia. Así que no creo que lo consiga, incluso si vivo otros cuarenta años. Así que creo que tendré que ser criopreservado, lo cual es un poco jodido. No quiero estar ahí. Pero es mejor que la alternativa en mi opinión.



SHUTTERSTOCK

En julio de 2016, Elon Musk fundó Neuralink, una empresa de neurotecnología especializada en el desarrollo de interfaces cerebro-computadora.

NAKAMOTO VIVIRÍA ETERNAMENTE

La criogenia y las criptomonedas eran simbióticas. Las personas con visión de futuro se sentían atraídas por ambas: Roger Ver, el primer bitcoiner conocido como Bitcoin Jesus (y más tarde demandado por Craig Wright), se había inscrito en Alcor cuando tenía veinte años. Vitalik Buterin había donado criptomonedas a organizaciones de prolongación de la vida, y en 2018 un inversor llamado Brad Armstrong hizo la mayor donación hasta la fecha a Alcor, cinco millones de dólares en una moneda llamada stellar para crear un Fondo de Investigación de Criónica Hal Finney. También existía una conexión más profunda. A principios de la década de los noventa, un extropiano llamado Mark Plus acuñó el término «aeonomics» para describir «el estudio de los problemas económicos de la existencia inmortal». La idea de prolongar radicalmente la vida requería repensar muchas cosas, entre ellas cómo los años adicionales en la Tierra podrían afectar a su plan 401(k). La criónica añadió el giro de cómo garantizar que el dinero que tenías cuando te desanimabas siguiera disponible cuando te reanimaras. Si los extropianos se iban a congelar, necesitarían una forma de enviar dinero al futuro, listo para ser reclamado al despertar. De esta manera, el dinero digital sería una bendición para la criónica.

Ralph Merkle intentó describir una vez por qué la gente técnica estaba tan enamorada del bitcoin, llamándolo «el primer ejemplo de una nueva forma de vida». Vivía en internet, pagaba a la gente para mantenerlo vivo y nadie podía cambiarlo, corromperlo o detenerlo. Cualquiera podía ejecutar su *software*. Cualquiera podía ver lo que hacía y cómo funcionaba. «Si una guerra nuclear destruyera la mitad de nuestro planeta, seguiría viviendo, sin corromperse», escribió Merkle. «Seguiría ofreciendo sus servicios. Seguiría pagando a la gente para mantenerlo vivo».

Andreas Antonopoulos, autor del libro *Mastering Bitcoin*, lo había comparado con «una rata de alcantarilla». Nick Szabo y Elaine Ou, en los últimos años, habían estado trabajando en inocular al bitcoin incluso contra la muerte de internet. Ou se había inspirado en 2016, cuando China amenazaba con prohibir las criptomonedas, y ella y Szabo comenzaron a experimentar con la ampliación de la red bitcoin utilizando la radioafición.

La *blockchain* era eterna. Después de la muerte de Len Sassaman, unos amigos incrustaron en una transacción de bitcoin un retrato ASCII de su rostro barbudo, junto con la inscripción «Len rabbi Sassama (1980-2011). Len era nuestro amigo. Una mente brillante, un alma bondadosa y un auténtico misterio». La transacción pasó a formar parte del bloque 138725, lo que significaba que viviría en la *blockchain* mientras esta existiera, con copias en todos los ordenadores que componían la red.

Como proyecto utópico, bitcoin nunca tuvo, como todos los proyectos utópicos, ninguna oportunidad. La magia y la locura se estaban desvaneciendo. Pero, como nueva clase de activos, había demostrado su resistencia. Su precio volvió a subir, y alcanzó un nuevo máximo histórico por encima de los 73 000 dólares en marzo de 2024. Fidelity ahora aconsejaba a los clientes minoristas que asignaran una pequeña parte de sus carteras de inversión a las criptomonedas. Y la tecnología *blockchain* parecía inevitable, el espacio creativo que abría seguía siendo emocionante.

Satoshi Nakamoto representaba algo que quien estuviera detrás del seudónimo jamás podría encarnar. Era un nombre y una idea que, libre de las limitaciones de un cuerpo físico o una historia personal que lo anclara, viviría eternamente. ■

BIBLIOGRAFÍA

❏ Adrian Chen, *«The Underground Website Where You Can Buy Any Drug Imaginable»*, Gawker, 1 de junio de 2011.

❏ Álvaro D. María, *La filosofía del Bitcoin. La caída del Estado.* Editorial Deusto, 2024.

❏ Andrew O'Hagan, *«The Satoshi Affair»*, London Review of Books, 30 de junio de 2016.

❏ Benjamin Wallace, *«The Rise and Fall of Bitcoin»*, Wired, diciembre de 2011.

❏ Bob Woodward, *The Secret Man: The Story of Watergate's Deep Throat* (Nueva York: Simon and Schuster, 2005), 131-32.

❏ Bobby C. Lee, *La promesa del Bitcoin. El futuro del dinero y cómo puede funcionar a tu favor.* McGraw-Hill Interamericana de España, 2022

❏ Brian Fung, *«Marc Andreessen: In 20 Years, We'll Talk About Bitcoin Like We Talk About the Internet Today»*, *The Washington Post*, 21 de mayo de 2014.

❏ Carlos Domingo, *Todo lo que querías saber sobre Bitcoin, criptomonedas y blockchain y no te atrevías a preguntar.* Ed. Martínez Roca, 2018.

❏ *Craig Wright Reveals Himself as Satoshi Nakamoto, The Economist*, 2 de mayo de 2016.

❏ Jacqueline Lindenberg y Adam S. Levy, *«Kanye West Steps Out for a Solo Outing in Beverly Hills»*, *Daily Mail Online*, 17 de octubre de 2022.

❏ James O'Shea, *«The Secret Irishman Likely Behind Bitcoin, the Internet Currency Code»*, *IrishCentral*, 4 de octubre de 2011.

❏ Javier López Menacho, *La otra cara de las criptomonedas,* Holobionte, 2024.

❏ Jeff John Roberts, *Los reyes de las criptomonedas,* Empresa Activa, 2021.

❏ Jens Ducrée, *Satoshi Nakamoto and the Origins of Bitcoin: The Greatest Mystery in the Entire History of Science and Technology,* publicado por Ducrée, 17 de junio de 2023.

❏ Jim Epstein, *«Tim May, Father of "Crypto Anarchy", Is Dead at 66»*, *Reason*, 16 de diciembre de 2018; *y Nathaniel Popper, «Timothy C. May, Early Advocate of Internet Privacy, Dies at 66»*, *The New York Times*, 21 de diciembre de 2018.

❏ Jonathan Bier, *The Blocksize War: The Battle for Control Over Bitcoin's Protocol Rules* (publicación independiente, 2021).

❏ Jon Matonis, *«Cómo conocí a Satoshi»*, *Medium*, 2 de mayo de 2016.

❏ Josep Busquet, *Bitcoin. La caza de Satoshi Nakamoto.* Editorial Dibbuks, 2014.

❏ Nathaniel Popper, *«Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin»*, The New York Times, 15 de mayo de 2015.

❏ Nathaniel Popper, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* (Nueva York: Harper / HarperCollins, 2015).

❏ Nathaniel Popper, *«Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes»*, *The New York Times*, 12 de enero de 2021.

❏ Nick Szabo, *«Re: sobre el anonimato, la identidad, la reputación y la suplantación de identidad»*, CP, 18 de octubre de 1993.

❏ Nik Bhatia, *Del oro al Bitcoin.* Deusto Ediciones, 2022.

❏ Nour Al Ali y Chris Kingdon, *«Musk: I Am Not Bitcoin's Satoshi Nakamoto»*, *Bloomberg News*, 28 de noviembre de 2017.

❏ Phil Champagne, *El libro de Satoshi. La colección de escritos del creador de Bitcoin Satoshi Nakamoto.* Blockchain España, 2014.

❏ Phinnaeus Gage, *«Definitive Proof That Satoshi Nakamoto is James A. Donald»*, BF, 28 mayo, 2014.

❏ Roger Ver y Steve Patterson, *El secuestro de Bitcoin. La historia oculta del BTC.* Ed. Eda, 2024.

❏ Saifedean Ammous, *El patrón Bitcoin. La alternativa descentralizada a los bancos centrales.* Deusto Ediciones, 2025.

❏ Sahil Gupta, *«Elon Musk Probably Invented Bitcoin»*, HackerNoon, 22 de noviembre de 2017.

❏ Satoshi Nakamoto, «*Re: Quieren borrar el artículo de Wikipedia*», BF, 20 de julio de 2010.

❏ Simon Singh, *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography* (Nueva York: Doubleday Anchor, 2000).

❏ Sophie Elmhirst, «*The Disastrous Voyage of Satoshi*», *The Guardian*, 7 de septiembre de 2021.

❏ Stephen Katte, «*The Last Bitcoin: What Will Happen Once All BTC Are Mined?*», Cointelegraph, 21 de julio de 2023.

❏ Tim May, «*El manifiesto criptoanarquista*», en Peter Ludlow, *Crypto Anarchy, Cyberstates, and Pirate Utopias* (Cambridge, MA: MIT Press, 2001), 61-63.

❏ Tom Simonite, «*The Man Who Really Built Bitcoin*», *MIT Technology Review*, 15 agosto, 2014.

❏ Will Feuer, «*Statue of Anonymous Bitcoin Creator Satoshi Nakamoto Unveiled in Hungary*», New York Post, 17 de septiembre de 2021.

❏ Will Stephenson, «*Cryptonomicon*», *Harper's*, marzo de 2022.

❏ «*Bits and Bob*», *The Economist*, 13 junio, 2011.

❏ Para los registros de la lista de correo electrónico de los cypherpunks: cypherpunks.venona.com, https://marc.info y https://cryptoanarchy.wiki.

❏ Repositorios de la lista de correo electrónico de los extropianos.
-Colección de los resúmenes del grupo de 1992 a 1994 en https://diyhpl.us/~bryan/irc/extropians/raided-mailing-list-archives/archives/.
-Wei Dai aloja un espejo de la lista que abarca 1996-2002 en extropians.weidai.com.
- Las publicaciones a partir de 2003 se pueden encontrar en lists.extropy.org/pipermail/extropy-chat/.

❏ Los archivos de la revista Extropy están en https://hpluspedia.org/wiki/Extropy_Magazines y fennetic.net/irc/extropy/.

❏ NakamotoInstitute.org alberga una colección inigualable de textos relevantes para Bitcoin, incluidos los escritos completos de Satoshi Nakamoto. El foro de Bitcoin en bitcointalk.org.

MUY INTERESANTE

REDACCION
Directora: **Carmen Sabalete** (csabalete@zinetmedia.es)
Subdirectora: **Cristina Enriquez** (cenriquez@zinetmedia.es)
Coordinador de Diseño: **Oscar Alvarez**

Autor de los textos: **Benjamin Wallace.**
Texto original: *Mr. Nakamoto. El enigmático creador de bitcoin (The Mysterious Mr. Nakamoto: The Fifteen-Year Quest to Unmask the Secret Genius Behind Crypto).*

Colaboradores: **Javier Alvaredo** (edición), **Manuel Arrubarrena** (maquetación y documentación).

DIRECCION Y TELEFONO
C/ Alcalá 79 1º A - 28009 Madrid; tel.: 810 58 34 12
Suscripciones: suscripciones@zinetmedia.es

zinet MEDIA GLOBAL

Consejera Delegada: **Marta Ariño**
Director General Financiero: **Carlos Franco**
Director Comercial: **Alfonso Jullá** (ajulia@zinetmedia.es)
Brand Manager: **Marta Espresate** (mespresate@zinetmedia.es)

Editada por **Zinet Media Global, S.L.**
Distribuidor exclusivo en España: Logista Publicaciones
Distribuidor exclusivo en México: Sefeco México, S.A. de C.V., con domicilio en calle Corona No. 23, Colonia Cervecera Modelo, Municipio Naucalpan de Juárez, Estado de México. CP. 53330. Tel. (55) 7586 5532. Número de Certificado de Reserva de derechos al uso exclusivo del Título MUY INTERESANTE: 04-2025-011715474400-102 de fecha 17 de enero de 2025 ante el Instituto Nacional del Derecho de Autor.

IMPRESO EN ESPAÑA. EDICION: 12/2025
Esta publicación es miembro de la Asociación de Revistas de Información (ARI).

ARI

Depósito Legal: M-4343-2020. ISSN 1130 - 4081

«BITCOIN ES UN LOGRO CRIPTOGRÁFICO EXTRAORDINARIO. LA CAPACIDAD DE CREAR ALGO QUE NO PUEDA DUPLICARSE EN EL MUNDO DIGITAL TIENE UN VALOR ENORME»

Eric Schmidt (1955),
ex-CEO (2001-2011) y presidente del consejo de administración (2011-2015) de Google.

MUY INTERESANTE