LA ERA DE LAS CRIPTOMONEDAS

CÓMO EL BITCOIN Y EL DINERO DIGITAL ESTAN DESAFIANDO AL ORDEN ECONOMICO GLOBAL

PAUL VIGNA AND MICHAEL J. CASEY

Índice

Introducción

DINERO DIGITAL PARA UNA ERA DIGITAL

El dinero no creará éxito, la libertad de hacerlo será.

-Nelson Mandela

A pesar de que Parisa Ahmadi estaba en la parte superior de su clase en Hatifi High School en Herat, Afganistán, su familia inicialmente estaba en contra de inscribirse en clases ofrecidas por una empresa privada que prometía enseñarles Internet y redes sociales a niñas. habilidades, e incluso pagarles por sus esfuerzos. "Aquí en Afganistán, la vida de una mujer está limitada por las paredes y la escuela de su habitación", escribió en un correo electrónico. En Afganistán, las niñas no están expuestas a Internet, ni en casa ni en la escuela. Esa también se habría quedado si Ahmadi no hubiera persistido. Ella era una estudiante excelente y quería tomar aún más clases. En su mente, eso era razón suficiente. Ella presionó a su familia, por su propia admisión, "mucho".

La empresa que respalda estas clases es Film Annex, un grupo de artes basado en los EE. UU. Que utiliza las redes sociales y un sitio en línea para pagar a los trescientos mil bloggers y cineastas que contribuyen con su trabajo. Film Annex terminó en Afganistán por su afiliación directa con el Women's Annex, un programa de alfabetización digital creado junto con la empresaria afgana Roya Mahboob, que ahora educa a cincuenta mil niñas en escuelas de todo Afganistán. Mahboob es una especie de celebridad; nombrada una de las cien personas más influyentes en el mundo por la revista Time, dirige una compañía de software llamada Afghan Citadel, es una de las pocas mujeres CEO en Afganistán, y ha hecho de la educación de las mujeres afganas su causa central. El Anexo de la Mujer establece sus aulas en las escuelas secundarias locales, y las clases son impartidas por mujeres. Debido a esta última característica, la familia de Ahmadi finalmente cedió y la dejó inscribirse.

Ahmadi comenzó a tomar clases en 2013. Ella y sus compañeros de clase estaban aprendiendo acerca de la World Wide Web, las redes sociales y los blogs. Una amante del cine que también amaba escribir sobre las películas que la emocionaron, comenzó a publicar en un blog, y sus miembros respondieron positivamente a sus comentarios, lo que le valió el primer ingreso real de su joven vida.

Aún así, una de las otras cosas que la mayoría de las chicas no tienen en Afganistán es una cuenta bancaria. Si la adolescente afgana alguna vez tuvo dinero, tuvo que transferirlo a las cuentas bancarias de su padre o hermanos, y así es como es para la mayoría de las niñas donde vive. En este sentido, tuvo suerte, ya que muchas mujeres de su familia de origen masculino les impiden el acceso a sus fondos y tratan el dinero como propio.

La suerte de Ahmadi cambiaría a principios de 2014. El fundador de Film Annex en Nueva York, Francesco Rulli, consciente de la dificultad que enfrentan las mujeres como Ahmadi y frustrado por los costos de transacción en los que incurrió al enviar cantidades relativamente pequeñas de dinero en todo el mundo, implementó cambio radical al sistema de pago de Film Annex. Pagaría a sus bloggers en bitcoin, la moneda digital que parecía haber surgido de la nada en 2013, con una pequeña banda ferozmente dedicada a los utópicos digitales con inclinaciones libertarias y con mentalidad tecnológica que actuarían como sus portaestandartes, y jurando a cualquiera. quien escucharía que iba a cambiar el mundo.

Rulli, impulsado por una filosofía que es una especie de capitalismo de arranque, pronto "consiguió" bitcoin y aprovechó las ventajas que podría tener para personas como Ahmadi, que fue una de las más de siete mil mujeres afganas que cotizan como contribuyentes pagados en el Film Annex. Los bitcoins se almacenan en cuentas bancarias digitales o "billeteras" que cualquier persona con acceso a Internet puede configurar en su hogar. No hay un viaje al banco para configurar una cuenta, no hay necesidad de documentación o prueba de que eres un hombre. De hecho, bitcoin no conoce su nombre o género, por lo que permite a las mujeres en sociedades patriarcales, al menos las que tienen acceso a Internet, controlar su propio dinero. La importancia de esto no se puede exagerar. Estas mujeres están construyendo algo que es suyo, no el de sus padres o hermanos. Si bien no es una panacea, esta explosión de tecnología de punta del siglo XXI ofrece una promesa real como una forma de ayudar a desencadenar una franja completa de la población humana.

Muchos contribuyentes de Film Annex en los Estados Unidos, el Reino Unido, Italia y otros países ricos se quejaron de la inconveniencia de la moneda digital. Pocos negocios, en línea o no, lo aceptaron para el pago, y para muchos todo parecía poco fiable. Las quejas no son exclusivas de los contribuyentes de Film Annex; para mucha gente, Bitcoin parece una estafa medio perdida, algún plan para engañar a los tontos con su dinero. Además, Ahmadi sostiene los mismos problemas relacionados con el bitcoin que sus colegas de otros países han murmurado, en particular que las opciones para gastarlo son aún limitadas, especialmente en una economía tan poco desarrollada como la de Afganistán. Para enfrentar estos problemas, Film Annex estableció un sitio de comercio electrónico en 2014 que permite a sus miembros intercambiar bitcoins por tarjetas de regalo de sitios globales como Amazon que se enviarán a Kabul, Herat y otras ciudades afganas. En efecto, Film Annex está creando su propia economía bitcoin autoencapsulada, un enfoque que se ve reforzado al cambiar su nombre comercial por BitLanders.

Ahmadi usó sus bitcoins para comprar una nueva computadora portátil. Hace solo unos años, esto hubiera sido imposible. Ella le da crédito a bitcoin por "enseñarnos cómo ser independientes y cómo decidir por nosotros mismos, y lo mejor de todo, cómo pararnos sobre nuestros propios pies". Le permitió pensar en un futuro en el que no sea simplemente un apéndice de los hombres en su vida, un futuro en el que puede trazar su propio rumbo. "Me veo una doctora educada y activa en el futuro", dijo.

Normalmente no lee historias como Ahmadi en la cobertura de prensa de bitcoin. La mayor parte se ha centrado en la montaña rusa de lo que se ve como un concepto monetario sospechoso. Pregúntele a la gente de la calle lo que saben sobre Bitcoin, y si pueden responder algo, probablemente citarán los informes de prensa más destacados. Dirán algo sobre los traficantes de drogas que fueron arrestados usando bitcoins en el sitio web ilícito de Silk Road. O se referirán a movimientos de precios volátiles y emitirán la palabra burbuja. O quizás recuerden la desaparición repentina de una gran cantidad de bitcoins de una cosa con el nombre de Seuss del Dr. Seuss. Gox, sabiendo poco más que eso, era un oscuro intercambio en línea en Tokio. Tal vez ellos saben de la búsqueda de Satoshi Nakamoto, la figura sombría que creó Bitcoin.
Todos estos elementos del espectáculo secundario del circo que han surgido alrededor del bitcoin son coloridos e importantes para comprender su historia. Pero descartarlo como una estafa a causa de ellos es volver la espalda a algo que bien puede cambiar tu vida. Bitcoin es una tecnología digital innovadora con el potencial de cambiar radicalmente la forma en que llevamos a cabo la banca y el comercio, y para llevar a miles de millones de personas de los mercados emergentes a una economía moderna, integrada, digitalizada y globalizada. Si funciona, y aún así es una gran cantidad de cosas que hoy parecen parte del estado natural del mundo, van a parecer tan anticuadas como la imprenta de Gutenberg.

El sistema que usamos ahora para administrar los intercambios de divisas y activos se remonta a la época de la familia Medici del Renacimiento florentino, cuando los bancos asumieron por primera vez el dominio de la economía monetaria de Europa. Estos tipos fueron los disruptores tecnológicos definitivos, pensadores radicales que descubrieron una necesidad vital en la sociedad y luego la llenaron. En esencia, descubrieron cómo intermediar entre ahorristas y prestatarios, aportando el capital excedente de los primeros y parcelando a aquellos entre los últimos que lo necesitaban, todo por una tarifa. Esta fue una versión dramática de lo que un inversor de Silicon Valley llamaría actualmente una eficiencia de red. Al incorporar la miríada de deudas y reclamos de la sociedad en el libro central de un solo banco, los banqueros crearon un poderoso y nuevo sistema centralizado de confianza. Con la ayuda de sus servicios especializados de intermediación, los desconocidos que anteriormente no tenían forma de confiarse lo suficiente como para hacer negocios ahora podrían hacerlo. En efecto, los Medici crearon un sistema de creación de dinero de gran potencia: el dinero no es una moneda física sino un sistema para organizar, expandir y compartir las deudas y los pagos de la sociedad. Dio paso a una explosión en el comercio mercantil, que a su vez creó la riqueza y el capital que financiaría los proyectos de los que las grandes civilizaciones crecerían y conquistarían el mundo.

Pero... al crear este sistema centralizado de confianza y luego colocarse en medio de él, los bancos se volvieron extremadamente poderosos, eventualmente, demasiado. Como los extraños no podían hacer negocios entre ellos sin los bancos, las economías cada vez más complejas e interconectadas del mundo se volvieron completamente dependientes de la intermediación de los banqueros. Los registros que mantenían dentro de sus instituciones se convirtieron en los medios vitales a través de los cuales las sociedades llevaban la cuenta de las deudas y los pagos que surgían entre sus ciudadanos. Por lo tanto, los bancos crearon el negocio de búsqueda de rentas definitivas, posicionándose como porteros de pago, gerentes del tráfico financiero que hicieron funcionar a las economías. Cualquiera que esté sentado en el extremo emisor o receptor de ese tráfico no tenía más remedio que tratar con un banco, como lo hizo Parisa Ahmadi antes de que el Anexo cinematográfico cambiara su política de pago. A medida que este nuevo negocio financiero creció y se hizo más complejo, otros intermediarios rentistas se instalaron como proveedores especializados de fideicomisos intermedios: desde corredores de bonos y valores, hasta agentes de seguros, abogados financieros, procesadores de pagos y compañías de tarjetas de crédito. nuestro día moderno. Como funciona actualmente, nuestro sistema económico global altamente cargado colapsaría si estos intermediarios dejaran de hacer lo que hacen. Todo esto simplemente ha hecho que los bancos en el centro de todo sean aún más poderosos, tanto que finalmente un sistema que primero dio poder a las personas ha fomentado una dependencia peligrosa sobre ellos. Esto es lo que dio origen a los gigantes de Wall Street, que finalmente llevaría al mundo al borde del desastre en 2008.

Ingrese cryptocurrency, la categoría a la que pertenece bitcoin. El genio simple de esta tecnología es que corta el intermediario pero mantiene una infraestructura que permite a los extraños lidiar entre sí. Lo hace al quitarle a las instituciones financieras centralizadas el importantísimo papel de llevar el libro mayor y entregarlo a una red de computadoras autónomas, creando un sistema de confianza descentralizado que opera fuera del control de cualquier institución. En esencia, las criptomonedas se basan en el principio de un libro mayor universal e inviolable, que se hace completamente público y que constantemente se verifica mediante estas computadoras de alta potencia, cada una esencialmente actuando independientemente de las demás. En teoría, eso significa que no necesitamos que los bancos y otros intermediarios financieros formen vínculos de confianza en nuestro nombre. El ledger basado en red -que en el caso de la mayoría de las criptomonedas se llama cadena de bloques- funciona como un sustituto para los intermediarios, ya que puede decirnos con igual eficacia si la contraparte de una transacción es buena para su dinero.

Al eliminar a los intermediarios y sus tarifas, la criptomoneda promete reducir los costos de hacer negocios y mitigar la corrupción dentro de esas instituciones intermediarias, así como también de los políticos que se ven atraídos hacia su próspera órbita. Los libros públicos usados por las criptomonedas pueden sacar a la luz el funcionamiento interno de un sistema económico-político que anteriormente estaba oculto dentro de instituciones impenetrables y centralizadas. De hecho, el potencial de la tecnología como fuerza para la transparencia y la rendición de cuentas va más allá del dinero y los pagos, ya que puede eliminar a los intermediarios que controlan la información de muchas otras formas de intercambio humano en elecciones, donde los entusiastas de las criptomonedas ven la capacidad de terminar fraude electoral. En esencia, esta tecnología es una forma de organización social que promete desviar el control del dinero y la información de las poderosas élites y entregarlo a las personas a las que pertenece, poniéndolos a cargo de sus activos y talentos.

Si escuchamos al vecino de Mike, Scott Robbins, el mismo Scott de Pelham, Nueva York, cuyo escepticismo mesoamericano hacia la globalización también ayudó a fundamentar la introducción a The Unfair Trade, está claro que muchos occidentales de clase media luchan para comprender cómo todo esto podría mejorar sus propias vidas "Simplemente no entiendo por qué me importa un comino el bitcoin", dijo Scott una tarde. Y seguro, si nos enfocamos en, digamos, los ahorros del 2 o 3 por ciento que ofrece Bitcoin en cada tarifa de transacción de tarjeta de crédito, un beneficio que normalmente iría para los comerciantes, es difícil entusiasmarse con una "revolución de criptomonedas". cuando consideramos que la producción económica mundial asciende a $ 87 billones al año, y pensamos en cuánto de eso es compartido por los mismos bancos y cobradores de peajes financieros que las criptomonedas pasan por alto, es posible imaginar muchos billones de dólares en ahorros. Cada uno de nosotros puede reclamar esos fondos, indirectamente a través de las oportunidades de empleo e ingresos que las empresas pueden crear con lo que ahorran en costos financieros, o directamente a través de tasas de interés más bajas, comisiones bancarias y cargos de transacción de nuestro banco y crédito. cuentas de tarjeta. El día que comenzaste a ganar y gastar dinero es el día en que comenzaste a entregar repetidamente porciones de ese dinero a estos intermediarios, a menudo sumando millones de dólares durante la vida de una sola persona. La criptomoneda promete detener esa salida y devolver el dinero a su bolsillo. Esto, de la manera más básica, es la proposición de valor de bitcoins: el "¿Por qué debería importarme?" Que Scott estaba buscando.

La criptomoneda ciertamente no está exenta de defectos y riesgos. Algunos temen que si seguimos el modelo de Bitcoin, su mecanismo para incentivar a los propietarios de computadoras a mantener y administrar el libro público -que los impulsa a competir por lotes de bitcoins recién emitidos cada diez minutos- podría alentar una concentración políticamente perturbadora de poder de cómputo. Entonces, incluso cuando Bitcoin apunta a descentralizar el poder monetario, las tendencias monopólicas innatas del capitalismo podrían llevar a algunos jugadores a acumular suficiente poder de cómputo para tomar el control de la red y revertir un sistema confiable y descentralizado al que las instituciones egocéntricas y centralizadas controlan. Actualmente Bitcoin no está bajo tal amenaza, y muchos creen que nunca surgirá porque los propietarios de computadoras que se benefician de poseer bitcoins no tienen interés en destruirlo. Aún así, la amenaza no puede eliminarse por completo.

Además, Bitcoin y el crimen han sido asociados, como se ve en el caso de Silk Road, donde los usuarios intentaron explotar el anonimato de la moneda digital para vender drogas y lavar dinero. Algunos también se preocupan de que el bitcoin pueda fomentar crisis económicas porque despoja a los políticos del gobierno de la capacidad de ajustar la oferta monetaria y de contrarrestar el instinto de las personas de acumularla en momentos de pánico masivo. Examinaremos estas importantes preocupaciones y mostraremos cómo la comunidad de personas que trabajan en Bitcoin ya se está ocupando de ellas.

No hay forma de evitar que la criptomoneda sea una tecnología altamente disruptiva. En igualdad de condiciones, la disrupción tecnológica hace que una economía sea más eficiente y genera más riqueza en general. Pero nunca es indoloro. Eso será claramente evidente si la criptomoneda se afianza. Desatará tensiones políticas a medida que millones de personas que se ganaron la vida con el sistema anterior despierten y encuentren que sus trabajos están en riesgo. Esa reacción violenta ya se está generando, incluso antes de que la tecnología se establezca adecuadamente, como se verá en las luchas y debates que surgen en los capítulos siguientes. El conflicto político no es solo entre aquellos que se aferran al viejo sistema y aquellos que apoyan al nuevo, sino también dentro de las filas del último grupo, como idealistas, pragmáticos, empresarios y oportunistas compiten para controlar el futuro de la criptomoneda.

Cuando la disrupción es impulsada por una tecnología asociada al dinero, estos enfrentamientos pueden ser especialmente intensos. Sin embargo, cuando los cuchillos están fuera metafóricamente; aún no estamos al tanto de ningún asesinato relacionado con Bitcoin; a menudo es una buena señal de que algo grande está sucediendo.

El ex secretario del Tesoro de los Estados Unidos, Larry Summers, ha comprendido esto. "Si piensas en lo que es una economía moderna, básicamente implica cada vez más intercambio", nos dijo. "Y el intercambio, a menos que pueda ser literalmente simultáneo, siempre tiene problemas reales de confianza. Entonces, lo que el avance en comunicaciones y ciencias de la computación representado en Bitcoin hace es apoyar un intercambio más profundo a un precio más bajo. Y eso importa dentro de los países para los tradicionalmente excluidos y también es importante a través de las fronteras internacionales ".

Los "problemas de confianza" a los que se refiere Summers son el problema central que los banqueros de Medici primero trataron de resolver, el dilema que enfrentan los desconocidos cuando intentan hacer negocios entre ellos. Cuando Summers habla de "los tradicionalmente excluidos", hace una referencia oblicua a los "no bancarizados", los Parisa Ahmadis del mundo, los aproximadamente 2.500 millones de personas de Afganistán a África e incluso a los Estados Unidos que han sido excluidos del sistema financiero moderno. , que no tienen cuentas bancarias con saldos verificables, historial de crédito o cualquiera de los requisitos que los bancos nos imponen para hacer negocios a través de ellos. Sin acceso a la banca, están esencialmente excluidos de la economía moderna.

En esencia, la criptomoneda no se trata de los altibajos del mercado de divisas digital; ni siquiera se trata de una nueva unidad de cambio para reemplazar el dólar, el euro o el yen. Se trata de liberar a las personas de la tiranía de la confianza centralizada. Habla de la tentadora perspectiva de que podemos quitarle el poder al centro, lejos de bancos, gobiernos, abogados y líderes tribales de Afganistán, y transferirlo a la periferia, a Nosotros, la Gente.

Entonces, ¿qué es exactamente Bitcoin? Se pone un poco confuso porque las personas se refieren a dos cosas diferentes cuando hablan de bitcoin. La primera es la característica que tiene la mayor atención: bitcoin la moneda, las unidades digitales de valor que son usadas por las personas a cambio de bienes y servicios u otras monedas, y cuyo precio tiende a oscilar violentamente contra las monedas tradicionales emitidas por el gobierno. Pero esa definición estrecha distrae de una más amplia que capta la contribución mucho más importante de bitcoin, y eso es bitcoin en la tecnología, o, como algunos prefieren escribirlo en texto, Bitcoin, con una B mayúscula (con la moneda siempre referida con una minúscula b). *

En esencia, la tecnología de bitcoin se refiere al protocolo del sistema, una frase común en la terminología del software que describe un conjunto fundamental de instrucciones de

programación que permiten que las computadoras se comuniquen entre sí. El protocolo de Bitcoin se ejecuta a través de una red de computadoras que pertenecen a las muchas personas de todo el mundo que se encargan de mantener su contabilidad y su sistema monetario. Proporciona a esas computadoras las instrucciones de funcionamiento y la información que necesitan para realizar un seguimiento y verificar las transacciones entre las personas que operan dentro de la economía de bitcoins. El sistema emplea el cifrado, que permite a los usuarios ingresar contraseñas especiales para enviar dinero digital directamente entre sí sin revelar esas contraseñas a ninguna persona o institución. Igualmente importante, establece los pasos que las computadoras en la red deben realizar para llegar a un consenso sobre la validez de cada transacción. Una vez que se ha llegado a ese consenso, un beneficiario sabe que el pagador tiene fondos suficientes para que el pagador no envíe dinero digital falsificado.

Ahora, esto es lo que hace que los expertos en tecnología, los economistas y los futuristas estén más entusiasmados con la tecnología de bitcoin. Consideran que su protocolo de fuente abierta es una base sobre la cual desarrollar nuevas herramientas para hacer negocios y administrar los intercambios. Puedes pensarlo como un sistema operativo. (Debido a que está basado en software de código abierto, usaríamos la analogía de Linux para PC o Android de Google para teléfonos inteligentes en lugar de Windows de Microsoft o iOS de Apple). La diferencia es que el sistema operativo de bitcoin no proporciona instrucciones a una sola computadora en cómo funcionar solo, pero a una red de computadoras sobre cómo interactuar entre sí. Sus características principales son su modelo descentralizado de prueba "sin confianza" y una base de datos generada automáticamente que contiene cada transacción que se haya completado, se pone a disposición de todos en tiempo real y nunca se puede alterar. Del mismo modo que los fabricantes de aplicaciones móviles están ocupados creando aplicaciones sobre Android, los desarrolladores están creando aplicaciones especializadas además de bitcoins que explotan esas características clave. Estas aplicaciones pueden simplemente hacer que los intercambios de bitcoin en la moneda sean más fluidos y fáciles de usar, como las aplicaciones de monedero digital móvil que permiten a los usuarios de teléfonos inteligentes intercambiar dinero digital entre sí, o sus objetivos pueden ser mucho más amplios. Las reglas del protocolo bitcoin para compartir información les permiten a estos desarrolladores crear un conjunto de instrucciones basadas en software para administrar la toma de decisiones en las empresas, las comunidades y las sociedades. Debido a que viene con un registro de propiedad completamente verificable y transparente que no requiere registro centralizado, este sistema "sin confianza" permite a las personas intercambiar todo tipo de elementos de valor digitalizados y cualquier tipo de información útil con la confianza de que la información es precisa. Todo esto se produce sin la costosa intervención de los bancos, las agencias gubernamentales, los abogados y los muchos otros intermediarios necesarios para hacer que nuestro sistema centralizado funcione actualmente. Ese es el poder de bitcoin de la tecnología.

Debido a su rápido aumento de precios, los errores de alto perfil y legiones de creyentes y críticos apasionados, ocasionalmente mesiánicos, bitcoin ha inspirado volúmenes de acalorados debates que han tendido a abrumar los serios esfuerzos por explicarlo y su potencial. Este libro es un esfuerzo por restablecer el equilibrio en el tema de una manera que permita a los lectores de diversos niveles de experiencia y comprensión obtener una idea de lo que es, cómo funciona y lo que podría significar para todos nosotros.

Somos periodistas, no futuristas. Nuestro intento no es delinear un caso definitivo de cómo será el futuro. Pero si hemos aprendido algo desde la llegada de Internet, es que la tecnología no espera a que nos pongamos al día. Desde máquinas trilladoras y máquinas eléctricas hasta líneas eléctricas y de ensamblaje, computadoras centrales y correo electrónico, las personas y los gobiernos que no han prestado atención significativa a las nuevas tecnologías han sufrido una desagradable sorpresa. Creemos que el bitcoin, y más específicamente los avances que lo han hecho y otras criptomonedas herramientas particularmente efectivas para el intercambio

monetario, tienen el potencial de ser una fuerza importante en las finanzas. Simplemente considere esto: el control de una moneda es una de las herramientas más poderosas que ejerce un gobierno; pregúntele a alguien en Irlanda, Portugal, Grecia o Chipre que vivió la reciente crisis financiera de esos países. Bitcoin promete quitarle al menos parte de ese poder a los gobiernos y entregárselo a las personas. Solo eso augura choques políticos, culturales y económicos significativos.

Ves indicios de esos enfrentamientos en el fervor de las multitudes pro y contra. Los bitcoiners con los que hablamos al investigar este libro y con los que hablamos durante nuestros trabajos diarios en The Wall Street Journal tienen una pasión que raya en el fervor. Bitcoin adopta la apariencia de un movimiento religioso: las reuniones que recuerdan las reuniones sociales de la iglesia, las multitudes de culto que cantan los elogios de bitcoin en foros sociales como Reddit y Twitter, los evangelistas del movimiento, personas como Barry Silbert, Nicolas Cary y Andreas Antonopoulos , Charlie Shrem y Roger Ver (cuyo apodo es Bitcoin Jesus). En la parte superior de todo, instalado firmemente en un mito de la creación que inspira y nutre a los fieles, se encuentra Satoshi Nakamoto, la divinidad de Bitcoin.

Pero las criptomonedas podrían arder por completo, como el formato de video Betamax (para aquellos que tengan edad suficiente para recordarlo). O podrían tener solo aplicaciones marginales en el mundo real, de forma muy similar a como lo hizo el muy publicitado Segway. Nada menos que un bitcoiner dedicado que Gavin Andresen, el ingeniero de software a quien Satoshi Nakamoto designó efectivamente para convertirse en el desarrollador principal del software central de bitcoins, lo expresa de esta manera: "Cada vez que doy una conferencia, enfatizo que el bitcoin realmente es todavía un experimento; cada vez que escucho sobre alguien que invierte sus ahorros de vida en él, me estremezco ". Y ese es el tipo responsable de mantener todo funcionando. Más convencidos en su duda están los principales líderes empresariales como el jefe de JP Morgan Chase, Jamie Dimon, que calificaron a bitcoin como "una terrible reserva de valor" y al legendario inversor Warren Buffett, que lo llamó simplemente un "espejismo".

Estas no son reacciones inusuales, en realidad. La mayoría de las personas, descubrimos, reaccionan de la misma manera cuando comienzan a pensar en bitcoin y criptomonedas. Algunos superan la reacción intestinal inicial, otros no. Esperamos que pasen por una especie de modelo Kübler-Ross de reconocimiento de criptomonedas antes de que este libro termine. Sería algo como esto:

Primera etapa: Desdén. Ni siquiera negación, pero desdén. Aquí está esta cosa, se supone que es dinero, pero no tiene ninguna de las características de dinero con las que estamos familiarizados. No es tangible No es emitido por un gobierno o forjado con metales preciosos.

Etapa dos: escepticismo. Usted lee el periódico todos los días, y han aparecido suficientes historias para convencerlo de que el bitcoin es real, de que algunos empresarios, incluidos los gemelos Winklevoss de la fama de Facebook, esperan ganar mucho dinero con él. Pero los detalles no se suman. ¿Lo entiendes haciendo problemas matemáticos? ¿No? ¿Al hacer que su computadora tenga problemas matemáticos? ¿Cómo puede eso funcionar? En esta etapa, frases como esquema de Ponzi y manía de tulipán entran en tu mente.

Etapa tres: curiosidad. Has seguido leyendo. Se hace evidente que muchas personas, incluso algunas personas aparentemente sensatas como el pionero de Internet Marc Andreessen, personas con un historial de tener razón sobre estas cosas, están realmente emocionados por ello. Pero ¿por qué todo el alboroto? De acuerdo, es dinero digital, puede funcionar, pero ¿qué diferencia va a hacer eso con la gente común? ¿Y por qué la gente está tan acalorada al respecto?

Etapa cuatro: Cristalización. Este es el crítico. Elige la metáfora que prefieras, llámalo el momento de la mandíbula, el momento de la bombilla, el momento de la mente, ahora oficialmente volado, es un punto de realización que golpea a casi todos los que pasan un tiempo cerca de las monedas digitales, incluso si permanecen escépticos sobre los obstáculos para su aceptación. Algunas personas con las que hablamos hablaron de que no podían dormir durante días, rastreando cada palabra que podían encontrar en bitcoin. De una vez, redada digitalizada, una forma completamente nueva de hacer las cosas cristaliza en tu mente.

Etapa cinco: aceptación. No es algo fácil de entender, pero las grandes ideas nunca lo son. La conclusión es que incluso si el bitcoin no sigue creciendo, incluso si ninguna de las otras criptomonedas "altcoin" tiene éxito, y varios cientos de estas criptomonedas bitcoin con sus propias características y caprichos existen, hemos visto una forma de hacerlo negocios que son más rápidos y más baratos, que eliminan a los intermediarios y al rentista, atraen a millones de personas "no bancarizadas" y les otorgan a todos el control de sus finanzas y negocios que no existía antes. Una vez que vea esto, no hay forma de desvincularlo.

Por supuesto, existen razones para dudar del éxito de este gran experimento. Bitcoin tiende a atraer titulares sobre escándalos y brechas de seguridad, y si bien estos aún no son tan grandes como los que ocurren dentro del sistema de finanzas y pagos con tarjeta de crédito dominante, centrado en el banco, crean un problema de imagen. Imagine el golpe de PR si surgen informes de que bitcoin se ha utilizado para financiar un gran ataque terrorista. La ansiedad pública sobre tales riesgos podría provocar una respuesta excesiva de los reguladores, estrangulando el proyecto en su infancia. Esta reacción legal podría ser especialmente restrictiva si los funcionarios sienten que el bitcoin está empezando a afectar la capacidad de los gobiernos para controlar su sistema monetario y de pagos, que es el objetivo declarado de muchos de sus partidarios más apasionados y libertarios. Los primeros esfuerzos normativos serios están en curso ya que los funcionarios en Washington, Nueva York, Londres, Bruselas, Beijing y varias otras capitales financieras y políticas formulan reglas para los usuarios de monedas digitales. Si están bien diseñados, podrían reforzar las criptomonedas haciendo que las personas se sientan mejor protegidas de sus elementos más peligrosos. Pero los burócratas pueden ir demasiado lejos y anular la capacidad de las nuevas empresas innovadoras para aprovechar al máximo el potencial de esta tecnología para empoderar a las personas, romper monopolios y reducir los costos, el desperdicio y la corrupción en nuestro sistema financiero.

Mientras tanto, otras tecnologías emergentes podrían evolucionar para proporcionar una mejor competencia. Por ejemplo, en China, las personas actualmente tienen pocos incentivos para usarlo en los pagos debido a que las nuevas aplicaciones ubicuas basadas en teléfonos inteligentes móviles ya les permiten realizar pagos denominados en renminbi sin el riesgo de la volatilidad de bitcoins. Los sistemas heredados que están siendo atacados seguramente trabajarán para mejorar los servicios que ofrecen, reducir sus costos y apoyar la regulación diseñada para reducir la ventaja competitiva de bitcoins.

El comodín más grande en todo esto es la gente. El rápido desarrollo de la criptomoneda es, en cierto modo, una rareza de la historia: lanzada en plena crisis financiera de 2008, Bitcoin ofrecía una alternativa a un sistema -el sistema financiero existente- que explotaba y amenazaba con destruir a unos pocos millones de personas. eso. En unos pocos años, todo un movimiento de contracultura se formó alrededor de las criptomonedas, y ha continuado girando en torno a ellas. Sin esa crisis que expone dolorosamente los defectos del sistema financiero mundial, es difícil decir dónde estaría hoy el bitcoin. A medida que la crisis retrocede, ¿retrocederá el impulso de adoptar una moneda digital?

Nadie puede decir que sabe cómo todo esto se sacudirá. Por lo tanto, aunque no haremos predicciones, vamos a especular sobre las perspectivas de la criptomoneda, examinando lo que podría ser mientras reconocemos y detallamos las razones por las que podría no ser así.

Puedes ser escéptico. Esta bien; nosotros también lo estábamos Ambos empezamos a cubrir los mercados en la década de 1990. Vimos el auge de las puntocom y el colapso de las puntocom. Vimos el auge de la vivienda y el colapso de la vivienda. Vimos la crisis financiera, y la recesión mundial, y la crisis del euro, y Lehman Brothers, y Long-Term Capital Management, y Chipre. Entrevistamos a cualquier número de verdaderos creyentes del mundo de la tecnología que pensaban que tenían la próxima gran cosa. Usted pasa por suficiente de eso, y es instintivamente escéptico.

Así que ambos dudamos cuando escuchamos por primera vez sobre Bitcoin. ¿Dinero que no está respaldado por un gobierno? ¡Eso es una locura! (En nuestra experiencia, ese es el mayor punto de fricción para la mayoría de los escépticos, simplemente no pueden superarlo). Pero nuestra curiosidad nos ganó. Empezamos a escribir sobre eso, a hablar con la gente sobre eso y a escribir un poco más. Finalmente, la enormidad del potencial de bitcoin se hizo evidente para nosotros, y de alguna manera este libro refleja nuestro propio viaje por el mundo de las criptomonedas. Es una extensión de nuestra curiosidad.

Estamos contando la historia de bitcoin, pero lo que realmente estamos tratando de hacer es averiguar exactamente dónde se insertan las criptomonedas en el mundo, para armar este gran rompecabezas. Es una gran historia, una que se extiende por todo el mundo, desde el centro de alta tecnología de Silicon Valley hasta las calles de Beijing. Incluye visitas a las montañas de Utah, las playas de Barbados, escuelas en Afganistán y empresas nuevas en Kenia. El mundo de las criptomonedas comprende la realeza del capital de riesgo, los desertores de la escuela secundaria, los hombres de negocios, los utopistas, los anarquistas, los estudiantes, los trabajadores humanitarios, los hackers y la pizza de Papa John's. Tiene paralelismos con la crisis financiera, y la nueva economía compartida, y la fiebre del oro de California, y antes de que todo termine, es posible que tengamos que soportar una batalla épica entre un nuevo mundo de alta tecnología y el viejo mundo de baja tecnología que podría echar a millones de personas fuera del trabajo, mientras creas una raza completamente nueva de millonarios.

¿Estás listo para saltar por el agujero conejo de bitcoin?

Capítulo 1

DE BABILONIA A BITCOIN

El ojo nunca ha visto, ni la mano tocó un dólar.

-Alfred Mitchell Innes

Para que una moneda sea viable, ya sea una criptomoneda descentralizada emitida por un programa informático o una moneda tradicional "fiduciaria" emitida por un gobierno, debe ganarse la confianza de la comunidad que la utiliza. Para los defensores de la criptomoneda, como aprenderemos en los capítulos siguientes, el objetivo es ofrecer un modelo alternativo para esa confianza. Promueven un sistema de pagos en el que el beneficiario ya no tiene que confiar en instituciones "de terceros" como bancos o gobiernos para asegurar que el pagador pueda entregar los fondos acordados. En cambio, los sistemas de criptomonedas infunden confianza en un programa informático inviolable y descentralizado que, en teoría, es incapaz de defraudar a las personas. Nada de esto, sin embargo, saca las criptomonedas del anzuelo. Ellos también deben ganarse la confianza de la gente si quieren ser relevantes.

La confianza es el núcleo de cualquier sistema de dinero. Para que funcione, las personas deben sentirse seguras de que una moneda se mantendrá en la estima correcta por los demás. Entonces, antes de entrar en la dramática llegada de Bitcoin a la escena y su intento de cambiar la forma en que pensamos acerca de esas cosas, necesitamos explorar esa noción de confianza en mayor profundidad a medida que ha evolucionado a lo largo de la historia. Este capítulo nos llevará a un viaje a través de la evolución del dinero, uno de los inventos más notables y menos conocidos de la sociedad.

Comencemos con algunas preguntas básicas. ¿Qué es el dinero? ¿Que representa? ¿Cómo llegó la sociedad a desarrollar un sistema tal para intercambiar bienes y medir su valor? Como es el caso en cualquier campo de estudio, averiguar cómo funciona algo a menudo se aborda mejor examinando casos en los que el sistema no ha funcionado.

Un ejemplo contemporáneo de fracaso se encuentra en Zimbabwe, cuyas notas difuntas denominadas en miles de millones ahora se sientan en los escritorios de los reporteros financieros y los operadores de divisas como recordatorios de cómo las cosas desquiciadas pueden convertirse en dinero. Pero la lección más fuerte que las sociedades occidentales han aprendido viene de más atrás: la República de Weimar de los años veinte. El gobierno alemán entonces, no dispuesto a entablar un conflicto militar con sus vecinos europeos, pero también reacio a molestar al público al aumentar los impuestos, imprimió dinero para cubrir sus deudas y envió a la marca alemana a una espiral descendente incontrolable. A medida que la inflación se disparaba más allá de lo que cualquiera pudiera imaginar, los niños organizarían montones de notas sin valor de 50 millones de marcos en los teatros. La mayor precaución de todo esto proviene del conocimiento de que este caos monetario y gubernamental abrió una puerta a Adolf Hitler.

Con el tiempo, Alemania se convirtió en una nación en funcionamiento, generalmente amante de la paz, lo que demuestra que es posible que las sociedades democráticas restablezcan el orden después de un caos financiero y político. Lo mismo ocurre con Brasil, que, a través de duras reformas de la política monetaria, respaldan las tasas de inflación superiores al 30,000 y la dictadura de los años ochenta. Pero algunos lugares viven con una disfunción monetaria casi de forma permanente, y por eso pagan un precio formidable. De su experiencia, aprendemos que el

problema central no son las decisiones políticas irresponsables de los bancos centrales que imprimen dinero, aunque este es el mecanismo a través del cual se crea la hiperinflación. Por el contrario, el problema surge de una ruptura profunda de la confianza entre las personas que usan una moneda y la autoridad monetaria que la emite. Dado que esas autoridades monetarias son normalmente gobiernos nacionales, este colapso refleja una relación defectuosa de la sociedad con su gobierno. Es una forma instructiva de pensar en lo que una criptomoneda, con su sistema de intercambio monetario basado en matemática "sin confianza", ofrece como alternativa.

Si los ciudadanos no confían en que un gobierno represente sus intereses, no confiarán en su moneda, o mejor dicho, no confiarán en el sistema monetario en torno al cual se organiza su economía. Entonces, cuando se les presente una oportunidad, venderán esa moneda y huirán por algo que consideren más confiable, ya sea el dólar de EE. UU., El oro o algún otro refugio seguro. Cuando esta disfunción está arraigada, tales creencias son autocumplidas. La pérdida de valor en su moneda agota los recursos financieros del gobierno, lo que deja la impresión de dinero como el único medio para pagar sus deudas y garantizar la supervivencia política. Muy pronto, el exceso de dinero en circulación socava aún más la confianza, lo que puede dar paso a un círculo vicioso de espiral de inflación y caídas en los tipos de cambio.

Argentina ha vivido con esta relación rota por mucho tiempo. Un siglo de fracaso en resolver el problema de la confianza explica por qué Argentina ha pasado por muchas, muchas crisis monetarias y por qué ha caído del séptimo país más rico del mundo a comienzos del siglo XX para ubicarse alrededor del octogésimo a mediados de 2014. * Eso pone Argentina, que durante muchos años se presentó como un faro de sofisticación europea en un continente de atraso del Nuevo Mundo, más o menos a la par del Perú.

Mike sabe una cosa o dos sobre Argentina. Él recoge la historia desde aquí:

Mi familia y yo pasamos seis años y medio felices en Buenos Aires. La luz del sol, el bistec, el vino Malbec, todo completó la experiencia. La mejor parte fueron los amigos que creamos, las personas que te daban abrazos de oso, que siempre se desvivían por ayudarte, y que no pensaban en tomar un almuerzo de cuatro horas para entablar una conversación intensa sobre el estado de la situación. mundo.

Pero la mía era una relación de amor-odio con su país. Para el apasionado abrazo de amigos y familiares de los argentinos, su sociedad está en guerra permanente consigo misma. Esto se manifiesta en las heces de los perros que ensucian las aceras de Buenos Aires, los grafitis que desfiguran la arquitectura parisina que alguna vez fue hermosa, y los atascos interminables causados por la falta de voluntad de los conductores para ceder. Los políticos amargamente divididos del país defienden ideologías competitivas y anticuadas, pero en verdad su lealtad reside en una maquinaria política unificadora y corrupta instalada por Juan Domingo Perón hace medio siglo. El sistema de poder maquiavélico del peronismo ha atrapado a la política argentina en un círculo vicioso de miopía y corrupción, un fracaso que ha dejado a los argentinos sin fe en sus gobiernos. Saltarse los impuestos es la norma: ¿por qué, según la gente, le pagarías a ladrones que te robarán tu dinero? En este entorno, el interés propio se afirma constantemente y se desperdicia la gran cantidad de recursos naturales del país. Se acumularán grandes cantidades de dinero en ráfagas cortas de varios años por parte de los expertos en los esquemas de bombeo y volcado que se hacen pasar por políticas, pero eso solo significa que la economía se precipita hacia un acantilado cada diez años más o menos.

Llegué a Argentina a principios de 2003, justo cuando la última crisis de ese tipo apenas disminuía. Los bancos, que aún mantenían congelados los ahorros de las personas en cuentas que el gobierno había convertido forzosamente de dólares a pesos devaluados, habían encerrado sus sucursales

en placas de acero para proteger sus ventanas de las bombas de ladrillos lanzados por los depositantes que protestaban. Cuando me fui, en 2009, la siguiente crisis se estaba gestando. La inflación empujaba hacia un 30 por ciento anual, pero el gobierno mentía abiertamente al respecto, un acto de mala fe que solo hizo que los argentinos desconfiaran más de su moneda y llevó a las empresas a subir los precios preventivamente en un ciclo de auto-refuerzo. La gente estaba retirando lentamente los pesos de los bancos, y el gobierno estaba restringiendo las compras de monedas extranjeras, lo que, como era previsible, socavó aún más la confianza en la moneda nacional. Este juego del gato y el ratón, como los argentinos sabían muy bien, estaba destinado a terminar mal.

También complicó nuestra partida. Un año después de que nos fuéramos, finalmente vendimos el encantador departamento que habíamos comprado en el frondoso suburbio de Buenos Aires en Palermo. Pero cuando regresé a la ciudad para cerrar el trato, ahora era difícil sacar nuestro dinero del país.

La propiedad residencial en Argentina históricamente se ha vendido en dólares, literalmente, dólares verdes. La historia ha hecho que los argentinos desconfíen de su propia moneda, pero también desconfíen de cheques, giros postales y cualquier otra cosa que requiera la provisión de crédito. Las notas frías y duras en dólares pueden atravesar todo eso. Eso es lo que nuestros compradores querían. Reacios a enviar dinero a nuestra cuenta bancaria de EE. UU., Querían hacer las cosas de la manera tradicional. Sugirieron que completemos el trato en una casa de cambio en el distrito financiero de Buenos Aires, una de las numerosas casas de cambio que ayudan a los argentinos a administrar sus complicados asuntos financieros. La casa tomaría nuestro efectivo y crédito recién obtenidos en nuestra cuenta bancaria de EE. UU. Fácil. ¿Qué podría salir mal?

Con vestíbulos brillantes, insignias de estilo victoriano y nombres que transmiten integridad y seguridad, estas casas de cambio pueden parecerse a sucursales bancarias, pero operan fuera del sistema bancario. Además de intercambiar dólares por pesos, administran una red de cuentas para transferir dinero al extranjero a un costo menor que el de los bancos. Ahora que el gobierno estaba imponiendo restricciones estrictas a los servicios bancarios en el extranjero, estos lugares tenían demanda como transmisores de dinero extraoficiales convenientes.

Me sentía incómodo con esta opción aparentemente sombría, pero Miguel, mi mejor amigo en Buenos Aires, me dijo que esta casa de cambio manejaba su negocio semanalmente en transacciones totalmente legales con sus asociados en el extranjero. Él confiaba plenamente en ellos y yo confiaba en él. Así funcionaban las cosas en Argentina: confiabas en quien conocías, y para resolver tus asuntos comerciales, con frecuencia te apoyaste en esas relaciones más de lo que confiabas en la protección legal de un sistema judicial corrupto.

Para estar seguro, sin embargo, tuve una reunión inicial con la casa de cambio, en la que se me aseguró que la transferencia al extranjero sería completamente verificable y legal ya que tendríamos el contrato de bienes raíces como documentación de respaldo. Satisfecho, acepté el plan de los compradores. Días después, ocho personas se reunieron en una de las habitaciones selladas de la firma para completar el cierre: dos miembros del personal; la pareja comprando nuestro departamento; uno de sus padres, que estaba pagando por ello; un escribano oficial, o un notario público, requerido por la ley para autenticar el acuerdo; Miguel; y yo.

Un hombre entró cargando diez o más fajos de billetes y me los dio. Nunca había tenido tanto dinero en mis manos, pero todavía me sorprendió lo pequeños que eran $ 280,000. Fue contado por el personal de la casa de cambio, después de lo cual comenzó la firma de los documentos de transferencia. Una vez que el escribano se había cerciorado de que todo era claro y justo, él y el padre se despidieron y comenzó la transferencia internacional.

De repente, un miembro del personal se apresuró a entrar, gritando apresuradamente, "¡No puedes hacerlo! ¡Esto tiene que pasar por el sistema bancario! "Miré a Miguel y se hundió. El personal había malentendido un requisito clave de documentación bajo las siempre cambiantes leyes cambiarias argentinas. O tal vez, el conspirador argentino que estaba dentro de mí estaba empezando, nos habían preparado. ¿Por qué sucedió esto después de que el escribano se fue y firmó la propiedad? De cualquier manera, estábamos atrapados.

Estas fueron mis opciones: podría juntar el dinero, los ahorros de toda mi vida, y llevarlos a la ciudad, ¿en qué? ¿Una mochila? En mis calcetines? Y espero que la sucursal bancaria local en la que mantuve una cuenta inactiva en su mayoría para pagar mis facturas de electricidad aceptaría felizmente una pila masiva de dólares, conviértalos en pesos por una tarifa ya un tipo de cambio confiscatorio, y luego conviértelos de inmediato en dólares por otra tarifa y otra tasa de cambio cara antes de transferir el dinero a mi banco por una tarifa más grande. Estábamos enfrentando riesgos de seguridad y unos $ 15,000 más en costos, asumiendo que el plan volaría con los oficiales de cumplimiento del banco. O, la casa de cambio ofrecida, podría completar el trato con ellos, pero sin la documentación que me habían prometido. La institución tomaría mi dinero, y un agente en el extranjero depositaría el monto equivalente en nuestra cuenta, pero no recibiría ningún registro en papel de haber entregado dinero alguna vez. Tendría que confiar, una vez más, en que veinticuatro horas después podía llamar a mi banco y asegurarme de que el dinero se dirigía a mi cuenta, aunque pasarían tres días antes de que se registrara el crédito.

Pensé mucho al respecto. Decenas de miles de argentinos hicieron tales transacciones todos los días. Para ellos, era, irónicamente, un método más confiable de intercambiar valor que tratar con un sistema bancario que les había robado repetidamente sus ahorros. Más importante aún, Miguel, el hombre en quien confiaba más que nadie en Argentina, confió en este grupo de personas para cuidar sus cuentas. Lo hizo de una manera más transparente, más clara de lo que yo estaba contemplando, pero lidió con ellos regularmente. De hecho, la casa de cambio necesitaba mantener la confianza de Miguel. La confianza de sus clientes fue la base de su negocio. Por otro lado, era poco probable que fuera un cliente habitual.

De mala gana acepté la transacción no oficial. Todo lo que la casa de cambio podría darme es que un "registro" era una cinta de teletipo de una calculadora básica de impresión de recibos que simplemente mostraba los números en el texto: la cantidad total transferida, menos la tarifa, y nada más. Lo extraví esa misma noche.

Al día siguiente, Miguel y yo volvimos a la casa de cambio para obtener un código especial con el cual mi banco podría rastrear el pago. El caballero al que se suponía que íbamos a encontrar no estaba allí, o eso nos dijo el guardia de seguridad que cuidaba la entrada fortificada de las oficinas administrativas. A medida que mi presión arterial se disparó, pedí ver a otro miembro del personal. El guardia lo llamó, luego transmitió su mensaje: el dinero ya estaba depositado en mi cuenta. Estaba incrédulo. Se suponía que tardaría tres días. Mi corazón se aceleró. ¿Estaban mintiendo? ¿Me habían estafado? Nervioso más allá de toda creencia, salí a la calle y llamé a un agente de mi banco. La respuesta fue: "Sí, señor Casey, el dinero está en su cuenta". Miguel y yo nos abrazamos.

Contamos esta historia porque ilustra el vínculo entre la confianza y el dinero, que a su vez es fundamental para comprender las criptomonedas y la noción de que sustituyen la confianza en un emisor de dinero del gobierno por la confianza en un algoritmo computarizado. (En este sentido, llamar a bitcoin "sin confianza" es impreciso, a pesar de que es un descriptor conveniente todo el tiempo). Se necesita algún tipo de modelo de confianza para ejecutar un sistema monetario. Bitcoin busca abordar este desafío ofreciendo a los usuarios un sistema de confianza basado no

en los seres humanos, sino en las leyes inviolables de las matemáticas. Su propio desafío de confianza radica en el hecho de que no muchas personas están llenas de confianza por la imagen general de bitcoin: su sensación de inseguridad, su volatilidad. Para muchos, también, las matemáticas son un poco aterradoras, como lo es la idea de que las computadoras, en lugar de los seres humanos, son las que manejan cosas, aunque aplicar esas preocupaciones solo a bitcoin traicionará la ignorancia de cuán informatizados han sido nuestros mercados financieros basados en moneda fiduciaria. volverse.

En lugares como Argentina, donde la confianza en las instituciones políticas es débil, el problema de la confianza se resuelve al elevar la confianza que la sociedad tiene en las familias, los amigos y las relaciones basadas en la reputación. Desafortunadamente, esto es extremadamente ineficiente. Tales círculos de confianza son demasiado pequeños para cualquier economía que tenga una compleja red de interacciones económicas fuera de las pequeñas comunidades, y una que pretenda integrarse con el resto del mundo. Además, el sistema se estira hasta el punto de ruptura cuando una crisis impulsa a todos a apresurarse por las salidas y descargar sus pesos indignos de confianza.

La solución de este problema es lo que las criptomonedas pretenden hacer. Se comercializan como tales porque ningún sistema monetario administrado por el gobierno es perfecto. Argentina podría ser un caso extremo, pero como lo demostraron los acontecimientos de 2008, el modelo de cada nación también es vulnerable a fallas de confianza.

Comprender por qué la confianza es tan importante para el dinero, y antes de profundizar en el funcionamiento y la gran promesa de la criptomoneda, hagamos un recorrido por la historia y exploremos las teorías competitivas del dinero que se han desarrollado a lo largo de los siglos. Esperamos que al final tenga una idea de lo que es realmente el dinero. Pensarías que la respuesta a eso sería simple ahora, con personas que han usado el material durante milenios. Pero en realidad, la práctica de intercambiar dinero yace tan profundamente en la evolución cultural de la sociedad que le damos poca importancia.

En su reciente y provocador libro, Money: The Unuthorized Biography, Félix Martin argumenta que enfocarse en el dinero como una "cosa" -la concepción mercantil, o "metalista", del dinero, que veremos más adelante-es perderse el poderosa fuerza de construcción de la civilización que esta invención desató. Llamando al dinero una "tecnología social", declara que "la moneda no es dinero en sí misma". El dinero es el sistema de cuentas de crédito y su compensación que representa la moneda ". Concebida de esta manera, vemos cómo el dinero permitió una nueva forma de organización social más allá del tribalismo. Brindaba un sistema de valores universales, lo que significaba que las estructuras de poder en las comunidades tribales prehistóricas, donde el orden se mantenía a través de la amenaza de violencia en manos de quien fuera el más brutalmente poderoso, podían dar paso a algo que permitía a todos los miembros de la sociedad, no solo los físicamente poderosos o conectados, para prosperar. La riqueza definida por la acumulación de esta nueva medida abstracta de valor se convertiría en el punto de referencia del poder. Cambió completamente las reglas del juego.

Martin nos lleva a la isla de Yap en Micronesia para explicar su punto. Él describe un sistema monetario único que desconcertó a los primeros visitantes europeos, que consiste en ruedas de piedra conocidas como fei. Estos fueron extraídos a 550 millas de distancia y tenían 12 pies de diámetro. Después de un intercambio, con frecuencia era demasiado inconveniente transportar estas rocas de piedra caliza gigantes a su nuevo propietario, por lo que a menudo se dejaban en posesión del propietario anterior. Sin embargo, el entendimiento mutuo en toda la sociedad de Yapese era que los derechos de propiedad de estos fuertes símbolos de riqueza podían pasar de una persona a otra en una serie de transacciones, proporcionando así un medio para saldar las

deudas pendientes. Martin cita un relato del joven aventurero estadounidense William Henry Furness III sobre cómo uno de los peces se hundió en el océano en ruta desde Babelthuap, pero aún era reconocido como una unidad de moneda intercambiable para su nuevo propietario.

El sistema fei muestra cuán lejos puede llegar la sociedad en la creación de nociones abstractas de valor y poder. Este concepto se desarrolla en diversos grados a medida que las sociedades reconocen el valor universal, si bien ficticio, del dinero y es increíblemente poderoso. Así que vemos la llegada del dinero en la antigua Grecia y su revolucionario sistema de democracia coincidiendo con una ruptura con la sociedad que la precedió, donde las estructuras de poder fueron mucho más brutales y limitantes. El dinero abrió el mundo, creó posibilidades.

Pero tan poderoso como este acto comunitario de aceptar la abstracción ha sido el desarrollo de la civilización, es una lucha para nuestras mentes individuales, que prefieren explicaciones materiales sobre cómo funciona el mundo y especialmente para comprender el valor. Vemos esto ahora como una generación anterior que creció con tiendas físicas y productos físicos que se esfuerzan por comprender por qué alguien compraría "bienes virtuales", como los que se venden en juegos en línea como Second Life, y mucho menos pagar por ellos. con "moneda virtual". Intelectualmente podemos tener el debate "¿Qué es el dinero?", pero nos cuesta superar esta noción profunda de un dólar o un euro, o incluso un bitcoin, como una cuestión de material valor en sí mismo.

Continúa y elimina un billete de un dólar de tu billetera, o haz lo mismo con un euro o una libra o un yen, sea lo que sea que lleves (suponiendo que aún lleves efectivo). Eche un buen vistazo. Ahora, pregúntate, ¿cuánto vale?
Su primera respuesta, sin duda, sería algo así como "Duh, un dólar". Pero pregúntate a ti mismo otra vez. ¿Cuánto vale realmente? ¿Qué valor intrínseco tiene esa cosa en tu mano, esa hoja de papel de 2,61 pulgadas por 6,1 pulgadas?

Bueno, podrías escribir sobre él si así lo deseas, convirtiéndolo en un dispositivo para guardar notas, aunque sea extremadamente menos eficiente que una libreta perfectamente buena. Los usuarios de drogas han descubierto que es una herramienta útil para inhalar cocaína, aunque posiblemente sea más una afirmación "porque se puede" que un reflejo de la utilidad especial del billete de un dólar para este propósito. El punto es que, como un objeto material, poco es único sobre un dólar, o sobre el billete de cualquier país. No es una mesa, ni un martillo, ni un automóvil, ni una fuente de alimentos, ni siquiera un servicio prestado, como un corte de pelo o un viaje en taxi.

Hasta cierto punto, este papel es similar a aquellos otros papeles que juegan un papel importante en nuestra sociedad: contratos escritos. Los contratos no son valiosos para el material sobre el que están escritos, sino porque un tribunal reconocerá las palabras contenidas en ellos como evidencia de un acuerdo exigible. Son la prueba de un acuerdo entre dos partes y ofrecen a cada parte un reclamo opcional sobre nuestro sistema legal para que el otro cumpla con sus términos. Pero, ¿qué es exactamente el acuerdo contractual transmitido por un dólar? Sentado allí en la mano, contiene una promesa bastante oscura, una afirmación del gobierno de los EE. UU. De que le debe el valor de ese dólar. El Tío Sam promete aceptar esos pagarés y deducirlos de las deudas que usted le debe (su factura de impuestos, honorarios, multas, etc.), pero por el exceso de dólares después de eso, su sueldo neto, nunca va a pagar. para cumplir con esa deuda. Cuando lo piensas, ¿cómo podría?

En un sentido estrictamente legal, un dólar constituye un derecho sobre el sistema bancario y, por extensión, sobre la Reserva Federal de los EE. UU., Que establece los derechos de todos los futuros tenedores de ese billete de banco cuando lo emite por primera vez a un banco. El banco y la Fed

están obligados a reconocer su reclamo de acuerdo con el valor que pretende representar. En pocas palabras, si deposita una nota en dólares en su cuenta, el banco reconoce que le debe ese dólar. Pero esto realmente no resuelve el problema de qué le da valor al dólar. En un sentido práctico, su valor depende completamente de que todos los demás reconozcan de manera consensuada que su dólar puede canjearse por una medida acordada de bienes y servicios. Si ese consenso desapareciera, el valor de su dólar caería rápidamente, como los argentinos saben de las frecuentes fases de hiperinflación que han soportado. Con esta medida, el valor de un dólar no reside en el hecho de que un banco reconozca un pasivo hacia usted o que el banco registre un reclamo sobre el mismo con la Fed; más bien, depende de la voluntad de la sociedad de aceptarlo para liquidar una deuda. Esta medida de valor de consenso es muy diferente de decir que el billete de dólar tiene algún valor intrínseco.

Aquí los bichitos del oro, como el mundo de las finanzas llama cariñosamente defensores de los sistemas monetarios basados en el oro, se ponen al frente, prometiendo resolver nuestro problema de valor intrínseco. El oro, dicen, es una moneda real, ya que es dura, tangible, duradera e intrínsecamente valiosa. Bajo su amado estándar de oro, usted podría llevar su dólar al gobierno de los EE. UU. E insistir en que le devuelva una deuda, exigiendo el retorno del mismo valor en oro.

Pero eso plantea otra pregunta: ¿qué vale realmente una barra de oro? ¿Cuál es, de hecho, su valor intrínseco? Los insectos dorados apuntan a innumerables usos para este metal altamente duradero y totalmente fungible. Sus propiedades son impresionantes: es maleable y duradero. Se puede fundir y volver a formar, pero nunca pierde su brillo. Su conductividad eléctrica se utiliza en circuitos impresos, mientras que los implantes dentales se basan en su resistencia y resistencia al deslustre. Pero seamos claros: estos usos no son la razón por la que le asignamos valor al oro. De hecho, representan solo una pequeña porción de su suministro. No, el valor asignado tiene mucho más que ver con su belleza percibida, ejemplificada por su uso tradicional en joyería, en arquitectura y en artículos para el hogar. Aquí, sin embargo, terminamos en una discusión circular sobre el valor del oro: es difícil distinguir nuestra apreciación innata de la belleza del oro -como podríamos apreciar una flor, por ejemplo- de nuestra idea de que un adorno dorado transmite valor, que significa riqueza, prosperidad y prestigio.

El oro es escaso Se ha dicho que todo el oro extraído a lo largo de la historia llenaría solo dos piscinas olímpicas. Pero la escasez es relativa y relevante solo si hay demanda. Innumerables objetos materiales podrían considerarse escasos, pero no tienen valor porque no están en demanda. Todo lo que importa es que la gente quiere oro. ¿Pero por qué?

Estamos dando vueltas en círculos. La única conclusión a la que podemos llegar es tautológica: el oro es valioso como moneda o inversión porque creemos que es valioso (que es la misma razón para valorar el dinero en sí). El valor del oro como moneda es una construcción social abstracta. Sin embargo, ese valor en sí mismo es real. Tiene un impacto real en el mundo. A través de la historia, la sangre se ha derramado, las tierras han sido conquistadas y las naciones han sido construidas y destruidas en la búsqueda de este material brillante. Toda esa historia ilustre y, a veces fea, se debe al hecho de que las sociedades desde muy temprano reconocieron el oro como una excelente moneda práctica y un depósito de valor, que cumplía una serie de cualidades clave necesarias para ese propósito monetario: era escaso, durable, divisible, portátil, fácilmente verificado y fungible, es decir, sus cualidades no cambiaron de una unidad a otra, de modo que una tienda de oro era sustituible por otra del mismo peso exacto. Esas cualidades llevaron a las sociedades de todo el mundo a aceptar colectivamente que el oro sería aceptable como moneda. Es ese acuerdo lo que le da su valor. Una vez más, sin embargo, esto no significa que el oro tenga un valor intrínseco.

El debate de siglos sobre la naturaleza del dinero se puede reducir a dos lados. Una escuela ve el dinero simplemente como una mercancía, una cosa preexistente, con su propio valor inherente. Este grupo cree que las sociedades eligieron ciertas mercancías para convertirse en unidades de intercambio mutuamente reconocidas a fin de superar el engorroso negocio del trueque. El intercambio de ovejas por pan era impreciso, por lo que en nuestro pasado agrario, los comerciantes acordaron que una determinada mercancía, ya sean conchas o rocas o oro, podría ser un sustituto de todo lo demás. Este punto de vista del "metalismo", como se lo conoce, fomenta la noción de que una moneda debería ser, o al menos estar respaldada por, algún material tangible. Esta visión ortodoxa de la moneda es aceptada por muchos insectos del oro y defensores del dinero duro de la llamada escuela austriaca de economía, un grupo que ha experimentado un renacimiento tras la crisis financiera con sus críticas a las políticas expansionistas del banco central y monedas fiat inflacionarias. Culpan a la burbuja de activos que llevó a la crisis a la expansión monetaria imprudente de los bancos centrales sin restricciones.

El otro lado del argumento pertenece a la escuela "chartalista", un grupo que mira más allá de la moneda y se centra en cambio en el crédito y las relaciones de confianza entre el individuo y la sociedad en general que encarna la moneda. Este punto de vista, al que subscribimos y que informa nuestra comprensión de las criptomonedas, reconoce la presencia de un acuerdo implícito de toda la sociedad que permite que el intercambio monetario se perpetúe y que la deuda y el crédito se emitan y liquiden. Esta solución negociada, un proyecto intrínsecamente político, es el dinero. No es la moneda. La moneda es simplemente el token o símbolo alrededor del cual se organiza este complejo sistema. (Chartalist viene del latín charta, que significa "token".) Esta concepción del dinero atrajo naturalmente a economistas que creen que los legisladores tienen un papel que desempeñar en el manejo de la economía para el mejoramiento de la sociedad, un grupo representado principalmente por apóstoles de Juan Maynard Keynes. Sin embargo, también está arraigado en la estructura rígida de cualquier sistema monetario de criptomonedas, que no deja espacio para los intervencionistas keynesianos pero depende tanto en un convenio colectivo que la moneda digital puede ser aceptada en la liquidación de deudas.

Esta división filosófica sostiene un debate central sobre las criptomonedas y cómo o si regularlas. El auge del bitcoin ha atraído a muchos con la mentalidad metallista, un grupo liderado por libertarios y anarcocapitalistas, que quieren que el gobierno saque sus codiciosos guantes del suministro de dinero. Pasando por alto la naturaleza intangible de bitcoin, han tratado la moneda digital como una mercancía escasa, una cosa para ser "extraída" y almacenada, una cosa cuya provisión finita matemáticamente probada asegura que su valor subirá y superará el de las monedas fiduciarias ilimitadas tales como el dólar. Sin embargo, muchos otros creyentes de criptomonedas, incluida una muestra representativa de expertos en tecnología y negocios que ven una posibilidad de alterar el sistema de pagos centrado en el banco, son de hecho chartalistas. Describen el bitcoin no como una moneda, sino como un protocolo de pagos. Están menos preocupados por su atractivo como algo intrínsecamente valioso y más con la capacidad subyacente de la red informática para reordenar las reglas de confianza en torno a las cuales la sociedad gestiona los intercambios de valor. Ven el dinero como un sistema para liquidar y registrar las obligaciones de deuda.

Estas distinciones serán importantes ya que examinaremos en capítulos posteriores el futuro de las criptomonedas, pero por ahora demos un paso atrás en el pasado milenario y rastreemos los eventos que nos llevaron a este punto.

¿Cuándo comenzó el dinero? La respuesta a esa pregunta depende del campamento al que perteneces. Discutir la historia del dinero casi inevitablemente se dirige hacia una discusión sobre la historicidad del dinero porque es imposible describir su evolución sin también describir cómo ha sido concebida.

Sobre esa base, la multitud del metalismo ve los comienzos del dinero a través de los ojos de Aristóteles, que escribió: "Cuando los habitantes de un país se volvieron más dependientes de los de otro e importaron lo que necesitaban, y exportaron lo que tenían demasiado de , el dinero necesariamente entró en uso. "Este punto de vista, que una vez que el comercio se hizo tan complejo que el trueque ya no lo cortaría, fue resucitado dos mil años después por Adam Smith en The Wealth of Nations. Smith describió las comunidades del Nuevo Mundo de Perú y de otros lugares como agobiadas por el trueque hasta que se introdujo el genio de la moneda europea. La visión de Smith era crítica para la sabiduría convencional que hemos secuenciado de trueque a dinero a deuda. Sostuvo que como los seres humanos dividían el trabajo de acuerdo con sus talentos, producían bienes excedentes para comerciar, pero quedaban atrapados por el incumplimiento de lo que los economistas llaman una "coincidencia de necesidades". En otras palabras, no había garantía de que el siguiente hombre quisiera para cambiar sus ovejas por todas las puntas de flecha que necesitaba para descargar. Por lo tanto, se eligió un producto fácilmente distinguible y fácilmente intercambiable para funcionar como el estándar acordado para facilitar el intercambio. Esta mercancía se convirtió en dinero, y al pensar esto, era una cosa en sí misma, con un valor intrínseco. Una vez que lo incorporamos a este rol, el dinero abrió las puertas a todas las demás herramientas para el intercambio de valor, incluida la creación de deuda.

Si eres un chartalista, tu punto de partida histórico es muy diferente. Primero, descartas la historia de trueque como mito. Ustedes recurren a las obras de docenas de antropólogos del siglo XX que han visitado lugares donde no se usaron monedas; antropólogos que afirman no haber encontrado evidencia de que estos pueblos alguna vez se hayan dedicado al trueque, al menos no como el principal sistema de intercambio. En cambio, estas sociedades idearon elaborados códigos de conducta para clasificar sus diversas deudas y obligaciones. La deuda, en otras palabras, fue lo primero. El antropólogo David Graeber hipotetiza que los acuerdos de deuda específicos probablemente evolucionaron a partir de intercambios de regalos, lo que generó la sensación de deber un favor. Después de eso, los sistemas de valores codificados pueden haber surgido de las penas que las tribus impusieron por diversas infracciones: veinte cabras, por ejemplo, por matar al hermano de alguien. A partir de ahí los seres humanos comenzaron a pensar en el dinero como un sistema para resolver, compensar y liquidar esas deudas en toda la sociedad.

Dada esta amplia división en sus visiones del mundo, los metallistas y los chartalistas atribuyen motivaciones muy diferentes al papel prominente desempeñado por el estado en la acuñación de moneda a través de las edades. Para los metallistas, los gobiernos simplemente jugaron un papel de respaldo, autenticando la calidad y la cantidad de metal en cada moneda. Pero para los chartalistas, el estado evolucionó hasta convertirse en el último centro de compensación de deudas y créditos a través de su poder de monopolio sobre los impuestos, que solo podía pagarse con la moneda del reino.

Independientemente de dónde se encuentren las lealtades en esta división, la mayoría está de acuerdo en que el primer sistema monetario registrado apareció en Mesopotamia, el Iraq actual, alrededor de 3000 aC, cuando los babilonios comenzaron a usar plata y cebada como medios universales de intercambio y unidades de valor. Coincidió con el desarrollo del Código de Hammurabi, una de las piezas escritas más antiguas y el primer ejemplo de una regla que establece leyes, también en Mesopotamia. Ese código incluía un conjunto de reglas de pago por las cuales las deudas podían liquidarse con plata o cebada. Sobre la base de esas instrucciones, los contables de Mesopotamia de los primeros días mantendrían registros de las transacciones en la sociedad, a través de guiones especializados en tabletas de arcilla. Sus registros empleaban un estilo cuneiforme relativamente fácil de entender que reemplazó a los jeroglíficos, un antiguo sistema de escritura que se había limitado a la realeza y los sumos sacerdotes.

Con el tiempo, la posición de las personas en la sociedad se definiría por una medida monetaria de su capacidad para obtener ítems de valor, más que por un registro de su capacidad de infligir sufrimiento. El dinero, entonces, hizo que los asentamientos humanos fueran menos vulnerables al derramamiento de sangre y al caos. A medida que el mundo se volvió más ordenado, también fue más propicio para el comercio. Desde allí desarrollaron las grandes civilizaciones antiguas: Mesopotamia, Grecia y, con mayor éxito, Roma.

El ascenso y la caída de estas civilizaciones coincidieron con el dinero, y si uno impulsó al otro o viceversa es imposible de desentrañar. El vasto alcance del Imperio Romano era sinónimo de moneda legal en grandes franjas de Europa y Medio Oriente. La inestabilidad política que finalmente la debilitó y llevó a su colapso fue en parte generada por el deterioro del poder adquisitivo de esa moneda, ya que Roma sucumbió a repetidos episodios de inflación furiosa, empeorados por los intentos fallidos del Emperador Diocleciano de controlar los precios. Después de la caída de Roma, la Edad Media descendió a Europa y el continente perdió su sentido del dinero. Algunos esfuerzos intermitentes para revivir la práctica no encontraron tracción hasta el Renacimiento. Como nos recuerda el historiador Niall Ferguson, la devolución del dinero en ese momento y la invención relacionada de la banca por las familias Medici de Florencia financiaron una explosión en el comercio mundial y ayudaron a pagar el renacimiento arquitectónico y artístico de la época. Esto puso a Europa en el camino de la era moderna, en la que el dinero y las finanzas han estado durante mucho tiempo en su centro.

Durante la mayor parte de su historia, la moneda ha sido emitida por quienes gobiernan, ya sean reyes o gobiernos democráticamente elegidos. Consistentemente, esos gobernantes han sellado su autoridad, tanto figurativa como literalmente, en su moneda, recordando a los ciudadanos la profunda conexión entre el dinero y el poder.

Staters, las monedas de aleación de oro y plata que se cree que son la primera moneda acuñada, del reino de Lidia en lo que hoy es el oeste de Turquía, son notables por tener una cabeza de león. Esta insignia hace que el Rey Alyattes, presumiblemente el soberano detrás de estas monedas, sea el autor de una asociación milenaria entre arte y moneda, una práctica que ha otorgado a estos objetos inanimados poco prácticos, gran poder, importancia y valor percibido.

Mire su billete de dólar otra vez. Nótese en el lado de la cara las orlas adornadas y las hojas que corren a lo largo del borde y que encierran la cabeza de George Washington, así como también los sellos del Banco de la Reserva Federal regional y el Departamento del Tesoro de EE. UU. Vea en el reverso los diseños de frontera aún más elaborados que engloban las palabras UNO e In God We Trust, junto con los dos lados del gran sello del gobierno de EE. UU., El águila extendida a la derecha y el Ojo de la Providencia encaramado sobre una pirámide la izquierda. Esta complejidad barroca es difícil de replicar y ayuda a mantener a raya a los falsificadores, al igual que las fibras incrustadas, las marcas de agua y las tiras metálicas. Pero igual de importante, las imágenes convincentes son simplemente impresionantes. Está lleno de ruido semiótico que denota autoridad y orden.

Las imágenes artísticas sobre la moneda nos ayudan a participar en la ficción metalística de que una ficha de dinero tiene un valor intrínseco. Sin embargo, tampoco podemos escapar del simbolismo del poder estatal asociado con él. Incontables monarcas después del Rey Alyattes usaron símbolos dramáticos similares para poner su sello en las monedas. Dio autenticidad a la moneda, pero también funcionó como una especie de marca real, un anuncio de la omnipresencia del reino. Se nos recuerda que el dinero y el poder son inseparables.

La capacidad del soberano para emitir dinero proporcionó un beneficio específico: la creación del señoreaje, la capacidad de obtener ganancias directamente de la emisión de moneda. En estos

días, el señoreaje surge debido al préstamo sin intereses que obtiene un gobierno imprimiendo dinero en trozos de papel comparativamente inútiles. Pero cuando las monedas se asociaron con pesos particulares de metales preciosos, los monarcas explotaron este poder a través de métodos más abiertos. Muchos "recortarán" monedas de oro o plata para fundirse y redimir el valor de las virutas. Antes de que a las monedas se les asignaran valores numéricos específicos, los gobernantes "llorarían" el valor arbitrariamente asignado de una moneda específica, al declarar que ahora podían comprar menos de un producto útil determinado o contribuir menos que previamente a la liquidación de una factura tributaria. En efecto, el monarca se retractaba con la promesa de pagar los pagarés a cierta tasa y, así, llegó a cancelar sus deudas de acuerdo con el tamaño de la demanda. Por la misma razón, los sujetos de la corona se vieron obligados a aportar más dinero para cumplir con sus deudas. Huelga decir que esto irritó a las clases adineradas: los nobles y los aristócratas, y más tarde la burguesía, para quienes las depreciaciones periódicas y arbitrarias podrían significar reducciones significativas en la riqueza. A medida que su resistencia a este abuso de poder creció, dio lugar a algunas de las grandes ideas liberales sobre las que se basa la democracia moderna, ideas detrás de la fundación de América y la Revolución Francesa. Ahora, este mismo espíritu de resistencia se encuentra entre los evangelistas de bitcoin.

Mucho antes de que los monarcas europeos medievales incluso tuvieran monedas para jugar, los emperadores chinos estaban llevando dinero a su siguiente fase de desarrollo tecnológico. En el siglo IX d. C., cuando regiones como Szechuan experimentaron escasez del bronce que habían usado para las monedas, los funcionarios del gobierno comenzaron a experimentar con cartas de crédito que funcionaban como una forma de papel moneda. Luego, en 1023, la dinastía Song emitió billetes en toda regla por todo el reino.

Siglos antes, China ya había replanteado la posición intelectual de que el dinero era parte de la "maquinaria" del gobierno, como lo expresan los eruditos imperiales. Lo describieron como un medio "para preservar la riqueza y los bienes y así regular las actividades productivas de la gente, a partir de la cual trajeron la paz y el orden al Reino Subcelestial". Esto es diametralmente opuesto a la visión de los commodities sobre el dinero. Pero no está lejos del enfoque de los banqueros centrales modernos para la administración del suministro de dinero. La diferencia es que la responsabilidad de los gobernantes chinos no provino de la legislación, sino de un código moral hecho posible por la visión confuciana del emperador como el vértice benévolo de una sociedad coherente del "Reino Medio". Hoy, China lidia con la competencia de su moneda soberana, el yuan, debido tanto a la demanda de sus ciudadanos de monedas extranjeras como el dólar como a una amenaza incipiente pero potencialmente importante de las monedas digitales privadas como el bitcoin. A medida que navega por estos cambios y se ejerce en el escenario económico mundial, los líderes del país siguen pareciendo constreñidos por este antiguo concepto de dinero estatal, que en las sociedades modernas ha dejado de parecer tan esclarecido.

En Europa, la lucha entre el sector privado y el público por el control del dinero tiene una historia mucho más profunda. Si bien muchos se quejaron de la degradación constante de la moneda por parte del soberano, algunos desarrollaron soluciones alternativas que crearon dinero privado de facto.

El más impresionante de ellos fue el écu de marc, una forma de moneda desarrollada y utilizada por los banqueros mercantes que surgieron del Renacimiento italiano y que les permitió expandir sus negocios a nivel internacional. Con base en un tipo de cambio acordado conjuntamente por los comerciantes, el écu de orc permitió el intercambio de letras de cambio de diferentes bancos en diferentes países. Los soberanos de cada país mantuvieron un control estricto sobre sus monedas, pero esta clase de bancos estaba desarrollando sus propios intercambios internacionales a través de la maravilla de la creación de crédito. Los proyectos de ley financiaban los envíos, digamos de zapatos fabricados en Venecia a un importador en Brujas, que enriquecían

al fabricante, pero el verdadero beneficio estaba en negociar el papel, una lección que pasaría de generación en generación hasta el día de hoy. Por primera vez, una comunidad del sector privado había creado una máquina de creación de dinero de facto. Esta amenaza directa a la soberanía de los monarcas dio lugar a un choque político ya que los reyes y reinas de Europa temían que sus poderes de monopolio estuvieran siendo erosionados.

Pero los banqueros no querían el poder político per se. Eran hombres de negocios pragmáticos, como demostrarían ser durante siglos después. Utilizarían el apalancamiento del dinero privado para negociar acuerdos con los gobiernos, a veces como una amenaza, pero sobre todo para avanzar y alcanzar una mayor riqueza.

Esta negociación entre el soberano y estos nuevos generadores privados de dinero encontraría su máxima expresión en la carta real que fundó el Banco de Inglaterra en 1694. El BOE, como los operadores de bonos en la ciudad de Londres ahora lo llaman, se formó a instancias de King Guillermo III, que quería construir una armada de clase mundial para enfrentarse a Francia, luego la potencia dominante en alta mar. El banco de propiedad privada -el BOE no fue nacionalizado hasta después de la Segunda Guerra Mundial- le otorgaría a la Corona £ 1.2 millones, una suma masiva para su tiempo, y podría emitir billetes de banco contra esa deuda, efectivamente relegando el dinero. Luego, para dar el valor de los billetes como una moneda de facto, el soberano acordó aceptarlos en el pago de los impuestos. De una sola vez, el acuerdo creó una forma de papel moneda efectivamente respaldada por la banca soberana establecida de reserva fraccionaria -un principio rector de la banca moderna que permite a los bancos regulados retener la mayor parte del dinero que captan como depósitos- y concibió la idea de un banco central. El Banco de Inglaterra, en efecto, recibió una licencia para imprimir dinero.

Este fue el comienzo de la banca moderna, y tuvo un profundo impacto en la economía de Inglaterra. La nueva arquitectura financiera no solo ayudó al reino a desarrollar una flota naval de primera clase con la que gobernaría el mundo de un polo a otro, sino que también financió la revolución industrial. El crédito bancario efectivamente se convirtió en dinero, ya que se consideró respaldado por el soberano. Esta nueva definición de dinero ha prevalecido desde entonces. Finalmente, el nuevo sistema británico se extendió hasta el punto en que los ciudadanos comunes tenían cuentas de cheques y las compañías podían recurrir a todo tipo de instrumentos de crédito bancarios para financiar todo, desde operaciones cotidianas hasta proyectos a gran escala. Con los bancos ahora capaces de prestar sus buenos nombres a un prestatario como garantes, estos instrumentos se convirtieron en negociables, lo que dio lugar rápidamente a un mercado de bonos.

Este salto financiero dio un impulso exponencial a la liquidez en la economía, pero también a los riesgos. Si bien creó perspectivas de emprendimiento y creación de capital nunca antes imaginadas, también dio lugar a lo que ahora llamamos riesgo sistémico. Las pérdidas en una institución podrían extenderse y desestabilizar a muchas otras a través de las interconexiones del sistema financiero. Hizo que el sistema fuera vulnerable a los cambios en ese bien social tan importante: la confianza. La red en constante expansión de las relaciones de crédito interconectadas significaba que las fábricas textiles podrían financiar su expansión y, más tarde, se podían construir máquinas de vapor, pero no todas las fábricas textiles ganaban dinero y no todos los empresarios eran buenos para sus deudas. Si bien los incumplimientos de la deuda y las bancarrotas en forma aislada eran una parte normal de la asunción de riesgos, una vez que el sistema financiero se interrelacionó, podrían tener efectos de dominó. Si un prestamista comenzó a preocuparse de que un deudor grande no cumpliera con sus pagos, ese prestamista podría retener fondos de otros prestatarios, que ahora enfrentarían problemas de financiamiento, generando inquietudes aún más amplias. Así, la confianza pública endeble podría colapsar. Cuando se evaporó, el crédito podría agotarse repentinamente, dejando a los deudores

perfectamente solventes incapaces de pagar sus préstamos, lo que a su vez debilitaría las finanzas de sus acreedores, agotando aún más el fondo público de confianza. Así es como se hicieron las crisis financieras. El dinero había sido liberado, pero también se había vuelto más peligroso.

Esta inestabilidad financiera provocó feroces debates sobre cómo controlarla y sobre cómo definir la naturaleza misma del dinero. Los debates continuarán a lo largo del tiempo y darán forma a nuestros modernos sistemas monetarios y financieros. Todo se redujo a diferentes puntos de vista sobre la mejor manera de proteger la confianza en el sistema monetario.

Por un lado, los creyentes estaban sentados en oro. Basado en las ideas de pensadores liberales como el gran filósofo inglés John Locke, el patrón oro fue promulgado a fines del siglo XVII. Las personas sentían que era necesario vincular el dinero a esta cosa tangible para evitar que los gobiernos y sus nuevos socios en un sector bancario con fines lucrativos destruyeran el dinero del público. El modelo logró mantener baja la inflación, lo que ayudó a proteger los ahorros de los ricos. Sin embargo, las restricciones monetarias y el elevado valor del oro generalmente también llevaron a la gente a acumular dinero en las crisis, lo que detuvo el crecimiento del crédito, generó bancarrotas y llevó al desempleo. En esos momentos, las mayores víctimas eran inevitablemente los pobres.

A medida que los sistemas financieros se tambaleaban de una crisis a otra, surgió una concepción competitiva de lo que constituía la oferta monetaria y de lo que la hizo crecer o contraerse. No se centró en cómo restringir la capacidad de un gobierno de emitir moneda, sino en cómo administrar a los bancos en su papel único como creadores de dinero privado con crédito. Encabezado por Walter Bagehot, el editor de The Economist del siglo XIX, este pensamiento condujo al desarrollo de la banca central moderna. Respaldados por soberanos que nunca podrían ir a la quiebra, los bancos centrales como el Banco de Inglaterra serían el "prestamista de última instancia" para superar las crisis de confianza. Acordarían otorgar libremente préstamos a los bancos solventes si su acceso a la liquidez se agotara en períodos de tensión financiera. Si bien la regla de Bagehot era que tales préstamos tendrían una tasa de interés multa y se garantizarían con una buena garantía, el compromiso convirtió a los bancos centrales en un respaldo crítico para ayudar a superar los pánicos financieros. El estándar de oro aún existía, pero este nuevo y expansivo rol para los bancos centrales alarmó a sus defensores, quienes sentían aversión por el poder bancario desenfrenado y la deuda desenfrenada.

Tales preocupaciones sonaron fuertes en los Estados Unidos y retrasaron la entrada al juego de la banca central. El país atravesó un siglo y medio de cambios en los regímenes monetarios, a veces emitidos de manera centralizada, otras veces con monedas múltiples y en competencia que circulan bajo emisión de bancos comerciales bajo diversos acuerdos estatales y federales. Finalmente, el dólar se volvió dominante, pero no fue hasta una serie de severos pánicos financieros a fines del siglo XIX y principios del siglo XX que los estadounidenses decidieron que necesitaban un banco central; La Reserva Federal se fundó en 1913. Cien años después, la Reserva Federal sigue siendo motivo de controversia y burla en algunos sectores, atribuida por sus detractores a la creación de burbujas de activos e inflación, pero aplaudida por sus partidarios, que afirman, por ejemplo, que sin sus intervenciones masivas la crisis de 2008-9 hubiera sido mucho peor.

Claramente, el récord de la Fed en mantener el sistema financiero en línea recta no es perfecto. Anexo A: la Gran Depresión. Muestra B: Lehman Brothers. Aún así, el siglo XX también ha mostrado los peligros de restringir la discreción del banco central. Durante la Depresión, el patrón oro afectó las manos de la Fed en el peor momento al limitar su capacidad de crear nuevos fondos y compensar la aversión de un sector bancario congelado a emitir préstamos. Esto exacerbó la recesión. Eventualmente, la paridad de oro fue abandonada, liberando a los bancos centrales de

esa camisa de fuerza y ayudando a restaurar la liquidez de una economía global hambrienta de dinero.

Después de la Segunda Guerra Mundial, los gobiernos nuevamente profesaron un anhelo de un ancla monetaria firme y, en particular, un polo central de estabilidad para una economía internacional angustiada. Gran Bretaña, dirigida por el economista John Maynard Keynes, quería una solución internacional que fuera administrada por el recién creado Fondo Monetario Internacional. Pero al final, los Estados Unidos, como la única potencia importante no devastada por la guerra y con su moneda ahora dominante globalmente, tomaron las decisiones. El dólar de EE. UU. Se convirtió en el polo central alrededor del cual funcionaría la economía global. Lo sigue siendo hoy.

El pacto firmado en la Conferencia de Bretton Woods en 1944 replicó el dólar al oro y luego hizo que el resto del mundo fijara sus monedas al dólar. A los gobiernos extranjeros que tienen reservas en dólares se les otorgó el derecho de canjearlos en oro a una tasa fija. Funcionó como un estabilizador financiero durante dos décadas y media, pero a fines de la década de 1960 las propias limitaciones del sistema, en este caso impuestas directamente a la Fed, lo hicieron insostenible. Estados Unidos, obstaculizado por el costo de la guerra de Vietnam e incapaz de competir con productores extranjeros más baratos, no pudo traer suficientes divisas para reabastecer sus reservas de oro y así comenzó a quedarse sin ellas cuando países como Francia exigieron que su los dólares se canjean por el metal precioso. Sintiéndose atrapado, el presidente Richard Nixon dio el paso deslumbrante el 15 de agosto de 1971, de sacar al dólar de la paridad de oro. Lo hizo con una orden ejecutiva diseñada en consulta con solo un puñado de miembros del Tesoro, la Reserva Federal y la Casa Blanca.

El "Choque de Nixon" dejó sin sentido el acuerdo de Bretton Woods. Para 1973, una vez que cada país había tomado su moneda del par dólar, el pacto estaba muerto, un cambio radical. Los gobiernos ahora pueden decidir qué tan grande o pequeño debe ser el suministro de dinero de su país. Finalmente, al parecer, el momento de los chartalistas había llegado. En esta nueva era de monedas fiduciarias, la confianza en el dinero se convertiría en algo relativo y fluctuante: ¿Confías en el dólar más que en la libra, o viceversa?

El movimiento audaz de Nixon tuvo un efecto deseado: redujo la tasa de cambio del dólar y provocó un resurgimiento en las exportaciones de los EE. UU. También creó nuevas oportunidades enormes para que Wall Street desarrolle el comercio de divisas. Ahora que el dólar ya no estaba vinculado al oro, los bancos podrían llevar su negocio de creación de crédito a nivel mundial, preparando el escenario para la globalización de la economía mundial. También allanó el camino a los megabancos multinacionales que se volverían demasiado grandes para fallar... y todos los problemas que estos crearían.

La feliz experiencia de la reactivación posterior a 1971 de las manufacturas estadounidenses se vio empañada rápidamente por un flagelo nuevo y totalmente predecible. Junto con el bloqueo petrolero impuesto por las naciones exportadoras de petróleo en 1973, el dólar más débil y desquiciado generó inmediatamente la inflación; a medida que se hundía el valor de la moneda más importante del mundo, aumentaba el precio de todos los bienes y servicios que compraba. (Siempre es útil, creemos, recordar que los precios son conceptos bidireccionales, existe el valor de un bien en términos de dólares, pero también existe el valor de un dólar en términos de cuánto de bueno puede comprar. el valor de uno cae, el otro, por definición, debe subir. Esa es la esencia de la inflación.) Esta vez, el brote inflacionario estuvo acompañado por un alto desempleo, confundiendo a los economistas y agregando una nueva y fea palabra a su léxico: la estanflación.

Los precios furiosos continuaron a lo largo de la década de 1970, allanando el camino para un nuevo héroe financiero: Paul Volcker, de dos metros y medio. El combativo presidente de la Reserva Federal prometió romper la inflación, incluso si eso significaba llevar a la economía de regreso a la recesión, y con una serie de tremendos aumentos en las tasas de interés, eso es exactamente lo que hizo. Los recuerdos de ese período, donde la inflación erosionó drásticamente el valor de los dólares en los bolsillos de las personas y los obligó a una dolorosa contracción económica, son tan fuertes entre una cierta generación que alimentan el atractivo de las "monedas" independientes y escasas como el oro. y, como veremos, bitcoin.

Después del duro amor de Volcker, las cosas mejoraron enormemente, al menos por un tiempo. Un período conocido como la Gran Moderación se estableció en los países industrializados, con una inflación baja y predecible y un crecimiento constante marcado únicamente por la recesión ocasional y de corta duración. Europa se embarcó en un nuevo experimento verdaderamente audaz para crear una unión monetaria, una que durante los primeros diez años de su existencia parecía ser un éxito desgarrador, ya que el euro transmitió milagrosamente la calificación crediticia de Alemania a los países una vez atrasados como Irlanda y España, que disfrutó de una gran afluencia de capital y un auge inmobiliario sin precedentes. Los mercados emergentes como Brasil, Rusia e Indonesia tuvieron una avalancha de inversiones, aunque teñidas de crisis periódicas. Este fue el valiente nuevo mundo de las finanzas globales de moneda fiduciaria. Pero, como ahora sabemos, contenía un defecto destructivo.

En Wall Street, las nuevas tecnologías y un mantra de desregulación alentado por la aparente victoria del libre mercado sobre el comunismo impulsaron una máquina de ingeniería financiera a toda marcha. Aquí los gremlins estaban siendo eclosionados. Todo se veía bien en el frente macroeconómico: la inflación era baja, el crecimiento sólido, pero los economistas se centraban en las cosas equivocadas. La verdadera acumulación de riesgos no apareció en los números económicos principales. Diablos, los riesgos no estaban ni en el sistema bancario de rutina de depósitos y préstamos residenciales y comerciales. Se estaban escondiendo en un reino oscuro y difícil de comprender conocido como el sistema bancario en la sombra.

Allí, como ahora sabemos, grupos de hipotecas extrañamente agrupados y contratos de derivados de crédito, todos con un valor nominal en cientos de billones de dólares, dejaron a los fondos de cobertura, bancos, fondos de pensiones y otras instituciones enganchados entre sí en una red compleja y entrelazada que nadie podría esperar comprender. Como si aprendiera de los banqueros mercantes renacentistas, Wall Street había vuelto a encontrar una manera efectiva de tomar dinero soberano y multiplicarlo muchas veces a través de una forma de dinero privado basado en la deuda. Pero estaba sucediendo en un área que estaba mucho menos regulada que el sistema bancario tradicional. Cuando finalmente se dio cuenta de lo importante que era este sistema de sombras, ya era demasiado tarde. Con el colapso de Lehman Brothers, este frágil edificio se derrumbó.

La Gran Moderación había llevado una maldición. No solo fomentó una falsa sensación de seguridad, sino que también nos hizo olvidar nuestras responsabilidades como sociedad de utilizar nuestro proceso político para cambiar las circunstancias económicas desagradables. Todos, desde los votantes hasta los comerciantes de Wall Street, los congresistas y el presidente quisieron creer que el sistema financiero podría quedar en manos de la Reserva Federal. El muy respetado Paul Volcker dio paso al "maestro", Alan Greenspan, que fue igualmente venerado, hasta que no lo fue. En 1999, hicimos la vista gorda ante la derogación de la Ley Glass-Steagall, que había impedido la fusión de los bancos comerciales y de inversión desde la Depresión, y así bendijo a los emergentes gigantes bancarios para secuestrar cada palanca de poder. Cuando el sistema estalló en sus rostros, tiraron de su última palanca: rescates financiados por los contribuyentes.

Seis años después, todavía estamos muy lejos de solucionar este sistema. Los grupos de presión de Wall Street continúan financiando una gran parte de las necesidades de campaña política del Congreso, lo que les da una influencia indebida sobre la reforma. En parte, eso se debe a que todavía estamos dejando que los banqueros centrales hagan nuestro trabajo sucio, permitiendo que la droga del dinero fácil mantenga las cosas a flote mientras Washington se encierra en un estancamiento acre y egoísta. Las políticas de tasas de interés cero de la Fed y más de $ 3 billones en compras de bonos, junto con acciones similares de sus contrapartes en Europa y Japón, han evitado el desastre. Pero poco se ha hecho para resolver los desequilibrios fiscales a largo plazo en los Estados Unidos o para reestructurar un sistema financiero dominado por los mismos bancos TBTF (demasiado grandes para quebrar). Las fallas estructurales del sistema monetario europeo, con su división insostenible entre sus funciones políticas y monetarias, todavía están firmemente establecidas incluso después de haber estado expuestas cuando Grecia, Irlanda, Portugal, España y luego Italia se sumieron en una crisis a partir de 2010.

Mientras tanto, en una economía totalmente globalizada en la que el dólar es la moneda del mundo, no solo la de los Estados Unidos, también se han expuesto las limitaciones de una política monetaria dictada por imperativos políticos internos. Gran parte del dinero creado por la implacable compra de bonos de la Fed, todo destinado a impulsar la economía estadounidense, simplemente escapó al extranjero para crear burbujas no deseadas en los mercados de vivienda de los países en desarrollo y alimentar tensiones sobre lo que algunos describieron como una "guerra de divisas".. "Todo puede parecer tranquilo, como lo hizo en el momento de escribir estas líneas, pero no se equivoque: nuestro sistema monetario global todavía tiene serios problemas.

La historia del dinero revela un desafío central: cómo diseñar un sistema que facilite de manera más efectiva el intercambio de bienes y servicios y genere prosperidad a la vez que evita que las instituciones que administran ese sistema abusen de la confianza que conlleva ese rol. Queda por ver si bitcoin u otras criptomonedas representan una solución viable a este desafío. El primer paso será que sean aceptados ampliamente como dinero viable; es decir, convertirse en personas de confianza como un medio para expandir el intercambio y la prosperidad.

Un punto de referencia familiar dice que para que una moneda se convierta en dinero debe funcionar como un medio de cambio, una unidad de cuenta y una reserva de valor. Los dólares se pueden usar para comprar cosas en todo el mundo; se usan para medir el valor de casi cualquier cosa; y la mayoría de las personas, si no todas, creen que sus ahorros estarán más o menos protegidos con el tiempo si están denominados en dólares. Mientras que el bitcoin se usa actualmente como medio de intercambio por varias personas para comprar y vender cosas, pocas lo usan como una unidad de cuenta. Los comerciantes que aceptan bitcoins invariablemente enumeran los precios de sus productos en la moneda nacional del país en el que se basan. En cuanto a una reserva de valor, los especuladores que compraron bitcoin con la esperanza de ganar en el futuro ciertamente creen que tiene esta característica, pero para la mayoría de las personas su volatilidad lo impide. El precio de Bitcoin en dólares se elevó 8.500 por ciento en los primeros once meses de 2013, pero luego perdió dos tercios de su valor en los siguientes seis meses. ¿Quién pondría los ahorros de su vida en esa cosa?

Pero la pregunta más importante es si las criptomonedas pueden convertirse en dinero. Ahí es donde debe mantenerse la insistencia de que el dinero debe estar respaldado por algo "real". Lo que importa es si tiene utilidad. En última instancia, ¿mejora nuestra capacidad para participar en el intercambio, el comercio y la interacción humana? En ese aspecto, Bitcoin tiene algo que ofrecer: una notable capacidad para facilitar transferencias de valor a bajo costo y casi instantáneas en cualquier parte del mundo. Creemos que esto eventualmente hará que esta tecnología -si no el bitcoin en sí misma- sea ampliamente solicitada. Quizás entonces se convierta en dinero.

Se podría decir que una moneda es dinero cuando todos aceptan que es dinero. Para lograr esa prueba tautológica bastante difícil, el bitcoin debe atraer a los creyentes. Sus primeros usuarios han empleado estrategias directamente extraídas de nuestra historia monetaria. Estos van desde elegir un símbolo que se asemeje a los de otras monedas -más comúnmente se muestra como una B con líneas de dólar a través de él-, como notó el antropólogo Bill Maurer, imbuyendo la moneda digital del mito del valor físico y tangible al usar el término minería para describir el trabajo realizado para acuñar Bitcoin.

Pero los primeros adoptantes tienen un desafío mayor, y eso es construir una comunidad de usuarios mucho mayor alrededor de bitcoin. La comunidad que ha adoptado Bitcoin, que inicialmente consistía en un mínimo de dos personas, ya ha crecido sustancialmente tanto en números como en motivaciones para abrazarlo. Si aplicamos la visión de los chartalistas de que el dinero es un fenómeno social, entonces esta expansión comunitaria en curso representa nada menos que una moneda que se esfuerza por convertirse en dinero.

Capítulo 2

GÉNESIS

> Lo que se necesita es un sistema de pago electrónico basado en pruebas criptográficas en lugar de confianza.
>
> -Satoshi Nakamoto

El 31 de octubre de 2008, 2:10 p.m., hora de Nueva York. Los varios cientos de miembros de una lista de correo oscura que comprende expertos en criptografía y entusiastas reciben un correo electrónico de alguien que se hace llamar Satoshi Nakamoto. * "He estado trabajando en un nuevo sistema de efectivo electrónico que es totalmente par a par, sin confianza tercero ", escribe rotundamente. Su breve texto los dirige a un libro blanco de nueve páginas publicado en un nuevo sitio web que había registrado dos meses antes, que describe un sistema de moneda al que llama bitcoin.

El documento explica, en texto claro pero seco acompañado de ilustraciones, ecuaciones, códigos y notas a pie de página, este sistema de "moneda" digital. Ciertamente no es una moneda ya que casi cualquiera en la sociedad dominante entendería la palabra. "Definimos una moneda electrónica como una cadena de firmas digitales", escribe Nakamoto. "Cada propietario transfiere la moneda a la siguiente al firmar digitalmente un hash de la transacción anterior y la clave pública del próximo propietario y agregarlas al final de la moneda. Un beneficiario puede verificar las firmas para verificar la cadena de propiedad. "(Si, como la mayoría de las personas, usted no está familiarizado con la ciencia del cifrado de la computadora, eso puede sonar como un galimatías, aunque para cuando haya terminado con este libro esperamos que esas frases parezcan menos desalentadoras, pero era algo familiar para los entusiastas de la criptografía a los que apuntaba Nakamoto.) Explica las diversas características, incluida la forma inteligente en que se encuentra con la necesidad de un intermediario externo, un banco u otra entidad financiera. institución, para respaldar y garantizar las transacciones.

Está describiendo un sistema de intercambio en línea que usa encriptación para permitir que dos partes intercambien tokens de valor sin divulgar información vulnerable sobre ellos mismos o sus cuentas financieras. Su objetivo es operar fuera de la estructura bancaria tradicional y permite a las personas enviar dinero digital directamente entre sí, de igual a igual, ya que se conoce el concepto de comercio sin intermediarios. No se necesitan bancos ni compañías de tarjetas de crédito. No hay procesadores de pagos u otros terceros "de confianza" involucrados. En efecto, es una forma de efectivo digital. La revolución de bitcoin ha comenzado. La mayoría de los primeros invitados a unirse a él no se dan cuenta.

Entre la comunidad de criptografía muy unida invitada a revisar el trabajo de Nakamoto había miembros del movimiento Cypherpunk, una asociación informal de activistas con vocación tecnológica que habían ganado notoriedad en la década de 1990 con sus esfuerzos por utilizar herramientas de privacidad criptográfica para forzar un cambio político y cultural radical.. Este esfuerzo dio algunos frutos: el cruzado de transparencia Julian Assange y su organización activista de publicación, WikiLeaks, surgieron de este movimiento. Para los Cypherpunks, la idea de un sistema de efectivo digital anónimo no era nada nuevo. Había sido una de sus primeras grandes ideas, pero nadie la había convertido en algo viable. Varios habían intentado construir sistemas digitales de efectivo, uno incluso se había acercado tentadoramente, pero finalmente ningún sistema había alcanzado ningún tipo de masa crítica, y la causa se había esfumado.

A primera vista, bitcoin parecía similar a sus predecesores. Su protocolo de software, el conjunto guía de instrucciones de comunicación que sustentan el sistema, siguió las mismas ideas básicas de esas iteraciones anteriores. Al igual que ellos, utilizó el cifrado de clave pública para permitir a las personas compartir de forma segura valiosas cadenas de código. Una transferencia podría tener lugar cada vez que una persona usara una clave privada secreta, una cadena de código celosamente guardado, para autenticar digitalmente una clave emparejada, públicamente disponible, adjunta a una tienda de la moneda. También, al igual que sus predecesores, buscó establecer un conjunto de reglas irrompibles mediante las cuales una red descentralizada de computadoras colaborara para mantener la integridad del sistema monetario. Del mismo modo, cualquier persona con una computadora podría formar parte de la red, ayudar a mantener su integridad y pagar y recibir pagos en una moneda digital común. Persiguió el mismo objetivo que sus predecesores: prescindir del modelo existente para pagos globales y emisión de divisas y reemplazarlo por uno en el que las computadoras de propiedad individual, en lugar de los bancos, estuvieran a cargo de mantener el sistema honesto.

Todos los demás intentos de hacer esto habían fallado. ¿Había alguna razón para creer que el sistema de Nakamoto sería mejor para generar un atractivo masivo? La mayoría de los miembros del grupo que se molestaron en leer el libro blanco no vieron esa razón. La respuesta desdeñosa del programador de San Francisco Ray Dillinger reflejó los puntos de vista de muchos dentro de la comunidad cínica: "La gente no tendrá activos en esta moneda altamente inflacionaria si pueden ayudarla". * James A. Donald, un entusiasta de la criptografía que escribe una inclinación libertaria blog, aplaudió el intento de alcanzar el "viejo sueño de Cypherpunk" y permitió que el mundo "necesitara mucho ese sistema". Pero predijo que el sistema de Nakamoto nunca sería lo suficientemente robusto o escalable para soportar transacciones de "cientos de millones". ". John Levine, suscriptor de la lista de criptografía mejor conocido como el autor del libro The Internet for Dummies, dijo que los piratas informáticos serían en última instancia el" asesino "del sistema de Nakamoto ya que" los chicos buenos tienen mucha menos potencia de cómputo que los malos ". chicos ".

Nakamoto no se inmutó. Sabía que el sistema contenía dos grandes avances: un diario universal inviolable, al que denominó blockchain, contra el cual cualquiera podría verificar la validez de las transacciones, así como un conjunto único de incentivos monetarios para alentar a los propietarios de computadoras de la red a mantener ese libro -hasta la fecha. Esto es lo que mantendría su sistema honesto mientras lucha contra los piratas informáticos.

Nakamoto ya había creado un nuevo sitio web en bitcoin.org, un dominio que había comprado en el momento del lanzamiento de su libro blanco. Pero para llevar su sistema al siguiente nivel, sabía que tendría que poner en marcha el programa de software que también había desarrollado discretamente y así generar los primeros bitcoins. Cuando llega el año nuevo, enciende el algoritmo de la computadora y comienza a "extraer" su nueva moneda. Como veremos en el capítulo 5, la minería es un nombre poco apropiado porque la actividad más importante que hacen estos "mineros" o nodos en la red es confirmar las transacciones. Los bitcoins "minados" son una recompensa por ser el primer minero en resolver un rompecabezas matemáticamente complejo generado aleatoriamente que debe completarse antes de que las transacciones puedan confirmarse. Esa recompensa se vuelve cada vez más difícil de lograr a medida que los mineros agregan cada vez más poder computacional a la red.

Nakamoto, "Node Number One", cargó el software en su computadora de escritorio y comenzó el programa, su interfaz simple que muestra los resultados de sus esfuerzos en una grilla. Como no había nadie más en la red que él, sin una gran cantidad de transacciones de terceros para trabajar y confirmar, de hecho ninguna transacción en absoluto, simplemente podía dejar que su PC

permaneciera allí y entregar bitcoins en la "billetera" digital que él había creado para sí mismo. Hoy en día, la red está compuesta por usuarios de todo el mundo, y la dificultad computacional en la minería ha aumentado tanto que requiere vastas y costosas máquinas dedicadas en almacenes especiales para hacer el trabajo de forma rentable. Pero en aquellos primeros días de 2009, producir bitcoins para su propia cuenta era tan fácil como descargar una copia de, digamos, Microsoft Outlook y ejecutarla en un escritorio.

Al encender el software, Nakamoto creó el Bloque Génesis, el primer "bloque" de cincuenta monedas de bitcoins. Durante los siguientes seis días, extraería muchas bitcoins más: hasta cuarenta y tres mil si el software funcionaba según su cronograma intrínseco de un bloque cada diez minutos. A partir de agosto de 2014, un acarreo de ese tamaño tendría un valor de aproximadamente $ 21 millones, pero en aquel entonces valían exactamente cero, ya que Nakamoto no tenía a nadie más a quien transferirlos, no había forma de "gastarlos". Si el sello distintivo de una moneda es la utilidad, en este punto inicial, bitcoin no tenía absolutamente nada. Tenía que hacer que otros se unieran.

Entonces, seis días después del Bloque Génesis, Nakamoto regresó a la misma lista de correo de criptografía y les dijo a sus lectores que el programa estaba listo: "Anunciando el primer lanzamiento de bitcoin, un nuevo sistema de efectivo electrónico que utiliza una red de igual a igual. para evitar el doble gasto ".

Y luego el argumento de venta: "Está completamente descentralizado sin servidor ni autoridad central".

Las personas en esa lista, que habían escuchado reclamos como este antes, aún no tenían evidencia de que Nakamoto hubiera superado el desafío que había derribado a sus predecesores: evitar las transacciones fraudulentas, el llamado problema de doble gasto, cuando no se cobraba ninguna autoridad central con transacciones de autenticación. Por mucho que esta gente odiara admitirlo, parecía necesitar una autoridad central como un banco para hacer eso.

Una vez más, la respuesta a las insinuaciones de Nakamoto fue tibia. Algunos se enfocaron de inmediato en una crítica al bitcoin que se haría común: la energía que tomaría cosechar "bitbux" costaría más de lo que valían, sin mencionar que sería desastrosa para el medioambiente. Jonathan Thornburg, profesor de astronomía en la Universidad de Indiana, vio un gran desafío político: "Ningún gobierno importante es probable que permita que el bitcoin en su forma actual opere a gran escala".

Incluso dentro de un grupo tan pequeño, las personas en esa lista de correo inicial constituían un grupo de lectores ecléctico: un astrofísico, un ingeniero de software, un asesor de seguridad y un escritor de ciencia ficción. No estaban todos obsesionados con la idea del efectivo digital. Algunos se centraron en cuestiones de seguridad informática. Un grupo de ellos intentaba perfeccionar el correo electrónico encriptado. La mayoría simplemente no estaba interesada en lo que parecía ser una repetición de una vieja idea fallida.

"Todos decíamos, 'Uh-huh, sí, claro, está bien'", dijo Levine, riendo, cinco años después. "No teníamos idea de que el bitcoin sería un gran negocio". De hecho, hasta que le pedimos que reflexionara sobre ese intercambio, Levine había olvidado que había estado en la lista de correo, olvidó que estaba presente en el lanzamiento de Bitcoin, y olvidado que estaba entre aquellos que dudaban del ahora legendario y todavía no identificado Satoshi Nakamoto. Aún así, puede consolarse porque él no era el único. Lo que está claro del debate es que muchos sintieron que Nakamoto estaba buscando un hueso que hace mucho tiempo habían dejado de encontrar.

Probablemente no ayudó que nadie tuviera idea de quién era Nakamoto. Los miembros de Cypherpunks y las comunidades de criptografía estaban preocupados por el anonimato, pero no eran anónimos entre sí. La mayoría de ellos usaba sus nombres reales, y los que no lo eran eran conocidos por su apodo. Al igual que en sus contrapartes del mundo real, en las comunidades en línea las reputaciones se construyen mediante una participación sostenida. Antes de octubre de 2008, nadie había oído hablar de Satoshi Nakamoto, simplemente se presentó un día, lo que puede ser una de las razones por las que no fue tomado en serio. "Era solo un nombre en una lista de correo", señala Russ Nelson, un ingeniero de la Universidad de Clarkson, que recuerda que en ese momento no tenía la impresión de si el bitcoin tendría éxito o el impacto que tendría.

"Puede tener sentido solo conseguir algo en caso de que se ponga de moda", sugirió Nakamoto a un observador decepcionado. A medida que el marketing va, este fue un tono tenue, pero habló de un objetivo crucial. La obra maestra de Nakamoto no llegaría a nada a menos que otros la usaran. Tenía que comenzar en algún lado. Nakamoto había sido el primer adoptante de Bitcoin. Ahora, él necesitaba un segundo. Afortunadamente para él, y para bitcoin, alguien levantó la mano.

Hal Finney, que entonces tenía cincuenta y tres años, era un importante desarrollador de PGP Corp., una compañía fundada por Phil Zimmermann, un criptoactivo legendario cuyo irónico software Pretty Good Privacy ayudó a popularizar los sistemas de encriptación de clave pública para el correo electrónico. Primer miembro prominente del movimiento Cypherpunk, a Finney se le atribuyen diversas innovaciones criptográficas, incluidos los remailers anónimos, que permiten a las personas enviar correos electrónicos sin revelar sus orígenes. En 2004, Finney había presentado su propia versión de dinero electrónico. Al igual que el bitcoin, el modelo de Finney utilizó las funciones de codificación de "prueba de trabajo" introducidas en 1997 por el criptógrafo británico Adam Back para verificar y cuantificar la potencia de procesamiento necesaria para crear y respaldar el valor de una moneda digital. (Este es un concepto crítico, aunque bastante complicado, para comprender cómo los propietarios de computadoras "minan" las criptomonedas, las hacen existir y les infunden valor al gastar recursos en su creación, de ahí la "prueba de trabajo". Por ahora, es suficiente para comprender el concepto básico: a cambio del valioso privilegio de crear una moneda, se debe requerir una computadora para realizar una tarea, en este caso una difícil tarea computacional. Volveremos sobre ella, suavemente, cuando exploremos cómo las criptomonedas funcionan en el capítulo 5)

La conexión de Finney con la criptografía digital lo ubica dentro del esfuerzo científico central detrás de bitcoin y todas las criptomonedas, así como con sus fundamentos filosóficos. Durante gran parte de la historia, desde sus inicios en el antiguo Egipto, la esencia de la criptografía -que toma su nombre de las palabras griegas para "oculto" y "escritura" -lay en el lenguaje de codificación para mantener en secreto un mensaje. Los sistemas de criptografía fueron utilizados principalmente por gobiernos y militares para proteger los secretos de estado y engañar a los enemigos. Pero en la era digital, cuando la ciencia se mejoró exponencialmente mediante máquinas informáticas que podían desarrollar algoritmos elaborados para realizar tareas de encriptación cada vez más complejas, encontró una aplicación mucho más amplia, evolucionando hacia una forma de proteger la información personal, corporativa y gubernamental. En esta era, la fraternidad de criptógrafos desarrolló tensiones políticas variables, si no divergentes. Algunos tratan la práctica como una empresa comercial, encontrando empleo en empresas y en el gobierno. Pero otros parecen encontrarlo como un llamado más elevado, asociándolo con una lucha por la libertad y los derechos individuales. Los Cypherpunks anárquicos y de inspiración libertaria se contaban entre los más radicales de estos activistas; otros eran más tenues y comunales. Pero todos los que utilizaron sus conocimientos en un intento de promulgar cambios sociales vieron la criptografía como una herramienta para mejorar la privacidad individual y para cambiar el poder de las grandes instituciones centrales a los seres humanos que viven en su órbita. Hal Finney pertenecía a esta tradición: su exploración previa de la criptomoneda lo demostró. Lo

mismo hizo Satoshi Nakamoto, al menos por lo que sabemos de sus escritos. También lo hace bitcoin.

Por lo tanto, tal vez, naturalmente, Finney estaba intrigado por el sistema de Nakamoto. Pronto le escribió a este recién llegado desconocido a la lista de correo a través de la dirección de correo electrónico que Nakamoto le había proporcionado. (El fundador de bitcoin ha utilizado públicamente al menos tres direcciones de correo electrónico, naturalmente, todas están cifradas y no se pueden rastrear a la persona que las creó). Para el 10 de enero de 2009, la pareja había comenzado a trabajar juntas en lo que sería un semana, proyecto intensivo. Colaborarían y compartirían notas por correo electrónico mientras trataban de poner en marcha el protocolo Bitcoin. Siguiendo las instrucciones del fundador, Finney descargó el software, creó una billetera y comenzó a extraer un bloque de cincuenta bitcoins. Eso lo convirtió en el Nodo Número Dos. Como prueba, Nakamoto también transfirió una tienda de diez monedas a la billetera de su nuevo corresponsal. Finney se convirtió en la primera persona en recibir bitcoins de otra persona.

Los primeros intercambios de correo electrónico entre este par proporcionan una mirada fascinante al amanecer de Bitcoin. Al mismo tiempo, llama la atención lo mecánicas que son sus interacciones. No se intercambia información personal, no hay detalles que puedan proporcionar pistas sobre la identidad de Nakamoto, solo el intercambio de dos codificadores experimentados que también entienden los sistemas monetarios.

Finney comenzó tratando de descargar la versión 0.1.0 del software de bitcoin, y se bloqueó. Su interlocutor estaba sorprendido, no había experimentado tales problemas. Sin embargo, Nakamoto volvió a entrar, "reprodujo el error", cuando colocó una respuesta por correo electrónico y encontró las líneas de código defectuosas. "Fue absolutamente el último pedazo de código para entrar", escribió. "Estoy realmente consternado por tener este problema después de todas las pruebas de estrés".

Presionaron a través de la versión 0.1.2, encontrando un problema cuando el "nodo" de Finney dejó de responder a los mensajes de la computadora de Nakamoto, lo que requirió más depuración. Avanzaba y retrocedía, con ambos corriendo sus computadoras pesadamente, empujando el nuevo software para encontrar sus fallas. La versión 0.1.2 se estrelló, la versión 0.1.3 se colgó. Nakamoto estaba revisando el código, encontrando problemas, recibiendo mensajes de error, y luego reescribiendo y rediseñando el código una vez más.

"Definitivamente parece que 0.1.3 lo resolvió", escribe Nakamoto después de otro choque. Luego hace un comentario interesante que es difícil de descifrar sin él o Finney para proporcionar un contexto, pero que podría, intrigantemente, sugerir que otros habían descargado el software en secreto y también estaban tratando de extraer bitcoin, pero no se estaban comunicando con estos dos primeros usuarios. "Se estaba haciendo así que había tantos nodos zombies, estaba teniendo dificultades para obtener una respuesta a cualquiera de mis mensajes", dijo Nakamoto. Entonces el sistema colapsó nuevamente.

Finney mantuvo su computadora extrayendo bitcoins durante una semana más o menos y terminó con un alijo de alrededor de mil monedas. Pero el software no era un programa de Microsoft Word. Requería datos constantes e intensos, y temía que pudiera dañar su computadora. Además, el ruidoso ventilador del dispositivo, empujado al extremo, comenzaba a ponerle de los nervios. Entonces dejó de minar y nunca volvió a intentarlo.

En marzo de 2013, cuando sus monedas valían alrededor de $ 60,000, Finney miraría atrás en su decisión de dejar de extraer: "En retrospectiva, desearía haberlo conservado por más tiempo, pero por otro lado tuve la extraordinaria suerte de estar allí en el comenzando. Es una de esas cosas

medio llenas, medio vacías... Esperemos que [esas monedas] valen algo para mis herederos ". El futuro patrimonio de Finney se había vuelto importante diez meses después de haber hecho contacto con Nakamoto cuando fue diagnosticado. con ALS: esclerosis lateral amiotrófica, o enfermedad de Lou Gehrig, una afección degenerativa que destruye lentamente el cuerpo. Cuando nos pusimos en contacto con una silla de ruedas, él ya dependía por completo de las máquinas para mantenerlo con vida, y con su esposa, Fran, y su hijo, Jason, por su ayuda con la vida diaria. Luego, en agosto de 2014, murió. Uno de los pioneros de Bitcoin ya no estaba. De acuerdo con sus deseos y con la descripción de Fran Finney de su marido como "siempre ha sido optimista sobre el futuro", el alijo bitcoin de Finney está financiando la congelación criogénica de su cuerpo en una instalación en Arizona, todo con la esperanza de que algún día ser revivido si y cuando ALS sea erradicada.

En verdad, no importa cuántas referencias haga bitcoiners a los eventos de "Big Bang" o "Génesis", este proyecto no explotó en un vacío. Como cualquier invención brillante, está construida sobre las espaldas de los inventores anteriores. Las grandes criptomonedas de escritura pueden rastrear sus raíces a través de siglos de innovaciones que han mejorado la comunicación y el intercambio humano, desde la imprenta hasta el telégrafo y la Internet. Pero, como se señaló anteriormente, el precursor más directo vino de los Cypherpunks. El grupo comenzó a principios de la década de 1990 como una afiliación informal de los asistentes de la criptografía que compartían una preocupación común sobre la creciente erosión de la privacidad y el desempoderamiento individual en la sociedad moderna. (Esto fue mucho antes de que alguien usara el término Big Data, oyó hablar de Edward Snowden, o tuvo la sospecha de que la Agencia de Seguridad Nacional de EE. UU. Estaba espiando a todos). Una de las primeras ideas de este grupo era una moneda digital.

El movimiento fue fundado en septiembre de 1992, cuando una multitud de codificadores de cola de caballo fueron invitados a la casa de Oakland del entusiasta de la criptografía Eric Hughes. En los Estados Unidos, el gobernador de Arkansas, Bill Clinton, estaba a punto de derrotar al presidente George Bush en las elecciones de noviembre, poniendo fin a doce años de gobierno republicano. En Europa, el Tratado de Maastricht se encontraba en medio de una ratificación desordenada y polémica, aunque su aprobación ese año eventualmente conduciría a la formación de la Unión Europea en 1993 y del euro seis años después. La fundación de los Cypherpunks también llegó en la cúspide de la era de Internet, con la sede de facto del grupo apropiadamente ubicada en el Área de la Bahía de San Francisco, que se convertiría en el centro de la revolución en línea. El correo electrónico y los sitios web aún no se habían generalizado, pero Apple y Microsoft estaban sentando las bases necesarias a medida que las computadoras personales nuevas y fáciles de usar encontraban en los hogares estadounidenses. El momento era propicio para este nuevo movimiento, una rama evolutiva de la contracultura de los sesenta, pero uno más singularmente centrado en asuntos de libertad individual que las causas sociales de esa época.

Los codificadores de la reunión inaugural fueron recibidos por Tim May, un barbudo anarco-libertario y ex físico de Intel que, cuando no estaba leyendo o escribiendo ciencia ficción, pasó la mayor parte de su tiempo despierto concibiendo nuevas herramientas criptográficas de rebelión. Puede leer su "Crypto-Anarchist Manifesto", que se inició con una obra de teatro sobre el famoso manifiesto de Karl Marx: "Un fantasma inquieta al mundo moderno, el espectro de la criptoanarquía". El ensayo continuó prediciendo que "al igual que el la tecnología de impresión alteró y redujo el poder de los gremios medievales y la estructura de poder social, así también los métodos criptológicos alterarán fundamentalmente la naturaleza de las corporaciones y la interferencia del gobierno en las transacciones económicas. "Esto, en la mente de estos codificadores, fue todo positivo. Subvertiría el nexo de poder que creían que los bancos centrales y las agencias gubernamentales mantenían al servicio de sus clientes en las empresas estadounidenses. Revalorizaría a los ciudadanos.

El ensayo de May se convertiría en el documento fundador de Cypherpunks. A pesar de sus creencias centrales comunes, eran un grupo ecléctico. Algunos tenían empleos diurnos en firmas tecnológicas de EE. UU. Y usaban identificadores anónimos para mantener separadas sus vidas en línea. Otros, como mayo, abandonaron el empleo general. El nombre del grupo se extrajo en parte del cifrado, que en la criptografía se refiere a un algoritmo utilizado para el cifrado o descifrado, y en parte a un juego de cyberpunk, el género de ciencia ficción y el personaje protagonista genérico popular de esa época. Pero Cypherpunk también tenía la intención de sonar más matizado y sutil, distinguiendo el movimiento detrás del escenario del grupo de los intrépidos hackers de las novelas de William Gibson, aunque no eran menos radicales en su intento de cambio.

Guiados por el principio de que en la era digital proteger la privacidad sería crucial para mantener una sociedad abierta, los Cypherpunks establecieron sus mentes activas para crear herramientas que permitan a las personas mantener el anonimato. Compartirían estas ideas a través de una lista de correo electrónico común, cuyo archivo es ahora un artefacto vital en la historia del activismo criptográfico. Un producto que desarrollaron fue la versión Cypherpunk de un redireccionador de mensajes anónimos, que ocultaba la identidad de una persona que enviaba un correo electrónico e impedía que el destinatario respondiera, todo para impedir que los gobiernos o las corporaciones husmeen en las comunicaciones diarias de las personas. Otros productos tenían objetivos más subversivos, por ejemplo, el audaz proyecto BlackNet de mayo, un precursor de WikiLeaks, que solicitaba información secreta con la promesa de encriptación y pagos en dinero digital imposible de rastrear. Algunos productos fueron francamente atemorizantes. Jim Bell, quien al igual que May era empleado de Intel, propuso un mercado anónimo de asesinatos. La idea era que las personas pudieran contribuir anónimamente a una recompensa que pagarían para matar a una persona influyente en particular, suponiendo que el mercado pondría un mayor precio a las cabezas de aquellos que abusan más atrozmente de una posición de autoridad.

Todo esto, lo bueno, lo malo y lo feo del banco de ideas de Cypherpunks, entraría en la sopa intelectual de la que surgiría el bitcoin. La adopción del anonimato y de los principios libertarios de la libertad de la autoridad central por parte de la moneda y sus partidarios fueron casi una reencarnación de los principios de este movimiento de los noventa. Notablemente, también atraería a algunas de las cepas oscuras y antisociales que corrían a través de la lista de correo de Cypherpunks. En noviembre de 2013, se presentó bitcoin como la unidad de intercambio interna para un nuevo mercado cifrado de asesinatos basado en sitios web creado por alguien bajo el seudónimo samurái de Kuwabatake Sanjuro. Tras su lanzamiento, la figura pública con la mayor recompensa en su cabeza fue el presidente de la Fed, Ben Bernanke.

Pero lo más significativo, al menos en retrospectiva, los propios Cypherpunks fueron algunos de los primeros proveedores de ideas de criptomonedas. En los intercambios en los tableros de anuncios Cypherpunk alrededor de ese momento hay varias referencias a tales ideas y el proyecto ocasional en toda regla. Como se mencionó, Hal Finney incursionó en el diseño de dicho sistema. También lo hizo otro suscriptor de la lista de correo de Cypherpunk a quien Nakamoto se acercaría años más tarde: Wei Dai, un experto en criptografía y entusiasta cuyos intereses van desde las matemáticas hasta la criptografía y la filosofía. Seis años después de esa primera reunión de los Cypherpunks, Dai lanzó dinero b. Al igual que con bitcoin, destacaría las transacciones anónimas punto a punto, y un libro de contabilidad compartido con cada participante en la red mantendría un registro de las transacciones. Por la misma época, Adam Back, otro Cypherpunk, ideó un sistema de prueba de trabajo llamado hashcash. Fue diseñado en respuesta a la primera ola de spam de Internet, cuyos proveedores, irónicamente, habían sido cubiertos por los remailers anónimos desarrollados por Hal Finney y otros. Estos spammers estaban empezando a llenar las cajas de entrada de las personas con anuncios de Viagra y ampliación del pene. La solución de Back era forzar a las computadoras a hacer un trabajo costoso antes de darles permiso para enviar

información, requiriendo que cualquier que intentara inundar una red con mensajes incurriera en costos operativos, todo sin aplicar una tarifa monetaria.

Nakamoto usaría explícitamente el sistema de prueba de trabajo de Back como la base para el programa de dificultad computacional de minería de bitcoins y citaría el trabajo de Wei Dai en su libro blanco. El fundador de bitcoin estaba claramente impresionado por el dinero b, pero estaba decidido a superar sus limitaciones, incluido su sistema punitivo para imponer la honestidad entre la red de propietarios de computadoras. En el modelo de dinero b, cada contribuyente a la red tuvo que depositar dinero en una cuenta especial que podría usarse para multas o recompensas por pruebas de mala conducta. No es difícil imaginar que esta solución tenga inconvenientes para incentivar la cooperación. ¿Cómo puede una comunidad imponer un castigo sin una agencia de ejecución central para hacerlo? ¿Quién juzgaría? La solución de Bitcoin era hacer que todo se tratara de recompensas, no de castigo.

Nakamoto no menciona, sin embargo, el bit-gold, otra criptomoneda desarrollada por Nick Szabo, un científico de la computación, un experto en derecho y un hombre renacentista. Los amplios intereses de Szabo se presentan en su blog Unenumerated, donde un tesoro ecléctico de ensayos se basa en economía, informática, política, antropología y derecho. Wei y Szabo se habían comunicado y trabajado las ideas de los demás. Pero a pesar de que Wei dice que le contó a Nakamoto el proyecto de Szabo, este último nunca se menciona en el libro blanco de bitcoin, ni en los subsiguientes correos electrónicos y publicaciones en el chat de su autor. Eso, junto con un poco de trabajo lingüístico forense que encuentra similitudes entre los estilos de escritura de Szabo y Nakamoto, ha llevado a algunos a especular que el blogger y el fundador de bitcoin presumiblemente pseudónimo son la misma persona. Si las ideas de Szabo, que están moldeadas por una inclinación libertaria común a la subcultura bitcoin, lo conectan directamente con Nakamoto de una forma u otra, merecen reconocimiento dentro del amplio cuerpo de pensamiento intelectual sobre el que se construyó la primera criptomoneda verdaderamente exitosa.

Ninguna de las propuestas de dinero electrónico anteriores al bitcoin estuvo a punto de ser puesta en práctica como las de David Chaum, el criptógrafo altamente innovador e influyente que fue una especie de sumo sacerdote de los Cypherpunks en su apogeo en los años 80 y 90, incluso aunque no compartió sus tendencias anarquistas. Incluso antes de que los Cypherpunks comenzaran, este ex profesor de la Universidad de Nueva York y la Universidad de California en Santa Barbara había reclamado al menos diecisiete patentes, fue el autor de docenas de artículos innovadores sobre el uso de la tecnología digital y la criptografía para revolucionar todo, desde dinero para votar, y fue el fundador de la Asociación Internacional de Investigación Criptológica. La cosmovisión de Chaum evolucionó a través de este período para combinar la desconfianza de un criptógrafo clásico de los sistemas centralizados con una evaluación pragmática de que la única forma de cambiar el mundo era lidiar con los poderes fácticos. Gran parte de lo que se ha utilizado en bitcoin -la idea de un libro de contabilidad universal, de cuentas cifradas y sistemas para evitar el gasto doble- tiene sus primeras huellas en el trabajo de Chaum. Pero lo que más le conocen es la fundación de DigiCash, una compañía que casi incorporó la criptomoneda anónima a la corriente principal, allá por 1990.

Con sede en Ámsterdam, DigiCash extrajo algunas de las ideas innovadoras de Chaum sobre cómo compartir información monetaria, transmitir información de forma inalámbrica y gestionar el grado de cifrado de las identidades de las personas. Surgió con un sistema de moneda digital que en un momento parecía estar a punto de revolucionar el dinero en Europa. La onda cerebral de Chaum era una estructura criptográfica que protegería la identidad del pagador al tiempo que permitía que el pagador identificara irrefutablemente al beneficiario si era necesario. En una entrevista, Chaum nos explicó la gran promesa de esta forma de dinero, una idea que presentó a

los funcionarios del gobierno, los banqueros centrales, los banqueros comerciales, los líderes tecnológicos y los responsables de la política financiera, a cualquiera que los escuchara. Aquí había una forma de acabar con la corrupción, el crimen organizado, los secuestros, las extorsiones y los sobornos. "¿Qué político tomaría un soborno de alguien sabiendo que más tarde podría chantajearlos?", Explicó Chaum. DigiCash compartió algunas de las cualidades de bypass de intermediarios que se encuentran más tarde en bitcoin, el mismo principio de pagos entre pares sin mediación de terceros. Pero el tratamiento único del anonimato de este bitcoin, sin mencionar el enfoque descaradamente político de Chaum, hizo que su proyecto fuera fundamentalmente diferente del modelo que Satoshi Nakamoto presentaría al mundo en la década siguiente. Mientras que los poderes de anonimato de DigiCash eran asimétricos, los bitcoin eran simétricos, lo que permitía que ambos lados de una transacción ocultaran su identidad detrás de un código alfanumérico. Esto permite que Bitcoin funcione como una "moneda pirata", dice ahora Chaum.

A medida que desarrolló sus ideas durante la década de 1990, Chaum buscó deliberadamente comercializarlas a los gobiernos y bancos centrales, un enfoque que puede haber perturbado a algunos de los Cypherpunks anarquistas que se habían posicionado como discípulos de Chaum. El ambicioso criptógrafo no se preocupó. Él razonó que los bancos centrales o sus contrapartes comerciales reguladas centralmente podrían entregar las eficiencias y los imprimaturs oficiales necesarios para convertir DigiCash en la tecnología pionera que merecía convertirse. Lo que es más, podría ganar dinero haciendo eso. Vendería licencias DigiCash a estas instituciones, que emitirían esta nueva forma digital de dinero, denominada en sus monedas nacionales. Los servidores de esas instituciones centrales (los terceros de confianza) confirmarían las transacciones, evitarían el doble gasto y mantendrían el sistema honesto. Esperaba que el hecho de que estas instituciones adoptaran su modelo fomentaría un sistema monetario más honesto y reduciría los costos intermedios, como las tarifas de las tarjetas de crédito. Ese enfoque centrado en el gobierno y en el banco lo separa de los Cypherpunks inclinados a la anarquía de la década de 1990 y de los bitcoiners libertarios de nuestra época. Es por eso que aquellos que creen que David Chaum es Satoshi Nakamoto probablemente estén fuera de lugar.

DigiCash surgió cuando comenzó la revolución informática. Internet aún no era grande, pero las redes empresariales se estaban haciendo cada vez más grandes, y las empresas tendían cables interconectados para conectar sus redes informáticas internas y externas. En este entorno, y con los bancos desplegando redes internacionales de cajeros automáticos y sistemas integrados de contabilidad, muchas mentes líderes en tecnología y finanzas pensaron que el mundo de los pagos estaba maduro para una forma digital de dinero que viajaría a través de estas conexiones. Previeron una nueva forma de transferir valor que aprovecharía la privacidad y la franqueza del efectivo, pero que superaría los riesgos de seguridad y criminalidad de ese sistema centenario. Los gobiernos y los bancos centrales, así como los grandes bancos comerciales y las corporaciones, todos vieron la promesa de este nuevo sistema, y Chaum rápidamente ganó su oído. Firmó un contrato con el gobierno holandés para que los conductores realizaran pagos de peaje con DigiCash no rastreable; un grupo de grandes bancos, incluyendo Deutsche Bank en Alemania, Advance Bank of Australia, Credit Suisse en Suiza y Sumitomo en Japón, obtuvieron licencias, y los dos primeros incluso comenzaron a emitir DigiCash como proyectos piloto. Chaum conversó con Microsoft y Visa y varias otras grandes empresas intrigados por cómo podrían usar el nuevo sistema de pagos o incluso comprar una participación estratégica en él. Un grupo llamado Conditional Access for Europe (CAFE), una organización sin fines de lucro dedicada a crear pagos electrónicos con privacidad mejorada, contrató a la compañía de Chaum para explorar un sistema de alcance europeo para alcanzar esa meta, casi una década antes de la llegada del euro. Para colmo, el banco de inversión Credit Suisse First Boston le proporcionó a su equipo una oficina de esquina en un piso alto en sus oficinas en el centro de Manhattan, que Chaum utilizaría en viajes periódicos a Nueva York para discutir cómo se podrían empaquetar participaciones en DigiCash y vendido a los inversores. En esta época, a mediados de la década de 1990, la oferta pública inicial

se convirtió en la insignia principal del logro empresarial. Pocos dudaron de que DigiCash iría por la misma ruta de salida a bolsa.

Pero luego, tan rápido como creció, DigiCash se vino abajo. La salida a bolsa nunca sucedió; las conversaciones con Microsoft y Visa disminuyeron; los bancos dejaron de emitir DigiCash y simplemente dejaron de disminuir sus licencias. Sin un sistema bancario funcional detrás de él, DigiCash ya no podría funcionar como un medio de pago anónimo para los conductores en las autopistas de peaje de los Países Bajos. Al final, la solución no monetaria para autopistas de peaje se destinó a un modelo de servicios prepagos controlados centralmente, como el sistema E-ZPass en el noreste de Estados Unidos. Esto creó una nueva herramienta de monitoreo para los oficiales de policía. *

¿Por qué se derrumbó un proyecto con tal promesa? "Realmente no lo sé", dice Chaum cuando se lo pregunta ahora. Sin embargo, él cree que la nueva administración que asumió en 1997 contribuyó a la disminución. Fue entonces cuando un equipo de inversores de capital de riesgo instaló a Michael Nash, ex gerente sénior de Visa, como el nuevo CEO y separó Chaum. Dieciocho meses más tarde, con las oportunidades de negocios que Chaum había alineado escapando de las manos de la compañía, Nash fue obligado a abandonar. Seis meses después de eso, DigiCash solicitó la bancarrota del Capítulo 11. Otro punto de vista, transmitido en un informe de 1999 en la revista holandesa Next !, sostiene que Chaum era un micromanager obsesivo e incapaz de cerrar tratos, simplemente demasiado difícil de tratar como fundador y propietario principal. Chaum dice que tales puntos de vista fueron perpetuadas por sus enemigos y que su registro de acuerdos antes del cambio de gestión se sostiene por sí mismo.

La búsqueda de culpas personales pierde un punto más grande, sin embargo. DigiCash, más que una simple solución de pagos electrónicos, era de vanguardia en sus características criptográficas. Protege la privacidad del usuario; eliminó a los intermediarios de procesamiento de pagos y los costos que los acompañaban; incluso prometió poner patas arriba las estructuras de poder y terminar con la corrupción. Estas ideas estaban adelantadas a su tiempo. La sociedad no estaba lista para ellos, o, para ser más exactos, los bancos y otros grupos de interés que administraban la fontanería del sistema financiero no estaban preparados para ellos. ¿Serán alguna vez? Estas instituciones no vieron los problemas que abordaba David Chaum como los principales desafíos del momento. De hecho, es seguro suponer que también vieron en algunas de las características de DigiCash los núcleos de una amenaza subversiva para el sistema del que prosperaron: bancos, políticos, ambos.

Lo que los banqueros y hombres de negocios más interesados en ese momento estaban buscando era una forma eficiente de hacer comercio electrónico, el gran modelo comercial disruptivo que Internet estaba a punto de ofrecer. DigiCash ofreció una solución a eso, pero estaba lejos de ser la única opción. Estaba Mondex, una empresa de Estados Unidos que desarrolla tecnología de tarjetas inteligentes para almacenar unidades en efectivo en un chip digital integrado en tarjetas de crédito o débito. Fue abandonado después de un piloto decepcionante en el Upper West Side de Nueva York tanto por Chase Bank como por Citibank. Las compañías de tarjetas de crédito también formaron un consorcio llamado Transacciones electrónicas seguras, o SET, para descubrir cómo hacer que las compras de tarjetas de crédito en línea sean seguras para los hackers. Y luego, en 1998, PayPal fue lanzado por Elon Musk, el emprendedor en serie ahora mejor conocido por su automóvil electrónico Tesla. El servicio permitió a las personas abrir cuentas en línea con el equivalente digital de dólares y enviarlas a otros usuarios de PayPal, incluida la nueva generación de vendedores de bajo costo que utilizan mercados electrónicos como eBay. Ninguno de ellos podía hacer lo que DigiCash podía hacer, pero no era necesario. El mercado, al menos según lo definido por los bancos que controlaban el sistema financiero, simplemente quería que el sistema existente de pagos y finanzas se tradujera en un entorno de comercio electrónico. El

derecho a la privacidad y la necesidad de volver a empoderar a las personas no tuvieron en cuenta esto; una vez más, nunca lo habían hecho.

La carrera por una solución de comercio electrónico se ganaría con el mismo modelo de pagos administrado por grandes bancos como aquellos con los que Chaum estaba negociando. En otras palabras, terminaron sin tener ningún uso para él. Con la ayuda de nuevas soluciones de seguridad del sitio web y clasificaciones de terceros para darles confianza a los consumidores, la infraestructura de las redes de pago con tarjeta de crédito, con los intermediarios y los costos de transacción que la acompañaban, se acababan de atornillar a la de Internet. Algunas alternativas, como PayPal, crearían un puente para los minoristas sin medios de aceptar pagos con tarjeta, pero con el tiempo la mayoría simplemente migraría a tarjetas. Proporcionaría una enorme sacudida de nuevos negocios para las dos grandes asociaciones de tarjetas emitidas por bancos, Visa y MasterCard. Los bancos que los poseían, ambas compañías de tarjetas estaban en ese momento controladas por diferentes consorcios de bancos, disfrutarían de una gran cantidad de nuevos ingresos a través de sus negocios de procesamiento de pagos y crédito rotativo.

Muchos esperaban que los bancos controlaran el sistema que haría que los pagos en línea fueran seguros y rápidos. Lo que no es tan conocido es que incluso dentro de estas instituciones se estaba llevando a cabo una competencia a lo largo de la década de 1990 para determinar el futuro del dinero en la era digital. La forma en que se desarrolló prepararía el escenario para la gran crisis de 2008 y, a su vez, fomentaría una reacción pública que respaldaría el aumento del bitcoin. El mejor ejemplo de esa lucha interna se encontró dentro del banco arquetípico demasiado grande para fallar, una institución gigante cuyos problemas definirían esa crisis final: Citibank.

En la década de 1990, antes de que el holding Citiborp, Citicorp, se fusionara con Travelers Group para crear un polémico banco multipropósito llamado Citigroup, fue dirigido por John Reed, un graduado del MIT con afinidad por la tecnología. Bajo el liderazgo de Reed, Citibank fue pionera en el cajero automático y creó un servicio de información electrónica de vanguardia para conectar su amplia red global de sucursales y cuentas de clientes. Gran parte de esa innovación había sido liderada por un laboratorio de investigación interno cuyo gerente, un experto en tecnología llamado Paul Glaser, informó directamente a Reed. En 1990, Glaser fue reemplazado por Colin Crook, un británico conocido por desarrollar el microchip 68000 de Motorola, que luego fue utilizado por Apple Macintosh. Incorporando el mismo espíritu de inventiva, el laboratorio de vanguardia se embarcaría en lo que quizás fue su proyecto más audaz: la reinvención del dinero.

El hombre que condujo este proyecto fue Sholom Rosen, un tecnólogo con un yen de criptografía que había sido contratado por Glaser. Al igual que muchos expertos en finanzas de la época, Rosen estaba obsesionada con la forma de atraer dinero al mundo digital centrado en el consumidor que empresas como Hewlett-Packard, Microsoft, Intel, Apple y Sun Microsystems estaban creando. Internet aún no había despegado, y aplicaciones como Napster, iTunes y Kindle todavía estaban lejos en el futuro, pero Rosen ya estaba imaginando una era en la que las personas comprarían y usarían archivos de música digitalizados y otras formas de entretenimiento sobre sus ordenadores. Cómo digitalizar el dinero, entonces, fue el desafío.

Rosen llegó a Crook con un plan cuya amplitud fue capturada en su nombre autorizado: el Sistema Monetario Electrónico. No se trata solo de crear una nueva herramienta para Citibank; esta sería una nueva forma de dinero para los Estados Unidos, para todo el mundo, tal vez. Crook fue tomado por eso. Al igual que Reed, al parecer, quien le aseguró un presupuesto saludable. Los principales académicos de tecnología de MIT, Berkeley y Stanford fueron contratados para ayudar, incluido el pionero en encriptación pública Ron Rivest, el R en la legendaria compañía fundada por MIT RSA. Se hicieron consultas y se alcanzaron acuerdos con las principales compañías de tecnología: Intel y Sun Microsystems en los Estados Unidos, Acorn Computers en el Reino Unido. Rosen

incluso visitó a David Chaum en Ámsterdam, pero decidió que no podía trabajar con él, lo que solo alentó a Rosen a desarrollar su propio sistema de dinero electrónico desde cero.

Al igual que con DigiCash y luego con Bitcoin, el modelo de e-cash de Citi estaría compuesto por unidades monetarias independientes. Los usuarios no solo estarían transfiriendo saldos entre cuentas dentro de un sistema cerrado como PayPal, sino que podrían intercambiar dólares digitalizados completos con cualquier persona, en cualquier lugar, como si fueran dinero en efectivo. También como Bitcoin y otras criptomonedas, el proyecto de Rosen ejecutó un libro permanente de transacciones y permitió que el dólar digital se cortara en pedazos más pequeños para que el comercio pudiera ocurrir en cualquier denominación que se requiriera. El efectivo electrónico de Citi fue, en este sentido, una moneda perturbadora, desintermediadora y de igual a igual. No necesitaría la amplia red de comunicaciones que sustenta los pagos con tarjeta de crédito, por lo que los costos de transacción se mantendrían bajos, proporcionando ganancias tanto para los consumidores como para las empresas y haciendo que los micropagos sean viables.

Pero esto no quiere decir que Rosen quisiera eliminar a los bancos del sistema como, digamos, Satoshi Nakamoto. Lejos de ahi. Banks se sentaría en el corazón de su sistema, reflejando una visión profunda que había desarrollado sobre la teoría del dinero leyendo a personas como Milton Friedman y el periodista financiero del siglo diecinueve Walter Bagehot. "No se puede divorciar la banca del dinero, especialmente del dinero moderno", dijo Rosen en una entrevista para este libro. "La creación real de dinero es realizada por el sistema bancario, bajo la guía y el control de la Reserva Federal. Cuando vas a pedir prestado mil dólares a un banco, el banco crea esos mil dólares, no la Fed ".

De hecho, Rosen llevaría el modelo existente un paso más allá. Los bancos comerciales no solo crearían dinero secundario mediante el préstamo de depósitos; también tomarían la función principal de emitir moneda real, que en los Estados Unidos ha sido manejada durante los últimos cien años por la Fed a través de sus doce bancos de la Reserva Federal. Su sistema "era como un modelo de la Guerra Civil, cuando el gobierno estableció por primera vez el sistema bancario nacional, lo que hizo que cada banco emitiera moneda", dijo Rosen. La diferencia era que en esta versión de finales del siglo XX, los bancos estarían emitiendo dólares digitales, no papel moneda.

Rosen y sus siete o más miembros del personal perfeccionaron su modelo durante la década de 1990. Trabajando en su mayoría fuera de salas cuidadosamente vigiladas en las oficinas de Citibank en Nueva York, los miembros del equipo recibieron discos duros extraíbles que estaban encerrados en cajas fuertes al final del día. Utilizaron dispositivos de lectura biométrica para abrir puertas e instalar dispositivos de comunicaciones por infrarrojos en sus computadoras portátiles. El equipo, algunos vistiendo el modo de piratas informáticos rebeldes del día, se convirtieron en un equipo extraño contra los banqueros abotonados con los que compartirían ascensores. Pero para el grupo muy unido, fue un momento emocionante. "Sentí que estaba trabajando en algo realmente grande", recuerda Sandeep Maira, quien se unió al equipo de Rosen poco después de graduarse con un título en ciencias de la computación de Cornell.

Con el tiempo, desarrollaron veintiocho patentes. Estos describirían las características del e-cash de Citi que eran muy diferentes de DigiCash y las criptomonedas como el bitcoin que vendrían después. Por un lado, los dólares digitales caducarían después de un cierto tiempo, lo que requeriría que el titular contactara al banco y los reemplazara, un truco diseñado para evitar el lavado de dinero. Para mantener el sistema seguro, las computadoras que usaban e-cash se instalarían con chips especializados que harían un seguimiento del sistema monetario.

El gran salto de Rosen llegó en 1997, cuando el Departamento del Tesoro de EE. UU. Acordó probar este sistema. El gobierno de los EE. UU., Como el que más gasta en el país, estaba tan ansioso como

Rosen y su banco empleador por averiguar dónde iba la tecnología de pagos en el entorno de comercio electrónico en rápido desarrollo. Como parte de la investigación de ese proceso liderado por el jefe de una división especial de comercio electrónico, Gary Grippo, el Departamento del Tesoro llevó a cabo un extenso programa piloto hasta 2001. Por lo que podemos decir, el programa no se ha informado hasta ahora. Durante la vida del programa, el gobierno compró a Dell unas treinta mil computadoras personales y aceptó millones de dólares en pagos de impuestos especiales de la compañía tabacalera Brown & Williamson, completando alrededor de 350 millones de dólares en transacciones, todo en el e-cash de Citi. Para algunos de los involucrados, parecía que los Estados Unidos estaban en camino a un dólar digital.

Pero entonces, al igual que DigiCash, el nervioso proyecto de Sholom Rosen se cerró abruptamente, un resultado directo de la creación de Citigroup Inc. Este evento histórico en la historia bancaria de Estados Unidos presagiaría un desastre financiero una década más tarde y prepararía el escenario para la llegada de Bitcoin.

En 1998, John Reed llegó a un acuerdo con Sanford Weill, entonces CEO del conglomerado financiero Travelers Group, para que se fusionara con la operación de banca mayoritariamente comercial de Citi y formara un banco único y universal: un supermercado financiero, como el concepto fue descrito por sus patrocinadores. Combinaría el alcance global de banca comercial de Citicorp con la destreza de banca de inversión de Travelers 'Salomon Smith Barney, así como las ofertas de seguros integrales de este último.

Un problema: el trato era esencialmente ilegal. Según cualquier lectura, entró en conflicto con la Ley Glass-Steagall de la era de la Depresión, que decretó que los bancos comerciales y los bancos de inversión deben permanecer separados. La intención de la ley era que los fondos de los depositantes comerciales no se vean amenazados por un banco de inversión que podría utilizarlos para financiar inversiones especulativas en lugar de los préstamos residenciales o comerciales más confiables que persiguen los bancos comerciales. Pero Weill y Reed convencieron tanto al Congreso como a la administración Clinton de que Estados Unidos necesitaba bancos más grandes y más expansivos para competir en la era de la globalización. Entonces, el 12 de noviembre de 1999, el presidente Clinton firmó un proyecto de ley patrocinado por tres republicanos, el senador Phil Gramm de Texas, el representante Jim Leach de Iowa y el representante Thomas Bliley de Virginia, que puso el filo en el ataúd de Glass-Steagall. Esta "legislación histórica", dijo Clinton en su momento, "modernizará nuestras leyes de servicios financieros, estimulando una mayor innovación y competencia en la industria de servicios financieros". Los consumidores de Estados Unidos, nuestras comunidades y la economía obtendrán los beneficios de esto ". La firma de Clinton prepararía las cosas para la mayor crisis financiera que el mundo haya visto en ochenta años.

Nueve años más tarde, Citigroup simbolizaría ese fracaso cuando necesitó un rescate de $ 45 mil millones del gobierno de EE. UU. Pero en 1999, Sandy Weill podría tomar el sol encima del banco más poderoso de los Estados Unidos, si no del mundo. Y su poder recién estaba comenzando. El temerario negociador de Wall Street chocó con el amante de la tecnología geek con el que había aceptado una relación de copresidente. Entonces, en febrero de 2000, solo cuatro meses después de que el Congreso había bendecido su unión, Weill arregló un golpe interno. Reed fue forzado a salir y se ordenó la reorganización administrativa necesaria.

Con Reed fuera, Weill se dispuso a marcar su territorio y encontrar ahorros en los costos para pagar la cuenta de $ 70 mil millones en la que los accionistas habían incurrido en la fusión, en su momento la más grande en la historia corporativa de Estados Unidos. En ese contexto, no significaba nada cerrar un extravagante experimento de John Reed con dinero electrónico, especialmente dado que los pagos con tarjeta de crédito ahora se usaban ampliamente en línea, lo

que aparentemente negaba la necesidad del dinero electrónico. En la segunda mitad de 2001, el proyecto del Sistema Monetario Electrónico se redujo. Rosen, que entonces tenía sesenta años, se jubiló anticipadamente. Colin Crook fue a buscar intereses académicos como becario de Wharton. La idea del dinero electrónico de Citi se marchitó y murió.

Los miembros del equipo de Rosen describen la decisión de cerrar el proyecto del Sistema Monetario Electrónico en su mayoría burocrático, una forma de ahorrar dinero en un proyecto que simplemente no le interesaba a Weill. Pero también reflejó una diferencia filosófica entre los creyentes en proyectos innovadores que buscan obtener ganancias al ser los primeros en comercializar con nuevos modelos comerciales que reducen los costos, y creyentes en el espíritu prevaleciente de Wall Street que personificó Sandy Weill. La banca de Wall Street es, si no más, un ejercicio de búsqueda de rentas. Se inclinaría por preservar y fortalecer los flujos de ingresos centralizados, como las tarifas de transacción de tarjetas de crédito, en lugar de eliminarlas. Con la derogación de Glass-Steagall y las oleadas de fusiones comerciales y de bancos de inversión que siguieron al liderazgo de Citigroup-Chase Manhattan con JP Morgan, Bank Boston con Fleet Bank y más tarde con Bank of America-este ethos ahora tomaba el control de el sistema financiero estadounidense. Suponía que se podía ganar tanto dinero de los músculos, el dinero y la mierda como del cerebro.

Claro, estos gigantescos y nuevos bancos de supermercados contratarían hordas de geeks matemáticos en los años siguientes, pero en lugar de tratar de hacer que el sistema financiero sea más eficiente, sus innovaciones se usaron para monopolizar información y extraer ganancias excesivas de clientes a los que se mantuvo ignorantes sobre qué estaban comprando. Estos "quants" matemáticos tomaron los gigantescos grupos de préstamos hipotecarios ahora asentados en los balances de sus empleadores y los volvieron a empaquetar en valores altamente complejos, opacos y difíciles de valorar que se vendieron como apuestas seguras. A medida que más y más de estos valores arriesgados fueron comprados por fondos de pensiones, compañías de seguros y otros administradores de los ahorros del público global, la máquina de bursatilización de quants exigió más préstamos, lo que a su vez condujo a una expansión masiva de préstamos dudosos a bajos ingresos Hogares estadounidenses.

El resto es historia. Una vez que se demostró que los activos hipotecarios subyacentes eran de calidad mucho peor que las valoraciones implícitas en los valores reempaquetados, se derrumbó el castillo de naipes. Debido a que los bancos se habían vuelto muy, muy grandes e interconectados dentro del sistema financiero mundial, los gobiernos de todo el mundo se sintieron obligados a pagar billones de dólares, libras y euros de los contribuyentes para evitar derrumbar todo el sistema. El aumento de las criptomonedas se puede entender solo en relación con esos eventos cataclísmicos.

El miércoles después del colapso del 15 de septiembre de Lehman Brothers en 2008, Mohamed El-Erian, entonces codirector general del administrador de activos masivo Pacific Investment Management Co. y en ese momento trabajando a toda hora para tratar de extraer su empresa de los remolinos maelstrom financiero, se tomó el tiempo para llamar a su esposa desde la sede de PIMCO en Newport Beach, California. Debería ir a un cajero automático y retirar todo el dinero que pudiera. Ella no entendía por qué. Porque, le dijo, existía la posibilidad de que los bancos de EE. UU. No abrieran al día siguiente.

Esa perspectiva atemorizante -la completa parálisis del sistema financiero más importante del mundo- fue el precio que pagamos por dejar que Wall Street profundizara su modelo de poder centralizado y rentista. La pestaña social final aún se está contabilizando, pero sus costos van más allá de lo que cualquier tenedor de libros puede poner en dólares y centavos. Un lugar en el que se siente es en el sabor amargo que queda en la boca de los ciudadanos obligados a apuntalar estos

bancos. Eso se ha traducido en una pérdida de confianza en las instituciones en general, tanto en Wall Street como en Washington.
En este mundo de desconfianza, Satoshi Nakamoto colocó su proyecto de bitcoin, solo un mes después del colapso de Lehman.

¿Eligió la fecha de lanzamiento debido a esos eventos? Es imposible saberlo con certeza. Sus escritos públicos están resguardados. En una publicación del foro, Nakamoto dijo que había estado trabajando en Bitcoin desde 2007. Sin embargo, algunas pistas sugieren que, al menos, vio en el accidente la oportunidad de destacar las ventajas de su sistema.

En una publicación del 11 de febrero de 2009 en un foro para desarrolladores, escribió: "El problema de raíz con la moneda convencional es toda la confianza que se requiere para que funcione. Se debe confiar en que el banco central no degrade la moneda, pero el historial de las monedas fiduciarias está lleno de violaciones de esa confianza. Se debe confiar en los bancos para que conserven nuestro dinero y lo transfieran electrónicamente, pero lo prestan en oleadas de burbujas de crédito con apenas una fracción de la reserva. "Se trata de una acusación tan directa del sistema existente como él lo hace. En otra publicación, escribe con un élan inusual: "¡Huye del arbitrario riesgo de inflación de las monedas administradas centralmente!"

Otra pista está incrustada en el código del Bloque Génesis. Para autenticar la marca de tiempo de esa creación, Nakamoto hizo referencia a un titular de la página principal de The Times of London el 4 de enero de 2009: "Canciller al borde del segundo rescate financiero para los bancos".

El canciller en cuestión era Alistair Darling, entonces el canciller del Tesoro del Reino Unido, que luchaba por evitar el colapso total del sistema bancario británico. Su gobierno había inyectado £ 500 mil millones en préstamos y garantías a los bancos, incluidos £ 50 mil millones para comprar participaciones mayoritarias en tres instituciones gigantescas y tambaleantes: el Royal Bank of Scotland, Lloyds y HBOS. No fue suficiente. El 19 de enero, el gobierno de los EE. UU. Anunció otro paquete de rescate de £ 50 mil millones.

Estos fueron días oscuros. Además de la bancarrota de Lehman Brothers, Merrill Lynch había sido rescatado por el Bank of America ese mismo fin de semana. Días después, una implosión en la aseguradora AIG llevó a un rescate gubernamental que se incrementaría a $ 182 mil millones. Las economías occidentales comenzaron a sufrir una hemorragia laboral, las bolsas se colapsaron y el comercio mundial se detuvo. Si alguien alguna vez buscara un momento para lanzar un sistema monetario alternativo, la persona no podría haber escogido un mejor momento.

No olvidemos, también, que Nakamoto lanzó su proyecto con un recordatorio de que su nueva moneda no requeriría ningún gobierno, ni bancos, ni intermediarios financieros, "ningún tercero de confianza". Ofreció la antítesis del problema central de ese momento en historia. Para toda la magia técnica y legal empleada por los habitantes de Wall Street, para toda la innovación financiera practicada por los banqueros de Street, la confianza era el elemento más importante de los mercados de capitales: confiar en que las contrapartes eran buenas por el dinero que prometían; confíe en que los precios de mercado realmente reflejaron toda la información disponible en ese momento; confíe en que si un activo se representó en el balance general como si valiera X cantidad de dólares, en realidad valía X cantidad de dólares. El colapso de Lehman y AIG destrozó todo eso. Nadie confiaba en las valoraciones de activos, nadie confiaba en las cotizaciones de precios. Nadie confiaba en los balances de los bancos. Toda la maquinaria de los mercados globales de capital se apoderó, llegando a una parada aplastante, aplastante y desastrosa, porque ya nadie confiaba en nadie.

En los meses y años que siguieron, un número creciente de personas decidiría que tal vez la idea de Satoshi Nakamoto ofreciera una mejor alternativa a todo eso.

Si bien no tenemos pruebas de que las iniciativas de efectivo lideradas por la compañía con fines de lucro de la década de 1990 y la crisis bancaria de 2008 formaron el pensamiento de Nakamoto, ambos subrayaron las razones por las que los diseñadores de criptomonedas estaban ansiosos por el cambio. El mensaje en cada caso fue que la centralización del dinero es destructiva y que los intentos de cambiarlo desde dentro fracasarían. La solución solo podría ser la verdadera descentralización, al idear un nuevo sistema monetario rebelde. En la mente de los expertos en tendencias libertarias que creían en estos modelos, no fue suficiente para construir el tipo de funciones de anonimato que creó Chaum. Las criptomonedas necesitaban un modelo puramente independiente. Sin embargo, hasta que llegó el bitcoin, nadie podía encontrar la manera de construirlo, sobre todo porque era difícil reemplazar una estructura corporativa centralizada en la que las normas podían aplicarse desde arriba con una comunidad descentralizada en la que nadie está nominalmente a cargo. En ausencia de una autoridad central, ¿cómo logras que todos en la red cooperen? Y si no puedes crear una autoridad colectiva, ¿cómo evitas que las personas jueguen con el sistema, gasten bitcoins que no tienen?

Nakamoto ideó una solución doble. Uno de los componentes fue su gran libro de blockchain. Bajo su diseño, las transacciones se organizan en bloques ordenados cronológicamente que les dan a los mineros la capacidad de verificar sus contenidos al compararlos con el libro de contabilidad histórico de saldos de cuentas. Una vez satisfechos, reconocen su aprobación moviéndose para crear el siguiente bloque y encadenándolo al predecesor ahora aprobado. Esta verificación y encadenamiento de los bloques, y la aceptación de cada uno nuevo como la base legítima sobre la cual construir bloques futuros, constituyen un consenso de facto sobre la validez de las transacciones subyacentes. Eso hizo que fuera efectivamente imposible para una persona soltera "gastar doblemente" una moneda. La falsificación digital podría finalmente ser descartada.

La segunda solución se basaba en el algoritmo de recompensas mineras, que creaba exactamente la alineación de los incentivos necesarios para que los propietarios de las computadoras en red pudieran comprometer la electricidad y los recursos informáticos necesarios para que sus máquinas ayudaran a mantener el ledger blockchain. Juntas, estas características sentaron las bases para un mecanismo de confianza descentralizado.

Pero todavía había un problema: Nakamoto tenía que crear un sentido de valor arraigado en bitcoins, que se reducía a determinar la dinámica adecuada de oferta y demanda. Se dirigió a esto al jugar con el calendario para el lanzamiento futuro de monedas. En los primeros cuatro años, el protocolo establecería una cantidad fija de cincuenta monedas para ser lanzadas más o menos cada diez minutos. Luego reduciría la emisión a veinticinco monedas a fines de 2012 y la reduciría a la mitad nuevamente cada cuatro años, hasta que la oferta se redujera a cero en 2140, momento en el cual se habrían liberado un total de 21 millones de monedas. Esta liberación preprogramada y decreciente de un suministro finito de monedas creó una sensación de escasez, que construyó una base de apoyo para el precio de bitcoin que incentivaría a los mineros a seguir trabajando con ella. Sabía que el suministro cada vez menor de bitcoins eventualmente requeriría una zanahoria alternativa para mantener a los mineros comprometidos, por lo que incorporó un sistema de tarifas de transacción modestas para compensarlos por los recursos que aportaron. Estas tarifas entrarían en vigencia a medida que pasara el tiempo y a medida que disminuyera el rendimiento de los mineros. En resumen, se trataba de una solución elegante y de libre mercado para un dilema que ha perseguido a las sociedades durante siglos: cómo alinear la búsqueda de intereses propios con las necesidades de su comunidad.

Este logro fue crítico por razones filosóficas y prácticas. La descentralización conlleva beneficios reales para un sistema monetario que se presenta como una alternativa al sistema dominante controlado por los gobiernos y administrado por los bancos. Como no existe un único punto de control, no hay un servidor central para coordinar la red de computadoras distribuida de manera difusa y global, no hay forma de cerrar el sistema alternativo. El gobierno chino podría prohibir a sus bancos manejar servicios de transacciones relacionados con bitcoins o declarar que solo se usa el yuan dentro de las fronteras de la nación, pero no puede cerrar Bitcoin, que no reside en ninguna parte y en todas partes. El mismo desafío enfrenta cualquier gobierno. Esto atraía a una subcultura marginal pero no insignificante de activistas apasionados y muy motivados que son escépticos del dinero fiduciario administrado por el banco central. En términos más generales, fue consistente con una tendencia hacia la descentralización y el empoderamiento individual en la economía en general, un mundo en el que las personas están alquilando sus sofás para pagarles a los huéspedes, vendiendo electricidad generada por energía solar a la red y sacando noticias de foros descentralizados como Twitter.

En este entorno y frente a lo que Nakamoto había propuesto, un número creciente de personas llegó a confiar en que su sistema funcionaba. Muchos decidieron que era mejor confiar en este sistema inviolable basado en algoritmos que los seres humanos propensos al error y al fraude que manejan las grandes instituciones en el centro del viejo sistema monetario.

La salida de Hal Finney de la red de dos que él y Nakamoto formaron en enero de 2009 no resultó un retroceso para bitcoin, ya que otros con la claridad para recoger su significado rápidamente comenzaron a interesarse. Ese año atraería a nuevos usuarios que descargaron el software para convertirse en nuevos nodos para administrar la red y minar bitcoins. Para comunicarse, muchos usaron un canal de IRC que Nakamoto había establecido en el sitio de bitcoin.org. En octubre, una nueva sala de IRC enfocada en codificadores se había configurado en línea con el identificador # bitcoin-dev, y el mes siguiente se formalizó bajo el nombre Bitcoin Forum. Se estaba formando una comunidad de bitcoiners.

Cada vez que una persona nueva firmaba su computadora en la red, aumentaba la cantidad combinada de potencia computacional que se aplicaba a la búsqueda de bitcoins, así como también la electricidad total consumida, la principal variable de entrada para la minería bitcoin. También significó que la competencia se intensificó para los lotes de cincuenta monedas que el sistema estaba programado para lanzar, lo que significa que las posibilidades de ganar un nodo de cada computadora disminuirían. Con el tiempo, este aumento en el poder de cómputo en toda la red también induciría al programa central a aumentar automáticamente la dificultad de su acertijo matemático. Esto fue para que el aumento en el poder de resolución de rompecabezas combinado no descubriera la solución demasiado rápido y forzara una liberación prematura de bitcoins. De esa forma, el cronograma de liberación de diez minutos podría cumplirse con el tiempo.

Para que Bitcoin se desarrollara, sin embargo, necesitaba una alternativa a la minería como forma de adquirir las monedas. Debes poder comprarlos con dólares u otras monedas fiduciarias. ¿Pero a qué precio? Entonces, en octubre de 2009, algunos en la comunidad se encargaron de citar una tasa de cambio basada en dólares y publicarla en un nuevo sitio web llamado New Liberty Standard. Utilizando un cálculo basado en el costo de la electricidad para la minería, su primera cotización fue catalogada como BTC1,309.03 por $ 1. Dicho de otra manera, un bitcoin valía 0.08 de un centavo. Algunos pensaban que New Liberty Standard estaba cobrando de más, pero al menos ahora tenían un lugar para comprar y vender este activo virtual experimental. En lo que sería un sello distintivo de su negociación en los próximos años, la volatilidad de Bitcoin se mostró de inmediato, ya que el precio saltó un 70 por ciento a 0.14 por ciento el 13 de noviembre, para luego caer a 0.06 el mes próximo. Aún así, fue divertido intercambiar estos pequeños tokens.

Debido a que la comunidad todavía era relativamente pequeña y nadie había descubierto aún cómo encender su computadora para vencer a todos los demás en el acertijo matemático, los pagos se repartieron de manera relativamente pareja entre todos los mineros. Todo fue muy comunitario.

Esto cambiaría en el Año Nuevo cuando Laszlo Hanyecz, un ingeniero de software en Florida, descubrió que podía escribir un software que instruyera a la tarjeta gráfica de su computadora, o GPU, para hacerse cargo de la tarea minera, que hasta entonces había sido hecha por cada minero. UPC. Comprometerse con esta herramienta más enfocada y de mayor rendimiento incrementó el poder de cómputo que Hanyecz podía aplicar al rompecabezas matemático y aumentaba exponencialmente sus posibilidades de obtener uno de los bloques de cincuenta bitcoins.

Esto llamó mucho la atención. A pesar de que cada bitcoin valía tan poco, la creciente comunidad comenzó a creer que su valor en aumento presagiaba ganancias futuras. Coincidiendo con el lanzamiento de una versión 0.2 más robusta del software básico de bitcoins y con la creación de un segundo mercado de divisas llamado Bitcoin Market, las noticias de que este tipo Hanyecz se estaba convirtiendo en tantos bitcoins para él era como noticias del hallazgo de oro en Sutter's Mill en 1848. Nuevos aficionados se unieron rápidamente a la refriega. Se produjo una carrera armamentista, ya que las personas convirtieron sus computadoras hogareñas cargadas con tarjetas gráficas en miniaturas de moneda digital. Una vez que estas máquinas de atrapar electricidad se pusieron en marcha, la red comenzó a calentarse con energía, tanto literal como figurativamente.

A medida que las cosas se volvían más frenéticas y Bitcoin se alejaba lentamente de los límites geek de la sociedad tecnológica para adoptar un nuevo nivel de buscador de oro digital temprano, Nakamoto debe haber mirado con asombro lo que estaba sucediendo. ¿Celebraba o lamentaba lo que había forjado? Es posible que nunca lo sepamos. Un año después desaparecería del mundo de Bitcoin.

Capítulo 3

COMUNIDAD

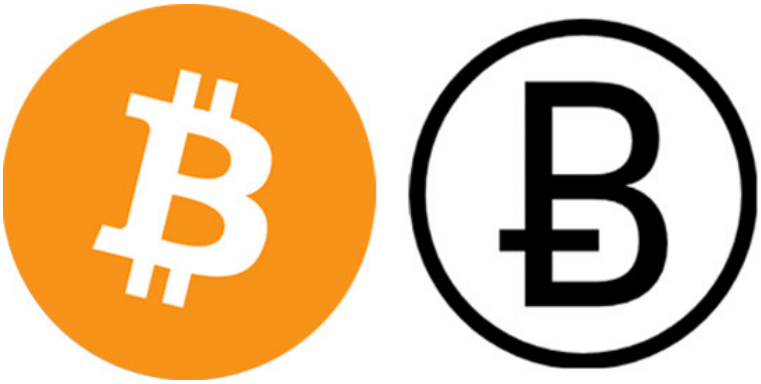
El dinero es como lodo, no es bueno, excepto que se propague.

-Francis Bacon

El 12 de diciembre de 2010, apareció la siguiente publicación en el Foro Bitcoin: "Hay más trabajo por hacer en DoS [denegación de servicio], pero estoy haciendo una compilación rápida de lo que tengo hasta ahora en caso de que sea necesario, antes de aventurarme en ideas más complejas. La compilación para esto es la versión 0.3.19. "Sería el último mensaje de Satoshi Nakamoto.

Eso fue todo. No hubo ningún mensaje de despedida, ningún discurso noble. Él simplemente dejó de escribir. El fundador mantuvo la comunicación con algunos de los desarrolladores de software que lo ayudaban a mejorar y mantener el sistema bitcoin, pero en abril de 2011, también les envió su último correo electrónico. Por lo que sabemos, el último fue para Gavin Andresen, un codificador con sede en Amherst, Massachusetts, que se había unido al grupo un año antes y en quien Nakamoto había otorgado un papel de liderazgo. Al igual que su última publicación en el Foro de Bitcoin, de hecho, como todo lo demás que escribió Nakamoto, ese último correo electrónico fue superficial, útil, carente prácticamente de sentimentalismo.

Pero si el legado escrito del fundador del bitcoin es un conjunto de palabras secas y utilitarias, su otro gran legado se encuentra en la ferviente comunidad de verdaderos creyentes que dejó tras él. Este grupo apasionado crecería en torno a las ideas que Nakamoto desarrolló y el código que implementó. Podría decirse que es su mayor creación, ya que, como hemos argumentado, una moneda no puede existir sin una comunidad. En el caso de una moneda descentralizada e independiente, sin una autoridad central para imponer el orden en el sistema monetario, los vínculos humanos que definen a esa comunidad son doblemente importantes.



Dos versiones del bitcoin "B"
(Izquierda) Fuente: Wikipedia
(Derecha) Fuente: bitcoinsymbol.org

Los marcadores de esta comunidad se encuentran en mucho más que la disposición de sus miembros para enviar bitcoins entre ellos o para explotarlos colectivamente y mantener el libro mayor de blockchain. Están integrados en una "cultura bitcoin" distinta, una forma de hablar, pensar y relacionarse entre sí y con los demás. La cultura está bruñida por fenómenos similares a

los que sustentan culturas más establecidas. Así como los significantes culturales como las banderas, los himnos y los animados discursos de los padres fundadores ayudan a las personas a imaginar un sentido abstracto de identidad nacional, también los iconos y memes alientan a los miembros de esta comunidad a autoidentificarse como bitcoiners y como seguidores de un cierto sistema de creencias, aunque mal definido. Bitcoin también tiene sus símbolos, el bitcoin B es el más ubicuo, aunque los miembros de la comunidad han debatido si debería verse como un símbolo de moneda (por ejemplo, $) o un logotipo de marketing. Al igual que otras culturas, bitcoin también tiene su arte, su música e incluso su poesía. También ha cultivado personalidades más importantes que los reconocidos como "líderes comunitarios".

Es revelador que estas personalidades a menudo se describan como "evangelistas". Del mismo modo, los trasfondos religiosos están en todas partes en el lenguaje y los conceptos vinculados a bitcoin: la etiqueta de Génesis en bloque clavada en el primer lote de monedas minadas de Nakamoto; el apodo de Bitcoin Jesús dado a Roger Ver, ahora uno de los representantes más prominentes de la comunidad; la idea misma de un "creyente"; y la noción de que uno tiene una epifanía una vez que se revela la "verdad" de la solución de bitcoin. La más importante de estas ideas cuasirreligiosas, sin embargo, radica en el bloque cultural básico que el propio Nakamoto estableció con su misteriosa aparición en el mundo de las criptomonedas en 2008 y luego con su desaparición igualmente misteriosa tres años después. Sea quien sea, Nakamoto le dio a Bitcoin su mito de creación.

El mito de la creación por excelencia es el de Génesis, y mira qué tanto eso llevó tanto al judaísmo como al cristianismo. En un sentido mucho menos espiritual, los especialistas en marketing se han dado cuenta del poder de los mitos y narraciones de la creación. La idea de que un negocio en particular nació de la brillante idea de que alguien trabaja en contra de las probabilidades ayuda a personalizar el producto y aumentar el atractivo. Tales alusiones están en todas partes en los negocios: el Modelo T de Ford Motor, la receta secreta de Coca-Cola, el garaje de Bill Hewlett y Bob Packard, Steve Jobs y la primera computadora Apple.

"En los negocios, las historias de creación refuerzan el papel del individuo como agente social de cambio y hablan a un público central de clientes", escribió Nicolas Colas, estratega jefe de mercado de la correduría ConvergEx, en una investigación que refleja la importancia del misterio. que rodea al fundador de bitcoin. "Ellos son la base de lo que los especialistas en marketing llaman 'marca' y la fuente del 'valor para los accionistas' de Wall Street".

La "marca" de Bitcoin está indudablemente ligada al fundador y al misterio que lo rodea a él, a ella o a él. Homenajes a Satoshi aparecen en toda la cultura bitcoin: la denominación más pequeña de un bitcoin se llama Satoshi, se realizan numerosas reuniones en lugares denominados Satoshi Square, varios negocios de bitcoins han utilizado el nombre del fundador, incluido el sitio de apuestas de alto perfil SatoshiDice.

Asumiendo que Nakamoto es una persona soltera, podría argumentar que como figura pública él o ella ya no tiene forma humana y se ha transformado en un mito total. Ninguna persona física se para frente a nosotros o está disponible en un video de YouTube. Nadie está sentado al otro lado de la mesa frente a Charlie Rose, siendo entrevistado por los canales de noticias. Nadie para escribir un libro o firmar los derechos de la película sobre su historia. Todo lo que tenemos es el espectro de un genio solitario, y una pista sobre la divinidad de Bitcoin.

¿Quién es Satoshi Nakamoto? Techies, investigadores de pasatiempos y periodistas han encontrado que esta pregunta tentadora es imposible de ignorar. Al perseguirlo, todos han ayudado a pulir aún más el mito de la creación de bitcoins y a imbuir al núcleo cultural de su comunidad con un sentido de maravilla, genio y un propósito mayor.

Por todo lo que se ha escrito sobre Nakamoto, por todo lo que él (o ella o ellos) han escrito, para todos los fisgones que han tratado de descubrirlo, sabemos asombrosamente poco sobre él. Se comunicó a través de canales cifrados que hasta ahora han demostrado que no se pueden rastrear. Sus escritos públicos están completamente resguardados; en ningún momento divulga información personal; en algunos momentos ofrece algo que parece una opinión. En ocasiones, se desliza una ortografía británica en una publicación, lo que ha llevado a algunos a suponer que es del Reino Unido. Pero la ortografía no es consistente, lo que ha llevado a algunos a suponer que es más de una persona escribiendo, y por lo tanto, Nakamoto no es una persona sino un grupo. Intentar agarrarlo a través de su escritura es como tratar de atrapar una anguila. Un cuerpo está allí, pero no hay nada a lo que agarrarse.

Cuando los periodistas vienen a buscar a Nakamoto, los bitcoiners inevitablemente nos dicen que dejemos a esta persona en paz, que respetemos su deseo de privacidad. Esta posición es ideológicamente consistente e inconsistente con los principios fundadores de los Cypherpunks. La filosofía de ese movimiento valoraba la privacidad por completo, pero también esperaba que se buscara su identidad, razón por la cual se creó el cifrado en primer lugar.

Incluso podría ser mejor para bitcoin si la identidad de Satoshi finalmente se revela. Inicialmente, la ausencia de un fundador identificable significaba que los agentes de ejecución no podían encontrar a Satoshi y cerrar su proyecto incipiente antes de que ganara tracción. Ahora está en una fase diferente. Más de seis años después de la existencia de Bitcoin, con una economía global formándose a su alrededor, el proyecto busca llevar a cabo el último ejercicio de expansión de la comunidad y abrazar la "corriente principal" amplia y global. Para ese ejercicio, la falta de transparencia sobre La fundación de Bitcoin es un obstáculo. Alimenta las dudas en las mentes de los funcionarios del gobierno y los legisladores, haciendo que la regulación amistosa que podría suavizar el desarrollo de bitcoins sea más difícil de vender para los cabilderos de criptomonedas. Lo mismo aplica para el público en general. Venir limpio acabaría con las teorías conspirativas de que Bitcoin fue creado por la CIA o la NSA o el FMI, o que todo es una estafa elaborada. El anonimato de Nakamoto en los primeros días de Bitcoin puede haber ayudado a desviar la atención de la figura principal y al proyecto, pero ahora ese secreto es en sí mismo una distracción. Mientras que el problema inicial fue que los primeros usuarios podrían haber desconfiado de un fundador que pensaba estar bombeando su propia moneda, ahora el problema es que el promedio de los afectados por los defensores de bitcoin ven el misterio como una razón para no confiar en él. "Misterioso en el caso del dinero no es tan bueno", dice Jeremy Allaire, fundador de la firma financiera de bitcoin Circle.

Además, el propio Nakamoto tiene un dilema. Se cree que es el propietario de alrededor de 1 millón de bitcoins, o alrededor de $ 500 millones en el momento de escribir este informe. Esa es la estimación que se le ocurrió al criptógrafo Sergio Lerner después de analizar los movimientos en las direcciones que identificó para Nakamoto del Bloque Génesis y los posteriores traslados mineros durante los dos o más años que estuvo involucrado en la red bitcoin. Desde que Lerner identificó esas direcciones, el mundo las ha estado mirando como un halcón. (Aunque no se puede identificar a su propietario, las direcciones de la billetera en las que residen las monedas se pueden ver fácilmente, junto con todas las otras direcciones de bitcoin, utilizando herramientas que rastrean la cadena de bloques). Ahora podría ser el momento para que Nakamoto cumpla - Exchange El CEO de SecondMarket, Barry Silbert, describe como uno de sus "sueños personales para bitcoins": que Nakamoto se autodefine y hace una donación de alto perfil de sus tenencias de bitcoins gigantes a una causa extremadamente digna.

Independientemente de lo que la transparencia en este tema pueda significar para bitcoin, la gente seguirá buscando a Satoshi Nakamoto. Los bitcoiners pueden protestar, pero no pueden aplacar

el deseo de saber. Como periodistas, tal vez experimentamos este instinto más fuerte que la mayoría, pero la mayoría de la gente tiene curiosidad natural. Lo vemos en nuestros propios hijos, de los cuales tenemos tres entre nosotros, todos ansiosos por saber qué están haciendo sus padres. Una de ellas, una niña de quinto grado, se ha sentido intrigada por las historias de bitcoin de las que escucha a su padre hablar. "¿Has descubierto quién es Satoshi todavía, papá?", Pregunta de vez en cuando. Ella parece verlo un poco como el popular videojuego infantil Where in the World Is Carmen Sandiego?

Desde que Nakamoto guardó silencio en 2010, se han presentado docenas de nombres como candidatos, comenzando por los más obvios de la comunidad Cypherpunk y de la criptografía que previamente habían incursionado en la criptomoneda: personas como Wei Dai, Hal Finney, David Chaum y las probabilidades. -en el favorito, Nick Szabo, cuyos escritos, nos dicen los lingüistas forenses, se asemejan bastante a las opciones de palabras y frases del fundador de bitcoins. Todos, en un foro u otro, han negado ser Nakamoto.

Otros investigadores se han ido en tangentes interesantes pero igualmente infructuosas. Escribiendo para The New Yorker, Joshua Davis se obsesionó con algunos de los deletreos británicos en las escrituras de Nakamoto y se dirigió a las Islas Británicas para encontrar a su autor. Se concentró en Michael Clear, un estudiante de ciencias de la computación con sede en Dublín que había trabajado para Allied Irish Banks en tecnología peer-to-peer y que respondió a las preguntas de Davis con la atractiva frase "No soy Satoshi, pero incluso si Lo era, no te lo diría ". El trabajo de Davis no fue concluyente, pero el comentario de Clear, que más tarde dijo que era una broma inofensiva, significaba que el irlandés estaba inundado de correos electrónicos. Desde entonces, ha negado con vehemencia la creación de bitcoin y ha suplicado a la gente que lo deje en paz.

Convencido de que Davis fue atrapado por una probable campaña de desinformación del fundador -como si la referencia de Nakamoto sobre Britishism y Times of London fuera plantada para dejar huellas- el profesor de periodismo de la Universidad de Nueva York Adam Penenberg volvió su atención a otro lado. En un artículo para Fast Company, señaló tres nombres que habían presentado conjuntamente patentes de cifrado relevantes para criptomonedas en el momento del lanzamiento de Bitcoin: Neal King y Charles Bry, que residían en Alemania, y Vladimir Oksman, que vivían en Estados Unidos. Obtuvo negaciones explícitas de ellos, incluyendo uno de King en el que criticaba a bitcoin por no tener "ningún valor intrínseco". Penenberg no se inmutó por esto y especuló que la declaración de King podría haber sido una pista falsa, pero la evidencia de Penenberg fue circunstancial e inconclusa, y él concedió eso.

Luego vino Ted Nelson, un teórico de la información famoso por acuñar el término hipertexto en la década de 1960. En un monótono videojuego en el que adoptó acentos británicos falsos para imitar a Sherlock Holmes, Nelson declaró que el inventor del bitcoin era el matemático japonés Shinichi Mochizuki y se atrevió a negarlo. Mochizuki no solo tenía la clase de mente capaz de diseñar tal esquema, dijo Nelson, sino que también tenía el hábito sospechoso de dejar silenciosamente sus descubrimientos matemáticos en Internet para que la gente los encontrara. El matemático no ha respondido públicamente al desafío de Nelson, pero otros han encontrado dificultades en el argumento, señalando que Mochizuki no es un criptógrafo y parece que no tiene una gran experiencia en la escritura de código.

Luego, el 6 de marzo de 2014, la revista estadounidense Newsweek relanzó su edición impresa, y por su historia de tapa fue una gran primicia. "El rostro de Bitcoin" era el título, con una imagen artística de una persona sola escondida en negro, una máscara en forma de símbolo de moneda B de bitcoin que se estaba pelando. La periodista Leah McGrath Goodman declaró que había encontrado a Satoshi Nakamoto escondido a plena vista, un hombre japonés estadounidense que

vivía en un suburbio de Los Ángeles cuyo nombre había sido Satoshi Nakamoto antes de que se lo cambiara a Dorian Nakamoto. Decir que la historia se volvió viral sería una subestimación.

Durante varias horas, Newsweek fue el dueño de la historia, pero fueron las principales noticias en todas partes, en la televisión por cable, en Reddit, en Twitter, en el Foro Bitcoin, en periódicos como el nuestro. Todo el mundo estaba asombrado con este cuento, todo el mundo estaba sorprendido de que Newsweek hubiera enjuagado al verdadero Nakamoto. ¡Qué primicia! ¡Qué golpe! Goodman hizo una ronda en el circuito de medios, explicando cómo se había llevado la revista. La intensa reacción a la historia mostró cuánto lucía este mito de Nakamoto en el ojo público. Entonces se puso raro.

Dorian Nakamoto finalmente emergió, horas después de que la revista llegara a los quioscos de periódicos, para enfrentar a la multitud de periodistas que habían tomado posiciones en el jardín delantero. Negó cualquier participación en Bitcoin y lo hizo de una manera tan idiosincrásica que sugería que no era un buen candidato para el perfil del personaje del fundador de bitcoins. Se paró junto a la puerta de su casa y le prometió una entrevista exclusiva al primer reportero para ofrecerle un almuerzo gratis. Un reportero de AP lo hizo rápidamente y lo llevó en un automóvil a un lugar de sushi. Los otros periodistas siguieron, con al menos uno, Joe Bel Bruno, de Los Angeles Times, en vivo twitteando la "persecución" en una escena extrañamente reminiscente de la infame persecución de O. J. Simpson.

Lo más intrigante fue una publicación más tarde ese día en un tablero de mensajes en línea relativamente oscuro propiedad de la P2P Foundation, una organización sin fines de lucro que busca construir aplicaciones peer-to-peer a través de criptografía y herramientas de software. La publicación se hizo a un hilo que data del 12 de febrero de 2009, que había estado inactivo durante años, un hilo iniciado por Satoshi Nakamoto cuando estaba difundiendo la palabra en bitcoin. El nuevo mensaje era simple, pero fue el primero que alguien supo de él en años.

Simplemente dijo: "No soy Dorian Nakamoto".

En el mejor de los casos, el informe de Newsweek no fue concluyente, y en el peor, periodismo descuidado. Aún así, el circo mediático que generó demostró cuánto bitcoin ahora estaba insertado en la conciencia pública y cómo el misterio de Satoshi había energizado la fascinación de la gente, una fascinación que dice mucho más sobre las personas que se apoderaron de ella que sobre la fuente de su fascinación.

¿Qué pensamos? Bueno, el fundador de bitcoin casi seguro que no es Dorian Nakamoto. Lo que nos parece más probable es que, al menos inicialmente, una persona lo haya soñado. Viendo que Wei, Szabo, Finney y Chaum surgieron individualmente con sistemas de moneda digital, parece razonable suponer que el bitcoin también podría ser el proyecto de una persona. De hecho, la mayoría de los elementos para una moneda digital ya se habían establecido; en esencia, Nakamoto tomó un rompecabezas existente, encontró las pocas piezas faltantes y lo armó. También creemos que es muy posible que esta persona haya salido del movimiento Cypherpunk, y que sea posible que, al concebirlo, alistara otros Cypherpunks para ayudar con el proyecto. Las inconsistencias en el estilo de escritura -la inserción ocasional de deletreos británicos, por ejemplo- dan peso a la idea de que un grupo pequeño estaba detrás de esto. Eso probablemente coloque al fundador o grupo fundador de bitcoin en algún lugar de la región de San Francisco / Silicon Valley. Es lo mejor que podemos hacer por ti. Probablemente un hombre, muy posiblemente un grupo.

La idea del grupo nos atrae, en parte porque un pacto como ese le daría a cada miembro una negación plausible, la capacidad de decir "no soy el fundador de bitcoin" cuando los entrometidos periodistas vienen fisgoneando. Sin embargo, igual de importante, incluso si una persona tenía la

idea original de una moneda descentralizada y conectada en red, su desarrollo en última instancia tuvo que convertirse en un esfuerzo grupal, como ya hemos discutido, necesitaba crecer en una comunidad. Como corresponde a esa noción, se dice que a veces se escucha entre los bitcoiners abordar el misterio de la identidad del fundador. Es una especie de grito de guerra, y parece que en la relación simbiótica entre bitcoin y su comunidad, la forma en que uno fortalece al otro, realmente explica la realidad detrás del mito.

"Todos somos Satoshi".

Hasta cierto punto, el desarrollo más temprano de la comunidad bitcoin fue una consecuencia natural de la naturaleza descentralizada y de código abierto de su código fuente de computadora. Los proyectos de código abierto tienen una historia distinguida de atraer a personas inteligentes para unirse a las comunidades dedicadas al perfeccionamiento y la evangelización, al igual que con la comunidad que ha apoyado el sistema operativo Linux de código abierto durante décadas. Del mismo modo, el software de código abierto de bitcoin ha sido esencial para la ampliación de su comunidad.

No compra el software de bitcoins como lo haría con otros productos, lo que significa que no es solo un cliente. Además, no hay ningún propietario del software, a diferencia, por ejemplo, de PayPal, que es parte de eBay. Por eso, todos los que lo usan tienen una relación definida con el programa bitcoin. Aunque eBay vende un servicio, es dueño del producto. El usuario final nunca tiene ninguna propiedad del producto. Bitcoin elimina esa distinción.

Cualquiera puede ir a la Web, descargar el código sin costo y comenzar a ejecutarlo como minero. Enhorabuena, ahora es un "nodo", uno de los miles responsables de mantener la red en funcionamiento mediante la confirmación de transacciones y la generación de monedas. La comunidad de personas que han dado este paso ejecuta bitcoin. Todo el mundo que ha invertido tiempo y poder de computación es, en un sentido real, el sistema. Esto te da una participación en su futuro. Ayuda a construir una comunidad de usuarios dedicados.

Esa comunidad creció lentamente al principio, con la difusión de la palabra en círculos de criptografía y en varios foros en línea. Los puñados a la vez estaban descargando el código hasta 2009. Los foros que Nakamoto había establecido en bitcoin.org atraían a un par de docenas de nuevos usuarios cada mes. Algunos de ellos eran programadores informáticos y codificadores serios, del tipo que se sienten atraídos incesantemente por ideas nuevas e interesantes. Una de esas personas fue Gavin Andresen, quien en mayo de 2010 tropezó con un artículo sobre interesantes proyectos de software de código abierto en el que se mencionaba bitcoin. "Me despertó mi interés", dice Andresen, pero su naturaleza escéptica lo obligó a realizar una gran diligencia debida. "Al principio, pensé que esto no podría funcionar, pero leí el libro blanco de Satoshi y luego básicamente todo lo que se había escrito sobre bitcoin hasta ese momento. Luego leí el código fuente... y me convencí de que no iba a infectar mi computadora con algún virus desagradable si lo ejecutaba, y luego decidí que realmente podría funcionar ". El 28 de mayo, se registró como usuario en el Foro Bitcoin.

Para obtener sus "pies mojados", Andresen comenzó un proyecto que llamó Bitcoin Faucet, que era literalmente un plan de regalo. Compró diez mil bitcoins en Bitcoin Market, uno de los primeros intercambios de bitcoins, por $ 50 y se los regaló a todos, con la intención de expandir el uso, hacer crecer la comunidad y aumentar la divisa. Andresen creía que Bitcoin necesitaba que la gente lo usara y difundirlo si se animaba a los desarrolladores a construir herramientas útiles a su alrededor. De esta manera, vio a Bitcoin Faucet como "la clave para poner en marcha la infraestructura" del ecosistema bitcoin. Cuando Andresen se insertó en la comunidad a través de las salas de chat de bitcoins, su actitud tranquila y cuidadosa pronto atrajo la atención de

Nakamoto. El creador de Bitcoin todavía estaba activo en la comunidad, todavía trabajaba con personas y seguía respondiendo preguntas. Andresen se convirtió en un socio clave de Nakamoto en el trabajo de desarrollo, y hoy, con el fundador fuera de las ondas públicas, es el desarrollador principal de bitcoin.

Sin embargo, al principio, Andresen era un jugador suplente. Cuando descubrió Bitcoin por primera vez en mayo de 2010, otros adoptadores anteriores más allá de Nakamoto estaban teniendo mucha más influencia en el desarrollo de la comunidad. Uno en particular cambiaría la trayectoria de bitcoin.

Nos encontramos por primera vez con Laszlo Hanyecz en el capítulo anterior. Él es el codificador cuyo descubrimiento de la minería basada en GPU cambiaría rápidamente la forma en que funcionaba la red minera más importante de bitcoins. La contribución de Hanyecz al desarrollo de bitcoin, y en particular al pulido de su comunidad y cultura, va mucho más allá de su lugar en una de las historias fundamentales de la comunidad.

El 21 de mayo de 2010, Hanyecz comió una pizza de queso de Papa John's. Nada sobre la pizza en sí fue extraordinario. Lo extraordinario fue la forma en que lo pagó.

A poco más de un año de la existencia de Bitcoin, el codificador basado en Jacksonville, Florida ya había minado un montón de bitcoins. Su descubrimiento de tarjetas gráficas había acelerado más de ochocientas veces la capacidad de computación que podía aplicar a la minería, dándole un dominio virtual sobre las recompensas que el protocolo de bitcoin estaba pagando en ese momento; estaba recibiendo aproximadamente la mitad de todos los bitcoins extraídos. "Tenía mucho", dice, tantos que su problema era qué hacer con ellos. "Si nadie los tomará, no valen nada", pensó. Entonces Hanyecz tuvo una idea.

"Pagaré 10.000 bitcoins por un par de pizzas, como quizás dos grandes, así que me quedan algunas para el día siguiente", escribió el 18 de mayo en el Bitcoin Forum, que solo contaba con unos 230 miembros. No tenía motivos para pensar que alguien lo aceptaría. Nadie había usado bitcoins en el mundo real. Ciertamente, ninguna pizzería en su parcela de Florida aceptaría el bitcoin como forma de pago. Hanyecz necesitaba un intermediario y calculó que valía alrededor de $ 41 en base a los precios que se cotizan en algunos mercados rudimentarios de bitcoin, le daría los dos pasteles y compensaría a los intermediarios por los problemas.

Después de tres días, un bitcoiner en Inglaterra, que fue por el nombre de chat jercos, se intensificó. Jercos hizo un pedido en línea con un Papa John's en Jacksonville y pagó a través de Internet con una tarjeta de crédito. Hanyecz transfirió los bitcoins de su propia billetera al remitente en Inglaterra. Poco después, un repartidor confundido llegó a la casa de Hanyecz con los dos pasteles y una mirada perpleja en su rostro. "Pizza fresca", dijo, "de Londres". Fue el primer paso de la moneda para convertirse en dinero real, y por una métrica convincente, ha recorrido un largo camino desde entonces. Si valoramos los bitcoins que Hanyecz gastó en 2010 según su precio de mercado en agosto de 2014, esas dos pizzas le costaron $ 5 millones.

En el año y medio transcurrido desde que Nakamoto lanzó su primer globo de prueba, la comunidad bitcoin había crecido lentamente. En aquel entonces, dice Hanyecz, "era como un club de radioaficionados". Muy unidos, estaban unidos por su interés en el bitcoin, pero no estaban seguros de su futuro. En marzo de 2010, por ejemplo, uno de los primeros miembros del foro que se hizo llamar SmokeTooMuch ofreció subastar diez mil bitcoins. Su oferta inicial fue de $ 50. No hubo tomadores.

Los nuevos miembros, a menudo confundidos acerca de lo que estaban haciendo y propensos a cometer errores, encontraron un grupo de bienvenida. "Entonces, finalmente conseguí que mi cliente comenzara a generar", escribió un usuario llamado AgoraMutual, luego de descargar el software a su computadora portátil. "Mi primera transacción completada resultó en +50 monedas. ¡Yay! "Pero no estaba seguro de si su computadora todavía estaba generando monedas. Al parecer, el programa simplemente había dejado de funcionar. Pronto obtuvo una respuesta. Estaba leyendo el programa mal. Él todavía estaba generando monedas. ¿El demandado? Satoshi Nakamoto. "En aquel entonces, había mucha gente ayudándose entre sí", dijo Hanyecz, uno de ellos siendo Nakamoto.

Laszlo Hanyecz's pizzas, pagadas con bitcoin
(Cortesía de Laszlo Hanyecz)

Hanyecz describió una comunidad en la que las personas se ayudaban mutuamente a superar los baches técnicos en el camino que acompañaban los esfuerzos por descubrir esta nueva tecnología. A medida que aprendieran más, las nuevas personas se convertirían en ayudantes y comenzarían a experimentar con el código bitcoin. Una de las otras contribuciones tempranas de Hanyecz incluyó escribir una versión que podría funcionar en computadoras Mac.

La venta de la pizza y el aumento de la extracción de GPU pronto cambiarían la experiencia. Hanyecz dejó la oferta en pie, imaginando que si pudiera extraer suficientes bitcoins para comprar una pizza a la semana, estaría bien. Al principio, sus nuevas y potentes máquinas, que según él "sonaban como una aspiradora cuando estaban ocupadas", lo conseguían fácilmente. Hizo varias ofertas más de pizza, pero luego notó un problema: no estaba extrayendo tantos bitcoins como antes. Su oferta, que mostraba al mundo exterior que los bitcoins tenían un valor real, había llamado la atención en línea. Eso, a su vez, atrajo la competencia en la minería, con todos los recién llegados configurando la estrategia de GPU que Hanyecz había sido pionera y con más y más tarjetas gráficas desplegadas. El algoritmo de Nakamoto lanzó solo un número finito de bitcoins cada día; más gente, con hardware más potente a su disposición, aumentó la dificultad de los acertijos matemáticos, lo que hace que la minería sea cada vez más lenta y menos gratificante.

"En una semana, la dificultad subió tan alto que la gente común no podía extraer", dijo Hanyecz. Donde antes recibía decenas de miles de monedas al mes, pronto estaba extrayendo solo un bitcoin por día, y estaba agotando su oferta comprando las pizzas de Papa John. Él dice que continuó con la oferta de pizza cuatro o cinco veces, gastando alrededor de 40,000 BTC en total.

Nakamoto no estaba muy contento con este cambio, dijo Hanyecz, recordando las interacciones del fundador en la sala de chat. El fundador quería un sistema al que pudieran acceder las personas comunes que usan equipos comunes. Se estaba volviendo imposible explotar sin poderosas computadoras. Mientras que dos semanas antes, la CPU en una computadora normal podía entregar al propietario varios cientos de bitcoins, ahora ganaría uno o dos si el propietario tuviera suerte. En poco tiempo, la minería se había vuelto más costosa: los costos de la energía se habían disparado. Ya no era una empresa sin costo para un aficionado a la radioafición. En términos de costos, a algunos les pareció más sensato comprar bitcoins. Con el tiempo, la gente comenzó a hacerlo, y esta es la razón por la cual el alijo de bitcoins de Hanyecz todavía valía una suma decente.

El truco de la pizza había más que probado el punto original de Hanyecz. Se generó un nuevo interés en bitcoin, y la comunidad de usuarios comenzó a expandirse. En junio, 55 personas se registraron en el Foro Bitcoin. En julio, 370 lo hicieron. El precio también se estaba moviendo. Durante cinco días, el tipo de cambio de Bitcoin saltó nueve veces, de $ 0.008 a $ 0.08 el 18 de julio. Un solo bitcoin ahora por primera vez valía más de un centavo. En el verano de 2010, cuando Hanyecz estaba terminando su empresa de pizza, este interés en rápida expansión estaba a punto de dar lugar a otras empresas que ampliarían enormemente la comunidad, aunque de maneras que atrajeron una gran controversia. En esa misma fecha del 18 de julio del pico de precios cíclico de Bitcoin, un nuevo usuario apareció en el Foro Bitcoin. "Hola a todos", escribió, "Acabo de poner un nuevo intercambio de bitcoins". El nombre del usuario era mt gox.

El usuario del foro era un programador desempleado llamado Jed McCaleb. McCaleb era una raza diferente de los primeros bitcoiners, los aficionados y los maleantes. Fue uno de los primeros de un nuevo grupo que pronto se vería atraído por Bitcoin: el emprendedor. Con su llegada vendrían tanto un gran crecimiento como los problemas que pueden traer.

En 2007, McCaleb había comenzado una plataforma en línea para intercambiar cartas relacionadas con el juego Magic: The Gathering, que es un juego de cartas intercambiables con millones de jugadores. Él lo llamó Mt Gox, una amalgama de "Magic: The Gathering Online Exchange". La plataforma de tarjetas de intercambio no despegó como él había esperado, pero McCaleb se aferró al nombre de dominio. En 2010, se dio cuenta del bitcoin y se dio cuenta de que carecía de una aplicación de negociación intuitivamente fácil de usar para que las personas compraran y vendieran criptomonedas. Entonces él creó uno y lo colocó bajo el viejo monte. El nombre de dominio Gox, del cual su nuevo intercambio también tomaría su nombre. Atrajo mucho interés, atrayendo la atención de algunos nuevos inversores notables que buscan entrar en este nuevo y emocionante mercado. El comercio aumentó rápidamente. El primer día de operaciones, el 17 de julio, el volumen fue de 20 BTC. El 10 de octubre, alcanzó 187,000 BTC. El volumen fue irregular, pero en el otoño, el intercambio había visto un pico de volumen tan alto como 200,000 BTC, y 50,000 días eran comunes. Para noviembre de 2011, las operaciones promediarían 27,541 BTC por día.

El crecimiento fue emocionante, pero McCaleb tiene un historial de proyectos iniciales y poco después de perder interés. Esto no sería diferente. En marzo de 2011, dijo al foro que si bien había sido "divertido e interesante" establecer el monte. Gox "enloquecido" y verlo crecer, ya no tenía tiempo suficiente para administrarlo, así que se lo vendió a "alguien más capaz de llevar el sitio al siguiente nivel". Ese alguien era el programador francés Mark Karpelès, conocido por algunos en foros de chat de bitcoin como MagicalTux. Amante de los pasatiempos japoneses de manga y cosplay, Karpelès rápidamente movió el monte. La sede de Gox en Tokio.

monte Gox fue el primer intercambio importante de bitcoins, y en aquellos primeros días era prácticamente el único lugar para intercambiar monedas. Como el primer negocio realmente

visible en el mundo bitcoin, validó aún más que esta moneda digital era mucho más que un simple juguete para los expertos en tecnología. Traería muchos nuevos bitcoiners a la comunidad. Mientras que el Foro Bitcoin había agregado nuevos miembros a una tasa promedio de 36 por mes en sus primeros ocho meses de existencia para elevar su membresía total a 286 en junio de 2010, en adelante desde julio, el mes en que McCaleb lanzó su sitio, el foro agregó varios cientos de nuevos usuarios cada mes y a un ritmo creciente. En febrero de 2011, las adiciones mensuales cruzaron 1,000 por primera vez, y en junio de ese año, con Karpelès a cargo en el monte. Gox, 14,483 miembros se unieron al Foro Bitcoin para llevar una membresía total a 31,247.

Para la mayor parte de los clientes de Mt Gox, era su primera puerta de entrada al bitcoin, su primera experiencia con la criptomoneda. Pero el intercambio se había desarrollado rápidamente, como una diversión, y estaba mal equipado para manejar los desafíos de una plataforma global de comercio de divisas. Karpelès se encontró luchando por actualizar la plataforma, ya que el valor de Bitcoin aumentó de $ 1 en abril a $ 30 en junio; durante ese mismo período, cuentas en el monte. Gox se levantó de seis mil a sesenta mil. Junio también traería el primer gran desafío para la supervivencia de bitcoins.

Alrededor del 13 de junio de 2011, la gente comenzó a notar que faltaban bitcoins en su monte. Cuentas de Gox Parecía que un pirata informático había accedido al sistema de intercambio y había robado una gran cantidad de monedas: los informes indican que la cantidad oscila entre dos mil y medio millón de monedas; Karpelès dijo que era mil. Poco después, las monedas comenzaron a aparecer en el mercado en venta, por un centavo. Estas órdenes de venta se cumplieron, y el resultado? Los precios de Bitcoin se desplomaron para satisfacerlo, el valor de la moneda cayó de $ 17 a meros centavos. Peor aún, las contraseñas y otra información del cliente comenzaron a circular, lo que indica que la violación fue más que una o dos cuentas pirateadas.

La situación finalmente se estabilizaría. Pero antes de eso, Karpelès tuvo que dar el paso sin precedentes de cerrar el intercambio y deshacer los intercambios. Esto calmó la situación, pero las personas no tenían otra opción que confiar en el sitio. En julio de 2011, el monte. Gox manejaba el 80 por ciento de todas las operaciones de bitcoin. Esta primera crisis en el monte. Gox -una aún más grande iba a aparecer tres años más tarde- mostró la vulnerabilidad que podría venir con un rápido crecimiento en el mundo de bitcoins.

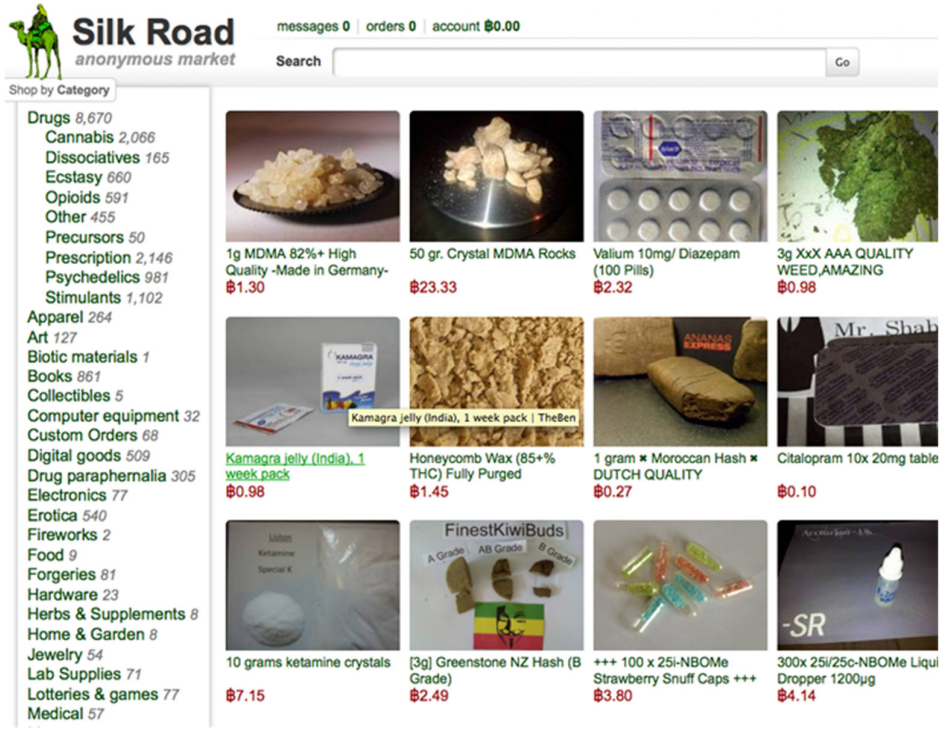
El episodio también reveló la importancia de ese elemento clave del desarrollo de la moneda al que seguimos volviendo: la confianza. Mientras que el nombre de Karpelès es bien conocido hoy en día, en 2011 pocos de la comunidad de codificación que habían interactuado con MagicalTux en los foros de chat sabían quién dirigía el Monte. Gox. El servicio al cliente del intercambio era notoriamente pobre. En una amarga ironía, una moneda basada en un intercambio sin confianza ahora estaba siendo controlada por un intercambio en el que la gente no confiaba, pero que estaba obligada a usar.

El primer gran Monte. La crisis de Gox anunció el inicio de la fase de Wild West de Bitcoin. La comunidad se había transformado de una camarilla de primeros fanáticos de la tecnología a una en la que una nueva generación de aventureros veía todo tipo de esquemas de hacerse rico rápidamente, todo dentro de lo que parecía ser un refugio sin ley. Las manifestaciones más extremas de esa idea llegarían a existir cuando otro nuevo miembro del foro publicó el 1 de marzo de 2011, "Silk Road está en su tercera semana después del lanzamiento y estoy muy satisfecho con los resultados". En referencia al nuevo sitio como un "mercado anónimo en línea", preguntó a los miembros de la comunidad qué pensaban del sitio. Con el foro de Bitcointalk ahora con 5.343 miembros, el puesto de Ruta de la Seda recibió cientos de respuestas. A algunos les gustó la idea, algunos la odiaban y algunos, comprendiendo de inmediato sus implicaciones, hicieron bromas sobre ser arrestados por los policías solo por responder.

Silk Road, que permitía a los compradores y vendedores disfrazar sus identidades, era administrado por una persona que usaba el controlador Dread Pirate Roberts (un personaje del libro y la película The Princess Bride). Hizo uso de la red Tor, un sistema de cifrado sofisticado y un navegador web que hace que el tráfico web sea casi imposible de rastrear, para mantener ocultas las identidades de compradores y vendedores. Fundamentalmente para nuestros propósitos, Silk Road usó el bitcoin como su medio de intercambio.

Si bien Silk Road ostensiblemente permitió la venta de casi cualquier cosa, su producto central se convirtió rápidamente en drogas. Absolutamente cualquier droga imaginable estaba disponible en vendedores de todo el mundo, así como en muchas otras sustancias y servicios ilícitos. El sitio web Gawker, en junio de 2011, lo comparó con Amazon, "si Amazon vendiera drogas que alteran la mente". En realidad, era más parecido a eBay, donde los compradores y vendedores se emparejaban. De todos modos, su reputación se extendió como un reguero de pólvora.

"El sitio se popularizó mucho más rápido de lo que esperábamos y no estábamos preparados para el tráfico", escribió el cartel, que se inspiró en el nombre silkroad, en el foro. "Realmente no esperábamos que todos los medios se entendieran tan rápido, y deberíamos habernos preparado con un sistema semicerrado. Haremos todo lo posible para salir del centro de atención y esperamos que los méritos de Bitcoin se conviertan en el centro de atención. "Eso no sucedió. Otros sitios de noticias recogieron la historia. Algunos proporcionaron instrucciones sobre cómo encontrar el sitio. Esto fue notado no solo por tu embriagador promedio, sino por la aplicación de la ley y los políticos. El senador por Nueva York Chuck Schumer lo llamó "el intento más descarado de vender drogas en línea que jamás hayamos visto" y pidió que se cerrara.



La página Silk Road
(Fuente: Business Insider)

La respuesta en el Foro de Bitcoin fue mixta. Algunos están preocupados por los agentes de la DEA que se infiltran en el sitio de Silk Road. Otros estaban vigilando para ver si el sitio aún estaba

activo. Algunos querían unirse; Silk Road y el monte. Gox fueron los dos negocios de bitcoin más prominentes. "Una lesión en uno es una lesión para todos", escribió un afiche. Pero otros estaban preocupados por las consecuencias. Un cartel respondió con un humor típicamente cínico: "¡Creo que ahora están trepando por nuestras ventanas!"

A pesar del calor de los federales, Silk Road operaría encriptada, protegida y totalmente abierta durante más de dos años después de eso, con miles de listados de drogas, servicios de piratería, medios pirateados e incluso servicios de falsificadores. Tenía casi 1 millón de cuentas. Las estimaciones de sus ventas variaron. En agosto de 2012, Andy Greenberg de Forbes estimó que estaba haciendo $ 22 millones en ventas anuales, el doble que seis meses antes. El FBI calculó que entre el 6 de febrero de 2011 y el 23 de julio de 2013, más de 1.2 millones de transacciones en el sitio generaron ventas de 9.5 millones de bitcoins. (Dadas las salvajes fluctuaciones en el precio durante ese tiempo, es difícil extrapolar cuánto es eso en dólares).

Llegaría a su fin en octubre de 2013 cuando el FBI arrestó a un nativo de Texas llamado Ross Ulbricht en una biblioteca de San Francisco. La agencia lo acusó de lavado de dinero y conspiración para traficar narcóticos, a lo que Ulbricht, al momento de escribir este documento, se declaró inocente; su abogado ha dicho que no es Dread Pirate Roberts. La agencia también dijo que solicitó seis asesinatos por contrato, aunque no hubo evidencia de que alguien haya muerto. También incautó decenas de miles de bitcoins por valor de millones de dólares, convirtiendo al FBI en un titular de billetera de bitcoin, uno de los miembros más grandes e improbables de la "comunidad" bitcoin. Esos sucesos posteriores traerían otro punto de inflexión en el desarrollo de Bitcoin, anunciando una era de regulación gubernamental. Pero en los primeros años en los que nos enfocamos, Silk Road, a pesar de su notoriedad, jugó un papel clave en el desarrollo de bitcoins, al expandir su comunidad de usuarios. Al igual que el porno en línea fue una de las primeras grandes empresas rentables en los primeros días de Internet, lo que demuestra que había un modelo de negocio allí, Silk Road fue el primer gran negocio de bitcoins. Entonces, aunque los productos del sitio podrían haber sido moralmente ofensivos para muchos, como sucedió con la pornografía, sí probaron que el bitcoin podría funcionar como una moneda legítima. Junto con Mt Gox, que durante el mismo período proporcionó pruebas de un interés especulativo e inversor en la moneda, ayudó a poner el bitcoin en manos de miles de recién llegados, muchos de los cuales ahora buscaban usarlo para otras cosas además de las drogas. Silk Road fue un catalizador crítico para esta fase particularmente rápida de formación de la comunidad.

A pesar de que su comunidad se expandió rápidamente, Bitcoin aún estaba lejos de ser un nombre familiar en 2011 y 2012. Wall Street y Washington lo ignoraron en su mayoría. Aún así, esa expansión atrajo a otros empresarios a seguir la iniciativa de McCaleb y Dread Pirate Roberts. Nuevas ideas comenzaron a surgir para las empresas que crearían la infraestructura financiera, técnica y social para sostener el crecimiento de bitcoins. Críticamente, fue un asunto global.

Durante este período, surgieron nuevos intercambios como competidores del monte. Gox, entre los primeros y más notables, Tradehill en los Estados Unidos, formado por Jered Kenna, y Britcoin en Londres. Otros seguirían. Las plataformas de negociación para bitcoins comenzaron a aparecer para todas las monedas, desde el zloty polaco hasta el real brasileño. La integración requerirá interfaces más sencillas. Del mismo modo que Microsoft Outlook y Hotmail hicieron accesible el correo electrónico para la persona promedio, Bitcoin también necesitaría billeteras digitales más fáciles de usar. Efectivamente, las nuevas empresas comenzaron a ofrecerlas, destacadas por la fundación de Blockchain.info, la ahora reconocida firma de billetera y análisis, en agosto de 2011. Mientras que la billetera de Nakamoto era torpe y difícil de descifrar para los forasteros, la interfaz más bonita de Blockchain ayudó a los recién llegados a concebir con mayor facilidad una versión digital de las billeteras físicas que guardaban en sus bolsillos.

Era necesario resolver otro problema: la larga espera interminable para obtener el dinero fiduciario tradicional dentro, fuera y entre los intercambios de bitcoins. Para solucionar esto, Charlie Shrem, un estudiante universitario de 21 años de Brooklyn con experiencia en comercio electrónico, se asoció con el operador de bitcoin Gareth Nelson del Reino Unido para fundar el servicio de transferencia Bitcoin BitInstant en agosto de 2011. El servicio, por una tarifa, reenviará dinero a crédito para acelerar la transferencia de fondos entre los intercambios. Los servicios profesionales de procesamiento de pagos también surgieron en esta época, con BitPay y Coinbase entrando en escena en previsión de ofrecer interfaces fáciles para que los comerciantes reciban bitcoins y, si lo desean, convertirlos en dólares. Mientras tanto, SatoshiDice, un servicio de juego de bitcoin en línea que usa la tecnología de bitcoin para ofrecer un modelo de apuestas "probadamente justo" para que los usuarios puedan confiar en que su juego de azar impulsado por computadora no fue amañado, despegó. A mediados de 2012, SatoshiDice, cuyo sistema interno requería la generación de miles de pequeñas transacciones, representaría la mitad de todas las transferencias de bitcoin en términos de volumen, si no de valor. A medida que surgieron todos estos desarrollos y oportunidades para nuevas empresas, los primeros inversores comenzaron a concebir formas de fomentar más innovación. Uno de los primeros fue Peter Vessenes, quien a fines del verano de 2011 creó CoinLab, una incubadora con sede en Seattle para desarrollar nuevos talentos y empresas nuevas dedicadas a los productos de bitcoin.

También aparecieron otros símbolos de la mayoría de edad de la comunidad. Comenzaron los primeros artículos de prensa sobre Bitcoin, y Bitcoin Magazine, fundada por Mihai Alisie y Vitalik Buterin en 2011, comenzó a publicar una edición impresa en mayo de 2012, convirtiéndose en la primera publicación seria dedicada a las criptomonedas. Las conferencias de Bitcoin se hicieron más comunes, con Nueva York, Londres y Praga en el circuito temprano. En septiembre de 2012, se fundó la Fundación Bitcoin en Seattle. Fundado por el desarrollador líder de bitcoin, Andresen, BitInstant's Shrem, Mt Gox's Karpelès, CoinLab's Vessenes, el inversionista y "evangelista" Roger Ver, y el abogado Patrick Murck, intentaron representar a la creciente comunidad bitcoin a nivel internacional y, en las palabras de su documento fundador, ayudar a "estandarizar, proteger y promover el uso de Bitcoin criptográfico" dinero para el beneficio de los usuarios de todo el mundo ".

En ese momento, el Foro de Bitcoin tenía alrededor de sesenta y ocho mil miembros, más de unos treinta y cien a finales de 2010. Pero la comunidad estaba creciendo no solo en el entorno del ciberespacio. En todo el mundo, el fenómeno de la "reunión" de bitcoin despegó, y los entusiastas de la criptomoneda formaron grupos informales que se reunirían en bares y cafeterías de todo el país, desde Buenos Aires hasta Beijing. De esta manera, la comunidad bitcoin recibió una base física, pero que, de manera importante, no tenía una base central.

Los eventos más siniestros también desafiaron la resolución y solidaridad de la creciente comunidad. Se reportaron los primeros robos importantes de bitcoin. A partir de marzo de 2012, se produjeron robos por un total de más de $ 500,000 de Bitcoinica, una compañía que permitió a los inversionistas especular sobre bitcoin con contratos de derivados. La compañía dijo que su cuenta en el monte. Gox había sido comprometido por los piratas informáticos. El software principal de Bitcoin permaneció intacto, pero las empresas mostraban vulnerabilidades. Mientras tanto, varias empresas nuevas ya enfrentaban problemas, particularmente debido a relaciones incómodas con bancos reacios y servicios de procesamiento de pagos, negándoles un vínculo con el mundo de moneda fiduciaria y destacando un problema que continuaría en los próximos años. El intercambio de Kenne Tradehill se vio obligado a cerrar sus puertas en febrero de 2012, solo once meses después de su fundación.

Sin embargo, todo el tiempo, el precio de Bitcoin subió, subió y subió. Hubo hipo, seguro, especialmente los asociados con el monte. Gox a mediados de 2011, pero entre el inicio de 2011 y

el final de 2012, cualquiera que haya invertido habría tenido un retorno de 5.000 por ciento, con un precio que pasaría de $ 0.25 a $ 6 a fines de 2011 y luego a $ 13. otro año después A pesar de que el 28 de noviembre de 2012, el software básico de bitcoin, según lo programado, redujo a la mitad el pago de bitcoins para los mineros a veinticinco por bloque, el interés en la minería de bitcoins continuó aumentando. Las personas se prepararon para el inicio en enero de plataformas de minería dedicadas y de alta potencia con chips ASIC (circuito integrado de aplicaciones específicas). Fue un período de auge. La carpa comunitaria se estaba ensanchando cada vez más.

De hecho, la tienda se estaba ampliando de maneras diferentes y confusas. Una era que para el 2011, el bitcoin era imitadores inspiradores, algunas copias directas, otras claras intentos de eliminar lo que se veía como algunos de los defectos de bitcoin. Los Altcoins, como se los conocía, usarían los mismos aspectos o similares del sistema de bitcoin, todo esto fue posible gracias al protocolo de código abierto de bitcoin y su falta de propietario. Cualquiera puede descargar el software, copiarlo y crear algo nuevo a partir de él. Demandas por infracción de derechos de autor o patente simplemente no son una preocupación.

Al momento de escribir esto, existen varios cientos de estas monedas digitales, la mayoría demasiado pequeñas para ser dignas de mencionarse, pero algunas tienen muchos seguidores. Todos están muy por debajo del bitcoin en rangos. Litecoin, la más antigua y más grande de las altcoins, tenía una capitalización de mercado de aproximadamente $ 150 millones en el momento de la escritura. El de Bitcoin fue de alrededor de $ 6.5 mil millones. Algunos son proyectos de aspecto dudoso, esquemas bastante flagrantes de bombeo y descarga. Algunos no son realmente competidores del bitcoin en absoluto porque existen con el propósito de crear nuevas formas de comercio descentralizado a través de la tecnología blockchain: exploraremos algunos de ellos en el capítulo 9. Pero muchos son intentos legítimos de crear otra forma, y posiblemente una forma mejor, de dinero basado en criptomonedas.

Algunos de ellos han desarrollado seguidores leales, lo que contribuye a la impresión de una comunidad de criptomonedas más variada que la de bitcoin. Muchos bitcoiners dan la bienvenida a estos proyectos como nuevos elementos de la misma revolución de criptomonedas en la que participan. Pero otros son abiertamente hostiles a lo que ven como intrusos, por temor a que los movimientos nacientes que se agrupan a su alrededor puedan menoscabar la misión más amplia del cambio.

Al mismo tiempo, el desarrollo de la comunidad en torno a estas altcoins es instructivo para la cuestión más amplia de cómo se desarrollan las comunidades en torno a las criptomonedas. Los bitcoiners pueden aprender de cómo algunas de ellas han despertado las pasiones. Un ejemplo: dogecoin, un altcoin que comenzó como una broma por Billy Markus y Jackson Palmer en diciembre de 2013, que rápidamente cobró vida propia. El "doge" se apropió de un meme de Internet que comenzó con un espectáculo de marionetas de 2005 en YouTube, en el que uno de los títeres escribe mal el perro como dux, y el otro lo pronuncia mal como "dohj". Ese nombre fue aplicado por otra persona a una foto de un perro Shiba Inu que parecía estar sonriendo. Para su software, dogecoin tomó prestadas algunas de las ideas del fundador de litecoin, Charlie Lee, quien había modificado el sistema de minería para obtener sus monedas, de modo que los mineros no estuvieran tan incentivados a acumular poder de computación ávido de energía en competencia entre ellos como lo estaban con bitcoin. Pero igual de importante, si no más, el atractivo de Dogecoin fueron los dos objetivos principales que su comunidad emergente se propuso: dogecoin iba a ser divertido, y sus miembros iban a usar su moneda para hacer buenas acciones. Dogecoin iba a ser filantrópico.

El interés en la moneda subió, al igual que su precio en los mercados de criptomonedas, donde cotizaba contra los bitcoins, que luego podían venderse en dólares. Esto significaba que los

dogecoins tenían un valor real y podían usarse para recaudar dinero por causas. Un miembro de la Fundación Dogecoin leyó que el equipo jamaiquino de trineo no tenía fondos para un viaje a los Juegos Olímpicos de Sochi en 2014 y propuso recaudar dinero para su viaje. A través de campañas lanzadas en Reddit y en otros lugares, con instrucciones sobre qué billetera enviar dogecoins, rápidamente aumentaron el equivalente a $ 25,000 en su moneda. Luego, alguien sugirió pozos de agua limpia en Kenia. Recaudaron $ 30,000 para pozos en Kenia. Recaudaron dinero para una cafetería en Manchester, Inglaterra. Sin embargo, nuestro esfuerzo favorito de dogecoin tenía más que ver con el marketing que con la filantropía. Alguien leyó sobre un joven piloto de NASCAR, Josh Wise, que corría sin un patrocinio. La persona sugirió -de nuevo, en una alondra- que recaudaran dinero para comprar un patrocinio con Wise, con el fin de correr la voz. En poco tiempo, los perversos se unieron a la idea, transfirieron monedas a la billetera designada y recaudaron más de $ 55,000 (alrededor de 67 millones de dogecoins), lo suficiente para que su amada Shiba Inu apareciera en la capucha del Wise # 98 Moonrocket, que hizo debut en mayo de 2014 en el Talladega Superspeedway.

"Doge es una criptomoneda de Internet", dijo el locutor de Fox en la televisión nacional. "No se transmite en dólares, pero una victoria aquí pagaría 596,664,147 dogecoins".

En aproximadamente cuatro meses, se materializó una comunidad de miles de personas. Su pasión y celo por su marca ha catapultado al dogecoin de una broma basada en un meme a lo que podría ser una criptomoneda relativamente legítima. Cuando GoCoin decidió que comenzaría a ofrecer servicios de procesamiento de pagos en dogecoin, así como bitcoin y litecoin, el presidente Brock Pierce explicó que fue impulsado por el poder de su comunidad. "La comunidad lo es todo por una moneda", dijo.

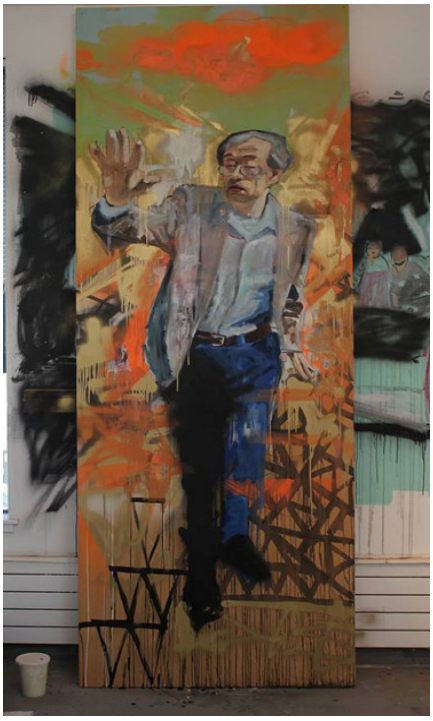
La pregunta es si la aparición de comunidades de altcoin como esta socava la comunidad bitcoin en general o la beneficia. Algunos se preguntan si estos imitadores simplemente le quitarán cuota de mercado a bitcoin, aunque con la capitalización de mercado de bitcoin más de diez veces mayor que las noventa y nueve nuevas altcoins más altas, ninguna amenaza de ese tipo surgió en septiembre de 2014. Otros piensan que al expandir ambos el rango de innovación tecnológica y la marca y la producción cultural asociadas con la criptomoneda, estas comunidades alternativas están ayudando a una comunidad de criptomonedas más amplia a cumplir un propósito más amplio y compartido.

* * *

El componente filantrópico de dogecoin brinda una valiosa lección a bitcoiners sobre el poder de las buenas acciones para fomentar el apoyo. Dentro de la comunidad bitcoin, un ethos similar se ha desarrollado por sí mismo. Muchos bitcoiners han buscado vivir la esperanza de sus antepasados de que las criptomonedas podrían desempeñar un papel en la creación de una sociedad menos cáustica y más humana. Andreas Antonopoulos, jefe de seguridad del proveedor de billeteras Blockchain.info y una destacada personalidad de bitcoin, recaudó unos 21,000 dólares a través de bitcoin en un fondo dedicado para Dorian Nakamoto, el hombre señalado incorrectamente en marzo de 2014 por la revista Newsweek como Satoshi Nakamoto. El escritor de Forbes, Andy Greenberg, comenzó un esfuerzo para recaudar bitcoins para Hal Finney, el programador que había ayudado a Nakamoto a establecer Bitcoin, y que se enfrentaba a importantes facturas médicas por su debilitado ALS. Sean's Outpost es un refugio para personas sin hogar en Pensacola, Florida, financiado casi en su totalidad con donaciones de bitcoin. Estos esfuerzos y otros como estos muestran la huella inconfundible de los primeros bitcoiners, que querían que su moneda se usara como una herramienta para empoderar a las comunidades y ayudar a los menos afortunados dentro de ellas. Pero también son conscientemente parte del esfuerzo más amplio de construcción de la comunidad. Si tales esfuerzos pueden ayudar a mejorar la imagen de bitcoin, se puede conquistar a más adeptos, y con el tiempo eso significa que realmente se puede convertir el bitcoin en una moneda.

La filantropía ayuda a difundir físicamente el bitcoin y crear una imagen positiva para él, todo lo cual funciona directamente en la expansión de la comunidad. Pero también es importante que aquellos que se han unido al núcleo de creyentes mantengan su pasión. En esta parte de la formación y reafirmación de la comunidad, los que crean productos culturales tienen un papel que desempeñar. Así como las canciones que se cantan en los partidos de fútbol, las obras de arte que representan las barras y estrellas en la parte posterior de Jeeps y los conmovedores recitales de la Declaración de Independencia contribuyen a pulir la fe de los estadounidenses en la grandeza de su nación, también la producción cultural puede ayudar a fortalecer otras comunidades, incluso una formada alrededor de una moneda. Y así encontramos literatura bitcoin, poesía bitcoin, obras de bitcoin, fotografía bitcoin y canciones bitcoin. Es una demostración sorprendente de cuánto ha capturado esta idea la imaginación de las personas. Nadie escribe canciones sobre PayPal.

"Oh, bitcoin, sé que vas a reinar, reinarás", John Barrett canta en su bluegrass "Ode to Satoshi", grabado en un estudio en East Nashville, Tennessee. "Hasta que todos lo sepan, todo el mundo lo sabe, hasta que todos sepan tu nombre". No está solo en su elección del tema de la canción: "10,000 Bitcoins" es una canción de amor de Laura Saggers; "Bitcoin Barons" es una pieza de rap de YTCracker; y hay un puñado de otros. Mientras tanto, el artista alemán Kuno Goda pintó 200 Bitcoins, con el logotipo de bitcoin repetido doscientas veces en un lienzo, una obra de teatro con los 200 One-Dollar Bills de Andy Warhol. La fotógrafa de L.A. Megan Miller hizo una serie completa de piezas que muestran bitcoin en la vida cotidiana. Oakland, California, el artista Dave Kim quedó fascinado con la historia de Dorian Nakamoto y lo eligió como el tema de su pintura Almuerzo Gratis.



Almuerzo gratis de Dave Kim
(Cortesía de Dave Kim)

Todo esto habla de otro aspecto de lo que representa bitcoin. Más que solo una moneda y una tecnología, es un movimiento contracultural. Pero como todos los movimientos contraculturales, no irá a ninguna parte como una fuerza para el cambio social a menos que vaya más allá de esa definición de sí mismo y encuentre un punto de apoyo en la cultura popular, en la corriente

principal. Y hacerlo requiere más que cantautores y poetas para cantar las alabanzas de una nueva idea; también necesita que la gente común encuentre algo atractivo en ella y, a través de sus contactos con otros, difunda esa idea.

Por mucho que una comunidad descentralizada no pueda tener un líder central, para crecer aún necesita individuos que tomen la iniciativa. Sin primeros movimientos, no puede haber comunidad. Ya hemos conocido a algunos de estos primeros usuarios: los programadores, empresarios y evangelistas que tomaron Bitcoin y lo promovieron. Pero su crecimiento también ha dependido de individuos de bajo perfil que simplemente han buscado usar la criptomoneda para hacerla funcionar como un elemento de la vida cotidiana. Gente como Austin y Beccy Craig de Provo, Utah.

Los Craig eran improbables proselitistas. Ella era una artista gráfica; él hizo videos corporativos. Tampoco es un codificador o un emprendedor. No fueron Cypherpunks. Pero Austin, un joven con una inclinación libertaria que tenía experiencia en la producción de videos, había oído hablar de bitcoin en 2011 y estaba intrigado por su potencial democratizador, y también tenía una idea creativa sobre la plantación de la bandera de bitcoin en la cultura popular.

Después de proponer a Beccy, hizo una segunda propuesta: después de su luna de miel, realizarían un experimento: vivirían durante noventa días con nada más que bitcoins y filmarían todo para un documental. Era el tipo de diversión que solo los jóvenes podían hacer, y para su sorpresa, Beccy rápidamente aceptó el desafío. Como si todo eso no fuera lo suficientemente desafiante, los Craig agregaron otra arruga: cruzarían los Estados Unidos, volarían a Europa, volarían a Asia y luego volarían de regreso a Utah. Pagarían por cada etapa de este viaje alrededor del mundo con bitcoin.

Lanzaron un proyecto de Kickstarter para financiar la película, recaudaron $ 72,000, se compraron un poco de publicidad y contrataron a un equipo de filmación. Si bien es razonablemente factible en la actualidad, en 2015, no gastar más que bitcoin durante tres meses, esto fue a mediados de 2013, justo antes de que un desfile de conocidas empresas anunciaran que aceptarían Bitcoin, como veremos en el próximo capítulo. En ese momento, la búsqueda de los Craig parecía quijotesca en el mejor de los casos. Pocas empresas tomaron Bitcoin, y la mayoría de los vendedores ni siquiera habían oído hablar de él. Tuvieron que convencer a una gran cantidad de personas en su ciudad para que aceptaran la moneda: su propietario, sus empleadores, un tendero local. El tendero, que dirigía LoLo's Fresh Food Warehouse, se convirtió cuando le explicaron la diferencia en las tarifas entre bitcoin y tarjetas de crédito. En cada parada, perfeccionaron su tono, en efecto convirtiéndose en evangelistas de bitcoins. Su experimento comenzó el 25 de julio de 2013.

La parte más difícil de vivir en Bitcoin en Provo resultó ser encontrar una estación de servicio. "Durante las primeras dos semanas", dijo Austin, "no teníamos lugar para llenar". Así que apenas usaban el automóvil. Tuvieron la suerte de que Jeremy Furbish, un empleado nocturno de la estación de servicio y entusiasta de los bitcoins conocido por la comunidad como Furb, escuchó acerca de su búsqueda. Invitó a los Craig a su estación. "Manejar una hora allá afuera el viernes por la noche a las diez se convirtió en parte de nuestra rutina", dijo Beccy. A principios de octubre, salieron a la carretera.

Nos encontramos con los Craig ese mes en una pizzería en Brooklyn llamada Lean Crust Pizza en Fulton Street. En este día inusualmente cálido, Fulton Street estaba en plena floración de Nueva York, caliente y ruidosa. El dueño, Dan Lee, es un entusiasta de los bitcoins, y Lean Crust había comenzado a aceptar bitcoins poco antes, al igual que sus otras dos tiendas en el vecindario. Pero

que un negocio aceptara bitcoin no significaba que las personas que trabajaban allí supieran cómo tomarlo.

Austin se paró frente al mostrador, esperando pagar. En su mano no tenía su billetera, sino un teléfono.

"Eso equivale a treinta y cuatro dólares", dijo la joven detrás del mostrador.

"Está bien", dijo Austin. "¿Podemos pagar en bitcoins?"

"¿En que?"

"En bitcoin. ¿Podemos pagar en bitcoin? "

"bit... qué?"

Eventualmente, Austin pudo pagar su comida con bitcoin, pero solo después de que la chica del mostrador llamó a Lee, quien envió a un empleado de una de sus otras tiendas para procesar la transacción. Una vez que esto sucedió, fue sin problemas. Austin tomó la dirección de la cuenta bitcoin de Lean Crust, la ingresó en su propia cuenta, ingresó el monto y presionó enviar. La transacción duró unos cinco segundos.

El intercambio resumió bastante sobre Bitcoin: la confusión sobre lo que es; las dificultades iniciales para usarlo; y luego la simplicidad una vez que el sistema está configurado. Mientras comíamos nuestra pizza en la acera, la cajera pasó, obviamente interesada en descubrir lo que acababa de ver. Se detuvo para hablar por un minuto, se disculpó por su malentendido anterior y, diciéndoles a los Craig si querían algo más, los ayudaría con eso.

Unas semanas más tarde, mientras recopilábamos datos para una historia sobre los Craig, volvimos a estar en contacto con la joven cajera, Nadia Alamgir, y descubrimos que se había convertido. El encuentro casual con Bitcoin había despertado su interés, se había ido e investigado un poco y se había interesado más, y antes de que se diera cuenta, iría a las reuniones de bitcoin en Brooklyn.

Así es como bitcoin crece, de boca en boca y encuentros fortuitos. Para un sistema que está descentralizado, uno que no está siendo administrado por una empresa con fines de lucro, donde nadie va a poner dinero en marketing o publicidad, es la única forma en que la comunidad puede crecer. En el caso de los Craig, las noticias sobre su proyecto se filtraron, en los foros y a través de la confusa confederación de reuniones. En cada parada de su viaje, en los Estados Unidos y en el extranjero, se encontraron con al menos un bitcoiner que quería echar una mano. "Fue en gran parte debido a la comunidad bitcoin que lo hicimos", dijo Austin.

Al final, los Craig vivieron durante 101 días sin gastar nada más que bitcoin. Demostraron que era posible hacerlo, si no práctico. La comunidad los abrazó, y se convirtieron en celebridades minoritarias de bitcoins antes de que su película siquiera hubiera sido lanzada. Un año más tarde, cuando Dish Network estaba buscando una "cara de bitcoin" para ayudar a lanzar sus opciones de pago de bitcoin, recogió los Craigs. Sin embargo, lo que realmente demostró su viaje fue que un proyecto que había comenzado casi cinco años antes con una sola persona, Nakamoto, se había convertido en una comunidad global cuyos miembros habían podido establecer fuertes conexiones sin la ayuda de una autoridad centralizada.

Capítulo 4

MONTAÑA RUSA

> El dinero... se clasifica con amor como la mayor alegría del hombre. Y se clasifica con la muerte como su mayor fuente de ansiedad.
>
> -John Kenneth Galbraith

Si la comunidad es una parte importante del crecimiento de una moneda, la otra parte es una ventaja comparativa. Tiene que ser fundamentalmente más útil que lo que espera reemplazar. En los siguientes capítulos, exploraremos las diversas maneras en que la criptomoneda podría remodelar la economía global más allá de cómo nos enviemos dinero entre nosotros. Pero el discurso central, especialmente para los usuarios en el mundo desarrollado, por ahora debe centrarse en la capacidad de hacer que los pagos electrónicos sean más baratos y más eficientes. Para ver cómo es el caso, primero debemos ver cómo funciona el sistema de pago tradicional y los muchos costos que genera. Entonces, salgamos y compramos una taza de café.

Estás en un Starbucks en Nueva York, donde un gran café con leche cuesta $ 4.30. Puede dudar un momento sobre el precio (a menos que sea de Oslo, donde el mismo tamaño es de $ 9.83), pero una vez que haya decidido continuar con la compra, no lo pensará dos veces antes de entregarlo. una tarjeta de crédito al cajero (un título de trabajo cada vez más obsoleto). En cuestión de segundos, y sin siquiera firmar, su tarjeta ha sido pasada y está de vuelta en su billetera mientras se dirige hacia la puerta, bebiendo de una taza de café espumoso. ¿Quién necesita llevar efectivo más? ¿Quién necesita el riesgo de tirar un billete de veinte en el piso o la molestia de las frecuentes visitas al cajero automático? ¿Y ese absurdo precio de latte? No sería diferente si hubiera pagado en efectivo. Toda esta conveniencia extra y moderna del pago electrónico no le cuesta nada... o eso parece.

Ahora echemos un vistazo más de cerca a lo que sucede cuando el cajero desliza su tarjeta. Con esa acción, la información personal contenida en su banda magnética (su número de cuenta, la fecha de vencimiento, el código postal de la dirección de facturación y el código CVV (valor de validación de la tarjeta de crédito)) se envía a un procesador de front-end. Esa firma, una de las cientos que operan actualmente en todo el mundo, se especializa en el manejo de información de pago en nombre de su cliente comercial, en este caso Starbucks, y del banco en el que se depositan los recibos de venta, una institución a la que se hace referencia en la transacción. cadena como el banco adquirente. Por ahora, tanto Starbucks como su banco simplemente necesitan saber si la cuenta de la tarjeta de crédito adjunta a su tarjeta tiene fondos suficientes para cubrir el pago. (Se ocuparán de si en realidad se trata de su tarjeta y su cuenta un poco más tarde). El trabajo del procesador front-end es verificarlo, y rápidamente. Por lo tanto, reenvía la información contenida en la tarjeta a la red de la asociación de tarjetas correspondiente (MasterCard, Visa, American Express u otra), que determina de qué banco emisor proviene su tarjeta. Habiendo dejado huellas de sí mismo en múltiples bases de datos, ahora es tiempo de que su información personal se mueva a un procesador de pagos por separado que representa al banco emisor, aquel cuyo nombre está en su tarjeta y administra su cuenta. Una vez que su banco haya verificado la validez de la información y verificado que tenga suficiente crédito, la señal se remonta hacia el otro lado. El banco le dice a su procesador que deje todo en claro a la asociación, que lo transmite al procesador de entrada para que Starbucks y el banco adquirente puedan estar satisfechos... por ahora. El cajero recibe la notificación de la aprobación a través de un mensaje "autorizado" que

aparece en la pantalla del lector de tarjetas. Esta larga serie de comunicaciones electrónicas se ha producido en segundos.

Ahora estás caminando por la calle, copa en mano. Pero el sistema de pago está lejos de hacerse con usted o Starbucks. Por un lado, el café todavía no ha sido pagado por entregar el café. Para eso, debe enviar una solicitud de seguimiento a su banco adquirente, generalmente en un lote de recibos al final del día. El banco adquirente le pagará al comerciante por esos recibos, pero tendrá que solicitar el reembolso al banco emisor, utilizando una red de cámara de compensación automática (ACH) administrada por los bancos regionales de la Reserva Federal o la Red de pagos electrónicos del clearing. House Payments Co., una compañía propiedad de dieciocho de los bancos comerciales más grandes del mundo. Aún así, su banco no liberará los fondos si no está convencido de que realmente fue usted quien compró el café con leche. Entonces, incluso antes de recibir la solicitud de pago, su equipo antifraude ha estado trabajando arduamente para analizar la transacción inicial, buscando banderas rojas y patrones de comportamiento fuera de su actividad habitual. Si el equipo no está seguro de quién estaba deslizando la tarjeta, llamará a su celular y a su número de teléfono particular, le enviará un mensaje de texto y le enviará un correo electrónico para que confirme que realmente estuvo allí en Nueva York. Después de todo, años de actividad de transacciones en su cuenta muestran que generalmente compra su café de la mañana en un restaurante de su ciudad natal de Seattle, a menos que esté en San Francisco para sus reuniones mensuales con el empleador citado en su solicitud de tarjeta de crédito. Una vez que su banco esté convencido de que todo está por encima de la borda, liberará el pago de liquidación de ACH y registrará un débito en su cuenta de tarjeta de crédito. El dinero luego fluye al banco adquirente de Starbucks, que acredita la cuenta de Starbucks. Este proceso generalmente toma hasta tres días hábiles para completarse.

Si ha estado contando las palabras en negrita de arriba, sabrá que siete entidades diferentes, además de usted y el café, participaron en esta transacción, cinco de las cuales, además de Starbucks, tuvieron acceso a la información de identificación de su tarjeta (número de cuenta, código postal, código CVV). Cada uno exige un recorte para su parte de la operación, sumando un total de tarifas de transacción de entre el 1 y el 3 por ciento de cada venta, dependiendo de si se usa una tarjeta de débito o crédito. La mayor parte del pastel se destina a los bancos, que en los últimos años han convertido el procesamiento de pagos en una de sus fuentes más importantes de ganancias, y en algunos casos, lo más importante. Esas tarifas son pagadas por el comerciante. Esto es adicional a los contracargos que el banco adquirente impondrá si un cliente disputa un cargo, requiriendo que el comerciante pierda el dinero y la mercancía. También se pueden aplicar otras multas y tarifas para reembolsar a los bancos cuando se produce un fraude.

En los Estados Unidos, la mayoría de los comerciantes simplemente absorben todos estos costos de transacción, y solo unos pocos, como algunas gasolineras, cobran una prima por las transacciones con tarjeta en lugar de efectivo, y la mayoría de los bancos reembolsan al cliente por transacciones fraudulentas. Aún así, es una ilusión pensar que no estás pagando por esto. Los costos se dividen en varios cargos bancarios: tarifas de emisión de tarjetas, tarifas de cajeros automáticos, tarifas de cheques y, por supuesto, los intereses cobrados a los millones de clientes que no pagan sus saldos en su totalidad cada mes. Y luego está ese loco precio de $ 4.30 por el café con leche. Starbucks tiene que cubrir sus costos de alguna manera.

Imaginemos que está comprando ese café con leche en un café en París o en un hotel resort en Cancún. En ese caso, una serie de otros intermediarios se unen para facilitar el intercambio de dólares por euros o pesos: bancos y corredores de bolsa de divisas, operadores de liquidación y liquidación de moneda extranjera y servicios de mensajería de moneda como SWIFT. Esta vez, los costos directos se le cobran a través de tarifas de transacciones extranjeras, y usted incurrirá en costos ocultos a través del "diferencial" cambiario desfavorable entre el precio al que se le cobra

por adquirir dólares y el precio que le cuesta a su banco obtenerlos. Estos costos, en su mayoría ocultos, pueden sumar hasta un 8 por ciento en una sola transacción, tarifas que están saliendo de su bolsillo, además de las que recaen sobre el dueño del café francés o el hotelero mexicano.

Si esto le parece una carga para usted como individuo, piense en la carga que representa para la economía en general. Extrapolando de la tarifa promedio estimada del 2 por ciento para pagos con tarjeta de crédito y débito y de la enorme cantidad de $ 11 billones en pagos procesados por Visa y MasterCard en 2013 -alrededor del 87 por ciento del mercado global- estimamos que estas operaciones le costaron a los comerciantes $ 250 mil millones ese año. Beneficiándose de una explosión global en el comercio electrónico, que según las proyecciones se duplicará entre 2013 y 2017, el volumen total de tarjetas de pago está aumentando en un 10 por ciento cada año. Agregue el costo del fraude, y puede ver cómo esta "arena en los engranajes" del sistema de pago global representa un obstáculo para el crecimiento, la eficiencia y el progreso.

Por supuesto, cientos de miles de personas son empleadas por bancos, procesadores de pagos y compañías de tarjetas de crédito en todo el mundo para mantener este sistema en funcionamiento. Necesitamos estos intermediarios porque la economía mundial todavía depende de un sistema en el que es imposible enviar dinero digitalmente de una persona a otra sin recurrir a un tercero independiente para verificar la identidad del cliente y confirmar su derecho a llamar los fondos en la cuenta. Ayudan a crear la confianza institucional de la que dependen nuestros intercambios de valor. Si pudiéramos encontrar una manera de realizar esas transacciones sin tener que confiar en estas instituciones intermediarias, hordas de personas quedarían sin trabajo. Hacer lo mismo con el sistema, entonces, no sería completamente gratuito para cada miembro de la sociedad. Pero el punto más importante es que al eliminarlos, y las tarifas que se cobran por el trabajo que realizan, al permitir que una persona compense a otra por entregar un bien o servicio sin que una serie de instituciones financieras reciban un recorte, también liberaríamos fondos para invertir en nuevas empresas, nuevos productos y nuevos empleos.

Al permitir que el sistema existente se desarrolle, permitimos que Visa y MasterCard formen un duopolio de facto, lo que les da a ellos y a sus socios bancarios el poder para manipular el mercado, dice Gil Luria, analista que cubre sistemas de pago en Wedbush Securities. Esas empresas de redes de tarjetas "no solo obtienen extravagantes comisiones por sí mismas, sino que también crean un mercado en el que los bancos pueden cobrar sus propias tarifas excesivas", afirma. Además de American Express, que funciona como un banco independiente, los diez principales emisores de tarjetas de crédito en el mundo son gigantescos bancos multinacionales como Barclays, HSBC, Wells Fargo y Citibank, que los liberan bajo acuerdos de asociación y licencia con Visa o Tarjeta MasterCard. Los mismos bancos también trabajan bajo licencias de banco adquirente con las compañías de tarjetas para que puedan procesar pagos recibidos por comerciantes como Starbucks. Así es como esas dos empresas y sus socios bancarios han cosido el sistema de pago global. Es cómo establecen los términos por los que funciona.

Toda la arquitectura de los pagos electrónicos se basa en la suposición de que los bancos pertenecen a la mitad de los flujos de dinero globales. Como vimos, los economistas consideran que la creación de deuda por parte de los bancos es fundamental para la creación de dinero privado; sin ellos, dicen, el efectivo simplemente estaría circulando a través de la economía sin activar el efecto multiplicador de la creación de crédito. Cada vez que desliza su tarjeta de crédito durante sus rondas de compras, participa en esa creación de dinero. El problema no es la deuda en sí misma: el crédito es un lubricante vital para la economía; es la complejidad del sistema para liquidar esa deuda. Al entregarle su tarjeta a Starbucks, no está transfiriendo tanto dinero como creando una serie de pagarés entre usted, su banco, el banco de Starbucks y Starbucks. Una vez que los cheques y las transferencias electrónicas se agregan a la mezcla, este intercambio constante y la compensación de los créditos y débitos deja a los bancos con saldos gigantes que se

concilian y liquidan al final de cada día. Para eso, aún más proveedores de servicios se involucran: cámaras de compensación, agencias de liquidación, bancos custodios que se encargan de las garantías utilizadas para garantizar los préstamos, y los vendedores del mercado monetario que comercializan inversiones y préstamos a corto plazo. En los Estados Unidos, este proceso de compensación está coordinado por el servicio Fedwire de la Fed, que maneja $ 3.5 billones por día en transferencias electrónicas entre bancos.

Sustentando estas transacciones se encuentran los pilares tradicionales de la economía y los símbolos del poder nacional: billetes y monedas. Sus reguladores exigen a los bancos -la Fed en los Estados Unidos, el Banco Central Europeo en la zona euro, la Autoridad de Regulación Prudencial en el Reino Unido- que lleven una proporción mínima de reservas de efectivo a depósitos en caso de que los depositantes soliciten sus fondos nuevamente. forma de papel. La banca fraccionaria de reserva, que permite a los bancos retener fondos y "crear" dinero privado con crédito, significa que la cantidad de deuda en la economía es muchas veces mayor que estos saldos de efectivo. No obstante, la ley exige que haya una cantidad proporcional de efectivo mantenido latente dentro del sistema financiero para mantener toda esa deuda.

En resumen, nuestro sistema de pago "electrónico" de alta tecnología depende de la presencia de una cantidad mínima de papel, que debe asegurarse en bóvedas con sistemas de alarma, guardias de seguridad, carros blindados, etc. Asegurar y distribuir todo este efectivo le cuesta a los países entre 0.5 por ciento y 1.5 por ciento de su PIB, dice Ajay Banga, CEO de MasterCard Inc., que ofrece un estimado que llega a $ 1.4 trillones cuando se aplica a todo el mundo. Banga deja caer estas grandes cifras para abogar por un mayor avance en los pagos electrónicos, del tipo que, presumiblemente, se ejecutará en la red de MasterCard. Pero como hemos visto, ese sistema engorroso, tal como está diseñado en la actualidad, está estrechamente entrelazado en el sistema bancario tradicional, que siempre exige su recorte.

A medida que el calendario avanzaba hasta 2013, una vanguardia de las empresas minoristas comenzó a detectar las ventajas del sistema de pago más rápido y de menor costo de la criptomoneda y comenzó a suscribirse para recibir servicios de procesamiento de pagos ofrecidos por empresas de bitcoin financiadas por Silicon Valley como BitPay, Coinbase, y GoCoin. Estas firmas promocionaron un nuevo modelo para romper el paradigma de la dependencia de los comerciantes del sistema de pago centrado en el banco descrito anteriormente. Estos servicios cobraban tarifas mensuales que equivalían a costos de transacción significativamente más bajos para los comerciantes que los cobrados en transacciones con tarjetas de crédito y entregaban pagos rápidos y eficientes en línea o in situ.

En estos casos nuevos, el cliente usa bitcoin para realizar el pago, pero los comerciantes tienen la opción de pagar en dólares o en su moneda local. Esto es posible porque esos procesadores de pago de bitcoin más grandes absorben las bitcoins, luego administran su riesgo mediante la negociación activa en las bolsas de monedas digitales.

Dada esta opción, no hay escasez de comerciantes que la estén abordando. Ellos son los que ahorran el dinero, no el cliente; pocos, hasta el momento, optan por transferirle ahorros al comprador. Muchos ven que no tienen nada que perder, ya que los clientes aún pueden pagar con tarjetas de crédito, tarjetas de débito, efectivo y todos los demás métodos de pago asociados con el sistema heredado. Entonces, una cantidad de negocios estadounidenses de alto perfil ahora han agregado Bitcoin como una opción de pago. Desde finales de 2013 hasta el verano de 2014, firmas como el minorista en línea Overstock.com, el equipo de baloncesto Sacramento Kings, el proveedor de cable Dish Network, las computadoras Dell y el sitio de viajes Expedia agregaron sus nombres a una lista de comerciantes que aceptaban bitcoin. , según el recuento de CoinDesk, había llegado a sesenta y siete mil comerciantes a fines de junio de 2014.

El desafío para los vendedores de bitcoins ahora no radica en convencer a los comerciantes de los beneficios de la criptomoneda, sino en convencer a los clientes de ellos. Hasta ahora, esos resultados son mixtos. Las buenas noticias se encuentran en la constante expansión en la adopción de carteras digitales, el software necesario para enviar y recibir bitcoins, con Blockchain y Coinbase, los dos mayores proveedores de estos, en camino a los 2 millones de usuarios únicos cada uno en el momento de escritura. El cofundador de Blockchain, Peter Smith, dice que una sorprendente mayoría de sus relatos: "muchos más de lo que uno pensaría", dice crípticamente, se caracterizan como "activos". La mala noticia es que otras cifras, especialmente el crecimiento lento en toda la red los volúmenes de transacción, indican que muchos de esos usuarios solo están retocando los márgenes. Durante los primeros ocho meses de 2014, alrededor de $ 50 millones por día se pensó la red bitcoin (parte del cual fue solo "cambio" que las transacciones bitcoin crean como una medida contable), en comparación con los $ 30 billones combinados con ab-eso procesado diariamente por Visa y MasterCard en 2013. En el número de transacciones, la cantidad diaria promedio era de alrededor de sesenta y cinco mil, y aunque eso es diez veces más de lo que era hace dos años, la tendencia parece haberse estabilizado desde un pico a más de uno cientos de miles durante el aumento máximo en el precio de Bitcoin frente al dólar. De nuevo, esta es una pequeña fracción de las transacciones con tarjetas de crédito. Además, no está claro cuántas de esas transacciones comprenden el comercio y cuántas comprenden el comercio real. El primero es principalmente especulación, y como pronto veremos, puede ser bastante destructivo. Solo el último demostraría claramente que el bitcoin se está adoptando como moneda.

Ya hemos discutido el aumento en la actividad empresarial diseñada para hacer que el bitcoin sea más atractivo y fácil de usar como moneda, y veremos esto con más detalle en el capítulo 7. Algunos de los frutos de su trabajo se han implementado y están en constante desarrollo. actualización: billeteras más fáciles de usar y basadas en teléfonos inteligentes para facilitar los pagos; mejores y más confiables intercambios en línea para comprar y vender bitcoins; cajeros automáticos de bitcoin que facilitan que la gente común ingrese y salga de su moneda local; tarjetas de regalo y otros trucos que permiten a los titulares de bitcoin comprar productos de los principales comerciantes como Amazon que no aceptan la criptomoneda; y herramientas tales como tarjetas de débito cargadas con bitcoin que funcionarán con máquinas de pase de tarjeta de punto de venta y cajeros automáticos de bancos.

Pero toda la tecnología en el mundo no llevará a la gente a esto si los incentivos no son lo suficientemente fuertes. Por ahora, los beneficios simplemente no son obvios para las personas en lugares como Estados Unidos y Europa. A menos que estén contemplando todos los costos ocultos que describimos anteriormente y se vean a sí mismos como activistas que buscan llevar al mundo a un sistema más eficiente y más justo para todos, los clientes típicos no pueden apreciar los ahorros en los costos de bitcoin. Eso se debe a que los costos recaen, al menos directamente, en los comerciantes. Algunos procesadores de pagos inteligentes, como PayStand, con sede en Santa Cruz, California, han descubierto la manera de ofrecerles a los comerciantes la opción de transferir sus ahorros de costos de transacción a los clientes de bitcoins. Si eso funciona, presumiblemente como una herramienta competitiva, podría estimular más gasto de bitcoins. Pero, por ahora, los usuarios finales no ven una clara ventaja en el uso de criptomonedas sobre, por ejemplo, una tarjeta de crédito. En cambio, están enfocados en los riesgos, de los cuales hay dos principales.

El primero es la seguridad. Recuerde, las funciones de bitcoin son muy similares al efectivo. Una vez que se envía, se envía; no hay forma de recuperarlo, no hay contracargos como los que las compañías de tarjetas de crédito imponen a los comerciantes cuando descubren que han vendido bienes a alguien con una tarjeta robada. Al igual que con el efectivo, si se roban sus bitcoins, eso es todo. No puedes recuperarlos, a menos que, por supuesto, atrapen al ladrón.

¿Cómo podrías perderlos? Podría suceder si divulgó la "clave privada", o contraseña, tan importante que se necesita para abrir una dirección de bitcoin que se le asignó. Si mantiene sus bitcoins en una "billetera caliente" que está instalada en una computadora conectada a Internet, un pirata informático podría ingresar a través de esa conexión para obtener acceso a su clave privada y robar las monedas. Igual de importante, si pierde su clave privada-literalmente la cadena de código necesaria para desbloquear bitcoins de una "billetera fría" que se ha desconectado-o si olvida la contraseña de su billetera caliente y usted es la única persona con ella , no hay forma de recuperar sus monedas. Son tan buenos como perdidos. Este riesgo surge si utiliza un servicio que lo deja a usted exclusivamente a cargo de sus contraseñas, como el monedero genérico que ofrece el equipo de desarrollo de core de bitcoin o el producto proporcionado por Blockchain.info.

Todo esto suena alarmante, particularmente porque se puede y se tendrá mucho más valor en una billetera de bitcoin que el efectivo que se guarda en una billetera normal. Pero recuerde también que el pirateo y el robo de identidad son comunes en los sistemas de tarjetas de crédito, con números de fraude en conjunto muy superiores a los de Bitcoin. Además, con algunas simples precauciones, puede hacer que sea mucho más difícil para alguien piratear su billetera digital bitcoin. Debe usar solo una contraseña alfanumérica y combinarla con un servicio de autenticación de doble factor a través de un teléfono inteligente o mensajes SMS. Y si tiene tenencias significativas de bitcoin, puede cambiar la mayor parte de ellas en una "billetera fría", en la que mantiene la clave privada en un pedazo de papel en un lugar seguro; piérdalo y habrá perdido el acceso a sus bitcoins. -Mientras conserva las monedas que usa día a día en una "billetera caliente" con una clave de fácil acceso almacenada en su computadora.

Afortunadamente, se están desarrollando soluciones más sofisticadas que estas, que mejoran la protección pero permiten una mayor facilidad de uso y menos riesgo de perder una llave. Estos incluyen billeteras de múltiples firmas, que requieren la aplicación de al menos dos de al menos tres claves posibles mantenidas por diferentes personas o instituciones para liberar las bitcoins. Algunas empresas nuevas también ofrecen alta seguridad y seguro. Representadas más prominentemente por Circle Financial y Xapo, estas empresas de nueva creación están ofreciendo carteras y servicios de custodia altamente sofisticados combinados. Por ahora, estas empresas no cobran nada para cubrir los costos de seguros y seguridad, apostando a que atraerán suficientes clientes y pagarán tarifas en otro lugar -por ejemplo, para comprar y vender bitcoins- o que su creciente popularidad les permitirá desarrollar ganancias servicios de pago mercantil también. Pero en general, estas empresas deben agregar costos a la economía bitcoin, sin mencionar una cierta dependencia de "terceros confiables". Es una de las muchas áreas del desarrollo de bitcoins, otra es la regulación, donde algunos empresarios defienden un enfoque pragmático para reforzar confianza pública, que requeriría compromisos sobre algunos de los principios filosóficos detrás de un modelo de descentralización. Naturalmente, esto no le sienta bien a los puristas de bitcoin.

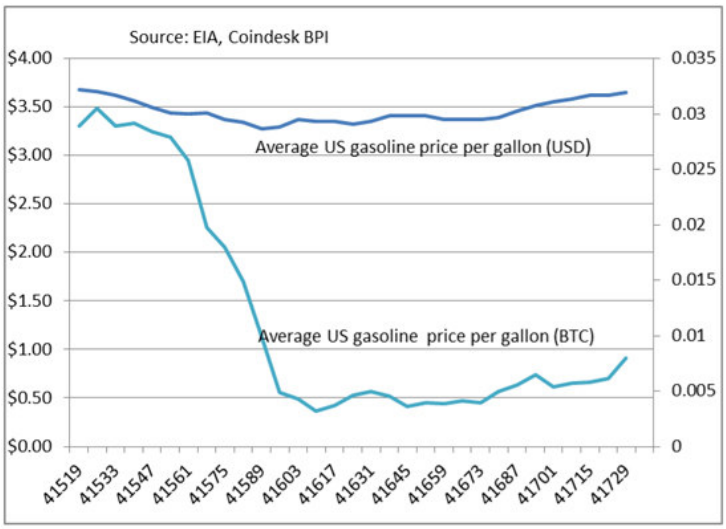
Aún así, hasta que se resuelva el problema de seguridad, las historias de hacks de bitcoin continuarán perjudicando la imagen de bitcoin. Al menos una vez al mes, según parece, surge un nuevo informe sobre el robo de miles de dólares de bitcoins. Después de que Bitcoinica perdiera casi medio millón de dólares en bitcoins de dos hacks, los robos seguían apareciendo en otros sitios: un hacker secuestró las computadoras de un proveedor de servicios de Internet para robar $ 83,000 en bitcoins de los mineros; una botnet con sede en Grecia utilizó Facebook para infectar 250,000 computadoras con malware para robar bitcoins; monte Gox, por su propia cuenta, había sido hackeado dos veces en tres años y finalmente había perdido 650,000 bitcoins. Bitcoin también estuvo indirectamente implicado en el ataque de pirateo que lanzó docenas de fotos desnudas de celebridades al público en agosto de 2014. Aunque en este caso fueron las cuentas en el servicio iCloud de Apple las que sufrieron la violación de seguridad, el hacker solicitó el pago

de esas las fotos en bitcoin crearon una asociación negativa con la moneda digital. Fue otra bandera roja para un público en general que ya desconfiaba de una tecnología desconocida.

Aún así, se necesita perspectiva. Puede argumentar fácilmente que los sistemas de pago heredados son en realidad más propensos al fraude que bitcoin. Esto se debe a que las redes de tarjetas de crédito y los sistemas bancarios requieren el intercambio de información privada, que fomenta el robo de identidad, a veces en grandes escalas, como el ataque de $ 148 millones en Target en diciembre de 2013 y la violación subsiguiente en Home Depot. 56 millones de tarjetas de crédito fueron robadas en agosto de 2014. Versiones más pequeñas de esos robos suceden todo el tiempo. Lo que es diferente de Bitcoin es que los cargos iniciales en los sistemas heredados son asumidos por los comerciantes. Además de la inconveniencia de las tarjetas de crédito perdidas, los consumidores no notan la carga, aunque, como discutimos anteriormente, finalmente los alcanza en forma de precios más altos y tasas de interés. Los bitcointers deben hacer un mejor trabajo educando a la gente acerca de esos costos ocultos si quieren incentivar adecuadamente a los usuarios promedio para usar bitcoin.

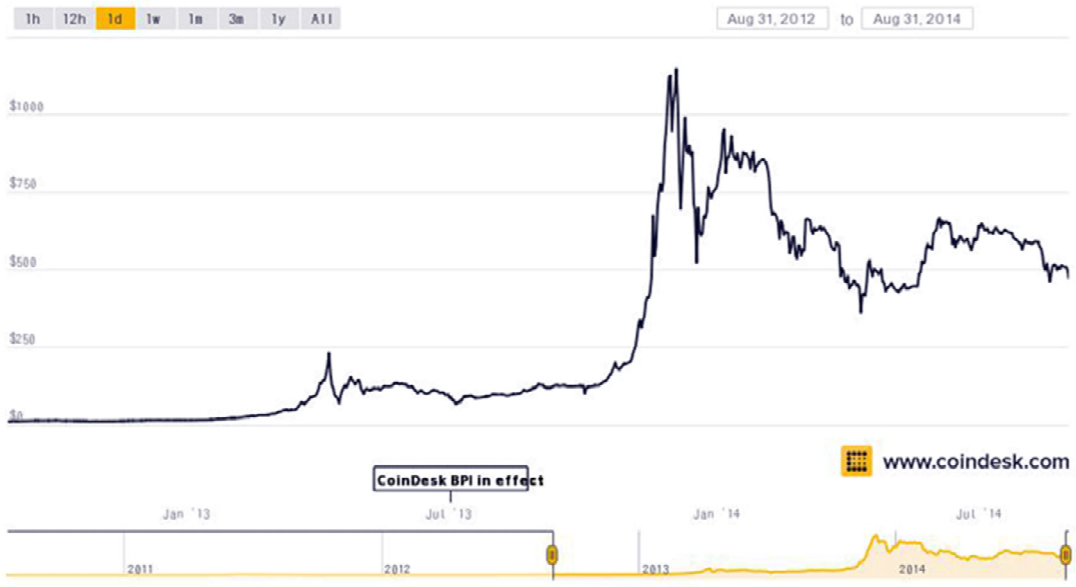
Otra gran preocupación es la volatilidad del precio. Nadie quiere ir a la tienda de comestibles semana a semana y ver su factura cambiar 10 por ciento o más simplemente porque la tasa de cambio de bitcoin subyacente es fluctuante. Hasta que vivamos en una economía basada en bitcoin, donde la moneda digital es la unidad de cuenta en la cual se cotizan los precios, esta fluctuación del tipo de cambio será inevitable en la vida cotidiana para los pagadores y beneficiarios de bitcoin. Comparemos el precio promedio de un galón de gasolina en dólares con el de bitcoin en los EE. UU. Entre septiembre de 2013 y finales de marzo de 2014. En los primeros tres meses de ese período, su factura de gas habría caído 90 por ciento, solo para verlo saltar un 50 por ciento en los siguientes cuatro meses. Por el contrario, el precio de la gasolina disminuyó y aumentó en no más del 12 por ciento en términos de dólares durante el mismo período.

Extrapolando de la definición de "dinero" en tres partes del libro de texto al que nos referimos en el capítulo 2, una moneda debe exhibir estabilidad de precios para que funcione adecuadamente como medio de intercambio, además de demostrar que es una tienda de valores confiable y una unidad de cuenta. Es difícil sugerir que Bitcoin ahora se acerca a la estabilidad de precios necesaria. Eso es un resultado directo de su fluctuación frente a otras monedas. En un extenso estudio del desempeño de los precios de Bitcoin frente a otras monedas y activos, el profesor de la Universidad de Nueva York, David Yermack, concluyó que el bitcoin es mucho mejor visto como un producto básico que como una moneda. No solo fluctúa violentamente frente al dólar, descubrió, sino que tampoco muestra fuertes correlaciones positivas o negativas con ninguna de las otras monedas principales, como el euro, el yen o el franco suizo, o incluso contra el precio del oro. Esta falta de un patrón predecible frente a otras medidas de valor hace que sea mucho más difícil para un empresario o un inversionista diseñar una estrategia de cobertura efectiva que pueda protegerse contra una pérdida de valor en sus tenencias de bitcoins. Mientras que usted puede protegerse contra una caída en el dólar al poseer oro, no está claro qué podría comprar para protegerse contra una caída en el bitcoin.



Un galón de gasolina, con un precio en dólares y bitcoin, semanal
(Fuente: EIA, CoinDesk)

Esta es solo otra forma de decir que Bitcoin es un activo volátil. No necesita mirar más allá de su gráfico de precios a doce meses desde septiembre de 2013. Durante los primeros tres meses, el bitcoin subió un 800 por ciento de $ 129.46 al máximo del 30 de noviembre de $ 1.165,89, ya que los reguladores estadounidenses hicieron algunos comentarios de bienvenida sobre la moneda digital tecnología y como una oleada de compras especulativas se apoderó de China. En ese momento, cualquiera que tenga bitcoin habría estado gritando. Pero alguien que descargó monedas en septiembre para, por ejemplo, comprar un automóvil podría haberse decepcionado. El remordimiento del vendedor en un mercado en alza es una característica normal de la inversión en acciones u otros activos volátiles, pero para una moneda desea que ambas partes en una transacción se sientan satisfechas de que no están renunciando demasiado. El arrepentimiento no es una emoción constructiva cuando se trata de monedas, que en última instancia deberían verse no como inversiones, sino como herramientas para hacer pagos. En cualquier caso, un poco más de cuatro meses después de ese pico de noviembre, el precio caía a las profundidades de $ 344.24 luego del colapso del monte. Gox y en medio de las noticias a principios de abril de una ofensiva de las autoridades chinas. Las cosas se estabilizaron un poco durante el verano, pero con episodios frecuentes de lo que todavía se consideraría una volatilidad extrema en cualquier otro mercado de divisas. Esto incluyó una desastrosa "crisis repentina" que ocurrió a mediados de agosto únicamente en la central con sede en Bulgaria, BTC-e, donde el precio bajó de $ 500 a $ 309 en tres minutos antes de rebotar la mayor parte del camino de regreso.



Índice de precios de CoinDesk Bitcoin
(Cortesía de CoinDesk)

Se puede argumentar que la volatilidad de Bitcoin es inevitable por el momento. Ganar respeto y la adopción generalizada como moneda es un proceso; no se puede lograr de la noche a la mañana. A medida que se desarrolle ese proceso, los defensores de Bitcoin dicen que la estabilidad vendrá una vez que atraiga a un número suficientemente grande de personas que hayan aceptado la promesa de Bitcoin como una nueva forma efectiva de enviar dinero a todo el mundo. Vale la pena señalar que a lo largo de sus seis años de vida, independientemente de las grandes fluctuaciones de precios, Bitcoin ha funcionado extremadamente bien como una inversión, ya que más y más personas han creído en esta idea. "The Honey Badger of Money" es como los fanáticos de bitcoin describen su tenaz habilidad para recuperarse de la adversidad. Incluso después de la gran ola de ventas a principios de 2014, el bitcoin era aproximadamente cuarenta veces más alto que cuando estaba a fines de 2012, un centenar de veces en el 31 de diciembre de 2011, y casi mil setecientos veces más que en el lugar donde estaba un año antes de eso.

Críticos como el economista de la Universidad de Boston Mark Williams, un fuerte escéptico de las perspectivas de Bitcoin, ven estas ganancias en una luz negativa. En una mordaz presentación ante el Departamento de Servicios Financieros de Nueva York, Williams dijo que era una señal de "acumulación extrema" que negaría a Bitcoin la posibilidad de convertirse en una "moneda transaccional útil". Pero sus defensores dicen que no se puede detener a los entusiastas de comprar y mantener bitcoin y que esta mentalidad de inversión es parte de una fase de transición inevitable, de hecho necesaria. "No diría que el acaparamiento es algo malo", dice Bobby Lee, CEO de BTC China, quien ha sido testigo del intenso enfoque especulativo del bitcoin de los inversores chinos. "Una vez que su precio ha subido lo suficiente y Bitcoin ha demostrado ser una reserva de valor, la gente comenzará a usarlo como moneda".

Gil Luria, el analista de Wedbush, incluso sostiene que la volatilidad es algo bueno, con el argumento de que atrae a los operadores que buscan ganancias al mercado. Su presencia alienta el desarrollo de intercambios sofisticados y mecanismos más confiables para intercambiar bitcoins en monedas fiduciarias, dice, señalando que los intercambios comerciales más grandes, de más alta tecnología y mejor regulados ya estaban en línea en 2014 para dar servicio a un creciente Wall Street. clientela basada El argumento es que esta construcción a su vez conducirá a la estabilidad, eventualmente. Para entender este argumento, debemos reconocer el papel

desempeñado en los mercados por los comerciantes, esa clase especial de inversores que compran y venden activos en un período corto para beneficiarse de los movimientos de precios en cualquier dirección. Al colocar estas apuestas a corto plazo, los operadores proporcionan la muy necesaria "liquidez" a los mercados, definida como el grado en que los inversores pueden encontrar fácilmente compradores de un activo que desean vender o vendedores de uno que desean comprar. A medida que más operadores ingresan al mercado, creando más posibles compradores y vendedores, la liquidez aumenta y los precios se estabilizan. Irónicamente, sin embargo, es la volatilidad, no los aumentos de precios, lo que primero atrae a los operadores, ya que eso es lo que genera beneficios. Si los precios están fluctuando, los traders pueden ganar más dinero estando a ambos lados de la operación. Vimos esto en la década de 1970, cuando el colapso del sistema de Bretton Woods hizo que los tipos de cambio se descontrolaran y los bancos se apresuraron a establecer mesas de negociación de divisas muy rentables. Con el tiempo, la expansión de estos escritorios y el desarrollo de herramientas comerciales cada vez más sofisticadas, generaron tanta liquidez que los tipos de cambio se volvieron relativamente estables. Luria está imaginando una trayectoria similar para bitcoin. Él dice que los bitcoiners deberían estar "adoptando la volatilidad", ya que ayudará a "crear la infraestructura de red de pagos y la base monetaria" que necesitará Bitcoin en el futuro.

Luego está el argumento de que para que bitcoin cumpla con su potencial real, y aquí estamos hablando de bitcoin la tecnología, no bitcoin de la moneda, la tasa de cambio en sí misma no importa. La idea es que algún día los consumidores y las empresas no tendrán bitcoins para su cuenta, sino que accederán sin saberlo a la red bitcoin cada vez que realicen pagos. Los procesadores de pago de Bitcoin, como BitPay y Coinbase, protegen a los comerciantes del riesgo del tipo de cambio al convertir inmediatamente las bitcoins entrantes en dólares. Se espera que la versión reflejada de esto se configure con el tiempo para que los consumidores conviertan sus dólares en bitcoins, que luego se enviarán inmediatamente al comerciante. Eventualmente, todos podríamos estar ciegos ante estas conversiones de bitcoin que ocurren en el medio de todas nuestras transacciones.

Aún así, alguien tendrá que absorber el riesgo de tipo de cambio, si no los procesadores de pagos, luego los inversores con los que comercian. Hasta que baje la volatilidad, estos jugadores cobrarán por hacerlo, ya sea directamente a través de tarifas o en los precios con descuento que cotizan para comprar bitcoins o dólares. No hay una bala mágica. Finalmente, la volatilidad debe contenerse para que Bitcoin cumpla con su promesa como una forma eficiente y de bajo costo para que las personas intercambien dinero.

En este punto, simplemente no está claro cómo se desarrollará todo esto. No es difícil imaginar bitcoin y otras criptomonedas convirtiéndose en víctimas de su inestabilidad, nunca escapando del problema de la volatilidad del huevo y la gallina. Además, a medida que la memoria del colapso de 2008 se desvanece, la necesidad de encontrar un modelo de pago alternativo se desvanece también, especialmente uno que parece tan impredecible. Por otro lado, el potencial de la criptomoneda para invertir un engorroso sistema de pago centralizado es claro.

El problema de todo este análisis es que no tenemos un modelo histórico actualizado para medir cómo se supone que evolucionará una moneda emitida independientemente, y mucho menos una que también funciona como un sistema único de procesamiento de pagos y un protocolo para descentralizar las relaciones sociales. Ninguno de los puntos de referencia que las personas utilizan tanto para elogiar como para criticar el bitcoin, "moneda", "mercancía", "protocolo de pago", es muy adecuado. Bitcoin tiene características de todos ellos, pero ninguno en su totalidad. Entonces, aunque parezca insatisfactorio, nuestra mejor respuesta a la pregunta de si la criptomoneda puede desafiar el duopolio de Visa y MasterCard es "tal vez, tal vez no".

La volatilidad de los precios de bitcoin en 2013-14 ciertamente la empujó al ojo público. Irónicamente, este aumento a un nuevo nivel de manía, incluso más allá de los primeros cuatro años de existencia de bitcoin, eventualmente obligaría a los partidarios de bitcoin a enfrentar los desafíos de sus días en el Salvaje Oeste y contemplar cómo podría madurar.

El punto de partida de la manía fue en marzo de 2013, con lo que llamaremos el golpe chipriota. La pequeña nación insular de Chipre, dividida entre los estados griegos y turcos, cayó en medio de una crisis financiera porque sus bancos, sus saldos de efectivo hinchados con depósitos de ricos rusos que buscaban un paraíso fiscal, habían invertido fuertemente en los bonos de la vecina Grecia. Ese vecino más grande se había convertido en el caso candente de la Unión Europea, que acababa de obligar al gobierno de Atenas a imponer un "corte de pelo" o pérdidas obligatorias a sus inversores. La UE hizo esto para asegurarse de que los inversores del sector privado que habían hecho apuestas arriesgadas a Grecia asumieran parte de la carga del rescate que estaban teniendo los alemanes y otros contribuyentes de la zona euro. Los bancos excesivamente apalancados de Chipre fueron una víctima no intencional de eso y ahora se enfrentaron a la aterradora amenaza de un banco dirigido por sus grandes depositantes rusos.

La solución dramática, una respaldada por Alemania y sus socios de la UE, que eran igualmente reacios a rescatar a los oligarcas rusos, era que el gobierno de Nicosia congelaría depósitos y confiscaría el 10 por ciento de ellos para pagar el rescate bancario. Este paso sin precedentes envió ondas de choque alrededor del mundo. "Si pueden hacer eso allí, pueden hacerlo en cualquier lugar", gritó Mark McGowan, un taxista londinense famoso por sus videos de YouTube con adverbios obscenos, donde se enfurece sobre asuntos de actualidad bajo el apodo chunkymark, todos entregados desde su taxi. La diatriba de Chipre es uno de sus clásicos de todos los tiempos. Si pueden hacer eso allí, pueden hacerlo en cualquier lugar. Él no era el único que pensaba eso.

De repente, la "propuesta de valor" de bitcoin fue clara. El gobierno podría sacar dinero de su cuenta bancaria local, pero no podría tocar su bitcoin. La crisis de Chipre provocó una estampida de dinero en Bitcoin, que ahora se consideraba un refugio seguro frente a la amenaza generalizada de la confiscación gubernamental en todas partes. El precio pasó de $ 33 a fines de febrero a $ 230 el 9 de abril, empujando la capitalización de mercado total de bitcoin a $ 1 mil millones por primera vez, pero también desencadenando uno de los viajes más salvajes del año que cualquier activo financiero haya visto alguna vez.

Luego hubo algunas malas noticias. Nuevos problemas técnicos en los propensos a problemas Mt Gox surgió, esta vez obligándolo a suspender el comercio durante dos días el 11 de abril, que luego se transformó en problemas legales más grandes. El precio de bitcoin se desplomó a $ 68 el 16 de abril, donde pareció encontrar un piso, a pesar de que un mes más tarde el gobierno de Estados Unidos congeló el monte. La cuenta bancaria de Estados Unidos de Gox es uno de los primeros signos de que Washington quería regular esta nueva moneda digital anárquica. Durante el verano, el precio se estabilizó, oscilando dentro de "solo" un rango de $ 65 a $ 130.

Luego, la policía de EE. UU. Llegó por primera vez a la escena de criptomonedas. A fines de junio de 2013, surgieron informes de que el FBI había incautado 11 bitcoins (entonces valorados en $ 800) de un traficante de drogas en lo que se consideró como una "picadura de honeypot" inicial en Silk Road. Un mes después, la Comisión de Bolsa y Valores presentó cargos contra Trendon Shavers, un tejano acusado de ejecutar un esquema de Ponzi bitcoin bajo el apodo pirateat40. Que los federales estaban tomando en serio el bitcoin era una propuesta alarmante pero estimulante para los bitcoiners, que estaban divididos entre aquellos que querían que su anarquía continuara y aquellos que creían que su crecimiento dependía de la legitimidad de la regulación y la aplicación contra la criminalidad.

Si bien la noticia de los arrestos por drogas y los esquemas de Ponzi engendraron cierta sospecha sobre esta desconocida y anónima moneda, también despertó la curiosidad entre algunos que todavía no habían llegado a las posibilidades de Bitcoin. ¿Cuál fue el alboroto? Las investigaciones llevaron a descubrimientos, que llevaron a inversiones. Los inversores de Silicon Valley comenzaron a invertir dinero en nuevos intercambios y proveedores de billeteras digitales, y algunos nombres prominentes se declararon creyentes. Llegaron inversionistas llenos de dinero, siguiendo los pasos de Cameron y Tyler Winklevoss, hermanos gemelos famosos por sus disputas legales con el fundador de Facebook, Mark Zuckerberg, que habían anunciado en abril que habían adquirido una enorme cantidad de bitcoin que valía 11 millones de dólares. A medida que el precio de Bitcoin comenzó a subir, subir y subir aún más, la inversión de los gemelos comenzó a parecer bien sincronizada. Ni siquiera la dramática noticia del 2 de octubre de que el Buró Federal de Investigaciones había arrestado a Ross Ulbricht, el supuesto cerebro de Dread Pirate Roberts del sitio de Silk Road, y se había apoderado de 26,000 bitcoins, que valían 3,6 millones de dólares, representaría un gran revés. El precio pasó de $ 125 a fines de septiembre a $ 198 un mes después, incluso cuando se corrió la voz el 26 de octubre de que el FBI había arrastrado 144,000 bitcoins adicionales (luego $ 28 millones) de su operación Silk Road.

Pero luego, en noviembre, las cosas realmente se volvieron bananas, impulsadas por el resultado de algunas audiencias del Senado ansiosamente anticipadas. Aunque la directora de la Red de Delitos Financieros del Departamento del Tesoro, Jennifer Shasky Calvery, anunció nuevas pautas sobre las reglas que la industria del bitcoin necesitaba seguir, dijo que su organización "reconoce la innovación que brindan las monedas virtuales y los beneficios que podrían ofrecer a la sociedad". bendición, motivo de celebración en bitcoinland. El partido no fue más evidente que en el precio de la divisa, que superó los $ 1.150 el 30 de noviembre.

Todo esto fue una gran noticia para los mineros bitcoin, que continuamente acumulaban bitcoins en sus computadoras. Sin embargo, su actividad estaba cambiando y se estaba industrializando rápidamente. En enero de 2013, una compañía china llamada Avalon, creada por dos estudiantes, Ng Zhang e Yifu Guo, comenzó a entregar una nueva computadora de minería independiente y especialmente dedicada que utilizaba un chip ASIC (circuito integrado específico de la aplicación). En los próximos meses, aparecerán en el mercado máquinas ASIC cada vez más rápidas y ávidas de energía, lo que provocará una implacable carrera de armamentos entre los mineros que persiguen el suministro limitado de bitcoins recién emitidos; a fines de año, la única forma de ganar esa carrera y seguir siendo rentable era creando granjas mineras gigantes basadas en centros de datos. Bitcoin se había convertido en una industria mundial, su expansión impulsada por el aumento del precio de la moneda.

Los aumentos de precios dieron lugar a los "barones bitcoin", muchos de ellos en sus veintes, que se convirtieron en la cara pública de la nueva industria impetuosa. En un momento decisivo, Bloomberg Businessweek publicó una historia el 10 de abril de 2013, con el título "Conoce a los millonarios de Bitcoin", con fotos de Jered Kenna, fundador del intercambio de bitcoin Tradehill, Bitstream Shrem y Avalon's Yifu Guo, todos ellos bajo treinta años de edad. Otros bitcoiners instantáneamente ricos comenzaron a aparecer en las noticias, como Roger Ver, el Bitcoin Jesus, tan conocido por su entusiasmo por regalar bitcoins para promover la moneda, y Mark Karpelès, el francés que había presidido la evolución del Monte. Gox en un monopolio virtual si se desmorona. A ellos se sumaron patrocinadores de bitcoin más establecidos, incluidos los gemelos Winklevoss y el pionero de Internet Jeremy Allaire. Algunas de estas personas se convertirían en clientes habituales en las conferencias de Bitcoin, que a partir de ahora habían evolucionado desde los asuntos de bajo presupuesto de los primeros años hasta los eventos de salas repletas en los centros de conferencias en Las Vegas, Amsterdam y Toronto.

En diciembre, el bitcoin superaba los $ 1.100 y su capitalización total de mercado apenas superaba los $ 14 mil millones. Pero en ese alto pico llegó la señal para que el partido se calmara, desde China. Los especuladores chinos habían desempeñado un papel clave en el aumento del precio del bitcoin, principalmente a través del intercambio BTC China de Bobby Lee, que en un momento incluso superó al Mt Gox en volumen. Los bitcoiners miraban con gran esperanza a China. Con más de mil millones de ciudadanos viviendo en una economía que todavía estaba parcialmente abierta al mercado libre y cuyo gobierno impuso controles estrictos sobre la cantidad de dinero que podrían enviar al extranjero, Bitcoin podría proporcionar una solución alternativa. Los funcionarios chinos parecían no importarles; no habían dicho nada. Luego, de repente, la prensa china informó que el Banco Popular de China no estaba contento con los bancos que trataban con los intercambios de bitcoins chinos. La decisión fue vaga pero suficiente para asustar a la gente. El precio de Bitcoin comenzó a caer.

En enero de 2014, el precio bajó a $ 770. El movimiento del 35 por ciento desde su pico veintinueve días antes hubiera sido un declive histórico si fuera, por ejemplo, el dólar frente al yen. Pero ese precio dejó intactas la mayoría de las fortunas hechas por personas que se metieron en Bitcoin a mediados de noviembre o antes. Entonces, cuando la comunidad descendió a Miami para otra conferencia de bitcoin a fines de enero, el ambiente aún era festivo. Eso cambiaría rápidamente.

El día después de la conferencia, Charlie Shrem, uno de los "millonarios bitcoin" de Businessweek y vicepresidente del grupo industrial Bitcoin, con sede en Seattle, fue arrestado en Nueva York a su regreso de una conferencia sobre pagos en Amsterdam. El alto perfil y franco de veinticuatro años fue acusado de ayudar a un traficante de drogas de Silk Road a lavar dinero a través de su servicio BitInstant. Shrem se declaró no culpable al principio, pero siete meses más tarde accedió a declararse culpable de un cargo notablemente menor de ayudar e instigar a una transmisión de dinero sin licencia. En el momento de escribir esto, aún no había sido sentenciado. Aunque Shrem continuó desempeñando un papel vocal en la comunidad mientras estaba bajo arresto domiciliario en el domicilio de sus padres en Brooklyn, los cargos contra una persona que una vez fue vista como portavoz de la comunidad dejaron otra mancha en Bitcoin.

Las cosas empeorarían. monte Gox, que había luchado con sus finanzas desde la incautación de sus cuentas bancarias en Estados Unidos y había dejado de permitir que la gente retirara dólares, llegó a su punto de quiebre cuando anunció que ya no permitiría a los clientes enviar bitcoins al extranjero. Culparía a un error en el software central de bitcoin, una acusación que fue refutada por los desarrolladores, que sospechaban que el CEO Karpelès estaba desviando la culpa, solo para descubrir que efectivamente había un error que los piratas informáticos explotarían, casi paralizando la red. mientras trataban de obtener pagos fraudulentos con miles de transacciones falsas. Mientras tanto, Mt Gox perdió el control. Cualquiera que sea la causa de sus problemas, no fue capaz de resolverlos, y el 28 de febrero anunció que se declararía en quiebra y agregó la deslumbrante revelación de que había perdido 850,000 bitcoins, * 650,000 de los cuales pertenecían a clientes: desaparecidos, solo como eso. La cantidad valía alrededor de $ 500 millones en ese momento. Los clientes estaban indignados. El público en general estaba perplejo. Y los inversores descargaron bitcoins en masa.

En todo el mundo, más gobiernos, entre ellos Rusia y Australia, comenzaron a establecer la ley en diversos grados. Para todos, excepto para los bitcoiners más doctrinarios, la pregunta no era si debería haber regulación -la mayoría vio efectos positivos del reconocimiento de la importancia de bitcoin y pensó que podría sofocar los temores de los usuarios-, pero si la sobrerreacción regulatoria restringiría la innovación. China consolidó esa preocupación con un dictamen más formal en abril que prohíbe a los bancos tener algo que ver con las empresas de bitcoin. Junto con

eso, los intercambios en los Estados Unidos estaban teniendo dificultades para abrir cuentas en los bancos, que eran cautelosos de tratar con ellos, dejando a algunos de los principales actores de la industria sin un salvavidas financiero clave. El 11 de abril, el precio del bitcoin tocó un mínimo intradía de $ 344.24, menos de un tercio de lo que era en su punto máximo cuatro meses antes. ¿Fue este el final? algunos se preguntaban

Una preocupación mucho más grande que China era lo que podría suceder en Washington o Nueva York, cuyos reguladores tenían más poder para dictar el desarrollo de criptomonedas. Eso se debe a que el papel del dólar como reserva dominante y moneda comercial del mundo pone a su sistema financiero en el centro de todo. El Servicio de Rentas Internas emitió una sentencia muy esperada, declarando que el bitcoin no era una moneda sino propiedad y que, por lo tanto, tributaría por ganancias de capital. Este no fue el peor anuncio para los entusiastas de criptomonedas, pero creó un dolor de cabeza para los usuarios, quienes, de acuerdo con las pautas iniciales del IRS, tendrían que hacer un seguimiento de cada bitcoin que gastaban para determinar si habían obtenido ganancias o pérdidas. desde que lo compraste Muchos temían que esto proporcionaría otra excusa para que los usuarios principales se mantuvieran alejados de Bitcoin. Mientras tanto, el Departamento de Servicios Financieros de Nueva York propuso establecer una "BitLicense", que regularía los negocios de monedas digitales y superaría parte de la ambigüedad que rodea a las licencias estatales de transmisores de dinero. Aunque el superintendente de Servicios Financieros, Benjamin Lawsky, describió el plan durante las audiencias en febrero como un esfuerzo constructivo para regular el bitcoin sin anular la innovación, el borrador que lanzó en julio fue una gran decepción para los bitcoiners. Parecía mucho más draconiano de lo esperado y provocó una reacción inmediata de parte de una comunidad bitcoin repentinamente bien organizada. Lawsky indicó que estaba dispuesto a cambiar algunas de las cláusulas y que algunas estaban siendo malinterpretadas, pero a la hora de escribir no estaba claro qué forma tomarían esos cambios.

Los reguladores no fueron los únicos que respondieron al pergamino de los titulares malos con medidas para controlar la caótica anarquía de Bitcoin. Muchos de los empresarios más inclinados a los negocios también querían dejar atrás la era de Mt Gox. Esto no le cayó bien a los radicales antigubernamentales que habían hecho del bitcoin su causa personal, pero sí estimuló parte de la innovación que, según predijo Gil Luria, vendría en el ámbito de la negociación. Varias firmas con pedigrí de Wall Street se movieron para construir intercambios de alta tecnología que podrían acomodar a inversionistas sofisticados como los fondos de cobertura y que serían pesados en los procedimientos clásicos de cumplimiento. Estos serían el antídoto contra la pérdida de confianza impulsada por Mt Gox, argumentaron. Pero hasta que llegaron en línea, las condiciones comerciales se mantuvieron delgada, lo que significa que algunas de las innovaciones que se trajeron a Bitcoin negociación y que de otro modo podrían haber ayudado a fomentar bidireccional flujos de compradores y vendedores simplemente exagerado el unidireccionales se mueve en tiempos de pánico. Estos alta frecuencia incluido, automatizados comerciales “bots” que se utiliza en algunas de las bolsas del continente chino, instalaciones margen de comercio introducidas por la bolsa de Hong Kong Bitfinex para los clientes a comprar bitcoin con préstamos, instalaciones para los futuros, y venta a corto apuesta por una disminución del bitcoin. En medio de la angustia creada por la propuesta BitLicense impopular Lawsky, estas estrategias de negociación nervioso, junto con un mercado ilíquido y más conniptions mercado en agosto, revivieron las preocupaciones de la gente acerca de la volatilidad hasta que el precio se estabilizó hacia el final del verano alrededor de $ 500.

A través de todos estos altos y bajos, toda esta alegría y ansiedad, bitcoin continuó creciendo su ecosistema. Muchos comerciantes levantan sus manos para aceptar Bitcoin. Cada vez más personas abrieron carteras (más de 5 millones al momento de escribir esto). Esta historia de adopción expandida ofreció un convincente contrapunto a la impresión de criminalidad,

incompetencia y represión reguladora que había dominado la cobertura de la prensa dominante en 2014.

Mientras tanto, la innovación en la tecnología de criptomonedas está encendida. En todo caso, se aceleró a medida que los desarrolladores de todo el mundo se entusiasmaron cada vez más con la posibilidad de una interrupción económica total y las ganancias que esto auguraba. No sólo se deciden a desarrollar una serie de nuevos servicios por lo que es fácil que la gente compra, venta, y realizar transacciones en bitcoin, pero expertos en tecnología también idearon nuevas "Bitcoin 2.0" proyectos que se comprometió a descentralizar todos los rincones de la economía. Era todo una muestra del enorme respeto que muchos habían desarrollado por la invención central de Satoshi Nakamoto y sus innumerables potenciales: la cadena de bloques. Esta es la máquina dentro de la máquina bitcoin. En el próximo capítulo, entramos en él.

Capítulo 5

CONSTRUYENDO EL BLOCKCHAIN

El amor al dinero crece a medida que el dinero crece.

-Juvenal, A.D. 60-140

Como se señaló anteriormente, una gran pregunta persiguió los primeros esfuerzos de la criptomoneda: ¿Cómo sé que la persona que me envía una ficha digital no le ha enviado una copia a otra persona? No puedo verificar la marca de agua, la banda magnética o las fibras físicas en la nota, como puedo con papel moneda. Aquí radica la amenaza del "doble gasto", la gran vulnerabilidad del dinero digital. Satoshi Nakamoto lo resolvió, no mediante el fortalecimiento de la seguridad de un token de moneda, sino mediante un verdadero avance en la tecnología social, en el sistema de créditos, débitos y saldos que los chartalistas reconocen como la verdadera naturaleza del dinero. El blockchain, el libro de contabilidad que funciona como el sistema nervioso central de bitcoins, fue el logro más destacado de Nakamoto. Si bien es de naturaleza técnica, refleja reflexiones importantes sobre la psicología del dinero y la comunidad, y lo que se necesita para crear reglas que hagan que las personas actúen en interés del grupo.

Hemos insinuado que una de las grandes ventajas de las criptomonedas es que están descentralizadas. ¿Qué significa esto? Todo se reduce al uso de un libro común, totalmente público.

Hasta ahora, los sistemas monetarios se han construido sobre la base de contabilidad centralizada, ya sea por los bancos o por los bancos centrales que operan en los libros mayores de toda la economía. Esto ha proporcionado eficiencia y seguridad para las comunidades que no han tenido otra manera de confiar en las cuentas de los demás sobre quién debe qué y a quién. El problema siempre ha sido, sin embargo, que este modelo confiere demasiado poder y ganancias excesivas a esos registradores centrales. El desafío consistía en encontrar una solución de compromiso: un sistema confiable y descentralizado para mantener en orden las pestañas de la sociedad sin perder la eficiencia y la seguridad que la centralización había entregado.

Para crear un sistema menos centralizado, tenía que encontrar la forma de asignar la tarea compartida de mantenimiento de registros a un grupo de personas o instituciones conectadas por una red, y darles algún incentivo para realizar esas tareas. También era necesario asegurarse de que su libro contable común se gestionara de tal manera que ningún registrador pudiera manipularlo e introducir errores que los demás no notarían. Finalmente, tenía que imbuir a todo el grupo de un sentido de confianza en sus propias reglas, o al menos confiar en que las barreras al mal comportamiento eran suficientes.

Advertencia temprana: la esencia de cómo funciona esto puede ser un poco complicado. Se basa en conceptos matemáticos que no son familiares para la mayoría de las personas. Una forma de evitar esto sería reconocer que no necesita comprender el funcionamiento de las criptomonedas. Ninguno de nosotros tiene una idea de cómo funciona un motor de combustión interna, pero aún manejamos automóviles y confiamos nuestras familias a sus mecanismos. Es muy posible que no pueda explicar adecuadamente el funcionamiento del sistema bancario de los EE. UU., Pero todavía confía su dinero a un banco. Aun así, es completamente comprensible, de hecho loable, que los usuarios potenciales de este nuevo sistema monetario no probado quieran comprender su fontanería interna. Es una razón clave por la que elegimos escribir este libro, y quizás una de

las razones por las que lo recogió. Entonces, sigamos adelante. Lo tomaremos con calma, trataremos de reducirlo a lo básico. Adelante.

En primer lugar, para ayudarnos a conocer el modelo que Nakamoto estableció como punto de referencia, tomaremos prestada una idea desarrollada por el ingeniero de software Yevgeniy Brikman. Se basa en la historia a la que se hace referencia en el capítulo 2 de cómo las piedras fei se utilizaron para rastrear y borrar las deudas en la sociedad micronesia de Yap en el siglo XIX. Imagínese, escribió Brikman, que a medida que el comercio y las transacciones se expandían, una tribu yapese tenía dificultades para rastrear quién poseía y le debía las piedras. Se hizo imposible determinar si una persona que afirmaba tener suficiente cantidad de dinero en efectivo tenía suficiente para pagar una deuda. Después de estallar las peleas y aumentar las tensiones, los ancianos de la tribu nombraron a una persona para que se hiciera cargo de un registro escrito compartido de las tenencias y transacciones de fei. Pero ese registrador comenzó a cobrar tarifas por registrar cada transacción, aplicando distinciones arbitrarias que favorecían a un miembro de la tribu sobre otra, y recompensando a sus compinches. Y no fue el único que comenzó a usar el sistema para su ventaja: los jefes pronto lo presionaron para que cocinara los libros.

Finalmente, un grupo de tribus interesadas tomó el asunto en sus manos. Eliminarían al registrador y su libro central. En cambio, cada familia mantendría su propio libro mayor. Cada vez que se producía una transferencia de fei, la persona que realizaba el pago iba al centro del pueblo y anunciaba a todos que se había realizado una transferencia; de hecho, el anuncio constituía el pago. Todo el mundo actualizaría su libro de contabilidad, introduciendo una entrada de débito en la cuenta del pagador y otorgando un crédito equivalente al del beneficiario. Si la mayoría de los hogares reconocieran una transacción como legítima, los demás tendrían que aceptarla.

Hasta hace poco, era imposible crear un sistema tan descentralizado en el vasto ámbito de la economía global. Pero luego Internet resolvió una gran parte del problema creando una red para la comunicación universal instantánea. Los siguientes pasos fueron (1) crear un mecanismo para mostrar públicamente el trabajo de cada registrador y mantener la integridad del libro de contabilidad común que todos acuerdan ser precisos, y (2) proporcionar los incentivos adecuados para que suficientes individuos o firmas dediquen recursos para el mantenimiento de ese libro mayor. Bitcoin manejó cuidadosamente ambos desafíos.

Hemos mencionado que el software de bitcoin está preprogramado para generar una cantidad consistente de bitcoins nuevos durante un período de 130 años, y que estos se emiten como recompensas a los propietarios de computadoras conocidos como mineros por su trabajo que confirma las transacciones. Por supuesto, esto no significa que las personas no puedan seguir usando bitcoins, que pueden dividirse en fracciones pequeñas. Se seguirán compartiendo de un lado a otro, y su valor cambiará de acuerdo con el precio que el mercado otorgue a los bienes y servicios que pueden comprar. Pero por ahora la publicación de esas recompensas es lo que asegura que el libro público de bitcoin, su blockchain, se actualice, mantenga y conserve. Con el tiempo, a medida que la generación de nuevos bitcoins se desacelere, el sistema de recompensa se convertirá en uno en el que los mineros serán compensados con modestas tarifas de transacción impuestas a cualquiera que realice pagos.

El libro mayor de blockchain de Bitcoin es una larga cadena de bloques, o agrupaciones, de transacciones que se producen al mismo tiempo. La cadena continuará creciendo indefinidamente mientras el sistema siga funcionando. Esta estructura cronológica es crucial porque confiere legitimidad a las transacciones más antiguas, y la idea es que los intentos posteriores de un usuario por volver a gastar el mismo saldo de bitcoin sean tratados como ilegítimos. Al crear una secuencia de gastos y recibos con sello de tiempo entre cada participante en la economía de bitcoin, el sistema realiza un seguimiento de dónde están los saldos de todos en un momento dado,

así como la información de identificación adjunta a cada bitcoin y fracción de bitcoin. creado, gastado o recibido. Si James utiliza una aplicación de billetera bitcoin en su teléfono inteligente para, por ejemplo, comprar una taza de café en Coupa Café en Palo Alto, se notificará a la red de una solicitud para enviar BTC0.008 desde una dirección que está vinculada de forma única a su billetera con una controlado por la billetera digital de Coupa Café. En este momento, la compra se presenta como una "transacción pendiente", una pendiente de confirmación. Pero después de que los mineros hayan completado las tareas requeridas para organizar un nuevo bloque de transacciones e insertarlo en la cadena de bloques, las transacciones de James y de otras muchas transacciones que ocurran dentro de los mismos diez minutos se registrarán permanentemente en ese libro. Eso establece su compra de café como autenticada e irreversible. (Nota: Blockchain no sabrá, ni siquiera le importará, que era para tomar un café, o que James y el Coupa Café participaron, todo lo que necesita son las contraseñas especiales y las direcciones de identificación asociadas con las billeteras de James y Coupa Café).

Ahora, imaginemos que James es un codificador consumado y que sabe cómo anular las instrucciones en el cliente de software que usa su computadora para acceder a la red bitcoin. También está quebrado y con sueño, por lo que hace que el cliente toque la misma información de la cuenta desde la que pagó el café para luego comprar una almohada de Overstock.com, tratando efectivamente de pagar con bitcoins que ya no tenía. Después de hacer esto, el registro cronológico de la cadena de bloques revelaría que el dinero ya se había gastado. No, los registradores declararían mientras revisaban el nuevo intento de transacción de James contra el registro permanente, él había gastado esos bitcoins antes.

Cada transacción que se agrega al ledger blockchain en constante aumento se compara con el ledger existente antes de que se le otorgue un sello de legitimidad. Con base en una opinión consensuada entre los mineros acerca de qué transacciones son legítimas y cuáles no, el libro mayor proporciona una prueba irrefutable de quién posee qué y qué se gastó y recibió.

Para facilitar la explicación, nos enfocaremos en cómo funcionan los sistemas de cadena de bloques, creación de moneda y confirmación de transacciones de Bitcoin, aunque existen muchas variaciones de cadenas de bloques en el universo de criptomonedas.
La taza de café de James representaba una transacción. El sistema debe procesar muchos más.

El blockchain se gestiona, como hemos mencionado, por el protocolo de software central de bitcoin. Cada usuario de la red bitcoin desde Nakamoto hasta el presente ha descargado de una forma u otra un conjunto de instrucciones de programación que le dicen a su computadora o teléfono inteligente cómo interactuar, hablar y trabajar con otros en esa red. Blockchain no vive en una sola computadora o servidor, sino que, al igual que nuestros Yapese ledger-keepers, se comparte alrededor de esa comunidad de propietarios de computadoras o nodos. Esos nodos incluyen máquinas que ejecutan billeteras bitcoin, una forma de software que ofrece a consumidores y empresas contraseñas especiales con las cuales proponer cambios a los balances de bitcoin (es decir, iniciar pagos) en las partes limitadas de la cadena de bloques que se les asignan. Los nodos también incluyen las PC individuales (o, más probablemente en estos días, equipos mineros especializados) que son utilizados por los mineros bitcoin para construir la cadena de bloques y ganar recompensas de bitcoins. Trabajando juntos de acuerdo con el sistema preordenado, estos nodos colectivamente aseguran que los contenidos del libro mayor sean legítimos y estén protegidos contra el abuso por elementos deshonestos.

El blockchain es todo para bitcoin. De hecho, esta contabilidad siempre cambiante de débitos y créditos constituye la moneda misma. Los bitcoins no existen per se, no en el sentido de que se puede mirar dentro de un recipiente electrónico y aislar un conjunto de monedas independientes. Los bitcoins existen solo en la medida en que asignan valor a una dirección de bitcoin, una mini

cuenta única con la que las personas y las empresas envían y reciben la moneda hacia y desde las direcciones de otras personas y empresas. Los bitcoins no constituyen documentos u otros archivos digitales. El saldo que ve en su billetera es simplemente un valor neto de poder adquisitivo basado en una contabilidad de las transacciones entrantes y salientes. Este modelo se extiende a través de la cadena de bloques, encapsulando todos los débitos, créditos y saldos asociados con cada dirección de bitcoin única. Esta es una distinción importante porque significa que no hay un archivo o documento de moneda real que pueda copiarse o perderse. Su derecho a bitcoin se define como el saldo que el libro mayor reconoce como suyo. Puede perder su capacidad de explotar esos saldos y cambiarlos a otra persona, es decir, si pierde la contraseña necesaria para liberarlos, pero no puede literalmente perder bitcoins ya que en realidad no existen.

También es crítico: el blockchain cada vez mayor de las transacciones confirmadas es público. Eso distingue bitcoin de los sistemas cerrados de moneda electrónica como PayPal, donde el libro mayor es un secreto bien guardado. Utilizando un software especialmente diseñado, más comúnmente, la herramienta gratuita provista por la compañía epónima Blockchain, con sede en Londres, puede ver los detalles de cada transacción de bitcoin jamás realizada. Solo puede cambiar, o solicitar el cambio, aquellas partes de la misma a las que se puede acceder a través de sus contraseñas especiales, pero en todo momento tiene una vista completa de cada otra transacción y dirección de bitcoin.

Al mirar estas direcciones en la cadena de bloques, no vemos nada para identificar a sus dueños. En cambio, aparecen como cadenas de letras y números de entre veintiséis y treinta y cuatro caracteres. Cada una de estas direcciones, creadas cuando se produjo una transacción anterior, representa lo que los criptógrafos llaman una clave pública. Como propietario de dicha dirección, puede compartirla con personas externas e invitarlos a realizar un depósito allí. Pero solo usted tiene el poder de realizar un retiro, lo que puede hacer con la ayuda de una billetera. Así es cómo podría llevarlo a cabo: podría abrir una aplicación de teléfono inteligente vinculada a su billetera en línea y luego usar su escáner de código QR incorporado para importar la dirección de un comerciante en la línea "A" de una ventana de transacción. Luego debe ingresar el monto del pago deseado y presionar "Enviar", instruyendo así al software de billetera para que encuentre un saldo de bitcoin suficiente en una o más de sus direcciones preexistentes y envíe ese saldo al comerciante. * Para ello, el programa de billetera accede a un código de acceso incorporado que se conoce como clave privada; cada clave privada está asociada de manera única con una dirección. Al combinar matemáticamente las claves pública y privada -o, en términos criptográficos, al firmar la primera con la última- se libera información, que en este caso equivale a una instrucción para transferir un equilibrio de bitcoins de una dirección de cadena de bloques a otra. *

Este sistema de encriptación de clave pública, que es similar a la aplicación de la contraseña secreta para su cuenta bancaria en línea a su nombre de usuario no tan secreto, se usa ampliamente en aplicaciones financieras y de Internet, incluidas la banca en línea y el correo electrónico; permite a las personas compartir datos seleccionados sin revelar el acceso a toda su información. Una característica importante de este sistema es que es prácticamente imposible, utilizando la tecnología informática actual, hacer el cálculo de la clave pública-privada en reversa y descubrir el código de acceso privado. † Pero eso no significa que un extraño no pueda descubrir una clave privada si , por ejemplo, él o ella accede a una computadora o teléfono inteligente en el que reside. Por eso es importante que las personas y las instituciones protejan sus billeteras y protejan sus bitcoins. No hacerlo es lo que sucedió en Mt Gox, al menos según su versión de cómo perdió 650,000 bitcoins.

La trazabilidad de este registro de transacciones ayuda a construir la confianza de la comunidad en el sistema monetario. Pero esta característica del bitcoin también ha sido explotada por las

fuerzas del orden, más famoso cuando el FBI confiscó bitcoins durante su campaña de 2013 en el mercado de drogas en línea Silk Road. ‡ A diferencia de las transacciones con tarjetas de crédito, que están vinculadas al nombre de una persona y se dan a conocer para el banco de esa persona y para cualquier otra persona con acceso a los registros de la cuenta de la persona, una dirección de bitcoin no tiene conexión personal. Esta es una de las razones por las que algunas personas recurren a Bitcoin para realizar transacciones embarazosas que prefieren que otros no conozcan. Por otro lado, si anuncian que tal o cual dirección de bitcoin es suya, entonces cualquiera puede ver cada transacción que hagan dentro o fuera de esa dirección. Debido a que solo aparecen identificadores alfanuméricos y no nombres, los agentes de la ley no pueden navegar fácilmente por este sistema. Sin embargo, la rastreabilidad presenta oportunidades para seguir pistas que de otro modo se ejecutarían con dinero en efectivo. Armado con poderes de citación, un investigador podría, en teoría, forzar a cualquier institución que proporcionara una billetera de bitcoin a divulgar la identidad del propietario. Esta es la razón por la cual algunas personas ven bitcoin como una herramienta más grande para los fiscales que como una capa para los criminales.

Esto plantea preguntas importantes. La tensión siempre existe entre los objetivos de mantener la privacidad individual y permitir que el acceso del gobierno a la información nos proteja. Al igual que en otras partes de Internet, el desafío para bitcoin, si es que se generaliza, será encontrar un equilibrio. Necesita preservar los aspectos positivos de su anonimato, ya sea la capacidad de una bloguera femenina en Afganistán para recibir pagos por sus contribuciones sin la interferencia de los demás o, más generalmente, el derecho de las personas a buscar legalmente la felicidad en la forma que prefieran contra el amenaza de que los actores nefastos lo explotarán.

Volver a cómo funciona la cadena de bloques. La billetera de James ha realizado la firma de clave público-privada e instruido a la red bitcoin que desea enviar BTC0.008 a una dirección controlada por Coupa Café, pero en este momento todavía es una transacción pendiente. Más tarde, si todo va según lo planeado y no se sospecha que la compra de James es un doble gasto, se confirmará como una transacción legítima y se instalará en el blockchain. Una vez que eso sucede, la transferencia de fondos no se puede revertir ni cancelar. No hay contracargos para el comerciante del tipo que los bancos imponen si un cliente de tarjeta de crédito disputa posteriormente un cargo, y ninguna de las partes puede deshacer por la fuerza el acuerdo fuera de un acuerdo común para realizar una segunda transacción de reembolso. Esta es la razón por la cual el sistema de bitcoin para verificar que el doble gasto no ha ocurrido es tan importante, lo que nos lleva a esos "mineros" trabajadores.

La minería de Bitcoin es, en nuestra opinión, un nombre inapropiado. El trabajo esencial que se realiza es más como la contabilidad.

El trabajo es otra palabra prominente en la lengua vernácula de la minería bitcoin, en este caso transmiten la sensación de que el valor subyacente de la divisa no se basa en la nada, sino en el trabajo, y el trabajo duro en eso. De hecho, la dificultad computacional es su característica definitoria. Cuanto más difícil sea, más recursos del mundo real se gastarán en la realización de la tarea, principalmente en forma de electricidad. Algunos criptoeconomistas argumentan que estos insumos son los que dan valor real a los bitcoins. Igualmente importante, la cantidad de trabajo, el equivalente informático de horas-hombre, otorga legitimidad al libro mayor, ya que representa una inversión colectiva significativa para garantizar su integridad.

Así es como los mineros "trabajan".

Una vez que James ha ordenado a su billetera que envíe bitcoins a Coupa Café, transmite esa transacción pendiente a la red, junto con una gran cantidad de información importante: las direcciones de billetera asignadas por las dos partes; el sello de fecha y hora; varios otros detalles,

como un código de transacción único; y cualquier otra información -un saludo, tal vez- que el remitente podría adjuntar.

Entra a los mineros Cada nodo o equipo minero reúne esta información y la reduce a una cadena alfanumérica cifrada de caracteres conocida como hash. Al igual que con los archivos de documentos que pueden "comprimirse", este proceso permite resumir cantidades relativamente grandes de información y reducirlas a un almacén de datos mucho más pequeño. Los hashes son una parte integral de los procedimientos de cifrado y almacenamiento de datos en todo el mundo de la informática. Puede haberlos visto sin saber lo que son. Dependiendo de qué algoritmo hash se esté utilizando, el proceso produce un hash de una longitud fija. En el caso de Bitcoin, el algoritmo se llama SHA-256, que entrega un hash de sesenta y cuatro caracteres de longitud tomado del rango completo de números (0-9) y letras (a-z). Para ver cómo se ve, puede visitar cualquier sitio web generador de hash y escribir algo en el campo de texto. Aquí es donde regresó quickhash.com cuando escribimos: "Lo único que tenemos que temer es el miedo mismo":

f72680b97551fc5eda1b3a33dda55796ba9619b371fdd03f66409f2c4958c2cb

Y esto es lo que sucedió cuando cortamos y pegábamos las 168 palabras del párrafo anterior de este capítulo en el mismo campo:

e52a16c11d5c45b768b1bc87f0c1494799e92c019101562bfb435950b36de17b

Ya sea un solo personaje o el texto completo de War and Peace, el hash sale con la misma longitud de sesenta y cuatro caracteres. Sin embargo, el cambio más pequeño en la información subyacente (un solo punto decimal o un espacio, por ejemplo) cambiará el hash por completo. Este poder para empaquetar mucha información en la misma estructura hash pero con resultados completamente diferentes cada vez hace que su función de encriptación sea poderosa. Mucha información puede ser reducida y codificada. Y aunque es virtualmente imposible descifrar ese código y descubrir qué contiene, es relativamente trivial si una computadora tiene acceso a los datos fuente subyacentes para verificar que el hash encapsule con precisión esos datos.

Los algoritmos Hash también le permiten construir una especie de jerarquía hash, que es útil porque crea una estructura dentro de la cual los mineros pueden agrupar transacciones concurrentemente sincronizadas. Así es como funciona: el cliente de software del minero toma el hash de la primera transacción -con el conjunto de datos subyacentes contenidos en él- y lo combina con los datos brutos de la siguiente transacción sin forma para formar un nuevo hash. Un registro completo de ambas transacciones ahora ha sido hash. A continuación, se produce una acción similar con la próxima transacción que recoge el cliente de minería. Combina el segundo hash, el que contiene dos transacciones por valor de datos, con la información de la siguiente transacción para formar un tercer hash. Este proceso continúa cuando se recuperan las nuevas transacciones, con las computadoras empacando constantemente todos los datos entrantes en un hash único, un código cuya información subyacente puede verificarse fácilmente en un momento posterior mediante el trabajo a través de la cadena ininterrumpida. Así es como las transacciones se empaquetan en los bloques de construcción cruciales de la cadena de bloques, llamados, apropiadamente, bloques.

Mientras todo esto sucede, las computadoras también participan en una especie de competencia / lotería para tratar de ser los primeros en "cerrar" uno de estos bloques, es decir, prepararlo para su inserción en el libro mayor de blockchain y llevarse a casa el premio de la próxima emisión de bitcoins. Hasta que eso suceda, la red no puede comenzar a confirmar la validez de la última ronda de transacciones. Cada minero ha procesado y vuelto a centrar los datos subyacentes de la manera descrita anteriormente, pero sus detalles aún no están listos para ser verificados por la red.

Todavía no hay consenso sobre su validez. El pago de James a Coupa Café permanece sin confirmar. Encontrar la solución al rompecabezas es, por lo tanto, una parte integral del negocio vital de la validación de las transacciones.

Las máquinas entran en la competencia de forma simultánea y rápida con nuevos hash de bloques potenciales para codificar y capturar todos los datos en el nuevo bloque completamente empaquetado y vincularlo al hash de bloques del bloque anterior. El hash del bloque ganador debe coincidir con uno que el algoritmo central de bitcoin haya decidido que será el número ganador del bloque actual. El emparejamiento es extremadamente difícil de hacer, por lo que las computadoras siguen generando hashes nuevos hasta que lo hacen bien, ajustando el proceso cada vez para cambiar la lectura una y otra vez. Cada uno de los innumerables hash nuevos producidos por la computadora se crea al agregar un número único generado aleatoriamente llamado nonce a los otros datos contenidos en el hash de bloque, que, como se mencionó, incluye la información de transacción subyacente y el hash de bloque del bloque anterior Agregar un nuevo nonce cada vez altera completamente el hash de salida. Vale la pena señalar que la palabra nonce se deriva de un pasaje de Lewis Carroll en el que desplegó la palabra frabjous, y la describió como una palabra "nonce" que se inventó para una ocasión y no es probable que se vuelva a utilizar. Tal es el destino de los miles de millones de nonces producidos y descartados, ya que las plataformas mineras de gran potencia buscan el hash de bloques ganador. Es una búsqueda de un pin digital en un pajar masivo de números.

Al final de este laborioso trabajo de ensayo y error, un nodo de minería finalmente obtendrá el algoritmo de bloqueo de bloques que buscaba el algoritmo de bitcoin, un número que debe contener la cantidad correcta de ceros y varias otras condiciones. Llegar allí requiere una fuerza de cálculo brutal, por lo que una plataforma de minería con la potencia de dispersión más rápida tendrá más posibilidades que una de ganar cada bloque. Dicho esto, el proceso de hash es totalmente aleatorio, lo que significa que si bien los equipos más poderosos ganarán la competencia con mayor frecuencia que los equipos de menor tamaño, no ganarán todo el tiempo. (Una forma de pensar es que invertir en potencia de hash es como comprar boletos de lotería adicionales; no hay garantía de ganar, pero sus posibilidades aumentan con cada boleto adicional.) De hecho, si el poder de hashing total de la red permanece constante, el La matemática de la función de generación de números aleatorios es tal que, durante un período prolongado, un solo nodo puede esperar ganar bitcoins proporcionalmente a la cantidad de energía que aporta a esa red. El problema es que con tantas plataformas mineras ahora en juego y solo se repartieron tantos premios en bloque, puede pasar mucho tiempo antes de que un número ganador de la plataforma de baja potencia se presente a un premio de veinticinco bitcoins. Es por eso que todos los operadores de minería, excepto los más grandes, se unen a grupos de minería, que dividen la entrada agregada de acuerdo con el poder de cálculo aportado por cada miembro, y los miembros más pequeños normalmente reciben solo fracciones de bitcoin cada mes.

Los mineros tienen la tarea de resolver el rompecabezas por dos razones. En primer lugar, impone un costo a la minería, ya que la potencia informática que demanda es costosa, tanto en términos de la maquinaria como de la electricidad que utiliza. Eso ayuda a regular la minería y crea una relación recíproca entre lo que de otra manera serían bitcoins gratis y el trabajo requerido para obtenerlos. Y dos, crea una competencia con un pago al final, que incentiva a los mineros a hacer el trabajo necesario para confirmar las transacciones.

Una vez resuelto el acertijo, el cliente de software bitcoin que se ejecuta en la máquina del nodo ganador "sella" un nuevo bloque de transacciones con el hash de bloques y le asigna un número de bloque que sigue secuencialmente el último número de bloque en la cada vez mayor cadena de bloques. (En el momento exacto en que se escribieron estas palabras, la cadena de bloques estaba trabajando en el bloque número 318,685, es decir cuántos bloques se habían completado desde

que Nakamoto extrajo el Bloque Génesis, y si convertiste eso en tiempo multiplicando ese número por diez minutos, lo sacaría más o menos en enero de 2009). Debido a que el hash de bloques anterior se ha incluido en el nuevo hash, el último bloque ahora está matemáticamente vinculado a la cadena de bloques, como para formar lo último en una línea de tráiler cada vez mayor. enganches. Debido a la calidad hipersensible de hashes descrita anteriormente, donde el más mínimo cambio de datos alterará completamente su resultado, esta estructura significa que, en teoría, nadie puede meterse con ninguno de los datos contenidos en la historia de la cadena de bloques. Si lo hiciera, todo se convertiría en un charlatán. Esto lo hace a prueba de manipulaciones.

Una vez que se ha creado y agregado a la cadena un bloque de transacciones recientemente sellado, queda mucho por hacer: otros mineros ahora deben confirmar la legitimidad de las transacciones subyacentes contenidas en él. Sin su afirmación, no existe un consenso compartido sobre la verdad de lo que se encuentra en la cadena de bloques. No habría forma de decir con certeza que un minero deshonesto había incorporado transacciones falsas en un bloque. Podría enviar bitcoins que no tiene derecho a gastar, es decir, falsificarlos, y el sistema simplemente aceptaría ese fraude como si fuera una transacción legítima. Los otros mineros verifican así lo que se conoce como la prueba de trabajo del minero ganador, comparando los datos de las transacciones subyacentes con los datos hash dentro de ella para verificar su legitimidad y compararla con la historia en el blockchain. Si bien eso parece una tarea gigantesca, estas son computadoras de alta potencia; no es tan agotador como el juego que no crea juegos y se puede hacer de manera relativamente rápida y fácil. Las confirmaciones de los otros mineros se transmiten a la red y luego a los titulares de billeteras. Coupa Café ahora puede estar razonablemente satisfecho de que el pago de James es legítimo. Igualmente importante, la confirmación da a los mineros la satisfacción de que el último bloque de la cadena es legítimo, lo que significa que están preparados para seguir adelante y adjuntar el siguiente bloque si resultan ser el ganador. A partir de ahí, todo el proceso comienza de nuevo.

Un aspecto importante aquí: mientras que el proceso de finalización y confirmación de bloque implica al menos una espera de diez minutos hasta que una transacción se libere completamente, los comerciantes que usan los servicios de un procesador de pago bitcoin como Bitpay, Coinbase o GoCoin generalmente aceptarán un el pago del cliente de inmediato. Para todas las transacciones salvo las más grandes, el procesador generalmente corre el riesgo de no confirmación. Lo hacen porque las no confirmaciones (o las acciones de doble gasto que conducen a ellas) son muy raras. También se lanzan al mercado sofisticadas herramientas analíticas de "big data", incluida una de BlockCypher de nueva creación, que permite a los comerciantes y procesadores medir en segundos la probabilidad de que se acepte una transacción en particular, todo con una precisión cercana al 100 por ciento.

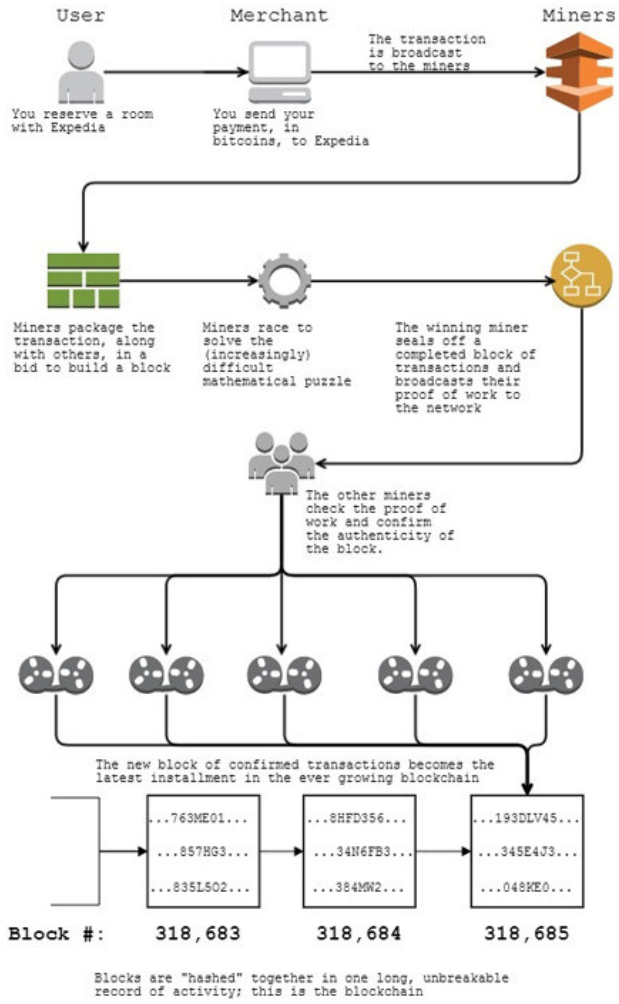
A pesar de estos trucos rápidos, el algoritmo de bitcoin establece ciertas reglas para generar confianza en el libro mayor a lo largo del tiempo y para garantizar que los mineros estén debidamente incentivados para confirmar solo las transacciones legítimas. Aunque a un minero se le asigna un nuevo lote de bitcoins una vez que sella un bloque y lo vincula con la cadena de bloques, el protocolo bitcoin no le permitirá utilizar esas bitcoins en un pago hasta que se hayan construido un total de noventa y nueve bloques adicionales. parte superior de su bloque. Eso asegura que, con el tiempo, el consenso de la red sobre la legitimidad de las transacciones contenidas en ese bloque original se convierta en una roca sólida. También motiva a cada minero a asegurarse de que todos los demás estén haciendo lo correcto.

Ocasionalmente, se encuentran dos bloques de manera prácticamente simultánea, lo que significa que un bloque queda "huérfano", ya que la red solo puede elegir uno para construir la cadena más larga. Los bitcoins adjudicados al bloque huérfano se dejarán sin valor, y cualquier transacción que estuviera contenida en ella pero excluida del bloque legitimado que ahora se inserta en la

cadena tendrá que procesarse más adelante a medida que se creen nuevos bloques. Esta capacidad para huérfanos de un bloque ilegítimo es importante porque significa que toda la red puede estar convencida de que la cadena cronológica ininterrumpida, simplemente en virtud de continuar, representa el verdadero registro reconocido por consenso. Pero también significa que algunas transacciones tienen tiempos de espera más largos antes de que estén completamente confirmadas e instaladas en el blockchain.

Cualquiera puede convertirse en minero y es libre de usar cualquier equipo informático que pueda encontrar para participar. Nakamoto sabía que a medida que más mineros ingresaran a la cacería, el incentivo sería fuerte para aumentar el poder de cómputo para vencer a la competencia. Entonces, para mantener todo sincronizado, programó el algoritmo bitcoin para calcular el denominado hashrate de la red global, de manera efectiva, la capacidad computacional total por segundo, y ajustó automáticamente la dificultad del rompecabezas matemático para que los bloques se volvieran más difíciles de sellar. De esta forma, el programa de recompensa de bitcoin podría ajustarse más o menos a un programa arraigado de diez minutos por bloque. La brecha de diez minutos es algo arbitraria, pero al elegir un intervalo y programar el software para que se apegue a ese cronograma fijo, puede organizar el cronograma de emisión de moneda para que sea coherente durante un período de 130 años.

En términos de teoría monetaria, el pago es señoreaje, la ganancia que un emisor de moneda -sea un soberano, una autoridad monetaria, o en este caso un minero ganador de bitcoin- deriva del privilegio de acuñar el dinero de la comunidad. El corolario es que este costo corre a cargo del resto de la comunidad, ya que el suministro nuevo agota el valor de mercado y el poder adquisitivo de la moneda existente. Seigniorage es inevitable; alguien tiene que ser el primero en poseer moneda recién emitida. La pregunta es cómo hacerlo justo. Algunos diseñadores de criptomonedas han creado fundaciones sin fines de lucro y les han cobrado la distribución de monedas en función de ciertos criterios, por ejemplo, para organizaciones benéficas elegibles. Pero eso requiere la participación de un fundador identificable y confiable para crear la fundación. Incluso entonces, ¿quién puede decir que esas reglas de distribución son justas? Es, por supuesto, subjetivo. Algunos diseñadores han otorgado asignaciones fijas a personas formalmente registradas como pertenecientes a un grupo particular, como un registro nacional. Pero eso crea el potencial de fraude ya que las personas pueden configurar más de una billetera por persona, escondiéndose detrás del anonimato del sistema, y obtener asignaciones más altas para ellos mismos. Algunos han creado las monedas y vendido porciones de ellas al público, obteniendo el señoriaje para sí mismas, al igual que un gobierno. A menudo, esta estrategia requiere algunas maniobras elaboradas para mantener la fe con la comunidad, ocasionalmente empleando una estrategia de "prueba de quema", donde los fundadores periódicamente transfieren algunas de sus tenencias de monedas a una billetera verificable inutilizable para mantener la escasez y reforzar el valor de las monedas de los demás.



Cómo se confirman las transacciones en Blockchain
(Cortesía de Michael J. Casey y Paul Vigna)

El fundador no identificado de bitcoin trató este problema de equidad recurriendo a los principios de competencia de libre mercado. Ese es uno de los propósitos de la implacable competición hash, un proceso que, para los no iniciados, puede parecer inútil. Es un truco. Los mineros realizan una tarea con el único objetivo de ganar una carrera para ganar bitcoins, y casi como resultado no deseado, terminan confirmando transacciones en el camino y manteniendo el blockchain actualizado. Esta es la base sobre la cual el protocolo de bitcoins decide quién debe ganar el señoreaje, un modelo fundado en la idea de que a cambio de este privilegio los destinatarios deben invertir recursos (equipamiento, electricidad) y que su computadora debe hacer el trabajo. Eso a su vez proporciona una base para poner un valor en bitcoin.

Para asegurarse de que su sistema de incentivos tuviera algún peso real, Nakamoto ideó una política monetaria mucho más estricta que la de la Reserva Federal, un elemento clave que reduce a la mitad la emisión de bitcoins cada 210,000 bloques, aproximadamente cada cuatro años. A partir de 2014, los bloques estaban pagando 25 bitcoins cada uno, frente a 50 antes de 2012. Caerá a 12,5 en 2016. Este cronograma significa que el bitcoin está cargado frontalmente, con más de la mitad de los 21 millones de monedas de por vida creadas en el mercado. primeros seis años de existencia del sistema. Esto crea una sensación de escasez en el tiempo, que, en teoría, debería respaldar el valor de bitcoin si la demanda se mantiene al día.

Los nuevos bitcoins no son la única forma en que los mineros son compensados. El software principal también contiene la capacidad de cobrar tarifas de transacción, pagadas por el remitente. A partir de ahora, algunas tarifas pequeñas son obligatorias solo para unos pocos tipos de transacciones. Estos incluyen transacciones de polvo, o pequeñas cantidades -la idea es que las tarifas antispam son necesarias para desalentar los ataques de negación de servicio por parte de actores nefastos que intentan saturar una red con cantidades masivas de transacciones o mensajes sin sentido- y transacciones que contienen cantidades excesivas de datos, definidos como más de diez mil bytes. Los usuarios también pueden agregar tarifas a sus transacciones para aumentar la probabilidad de que los mineros lo recojan e incluyan en bloque, reduciendo así el tiempo de espera potencial para la confirmación final. (No todas las transacciones que ocurren con un período de diez minutos terminan en un bloque confirmado dentro de ese tiempo).

A medida que la tasa de emisión de nuevos bitcoins se ralentiza aún más, es casi seguro que habrá que modificar el algoritmo para que las tarifas de transacción sean una parte más importante de la remuneración de los mineros para mantenerlos incentivados a hacer su trabajo. (Una vez que las tasas de emisión bajen a cero en el año 2140, las tarifas de transacción serán la única forma de compensación). El equipo de desarrollo central administrado por Gavin Andresen de la Fundación Bitcoin tiene un plan para crear una escala flexible de tarifas por espera de confirmación tiempos cuyas tasas serían establecidas por un mecanismo de mercado. Esto nos recuerda que si bien Bitcoin es mucho más eficiente como sistema de pago que el sistema centralizado centrado en el banco, no es gratuito. Tanto las tarifas de señoreaje como las de transacción representan una transferencia de valor para aquellos que manejan la red. Aún así, en el gran esquema de cosas, estos costos son mucho más bajos que cualquier cosa encontrada en el sistema anterior.

Con los mineros cautivados por los espectaculares aumentos de precio de 2012-13 y aparentemente inmutados por la gran caída de precios de 2014, la posible recompensa continúa atrayendo a la gente y sus computadoras a la minería. Incluso en medio de indicios de que los costos involucrados, especialmente el de la electricidad, hacen que sea más difícil ganar dinero, la minería ha experimentado un aumento absolutamente asombroso en la potencia de cálculo. Parece que no faltan personas que piensan que el bitcoin, como les gusta decir a algunos en la comunidad, se dirige "a la luna" y que la minería es su boleto a esas riquezas. La minería de Bitcoin se encuentra en medio de una carrera de armamentos o "guerra de hashrate", ya que los mineros traen crujidores numéricos cada vez más eficientes para vencer al rompecabezas de bitcoin.

Capítulo 6

LA CARRERA DE LAS ARMAS

El tiempo es dinero.

-Benjamin Franklin

La minería de Bitcoin, una vez realizada por geeks de criptografía en sus sótanos, se ha convertido en un gran negocio.

Un cálculo aproximado de un investigador estadounidense sugiere que los mineros invirtieron colectivamente hasta $ 1,000 millones en nuevos "equipos" especializados superrápidos en los doce meses hasta abril de 2014. Cualquiera en este juego ha tenido que elegir entre sacar la masa o aceptar un pago de bitcoin cada vez más bajo. Todavía hay dinero por hacer, pero los márgenes de ganancia se han reducido, y el retorno de la inversión es vulnerable a un precio de bitcoin extremadamente volátil.

Como hemos discutido anteriormente, la carrera comenzó cuando Laszlo Hanyecz se dio cuenta de que su tarjeta gráfica, o GPU, era en realidad ochocientas veces más rápida que la unidad de procesamiento central de su computadora para extraer bitcoins. A medida que sus monedas se acumulaban, otros mineros existentes pronto lo copiaron, convirtiéndolo en GPU para recuperar lo que habían perdido. A medida que los paneles de discusión tecnológica se iluminaron con la charla sobre el nuevo enfoque, y sobre las pizzas en las que su inventor había gastado sus monedas, oleadas de recién llegados se unieron a la búsqueda de bitcoins de todos los rincones del mundo.

Uno de esos recién llegados fue Jason Whelan, un estudiante de secundaria en Belleville, Ontario, cuyas pasiones gemelas fueron los juegos de computadora y las redes de computadoras. Su interés en este último lo llevó a los foros de criptografía en línea, y en el otoño de 2010, descubrió que las personas de repente estaban alborotadas por el bitcoin. Se enteró de que un nuevo intercambio llamado Mt Gox se había conectado a principios de ese año, lo que significaba que un número creciente de personas no solo estaba extrayendo bitcoins sino comprándolas, y su precio estaba subiendo; en el mes de octubre su precio se había más que triplicado, de seis centavos a más de veinte centavos. Por lo tanto, con la esperanza de hacer dinero rápido, Whelan hizo algunos ajustes en su computadora personal, una unidad que había personalizado para jugar con dos tarjetas gráficas Nvidia paralelas y superpotentes, y la convirtió en un minero bitcoin.

Desde el principio, hubo complicaciones. Un mes después, fue confrontado por su padre, preguntándose por qué diablos la factura de la luz se había ido por las nubes. Whelan había estado ejecutando el intenso programa de hashing del software de minería las 24 horas, los 7 días de la semana. Estaba tan caliente que Whelan se había preocupado por la seguridad de su "orgullo y alegría" y lo había trasladado a un rincón frío del sótano donde su padre no lo vería. Pero había otro problema: su amada computadora de juegos ahora estaba completamente ocupada realizando esta tarea mundana. Y no parecía estar haciéndolo rico.

"Estaba más interesado en jugar juegos con mi nueva computadora de juegos que verlo sentado allí generando algo de dinero mágico que realmente no entendía", recuerda Whelan. Entonces, apagó el cliente de minería cuando su recuento de monedas era a los treinta. En aquel entonces,

valían $ 6; cuando nos habló a finales de mayo de 2014, habrían valido $ 18,000. Lamentablemente, había sobrescrito el disco duro varias veces y no había anotado los códigos de acceso y las llaves de su billetera. Sin el conocimiento de la clave privada de código de acceso que había usado o incluso la clave pública adjunta a la billetera, las monedas probablemente se perderán para siempre. "Estoy seguro de que otros como yo fantaseamos con sus riquezas perdidas si hubieran continuado la minería desde los primeros días", dice.

Tres años más tarde, para entonces un estudiante de segundo año que estudiaba redes y seguridad de TI en el Instituto de Tecnología de la Universidad de Ontario, en Oshawa, Ontario, Whelan se sorprendió al saber que el precio de Bitcoin había subido a 120 dólares. Comenzó a leer sobre la moneda digital y, con su creciente experiencia en redes, pronto comprendió su importancia social y tecnológica, que se le había escapado cuando era adolescente. Entonces resolvió volver a la minería.

Esto era más fácil decirlo que hacerlo. En ese interregno de tres años, las GPU se habían vuelto obsoletas. Tras el avance de enero de 2013 en el que Avalon, con sede en China, envió sus primeros mineros utilizando ASIC (circuitos integrados específicos de la aplicación), el mercado se trasladó a "equipos" totalmente dedicados equipados con estos chips superrápidos, cada uno diseñado para procesar cálculos hash. Con el precio del bitcoin aumentando exponencialmente, la carrera estaba en marcha para hacer chips ASIC cada vez más rápidos y equipos más eficientes. En el momento de redactar este informe, las máquinas más nuevas, con una venta minorista de alrededor de $ 6,000, prometían tres terahashes por segundo: 3 billones de cálculos de hash por segundo o 1,800 billones en los diez minutos para la creación de bloques. Eso es aproximadamente 3 millones de veces más rápido que la CPU más rápida podría realizar la misma tarea cuando Nakamoto extrajo los primeros bitcoins en enero de 2009.

Pero a pesar de que el mundo virtual de la minería se ha movido a la velocidad del rayo, el mundo de fábricas y cadenas de suministro se ha esforzado por mantenerse al día. En septiembre de 2013, la prensa de bitcoin estaba llena de historias sobre retrasos en la entrega por parte de los principales fabricantes de equipos de gama alta. Se puede imaginar la frustración de que la gente gastara $ 4,000 para "preorder" un minero de Butterfly Labs Imperial Monarch, luego esperó seis meses para que se lo entregaran, sabiendo que por cada semana adicional, los bitcoins eran cada vez más difíciles de extraer y los equipos cada vez más rápidos. estaban siendo liberados Posteriormente, la Comisión Federal de Comercio suspendió sus operaciones en Butterfly Labs, con sede en Missouri. Y no fue la única empresa que creó relaciones ásperas con sus clientes: KnC Miner con sede en Estocolmo, CoinTerra de Austin, Alydian de Bainbridge Island en el estado de Washington y Hashfast con sede en San Francisco; todos tuvieron problemas de entrega, y los dos últimos cayeron en bancarrota. Se entablaron numerosas demandas alegando que las empresas habían estafado a sus clientes, destinando dinero para prerreglos que luego se utilizaron para financiar sus propias operaciones mineras. Por su parte, la industria lo atribuyó a proveedores de piezas mal preparados. El cofundador de Avalon, Ng Zhang, dijo que los fabricantes de ASIC en Taiwán al principio no tomaron en serio a los clientes del fabricante de la plataforma de minería de bitcoin. Pero a partir de mediados de 2014, los problemas de entregas seguían siendo los mismos para el curso en este negocio.

Para Whelan, la solución fue comprar una plataforma de segunda mano. Recogió una plataforma minera Jalapeño de Butterfly Labs en un anuncio clasificado local por $ 500, un poco como comprar un Mercedes usado con cien mil millas en el cuentakilómetros. A pesar de que su hashrate de cinco gigaheads por segundo estaba muy por detrás de las máquinas más rápidas del mercado, tenía la ventaja de estar disponible de inmediato. Con el valor cada vez mayor de los bitcoins, antes podría empezar mejor.

Luego, Whelan hizo lo que prácticamente todos los mineros pequeños y medianos hacen actualmente y se unió a un grupo minero. De esa manera, se aseguró un flujo constante de monedas, aunque en pequeños incrementos, en lugar de tener que esperar ese momento aleatorio, a años de distancia, si es que alguna vez, cuando su plataforma ganaría un bloque completo de veinticinco monedas. Sin embargo, el tamaño de los pagos no le molestaba. A diferencia de su primera incursión en la minería como estudiante de secundaria, esta tenía un fundamento más filosófico. "En 2010, vi que solo ganaba X dólares", dice, "pero ahora tenía una nueva mentalidad, que incluso si estaba perdiendo dinero en dólares, el movimiento de bitcoins es tan fuerte que estoy apostando por su futuro aumento ".

Whelan también tenía un as bajo la manga: la universidad cubría sus costos de electricidad. (Esto es relativamente común, las universidades todavía no han tomado medidas enérgicas contra la minería de bitcoin en el dormitorio universitario). Pero no pudo controlar el constante ruido y el calor que emanaba del artilugio en su pequeño dormitorio. Entonces, en los meses de otoño mantuvo la ventana abierta y usó un ventilador para aspirar el aire más fresco del exterior. En el invierno, cerró la ventana, pero conectó el ventilador a la máquina de su escritorio, y la combinación hizo un estallido todopoderoso. Mientras tanto, el precio subió a un máximo de principios de diciembre por encima de los $ 1.150, un aumento diez veces mayor al que había comenzado. Entonces, con su creencia en el futuro de Bitcoin, reinvirtió una porción de sus ganancias en algunos mineros adicionales, que a su vez necesitaron otro ventilador para mantenerlos frescos. "Me sentí como un traficante de drogas digital", dice. "Tuve que atender mis cultivos, mantenerlos frescos y al mismo tiempo evitar al personal de la residencia que podría oponerse a que las máquinas en constante funcionamiento se coman la electricidad".

Este negocio ruidoso y secreto era rentable, pero no resultó en una existencia cómoda. Y desde el principio, Whelan se enfrentó a la realidad matemática de que su hashrate estático se estaba reduciendo como una proporción de la red en constante expansión, cuyo poder de cómputo estaba casi doblándose cada mes. Eso aseguró que su pequeña parte del pago de bitcoin decayera sistemáticamente con el tiempo. A comienzos de la primavera de 2014, Whelan pensó en comprar un AntMinter S1 de segunda mano de Bitmain, que funcionaba a 180 gigaheads por segundo. Pero el tipo de cambio de Bitcoin estaba cayendo, ya que perdería dos tercios de su valor en los primeros cuatro meses del año, mientras que el índice de la red se disparaba. Esos dos factores ya habían agotado rápidamente el valor de una máquina que estaba siendo superada por equipos que funcionaban a más de un terahash por segundo. En diciembre, AntMinter había vendido al por menor por casi $ 3,000; pero ahora Whelan estaba buscando un modelo de segunda mano por $ 800. Sabiendo que esta rápida depreciación continuaría, cambió los planes.

Whelan sabía que el hashing en la nube ofrecía una alternativa. Estos servicios comprarían plataformas, las instalarían en centros de datos donde podrían ejecutarse a bajo costo y luego podrían alquilar partes de la potencia de hash. Los clientes obtendrían una porción de los ingresos totales de bitcoin proporcional a la cantidad total de hashing que estaban pagando. En el caso de Whelan, optó por un contrato de cinco años con pbcmining.com, reduciendo el precio total del contrato de 1.1 bitcoin, o alrededor de $ 600. De esa forma "podría sacarme las malditas máquinas de la oreja y no tener que preocuparme de que su valor se deprecie", dice.

Whelan nunca iba a huir con millones de esta manera, pero continuó obteniendo un modesto beneficio. A fines de la primavera, traía unos $ 200 al mes en bitcoins, el 50 por ciento de los cuales reinvirtió en potencia de hash adicional en pbcmining.com, una necesidad si quería mantenerse por delante de la tasa de dificultad en constante aumento: la medida de cómo Es raro que gane Bitcoin a medida que el sistema se adapta al poder de hashing de red cada vez mayor. Algunos creen que esta ecuación significa que muchos contratos de minería en la nube tienen un precio que los clientes nunca alcanzarán a alcanzar. Pero Whelan sigue convencido de que está haciendo

lo correcto. "Puede que no sea capaz de comprar un centro de datos lleno de hardware de minería de bits, pero puedo generar suficiente BTC para convertirme en parte de la revolución", dice.

El hash en la nube es posible gracias a la otra gran tendencia de agregación junto con la minería de pool: gigantescas granjas de datos, donde cientos o incluso miles de plataformas se apilan en depósitos diseñados para maximizar la potencia de hash y la eficiencia energética. Estas operaciones a menudo se ubican en climas fríos para mitigar los costos del aire acondicionado y aprovechar la energía relativamente barata. Las ubicaciones populares incluyen Islandia con energía geotérmica, las áreas alimentadas por las plantas hidroeléctricas del estado de Washington, Utah rico en carbón y Suecia, cuyos extensos proyectos hidroeléctricos, nucleares y eólicos mantienen las tasas y las emisiones de carbono bajas. No todos los centros de datos están configurados para el hash de la nube. Algunos operan plataformas para sus propias cuentas. Otros invitan a personas externas a ubicar sus plataformas en sus propiedades, cobrando por el espacio y la electricidad. Pero todos son parte de un fenómeno que en cinco años convirtió a la minería bitcoin en un negocio industrializado de gran escala.

Pilas de plataformas de minería
(Cortesía de CoinTerra)

En un centro de datos en las afueras de Salt Lake City, los visitantes primero deben pasar por una cabina cilíndrica no tripulada que se abre con una insignia electrónica y está equipada con sensores y una balanza para medir el peso, forma y tamaño de una persona, para evitar que robando el servidor impar. Al ingresar, cruzan aleatoriamente un centro de monitoreo donde el personal de seguridad entrena una pantalla de pantallas, algunas muestran videos en vivo de cámaras apuntadas a puntos vulnerables del complejo, otras exhiben simulaciones por computadora del flujo de aire y electricidad del centro. Una segunda puerta en el pasillo conduce a la instalación principal.

Dentro del edificio cavernoso, ventiladores de veinte pies de diámetro instalados en techos de treinta pies circulan lentamente el aire ambiente aspirado desde el exterior. Debajo de ellos, el objetivo de esa solución de refrigeración de alta eficiencia y baja energía se puede encontrar en los bastidores llenos de servidores y otros equipos de back-office propiedad de firmas financieras y sitios de comercio electrónico que venden de todo, desde libros hasta flores en línea. Lejos en un área separada, se ha configurado un bolígrafo cerrado para acomodar los planes de expansión

de un nuevo cliente: CoinTerra, un fabricante de plataformas de minería de bitcoin que en 2014 decidió incursionar en la minería. Mientras que los servidores de los clientes tradicionales del centro de datos discrepan, sus luces parpadean en rojo, verde y amarillo mientras administran con diligencia las bases de datos y actualizan las cuentas de los clientes, las máquinas de CoinTerra crean un enorme alboroto. Cincuenta columnas se alinean lado a lado en las que se apilan diez plataformas TerraMiner ASIC, que a 1.6 terahashes por segundo son 320 veces más rápidas que Whelan's Jalapeño. Con tres ventiladores incorporados y de alta potencia que funcionan a la velocidad máxima para enfriar la plataforma mientras su chip interno avanza a través de los cálculos, cada unidad consume dos kilovatios por hora, suficiente para ejecutar una computadora normal durante un mes. Eso genera 20 kWh por torre, cerca de diez veces la electricidad que utilizan los servidores vecinos de las empresas de comercio electrónico más ortodoxas para el mismo espacio.

"Aquí solo tenemos ochocientos terahashes de poder minero", dice Ravi Iyengar, CEO de CoinTerra, gritando para que se escuche sobre el estruendo mientras su cabeza ligeramente pelada de pelo negro sopla en el viento que se precipita hacia los ventiladores que zumban de las plataformas mineras. En una grabación digital de nuestra conversación, suena como si estuviera parado en un huracán. "En dos semanas, tendremos un total de veinticuatro cientos de máquinas en esta instalación por un poco menos de cuatro petahashes en total. Y en toda América del Norte, el objetivo es llegar a diez petahashes ".

Diez petahashes por segundo, o 10,000 billones de hashes por segundo, representaban alrededor de una décima parte de la capacidad total de la red de bitcoin cuando nos conocimos en junio de 2014. Lo que CoinTerra planeó hacer con toda esa potencia informática era diversificar su exposición. Iyengar explicó que la demanda de su equipo autónomo caería cuando el precio del bitcoin cayera, por lo que necesitaba una estrategia de cobertura. Eso se redujo a la instalación de sus propios equipos para hacerse cargo de la minería de bitcoin por su propia cuenta. Con algo del poder de hashing instalado, CoinTerra explotaría bajo su nombre; el resto se alquilaría a través de contraseñas en la nube a clientes que iban desde pequeños aficionados individuales a un cliente no identificado que había acordado alquilar un contrato petahash completo por un año a $ 1 millón.

Iyengar, un ex ingeniero de las plantas de microchips de Samsung Corp. en Austin, dijo que no solo está apostando a que el bitcoin continuará expandiéndose como un sistema de pago, sino que la cadena blockchain crecerá para soportar una gran cantidad de intercambios de valor agregado (el Bitcoin 2.0 conceptos para ser discutidos en el capítulo 9). "Por esa razón tiene que haber una red minera en constante crecimiento", dijo, explicando cómo va a ganar dinero cobrando a los clientes de la minería en la nube a un costo, pero luego aumentando el margen de ganancia en esos contratos mediante la banca en hashing cada vez mayor eficiencia de este negocio.

Una consideración clave para las operaciones mineras de Iyengar es la electricidad. Salt Lake City es más caro por kilowatt hora que el estado de Washington (donde también tiene plataformas), cuyas instalaciones de energía hidroeléctrica ofrecen la energía más barata del mundo. Pero Salt Lake City tiene sus propias ventajas: un aeropuerto internacional y una comunidad técnica e infraestructura establecida, lo que lo hace relativamente accesible desde las grandes ciudades como Los Ángeles y San Francisco y es más fácil atraer mano de obra para instalar nuevas plataformas para aumentar el rendimiento -Algo de la guerra hash lo obligará a hacer en poco tiempo. Debido a que el sitio se encuentra en un desierto, rodeado de montañas abrasadoras y cubiertas de nieve, y está posicionado a 400 metros sobre el nivel del mar, el aire es seco, libre de humedad corrosiva, relativamente frío y con poca electricidad estática. Utah también tiene un poder abundante y confiable a partir de una mezcla de carbón, plantas nucleares y solares bajas en carbono. En el negocio de márgenes ajustados a gran escala en el que se ha convertido la

minería de bitcoin, este tipo de consideraciones pueden marcar la diferencia entre una ganancia y una pérdida. La industria ha recorrido un largo camino desde el dormitorio de Jason Whelan.

La carrera de armamentos mineros que condujo a CoinTerra a Salt Lake City pone a la ley de Moore, que preveía que la capacidad informática de un microprocesador se duplicaría cada dieciocho meses, para vergüenza. En los doce meses hasta junio de 2013, el poder de hash de la red bitcoin se multiplicó por ocho. En los siguientes doce meses, creció otras 845 veces. En ese momento, la red, que producía 88,000 billones de hashes por segundo, tenía una potencia de cómputo seis mil veces mayor que la potencia combinada de las 500 supercomputadoras más importantes del mundo. Y solo dos meses y medio después, casi se había triplicado a 252,000 billones de hashes. El mundo no ha visto nada como este nivel de expansión computacional. Es por eso que algunos agoreros predicen que si Bitcoin continúa en su camino actual, el planeta enfrenta una catástrofe ambiental.

No hay forma de calcular la energía total utilizada por la red minera bitcoin, pero eso no ha impedido que algunos lo intenten. En abril de 2013, varios informes de prensa relataron que el bitcoin consumía 131,000 megavatios hora por día, a un costo diario de $ 19.7 millones. Meses después, Guy Lane, un científico medioambiental australiano, ideó su método BitCarbon para calcular la huella de carbono de bitcoin. Basándose en su suposición de que un minero bitcoin gastará en promedio 90 por ciento del valor del bitcoin minado en electricidad, Lane calculó que un precio de bitcoin de $ 1,000 resultaría en 8.2 millones de toneladas de carbono por año, aproximadamente el tamaño de las emisiones de Chipre, y que un precio de bitcoin de $ 100,000 produciría 825 megatones anuales, o el equivalente de las emisiones de Alemania. Si el tipo de cambio de bitcoin llegara a $ 1 millón, un número que algunos sostienen que es factible si Bitcoin se convierte en un sistema de pago mundialmente dominante, su red tendría una huella de carbono de 8.2 gigatoneladas, o 20 por ciento de la producción de carbono del planeta.

Bitcoin's Hashrate Mining en el tiempo
(Fuente: Blockchain.info)

El problema con estas proyecciones alarmantes es que se basaron en datos defectuosos de Blockchain.info, que aún utilizaba supuestos obsoletos basados en la GPU sobre el uso de electricidad. A principios del verano de 2014, los nuevos mineros de ASIC funcionaban con tan solo un vatio por gigahash, una velocidad que es 650 veces más eficiente que la de las GPU. Si cada minero utilizara estas plataformas, la red consumiría electricidad equivalente a la de siete mil hogares estadounidenses promedio, una cantidad manejable en todo el mundo. Por supuesto, las personas usan una amplia gama de configuraciones de minería eficientes e ineficientes. Sin embargo, sigue siendo rentable hacerlo. Entonces, a pesar de que el consumo total es

significativamente más alto que el estimado de siete mil viviendas, estamos muy lejos de que Bitcoin agregue al mundo el consumo de energía de todo un país.

También se están generando ideas innovadoras para compensar este costo. Una es explotar la producción principal de la minería, el calor, tal vez usarlo para calentar casas en el invierno y satisfacer otras necesidades energéticas. Sin embargo, la naturaleza ad hoc y dispersa de la red no se presta a una buena asignación de dicho recurso. Idealmente, la red minera pasaría por un ciclo estacional, con el hemisferio sur asumiendo la mayor parte de la minería en los meses de junio a septiembre, mientras que el norte se elevaría durante el invierno. Eso no sucederá bajo el modelo actual de laissez-faire, ganador-se lleva todo. Así que, en cambio, cuando nos acercamos al verano boreal del 2014 con la red minera funcionando a 845 veces más potencia informática que doce meses antes y por lo tanto estábamos mal preparados para el cambio de estación, los consultores del centro de datos aconsejaban a los mineros bitcoin que impermeabilizaran sus plataformas y guárdelos en un líquido de enfriamiento especial.

¿Vale la pena todo el gasto y el uso de los recursos? Adam Smith opinó sobre un asunto similar en el siglo XVIII, argumentando que gastar esfuerzos y recursos reales en extraer oro para las monedas era un desperdicio cuando una moneda no es más que un símbolo. Pero aunque el economista ganador del Premio Nobel y columnista del New York Times Paul Krugman ha utilizado los comentarios de Smith para burlarse de Bitcoin, la analogía pasa por alto una serie de factores cruciales. Por un lado, el consumo de energía debe medirse contra el valor de validar las transacciones en un sistema de pago, un servicio social que la minería de oro nunca ha proporcionado. En segundo lugar, los costos deben sopesarse frente a los altos costos de energía del sistema de pago tradicional alternativo, con sus sucursales bancarias, automóviles blindados y sistemas de seguridad. Y, por último, está el incentivo primordial para la eficiencia que el motivo de ganancia ofrece a los innovadores, y es por eso que hemos visto reducciones tan grandes en el consumo de energía para las nuevas máquinas de minería. Si los costos de energía hacen que la minería no sea rentable, se detendrá.

El día del juicio final ambiental de Bitcoin no está, por lo tanto, a la vuelta de la esquina. Aun así, sería irresponsable ignorar el uso de energía como una preocupación. Como señala BitCarbon's Lane, la eficiencia energética mejorada de las plataformas mineras simplemente aumenta la rentabilidad, lo que, combinado con un precio en alza, atrae a más mineros a la carrera de bitcoins y aumenta el consumo total de energía. Es uno de los muchos defectos que dejan a Bitcoin vulnerable a las amenazas futuras y que está impulsando a los inventores a imaginar maneras de mejorar el bitcoin o crear una criptomoneda mejor.

Una de esas vulnerabilidades se hizo evidente a las 22:27 GMT del 11 de marzo de 2013. Justo antes de ese momento, mientras la extensa red global de mineros estaba afanosamente confirmando transacciones y buscando bitcoins, un minero alerta notó algo extraño. Había visto un cliente de software de minería que estaba trabajando en un bloque con un número más alto que el registrado actualmente en blockexplorer.com, una versión escueta de Blockchain.info que se suponía que ofrecía información en tiempo real en el ledger de transacciones blockchain. . Esto generó dudas sobre qué bloque constituía la última extensión confirmada de la cadena. ¿Estaba su máquina haciendo las suposiciones correctas sobre a qué bloque adjuntar el siguiente?

El software Bitcoin se actualiza periódicamente por un pequeño equipo de desarrolladores de software que, por convención y con algunos fondos de la Fundación Bitcoin sin fines de lucro, se encargan de ejecutar el programa de mantenimiento de fuente abierta. El minero pensó que la discrepancia podría ser el resultado de sus esfuerzos por reconciliar su versión 0.7 del software core bitcoin con la versión 0.8 más reciente que esos desarrolladores habían lanzado recientemente y que otros mineros ya habían adoptado. Entonces, buscó respuestas en la sala de

IRC para desarrolladores de bitcoin en el Foro de Bitcoin. Apareciendo en la corriente de comentarios bajo su conexión como thermoman, un nombre compartido por un personaje británico de sitcom, un superhéroe del planeta Ultron, dirigió un mensaje a Pieter Wuille (inicio de sesión: sipa), uno de los cinco desarrolladores principales trabajando bajo el científico jefe de la Fundación Bitcoin, Gavin Andresen, quien asumió la responsabilidad de mantener el software central de bitcoin. Thermoman informó sipa de la discrepancia de conteo de bloques. Se produjo una discusión que arrastró a toda la confianza del cerebro detrás del programa de software de código abierto de bitcoin.

Jouke Hofman (inicio de sesión: jouke) en los Países Bajos intervino que él también estaba encontrando discrepancias en los conteos de bloqueos. Entonces Sipa sugirió soluciones, pero ninguna funcionó. Mientras tanto, los participantes de la sala de chat seguían revisando periódicamente los conteos de bloque en diferentes ubicaciones. Las discrepancias continuaron. Eventualmente, a las 23:06 GMT, el inventor del software de minería Luke Dashjr (inicio de sesión: luke-jr) reconoció lo que estaba pasando:

23:06 Luke-jr: entonces? yay hardfork accidental? :X
23:06 Jouke: Santa mierda.

Se supone que hay una sola cadena de bloques, con la idea de que los enlaces basados en hash organizados secuencialmente del libro de contabilidad crean un registro monolítico ininterrumpido de todas las transacciones confirmadas. Los bifurcadores de corta vida surgirán de vez en cuando en el blockchain, a veces cuando se crea un bloque huérfano que se considera incompleto o cuyas transacciones no están confirmadas. Eso sucede porque otros mineros han intentado verificar el bloqueo y no confían en adherirse a él. Pero el genio de la creación de consenso en el sistema bitcoin significa que no se debe permitir que esas bifurcaciones continúen por mucho tiempo. Eso es porque la comunidad minera trabaja asumiendo que la cadena más larga es la que constituye el consenso. La mayoría de los mineros, al trabajar juntos en una línea particular de la cadena, le confieren legitimidad, colectivamente tienen más poder de hashing total que cualquier grupo minoritario que erróneamente (o incluso fraudulentamente) siga una línea separada de la cadena sin el apoyo del consenso. Esa mayor cantidad de poder de hashing compartido significará que este grupo mayoritario ganará más premios de bloque y, por lo tanto, construirá una cadena más larga (con números de bloque mayores) a lo largo del tiempo. Esto será notado inmediatamente por las computadoras que estaban siguiendo la cadena más corta con números más bajos y esos mineros díscolos saltarán a la cadena más larga. Se considera que la opinión mayoritaria es la legítima, lo que, como veremos, sería un problema solo si un solo minero ha obtenido más del 50 por ciento del poder total de hash.

Sin embargo, este proceso de resolución normal no se estaba desarrollando aquí. La bifurcación continuaba, bloque tras bloque. Eso significaba que ya no existía un registro común de transacciones verificadas. Es como si la mitad de las familias en nuestra aldea imaginaria de Yapese estuvieran trabajando en un conjunto diferente de suposiciones sobre los balances fei de la comunidad. Este es precisamente el tipo de cosas que un actor fraudulento podría explotar para gastar doblemente bitcoins. Por ejemplo, si el administrador de un grupo minero que anteriormente representaba, digamos, 30 por ciento de la cadena de bloques combinada ahora tenía el control mayoritario de una de las nuevas mitades, podría hacer que su software de billetera reenviara bitcoins ya gastados de uno de sus direcciones a otro de los suyos. La apuesta sería que otros mineros reconocerían la segunda transacción como legítima y así reconocer un saldo para el administrador que debería haber sido reducido debido a la inversión anterior. Normalmente, la mayoría de los otros mineros los atraparían y comenzarían a trabajar en una cadena legítima más larga, pero bajo esta bifurcación perpetua, el grupo minero tendría efectivamente más del 50 por ciento del poder de hash con el que seguir confirmando esas

transacciones fraudulentas. Si se permite continuar, eventualmente destruirá la integridad de todo el sistema de bitcoin.

Wuille se dio cuenta desde el principio que esta particular bifurcación no fue causada por un pirata informático codicioso -una violación del bitcoin en sí mismo, que se cree imposible- sino por un error que ocurrió cuando sus colegas del equipo de desarrollo central presentaron la nueva versión 0.8. Se suponía que su base de datos reconstituida se conciliaba con los registros de la base de datos de la versión 0.7, pero no lo hacía. El desarrollador principal Andresen pronto intensificó. Después de consultar con Wuille y otros dos desarrolladores principales, Jeff Garzik y Gregory Maxwell, y después de registrarse con Mark Karpelès propietario de Mt Gox (iniciar sesión: MagicalTux), cuyo intercambio de divisas era entonces la institución financiera más importante de la red bitcoin, Andresen decidió abandone el nuevo software y vuelva a la versión 0.7.

Se descubrió un caso de gasto de $ 10,000, lo que sugiere que un pícaro oportunista podría haberse aprovechado de la trampa. Pero algunos mineros tuvieron que renunciar a los bitcoins que pensaban que habían ganado en la horquilla 0.8, un total de seiscientas monedas por valor de $ 26,000. Y este kerfuffle hizo que el precio del bitcoin cayera un 24 por ciento. El problema atemorizante obtuvo algo de juego en los medios de prensa enfocados en bitcoin, pero no atrajo mucha atención en otros lugares, en parte porque pronto se solucionó y el precio se recuperó con bastante rapidez.

* * *

La bifurcación de marzo de 2013 había sido un accidente, pero trajo nueva atención a una preocupación sostenida por algunos en la comunidad bitcoin, que las operaciones mineras industrializadas algún día podrían permitirle a un actor nefasto el poder de crear un tenedor intencionalmente al tomar el control mayoritario del total poder de hash Eso se conoce como un ataque del 51 por ciento. El documento original de Nakamoto afirmaba que se podía garantizar que la red de minería bitcoin trataría las transacciones de todos de manera justa y honesta, siempre y cuando ningún minero o grupo minero poseyera más del 50 por ciento de la potencia de hash. Si los actores malévolos crearan en secreto una cadena alternativa de transacciones fraudulentas para gastar bitcoins que no poseían, sus esfuerzos para que se confirmaran esas transacciones fracasarían si no tuvieran el poder de la mayoría de los hash. La probabilidad de que los mineros deshonestos ganen suficientes acertijos matemáticos para seguir produciendo la cadena más larga y así otorgar legitimidad a sus transacciones fraudulentas tenderá rápidamente hacia cero. A medida que progresaba cada bloque, la cadena legítima sería cada vez más larga. Nunca alcanzarían la extensión de noventa y nueve cuadras que, como explicamos en el capítulo anterior, es necesaria para legitimar su trabajo en bloque. Nunca podrían gastar los bitcoins que pensaban que se habían ganado. Los malos nunca pueden ponerse al día. Esa es la teoría, al menos.

Pero, ¿qué pasaría si un poderoso conglomerado tomara el control de todo ese poder minero? Luego podrían llenar un bloque con transacciones fraudulentas y luego (igualmente fraudulentamente) confirmarlas. Y dado que estarían ganando más de un segundo bloque, podrían seguir construyendo una cadena de bloques viable y larga que otros mineros asumirían como la más veraz, todo en virtud de su longitud.

De acuerdo con coinometrics.com, en el verano de 2014 el costo del equipo de minería y la electricidad requerida para un ataque del 51 por ciento ascendió a $ 913 millones. Es una propuesta costosa, pero con una posible solución: agrupar. De hecho, los grupos de minería ya se acercaron al umbral del 50 por ciento: en junio de 2014, el grupo GHash.IO vio su participación en el poder total de hash fluctuar entre 40 por ciento y 50 por ciento a lo largo del mes. Debido a que estas agrupaciones usan software que combina su poder de dispersión en una única fuerza formidable, también pueden confirmar las transacciones como un grupo. Eso pone el poder

concentrado en manos de los administradores del software del grupo, lo que comprensiblemente causa cierta ansiedad entre los bitcoiners. Los líderes de Bitcoin, como Andresen, están tratando de alentar a las personas a unirse a nuevos grupos de minería de igual a igual que quitan el poder de la confirmación de transacción al administrador de la agrupación y lo dejan en manos de mineros individuales a través de una red descentralizada. Pero los grupos más grandes tienen una presencia establecida y de primer impulso que es difícil de romper. Además, el gerente de GHash.IO, CEX.IO, ofrece la zanahoria atractiva de tarifas cero en un intento por dirigir el negocio a sus dos negocios secundarios: un intercambio de criptomonedas y un servicio de minería de nubes.

Para empeorar las cosas, los informáticos de la Universidad de Cornell Ittay Eyal y Emin Gün Sirer han demostrado que el umbral para un ataque en realidad puede ser inferior al 51 por ciento. En un documento polémico, mostraron cómo una minoría suficientemente grande de mineros en colusión podía participar con éxito en una "minería egoísta", desarrollando una cadena de bloques alternativa secreta que está oculta a la mayoría pero que se mueve más rápido que el tenedor honesto de los mineros. De esta forma obligarían a todos los demás a desperdiciar los recursos de la computadora en lo que erróneamente se cree que es la cadena y el juego correctos para ellos una mayor proporción de distribuciones de bitcoin que lo que su poder minero garantiza. El periódico molestó a muchos en la comunidad bitcoin: "los fanáticos que no quieren escuchar nada negativo", como dice Sirer. El ruido se calmó, sin embargo, después de que un fan de bitcoin, ansioso por probar la falibilidad de la teoría, lo sometió a una simulación y descubrió que Eyal y Sirer tenían razón. "La gente se calmó, y los que tienen interés, como nosotros, en ver el éxito de bitcoin, finalmente lo vieron como una contribución increíblemente positiva. Ahora la gente entiende que con un sistema descentralizado, necesitas tener algún tipo de buen punto de equilibrio integrado ", dice Sirer. "El protocolo no puede tener este tipo de vulnerabilidades".

Por lo tanto, la comunidad de desarrollo de código abierto ahora está buscando protecciones adicionales contra la minería egoísta y el 51 por ciento de los ataques. Para ser justos, nada malévolo como este ha sucedido hasta ahora o es probable que ocurra pronto, por una buena razón. Como Nakamoto explicó en su libro blanco: "Si un atacante codicioso puede reunir más poder de CPU que todos los nodos honestos, tendría que elegir entre usarlo para defraudar a las personas robando sus pagos o usándolo para generar nuevas monedas. . Debería considerar más provechoso seguir las reglas, reglas que lo favorecen con más monedas nuevas que todos los demás combinados, que socavar el sistema y la validez de su propia riqueza ".

El interés propio, en otras palabras, debería evitar que cualquier persona con un interés en bitcoin lo destruya. De hecho, la corta historia de bitcoin muestra que la misma motivación se extiende a las personas de minorías que desean mantener un equilibrio de poder en la red. Las agrupaciones mineras que se han cerrado con un 50 por ciento de poder de hashing han hecho que los miembros abandonen el barco y se unan a grupos competidores para mantener el sistema honesto. Y para apaciguar las preocupaciones sobre su tamaño excesivo, CEX.IO a veces ha dicho que declinaría aceptar nuevos participantes en el grupo GHash.IO.

Pero, ¿y si los malos actores no tienen interés en que Bitcoin tenga éxito? ¿Qué pasa si toda su motivación es derribar el sistema, no sacar provecho de las inversiones en bitcoins? Los bitcoiners a veces se refieren a esto como un ataque del Dr. Evil y arrojan amenazas hipotéticas: una organización terrorista que quiere arrojar al mundo occidental al caos, a una nación soberana-Rusia, quizás, o China-cuyo sistema monetario está amenazado por bitcoin, o un consorcio de bancos multinacionales que buscan proteger su monopolio en el sistema de pago. A primera vista parece poco probable. Después de todo, estos prospectos se vuelven relevantes solo si bitcoin alcanza suficiente penetración como para que su destrucción importara, y para ese momento los atacantes necesitarían desprenderse de más de $ 1 mil millones, con cada pedido gigante de chips

ASIC y equipos de minería llamando su atención sobre ellos. No obstante, la vulnerabilidad existe. Básicamente, bitcoin no es hermético, y ese es el tipo de cosas que pueden molestar a un abogado interno hipercausto para una compañía que se pregunta si negociar en él.

Estos escenarios extremos no son los únicos que despiertan preocupación porque las concentraciones de poder y riqueza pueden tener una influencia indebida sobre Bitcoin. A finales de agosto de 2014, el 44 por ciento de todas las bitcoins en circulación se asignaron a solo 1,528 direcciones, cada una con saldos de más de mil bitcoins ($ 507,000 en ese momento), según bitcoinrichlist.com. Eso es menos del 0.01 por ciento del total de 40.7 millones de direcciones en la red en ese momento, lo que sugiere una alta y potencialmente distorsionante concentración de riqueza.

Primero, algo de perspectiva. Como una medida de brecha de riqueza, esta es una mala. Por un lado, las direcciones no son billeteras. No se puede conocer el número total de billeteras, pero son, por definición, considerablemente menos que el recuento de direcciones, aunque muchas personas tienen más de una. Los titulares de billeteras son direcciones asignadas aleatoriamente para diferentes transacciones y generalmente generarán varias direcciones. Muchos de los 39 millones que ocupan el 96% inferior del montón de bitcoinrichlist.com, aquellos con saldos de menos de 0.001 bitcoin, son solo cuentas de "pequeños cambios" que el protocolo bitcoin asigna a los gastadores en cada transacción como parte de su único tres- forma de conciliación de saldos. Incluso si muchos de estos saldos pequeños se acumulan en billeteras con saldos agregados minúsculos, es muy poco probable que sean la única reserva de riqueza de sus propietarios. La mayoría de los usuarios de bitcoins tienen una existencia financiera mucho más rica en el mundo de las monedas fiduciarias. Este grupo de 96 percentros nunca puede ser visto como una subclase de mendigos.

Sin embargo, estas cifras revelan cuánto espectacular rally de precios de bitcoin ha creado una pequeña cohorte internacional de ricos "barones bitcoin", casi de la noche a la mañana. Estas élites tienen un gran impacto en la economía de Bitcoin. Tienen un gran interés en ver que la moneda tenga éxito y están dispuestos y pueden hacer pagos que otros no, simplemente para alentar la adopción. De ahí los informes de compras ostentosas basadas en bitcoin de villas en Bali, Lamborghinis en California y entradas de Virgin Galactica en el espacio exterior. Sus intenciones pueden ser buenas, pero si el dinero no tiene sentido en sus gastos, ¿cómo pueden aplicar la disciplina competitiva necesaria para reducir los precios del resto de la economía de Bitcoin?

La amplia brecha de riqueza se asienta mal con la imagen de las criptomonedas como dinero impulsado por la comunidad y un escape del dominio de los gatos gordos de Wall Street. La riqueza y el poder estrechamente controlados no atraen la confianza generalizada. Por supuesto, las economías del dólar, el euro y el yen ya afirman concentraciones profundas de ambos, y la desigualdad alcanzó los niveles de 1920. Pero esas monedas fiduciarias no necesitan ganarse a la gente. Para las criptomonedas, este tipo de desequilibrios pueden necesitar ser abordados si su futuro está asegurado.

En el lado positivo, muchos desarrolladores y empresarios están persiguiendo proyectos que tratan de abordar tales preocupaciones. Algunos están tomando la infraestructura existente y buscando formas de presentarla a un grupo más amplio, promoviendo a bitcoin como un vehículo para empoderar a los marginados del mundo. Las soluciones que ayudan a los "no bancarizados" del mundo en desarrollo a obtener acceso a la economía global son un área prometedora, que discutiremos en el capítulo 8. Pero igual de importante es el reconocimiento de muchos entusiastas de las criptomonedas inteligentes de que Bitcoin, tal como está, está lejos de perfecto y se puede mejorar de muchas maneras para evitar algunos de los desafíos y amenazas discutidos anteriormente.

La amenaza de ataque del 51 por ciento se come en muchos intelectuales bitcoin. ¿Por qué? Porque es la única debilidad estructural irrefutable en el sistema bitcoin. Todos los otros peligros de los que oye hablar: carteras pirateadas, delitos y volatilidad de los precios, no son problemas con el bitcoin en sí, sino con el ecosistema que se ha desarrollado a su alrededor. Muchos ya se están solucionando: las billeteras "multi-sig" de innovadores como BitGo brindan una protección casi impenetrable contra los piratas informáticos; los intercambios regulados de alta tecnología como el de Atlas ATS no podrían cometer los errores de Mt Gox; una supervisión gubernamental más estrecha atemorizará a los traficantes de drogas, hasta cierto punto. Pero es difícil ver una forma de protegerse contra un ataque del 51 por ciento. Incluso si los desincentivos y el costo de lanzar tal ataque lo hacen altamente improbable, algunos que han estudiado el diseño de Bitcoin están molestos porque la brillante y elegante solución de Nakamoto para alinear los intereses e incentivos de los individuos con los de la comunidad tiene esta debilidad fundamental.

El desarrollador principal de bitcoin, Jeff Garzik, uno de los cinco que trabaja con Gavin Andresen, ha presentado una solución parcial que aprovecha los continuos avances en empresas de espacio privado de bajo costo: busca recaudar $ 2 millones para lanzar una red flota de satélites pequeños y de bajo costo en el espacio en un proyecto destinado a reducir la concentración de la red minera. Estos "bitsats" de diez centímetros cúbicos proporcionarían conectividad de Internet con transmisión satelital a bajo costo a los nodos en el terreno y almacenarían un registro permanente de la base de datos completa de la cadena de bloques en sus discos duros internos. Los beneficios serían, en teoría, dos. En primer lugar, haría que la minería fuera más accesible para una gama más amplia de participantes al reducir el costo de convertirse en un "nodo completo", un rol vital en la red que requiere el almacenamiento de grandes cantidades de datos y que en estos días suele ser realizado por altos Plataformas ASIC de alto poder adquisitivo. En segundo lugar, como los satélites estarían fuera del control de cualquier persona, estado o empresa, podrían proporcionar una copia de seguridad crítica en caso de que un gran proveedor de servicios de Internet o un grupo de PSI detenga su funcionamiento. Tal evento, tal vez ordenado por un gobierno o una alianza de gobiernos, podría cortar a muchos mineros de la red y elevar así el riesgo de que un gran grupo que se encuentre fuera del área geográfica afectada pueda obtener más del 50 por ciento de control. Una fuente alternativa de ancho de banda basado en el espacio podría reducir el riesgo de un desarrollo tan desagradable.

Sin embargo, una alternativa mucho menos intensiva en capital a la concentración del control de red sería cambiar las reglas que siguen los mineros para ganar bitcoins y así eliminar el motivo para acumular enormes cantidades de poder de hash. Los ingenieros informáticos de criptomonedas que ahora están pensando en tales soluciones podrían desempeñar un papel central en la configuración del futuro de la tecnología. Sus ideas algún día incluso podrían darle una oportunidad a bitcoin por su dinero al ser el principal impulsor de ese futuro.

Gran parte de este replanteamiento está sucediendo a través del desarrollo de altcoins. Como mencionamos en el capítulo 3, ahora existen cientos de estos imitadores de bitcoins. Muchos no van a ninguna parte, descartados como esquemas de hacerse rico rápidamente o bromas. Pero algunos han ideado formas sofisticadas de cambiar las reglas del juego para la distribución de criptomonedas dentro de sus comunidades de usuarios. Sus fundadores están promocionando sus monedas como modelos más justos y más sostenibles. Afirman que toman los buenos aspectos de la estructura descentralizada de bitcoin, pero que se deshacen de sus elementos negativos, como la carrera armamentista con hashing-power, el uso excesivo de electricidad y la concentración de la potencia minera industrializada. Bitcoin tiene una gran ventaja como primer jugador sobre estos nuevos jugadores, por lo que muchos desarrolladores piensan que la mejor solución es solucionar sus fallas en lugar de crear sistemas completamente nuevos. Sin embargo, las mejores

altcoins están trayendo una fuerza de competencia trepidante y potencialmente constructiva para soportar en toda la arena de la criptomoneda.

De estas altcoins, litecoin, inventado por Charlie Lee, es hasta la fecha el más exitoso. La salsa secreta de Litecoin es su uso de un algoritmo diferente en el proceso de hash que los mineros usan para empaquetar transacciones en la cadena de bloques. El sistema de Lee todavía implica una competencia entre los mineros, pero su algoritmo de hash, conocido como scrypt, hace que sea más fácil para un minero llegar al codiciado objetivo de bloqueo de bloques que el SHA-256 de bitcoin. Sin ahondar en los complicados detalles de cómo funciona, Scrypt esencialmente modifica los objetivos para que los mineros no simplemente obtengan una ventaja al construir constantemente la potencia computacional bruta. El resultado es que el poder de la minería se mantiene algo más uniformemente extendido y más democrático con litecoin. Los mineros aún tienen un incentivo para perseguir las recompensas monetarias, pero la carrera armamentista y el uso de la electricidad no son tan intensos. También permite tiempos de respuesta más rápidos, con bloques completados en dos minutos y medio, en lugar de los diez minutos de bitcoin, lo que a su vez significa que la espera del sistema para la confirmación final de las transacciones por parte de clientes y comerciantes no es tan larga. La principal debilidad de Litecoin es el corolario de su fortaleza: debido a que es más barato extraer litecoins y porque las plataformas basadas en scrypt se pueden usar para extraer otras altcoins basadas en scrypt como dogecoin, los mineros invierten menos en el funcionamiento permanente de su blockchain. En teoría, eso podría aumentar el riesgo de un ataque del 51 por ciento si suficientes de ellos no están en línea en un momento dado. Algunos también se preocupan porque la minería basada en scrypt es más insegura, con una prueba de trabajo menos rigurosa, en teoría, permite que las transacciones falsas se lleven a cabo con confirmaciones incorrectas. Hasta ahora, sin embargo, litecoin ha evitado grandes averías. Con el tiempo, podría llegar a ser un competidor más democrático y más respetuoso del medio ambiente con Bitcoin.

Scrypt mining no es la única solución para la minería concentrada de bitcoin y el 51% de amenaza de ataque. Algunas altcoins, como nextcoin y peercoin, usan "prueba de apuesta" como alternativa a la computación derrochadora y costosa del paradigma de "prueba de trabajo". De esta forma, los derechos de recompensa de su computadora para confirmar transacciones aumentan cuanto más se invierta en el suministro monetario de la moneda. En el caso de nextcoin, que está basado en el 100 por ciento de las apuestas, las monedas no se extraen sino que se "falsifican". Un suministro preexistente y fijo de monedas circula en la economía de nextcoin, y cada vez que se usan en una transacción , genera una tarifa que debe pagarse al nodo ganador que sella cada bloque. Al igual que con bitcoin, el truco correcto para cerrar un bloque de transacciones se encuentra a través de una lotería aleatoria, pero a diferencia del bitcoin, tus posibilidades de ganar esa lotería no dependen de tu potencia de hashing sino de cuántas monedas probadas tienes. La idea es que esto elimina el incentivo para construir una potencia de cómputo destructiva y ambientalmente destructiva.

La existencia de estas alternativas subraya la conciencia de los defectos de bitcoin. La invención de Nakamoto enfrenta otros desafíos también. Por un lado, la red bitcoin actualmente solo puede procesar alrededor de siete transacciones por segundo, lastimosamente por debajo de los diez mil de Visa. Si se va a ampliar el bitcoin, se debe actualizar para que los nodos, actualmente limitados a un megabyte de datos por bloque de diez minutos, puedan procesar un conjunto de información mucho más grande. Eso no es técnicamente difícil; pero requeriría que los mineros redujeran bloques de transacciones mucho más grandes sin grandes mejoras en su compensación. Los desarrolladores actualmente están explorando un modelo de tarifa de transacción que proporcionaría una compensación más justa para los mineros si la cantidad de datos se vuelve excesiva.

El enfoque colaborativo y de código abierto de Bitcoin para las criptomonedas es su gran fortaleza. Hasta ahora, los desafíos que han surgido, desde los robos en los principales intercambios, a los tenedores de la cadena de bloques, hasta el descubrimiento de errores en el software subyacente, se han cumplido mediante respuestas basadas en el consenso, diseñadas para ser lo más justas posible. Aún así, los desafíos son complicados. Los diseñadores de proyectos de criptomonedas trabajan en el nexo de la economía (que enfatiza la creación de incentivos para el comportamiento individual que beneficia al grupo) y la tecnología. Los diseñadores de sistemas informáticos de empresas como SAP e IBM se centran en problemas similares en el equilibrio entre el comportamiento y la tecnología, pero lo hacen dentro de los entornos controlados de sus clientes corporativos centralizados. El laboratorio utilizado por los desarrolladores de criptomonedas, por el contrario, es potencialmente tan grande como el mundo en sí, la amplitud de la humanidad que sus proyectos buscan abarcar. Ningún manual de normas de la empresa o un conjunto descendente de instrucciones gerenciales mantiene las elecciones de las personas en línea con un objetivo corporativo común. Guiar a las personas hacia el comportamiento óptimo en las criptomonedas depende totalmente de cómo el software esté diseñado para afectar el pensamiento humano, qué tan eficazmente sus sistemas de incentivos fomentan ese comportamiento deseado.

Las vulnerabilidades y defectos enumerados en este capítulo inevitablemente dificultan que mucha gente común confíe en las criptomonedas, irónicamente, para un programa que se lanza como una forma de eludir la necesidad de confianza. Pero uno también debe sopesar estos contra las debilidades del sistema existente. Considere la cantidad de fraude y crimen llevado a cabo en dólares, por ejemplo. Y si quiere pensar en las vulnerabilidades de un sistema financiero, concéntrese en el mercado global de derivados financieros que los bancos continúan administrando a pesar del desastre provocado en 2008 por estas "armas financieras de destrucción masiva", como las llamó Warren Buffett. Ese mercado tiene un valor nominal o real de $ 710 billones.

Lo vital para recordar es que el poder mental colectivo aplicado a todos los desafíos que enfrentan Bitcoin y otras criptomonedas es enorme. Bajo el modelo de código abierto y descentralizado, estas tecnologías no se ven obstaculizadas por las mismas limitaciones que enfrentan las burocracias y las empresas obsoletas. La cantidad de innovación es tremenda, no solo para hacer que las criptomonedas sean más seguras, sino también para descubrir cómo hacer que sean aún más útiles para la sociedad. En el siguiente capítulo conoceremos a los jóvenes inventores que están impulsando ese esfuerzo.

Capítulo 7

ESCUELA DE SATOSHI

> Los hombres tienen una piedra para tocar el oro, pero el oro es la piedra para tocar al hombre.
>
> -Thomas Fuller

Bitcoin nació de una visión criptoanarquista de una sociedad descentralizada y sin gobierno, una especie de utopía encriptada y encriptada. Obtuvo su crecimiento temprano de un pequeño grupo de personas jóvenes con mentalidad tecnológica que fueron rechazados por los excesos y abusos del sistema financiero. Pero la siguiente etapa, el auge del bitcoin, ha sido impulsado por algo mucho más fácil de entender.

Los criptoanarquistas ya no manejan Bitcoin. Probablemente sucedió en algún momento en 2013, cuando el bitcoin se volvió parabólico, y la gente comenzó a entender que este dinero digital también podría significar dinero real. Una nueva raza tomó el timón. Si quieres entender quiénes son estas personas, tienes que ir a San Francisco, el epicentro de esta fiebre del oro global, moderna y digitalizada. Ubicada en el extremo de América, la ciudad tiene una sensación de fin del mundo y casi parece construida especialmente para atrapar a los exploradores, empresarios, indigentes e itinerantes que deambulan por el océano antes de que se caigan. Toda la región tiene un ambiente irresistible, lleno de éxitos, y mezclado con el mundo de bitcoins de alta tecnología, obtienes este extraño cruce de personas que quieren cambiar el mundo y hacerse fabulosamente ricas. No ven ninguna incoherencia en eso.

Esta ciudad y su gente se atraen magnéticamente entre sí, y este boomlet bitcoin es un descendiente directo de auges previos, comenzando con el famoso descubrimiento de oro en Sutter's Mill en 1848, un descubrimiento que provocó una emigración masiva de estadounidenses hacia el oeste. eso reformó y rehizo la joven nación. Algunos hombres hicieron fortuna, algunos perdieron fortunas. El propio John Sutter perdió una fortuna, ya que los exploradores salvajes invadieron la tierra que poseía. Otros, como Levi Strauss y Leland Stanford, se enriquecieron al proporcionar todos los servicios de soporte e infraestructura que los mineros necesitarían.

Stanford más tarde donaría tierras que poseía para el establecimiento de una universidad, Stanford (que lleva el nombre de su hijo, no él mismo). Décadas más tarde, dos jóvenes estudiantes de esa escuela, Bill Hewlett y Dave Packard, entablarían una amistad, y luego una empresa comercial que se convertiría en una importante corporación global. Por lo tanto, inadvertidamente lanzarían el siguiente gran boom de San Francisco: Silicon Valley. El Valle, como ya hemos explorado, atraería y se convertiría en el hogar de los Cypherpunks de Tim May, un grupo del cual es muy posible que surgiera el propio Nakamoto. Si eso es cierto, significa que puedes trazar una línea directa desde Sutter's Mill hasta, bueno, llamémosle Satoshi's Mill, la última de una serie de olas de prospección para llegar al Valle en su larga historia de auges y caídas.

Otros centros tecnológicos de todo el mundo también están viendo el calor y el bullicio en torno a la innovación de bitcoin, que ha cachet y ha capturado el espíritu del mundo tecnológico. Londres, Toronto, Singapur, Hong Kong, Tel Aviv, Zug en Suiza e incluso Nairobi en Kenia, por nombrar algunos, albergan una gran cantidad de nuevas empresas relacionadas con el bitcoin. Todo refleja la emoción que los desarrolladores de software y los ingenieros informáticos de todo el mundo -

un grupo con un número desmesuradamente grande de pensadores individualistas de mentalidad libertaria- tienen para este vasto nuevo campo que ahora está siendo explorado y minado. Pero el papel central de Silicon Valley en la revolución de la computadora que precedió a todo esto le da dibs para ser el corazón natural de la revolución de la criptomoneda. Así que simplemente tenía sentido ir allí y verlo de primera mano, para descubrir qué hace que estos millonarios de bitcoins actúen.

No representan la corriente principal, estos empresarios itinerantes e itinerantes que terminan allí. Son constructores compulsivos, construyendo constantemente cosas nuevas, derribándolos, reformulándolos, arriesgándose, esperando crear ese negocio multimillonario, yendo a donde la oportunidad parezca mayor. El fracaso es un lugar común. Tienen una indiferencia casi completa al riesgo. Su energía e ideas simplemente los impulsan a lo siguiente, y con esa energía y la miríada de negocios que surgen de ella, están haciendo todo lo posible para hacer de la criptomoneda la siguiente fase definitoria en la implacable reinvención de Silicon Valley.

Antes de dejarnos llevar demasiado, comprendan que esto todavía es temprano. Incluso en esta ciudad, donde las personas manejan en cuadrillas de Segway y los conductores alimentan el medidor a través de aplicaciones móviles, Bitcoin sigue siendo una curiosidad. Entramos en una tienda especializada, La mejor amiga del comprador, que aceptaba bitcoin, un letrero en la ventana lo proclamaba, y no encontré ninguna avalancha de niños prodigios de alta tecnología engullendo magdalenas. Cuando el negocio comenzó a tomar bitcoins en 2013, la chica detrás del mostrador nos dijo que había habido un poco de emoción y un aumento en el tráfico, pero eso desapareció. El negocio de bitcoins en estos días no está moviendo la aguja.

Entonces, Bitcoin se parece más a una escena en un globo de nieve que a una burbuja de estilo punto com en toda regla. Pero, como dijimos, es temprano. Este es solo el comienzo.

Si el Área de la Bahía es la región más importante desde la cual emana la innovación de bitcoins, su zona cero bien podría estar dentro de un edificio anodino en el funky, atestado y pequeño crisol de la Misión del Distrito de la Misión. Las chispas que condujeron a algunos de los desarrollos más emocionantes en bitcoin surgieron por primera vez de conversaciones y sesiones de lluvia de ideas dentro de esta desvencijada "hacker house". Sentada en la esquina de Twentieth y Mission Streets, con su entrada sencilla detrás de un olivo (los primeros misioneros trajo los olivos con ellos desde España y todavía salpican las calles), el edificio ahora conocido como 20Mission fue fundado en febrero de 2012 por Jered Kenna, el joven empresario de bitcoins que había fundado Tradehill anteriormente. Se ha convertido en un espacio de trabajo y de vida para los exploradores silvestres inteligentes, ambiciosos y con mentalidad tecnológica que impulsan el auge del bitcoin. Cuando Kenna arrendó este lugar por primera vez, albergó una zapatería en su planta baja y un hotel de residencia abandonado en el piso de arriba. Restauró las habitaciones del piso de arriba en pequeñas residencias y limpió los desechos de la zapatería. El área de la planta baja ofrecería un espacio común para trabajar, comer y comunicarse. Luego invitó a techies, hackers y bitcoiners a establecer su residencia. Fue casi un éxito instantáneo. A través de las reuniones de Bitcoin, rápidamente se convirtió en un hervidero de ideas y espíritu empresarial.

"Hay una sensación de que eres parte de un movimiento", dijo Taariq Lewis en una reunión dominical en 20Mission, "y parte de algo especial". Lewis es un bitcoiner que ahora dirige las reuniones regulares de la casa hacker. Salió a San Francisco del Spanish Harlem de Nueva York, por Boston, otro empresario compulsivo e inquieto. Obtuvo su MBA en el MIT, pero quería crear cosas, hacer sus propios negocios, así que se dirigió al oeste. Lewis era inicialmente un escéptico de Bitcoin, viéndolo como poco más que una herramienta para el tráfico de drogas. Pero después de dos intentos de arranque fallidos ("Matar a tus bebés rápidamente", bromeó), estaba buscando una nueva oportunidad, y una reunión casual lo forzó a reconsiderar. "Almorcé con un tipo

realmente inteligente que dijo que el bitcoin era una mierda", dijo Lewis, "y eso cambió mi vida". En la actualidad, él opera un sitio web de noticias de bitcoin, Bits of Coin, y una nueva empresa. fundado, DigitalTangible.

La entrada a 20Mission
(Cortesía de Paul Vigna)

Este grupo particular de los domingos por la mañana que Lewis había reunido no parecía tan revolucionario, pero era instructivo. La pequeña reunión, alrededor de una docena de personas, se presentó a una compañía de Bitcoin 2.0 llamada MaidSafe, que había ideado una forma para que la gente alquilara el espacio en disco en sus propios discos duros a una red descentralizada de usuarios. Esta reunión había sido organizada por Paige Peterson, una libertaria / anarquista de veintiséis años, pelo rubio y rastas, que había empezado a trabajar en MaidSafe un mes antes. Ella había hecho arreglos para que el fundador de la compañía, un ingeniero escocés llamado David Irvine, se "uniera" al grupo de San Francisco a través de un video chat. Durante unas horas, respondió todas las preguntas que tenía el grupo. MaidSafe está tratando de construir una red de Internet descentralizada, y esta reunión fue parte del esfuerzo de divulgación. Los grupos de Meetup, que funcionan casi como las reuniones sociales de la iglesia de la religión bitcoin y ahora se celebran en ciudades de todo el mundo, ofrecen una oportunidad para que todos estos jugadores descentralizados y anónimos se reúnan y partan el pan (o quizás deberíamos decir, bits).

Dan Held tenía veinticinco años cuando asistió a su primera reunión de bitcoin en 20Mission en enero de 2013. Una tarde soleada en el viejo bar beatnik Vesuvio, el ex apoyador rubio en el equipo de fútbol de la preparatoria Hebron de Carrollton, Texas, explicó cómo se mudó a San Francisco para tomar un trabajo en un pequeño banco de inversión. Seguía los pasos del amigo de su ciudad, Kevin Johnson, que se había mudado allí cuatro meses antes. En Texas, eran las únicas dos personas que conocían que se preocupaban por Bitcoin. En California, encontraron un grupo de personas que compartieron su pasión. Un año después de asistir a su primera reunión en 20Mission, la vida de Held había cambiado drásticamente.

"Kevin y yo realmente nos inspiramos" en las reuniones, dijo Held. "La energía allí fue tremenda". Esas reuniones tempranas eran pequeñas, dijo, tal vez quince o veinte personas. Pero las personas que asistieron se convertirían en grandes nombres del mundo bitcoin: entre ellos estaban Brian Armstrong y Fred Ehrsam, los fundadores de Coinbase, que es el segundo después de Blockchain como líder en servicios de monedero digital y uno de los mayores procesadores. de los pagos de

bitcoin para empresas. Jed McCaleb, el fundador de Mt Gox, también estaba allí. McCaleb estaba ocupado trabajando en el sistema alternativo de pago Ripple, que sería una especie de competidor de Bitcoin. McCaleb también tenía a parte del equipo de desarrollo de Ripple con él. También en la reunión estaba el propio Kenna, que ya había comenzado y perdido Tradehill y, a pesar de su juventud, es algo así como un bitcoin graybeard.

Held y Johnson estaban decididos a agregar su propia contribución. Durante un viaje de esquí al lago Tahoe, dibujaron en una servilleta-sí, literalmente una servilleta-la idea de que se convertiría en su puesta en marcha, ZeroBlock, esencialmente una aplicación de precios de bitcoin. Lo lanzaron en la primavera de 2013, un producto básico que proporcionaba precios de bitcoin en dólares, un suministro de noticias, notificaciones push para movimientos de precios y una calculadora de conversión de precios. Satisface una necesidad en un mercado en rápido crecimiento de inversores bitcoin ansiosos por obtener información sobre el mercado. La aplicación también salió más o menos al mismo tiempo que los precios de bitcoin aumentaron en respuesta a la crisis fiscal de Chipre, y luego disminuyeron. La aplicación de Held y Johnson recibió mucha atención, y para diciembre de ese año, la habían vendido a Blockchain por una cantidad no revelada de bitcoins, convirtiéndose en el primer acuerdo de fusiones y adquisiciones realizado en una criptomoneda. La adquisición fue esencialmente un "contrato de adquisición" (adquirir talento en el campo de Bitcoin es una tarea continua y desafiante) que atrajo a Held. Él todavía tiene su fortuna denominada en su totalidad en la criptomoneda. En poco más de un año, Held había pasado de ser un banquero a ser un barón de los bitcoins, y en estos días apaga su sed de retoques empresarial y crea nuevos productos para Blockchain. Las reuniones habían cambiado el curso de su vida. Él no sería el único.

"Es un tipo muy específico de cerebro obsesionado con Bitcoin", dice Adam Draper, el capitalista de riesgo de cuarta generación cuyo programa "acelerador" de Boost VC ya ha impulsado una serie de start-ups de bitcoin en el mundo, incluida América Latina. -el procesador de pago focalizado BitPagos y el intercambio de bitcoin de alta tecnología Vaurum. "Todos saben que es territorio sin pavimentar, y se emocionan con eso".

Es Kenna, el fundador de 20Mission, quien mejor ejemplifica la raza. Tenía una ruta tortuosa pero no infrecuente, que iba de la nada a la riqueza y luego a la riqueza. Mucho antes de que apareciera su foto en el artículo de Businessweek titulado "Millonarios de Bitcoin", Kenna no era la idea de nadie que cambiara el mundo, ya que se había graduado por última vez en su escuela secundaria de Oregón. No carecía de inteligencia o ambición, como luego se haría evidente, pero carecía de enfoque. Se dirigió a los Marines, se envió a Afganistán y luego terminó en Chile con un negocio importando tarjetas gráficas.

En Chile, en 2009, Kenna vio por primera vez una referencia a bitcoin en un foro en línea. No tuvo la confusión que la mayoría de las personas comienzan cuando se topan con el tema: "Me golpeó enseguida". Sabía por su negocio de importación lo difícil y costoso que era mover dinero internacionalmente, por lo que vio bitcoins potencial allí. Pero no estaba convencido de que despegaría, creyendo que era demasiado técnico, demasiado extravagante, para que la mayoría de las personas lo comprendiera y adoptara. "Honestamente pensé que las posibilidades son que moriría en la infancia", recordó.

Sin embargo, él estaba enganchado. "Nunca había visto un proyecto tan motivado como para ayudar a que tuviera éxito", dijo. Comenzó a reunirse en línea con otros entusiastas, y esto lo hizo aún más resuelto. Bitcoin cambiaría el mundo, y él sería parte de eso. Se trataba menos de dinero y más de ser parte de un movimiento que cambia el juego. "En los primeros días, no se hablaba de 'esto nos va a hacer ricos'. Nunca lo escuché al principio." Sin embargo, Kenna se dio cuenta rápidamente de un gran problema con el bitcoin. Para la adopción de la corriente principal, la

gente tenía que tener formas de adquirir Bitcoin de otra forma que no fuera minándola, lo que era una ruta para geeks y especuladores. Sin embargo, en esos primeros días, aunque se habían establecido muchos intercambios rudimentarios en línea, solo existía un sitio verdaderamente funcional en el que se podía establecer una cuenta comercial, transferir dólares desde una cuenta bancaria e intercambiar fácilmente esos dólares por bitcoin: el perenne en crisis Mt Gox. Incluso allí, el funcionamiento fue un término generoso. El sitio era inaccesible y no tenía ninguna de las características de servicio al cliente a las que él y otros estadounidenses estaban acostumbrados. Había tratado de llamar a Mt Gox varias veces para resolver problemas de servicio, pero descubrió con frustración que nunca podría comunicarse. Esta fue una bandera roja y una oportunidad potencial. Para la mente de Kenna, que una criptomoneda esté dominada por un intercambio mal administrado, solo un lugar para mover dinero, desafió el principio de descentralización en el que se fundó la tecnología.

Su solución, naturalmente, era comenzar otra. Tradehill sería diferente de Mt Gox. Kenna no solo contrató a un establo de ingenieros informáticos, sino que incluyó profesionales financieros en el equipo para tratar de imitar el funcionamiento de los intercambios tradicionales. Contrató representantes de servicio al cliente y respondió llamadas y correos electrónicos rápidamente. Contrató un CTO de Google e hizo de la seguridad de la cuenta una prioridad. Esparció la voz como lo hacía la mayoría de las personas cada vez que tenían un nuevo servicio para vender a la pequeña pero creciente comunidad de bitcoin: publicando información sobre la empresa en foros como Bitcointalk.org y Reddit bitcoin forums. Inmediatamente, la idea resonó en las personas. El primer día de la vida de Tradehill, el 8 de junio de 2011, el nuevo intercambio de bitcoins de Kenna recibió $ 250,000 en depósitos. En la primera semana, tomó $ 1 millón. El aumento, pensó, decía mucho más sobre Mt Gox que sobre Tradehill o él. "La gente estaba tan decepcionada con Mt Gox", dijo. "No pensé que iba a ganar un centavo".

Él no. En primer lugar, tuvo problemas con su procesador de pagos, Dwolla, que más tarde demandó por $ 2 millones por lo que Tradehill reclamó eran contracargos indebidos, esas inversiones de pago en transacciones en disputa de las que los comerciantes se quejan con tarjetas de crédito. (El caso aún no se había resuelto en el momento en que lo imprimimos). También enfrentó desafíos regulatorios, ya que las agencias estatales comenzaron a mirar con sospecha este servicio poco ortodoxo para mover dinero digitalmente. Mientras tanto, otros competidores comenzaron a brotar en lugares menos cargados por las demandas bancarias y regulatorias, incluyendo Bitstamp en Eslovenia y BTC-e en Bulgaria. El pastel de bitcoin estaba creciendo, y cada vez más personas querían una pieza. Kenna amplió el personal para ayudar a construir un sitio más competitivo. Pero Tradehill perdió más de $ 100,000 debido a las complicaciones con Dwolla, y con el aumento de las facturas legales, las bajas tarifas comerciales que Tradehill se vio obligado a cobrar para seguir siendo competitivo no fueron suficientes para que obtuviera ganancias. Para el verano de 2012, Kenna no pudo cumplir con la nómina y sabía que tenía que cerrar el intercambio.

Kenna tuvo que devolver todo el dinero que sus clientes habían confiado a Tradehill y cerrar el intercambio. La única otra opción era "convertirse en un banco de reserva fraccionaria", dijo en tono de broma, refiriéndose al modelo de banco que permite a los bancos prestar depósitos manteniendo solo una fracción de esos fondos en reserva. "Lo llaman un esquema Ponzi a menos que tengas una licencia bancaria". Había hundido todo lo que tenía en Tradehill. Ahora, estaba arruinado, tan arruinado que no podía pagar el alquiler. Pensó que la única forma en que podría encontrar refugio era convertir un lugar en una sala de estar común. Si pudiera organizarlo, pensó, podría arreglárselas con la renta.

A Kenna siempre le había intrigado la idea de lo que popularmente se llama una hacker house, con personas que trabajan juntas y reúnen recursos, "pero hasta que llegué a San Francisco, no me di

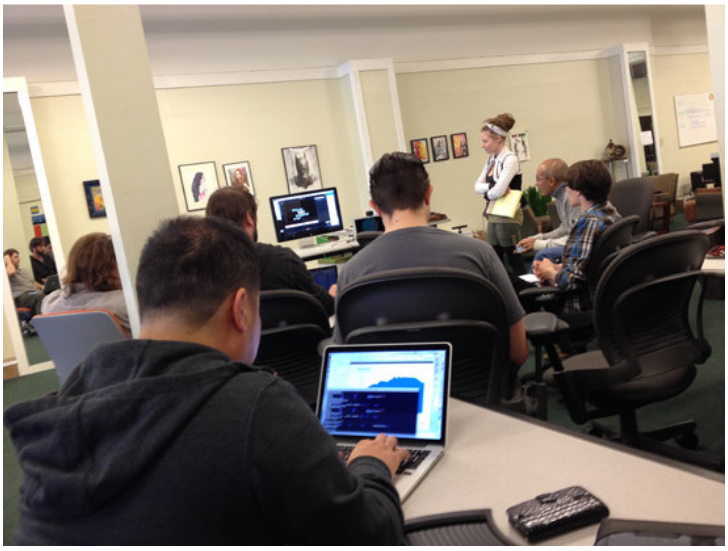
cuenta de que realmente podías hacerlo". Pronto encontró un almacén en el distrito de SoMa y se mudaron con diez amigos, pero después de solo seis meses fueron expulsados porque el edificio no tenía zonas residenciales. Buscó otro lugar hasta que un amigo dijo que había visto un edificio en alquiler en la Misión que podría encajar en la factura. El único problema: "Es un completo shithole".

Kenna, sin embargo, tal vez como resultado de la necesidad, o de un buen ojo, o de ambos, echó un vistazo al edificio, de doce mil pies cuadrados en la esquina de Twentieth y Mission Streets, y vio justo lo que estaba buscando. El espacio de arriba, que una vez fue un hotel residencial, había sido abandonado más de quince años antes, por lo que no tuvo que tirar a nadie. El propietario, entusiasmado con el interés de Kenna, aceptó perdonar nueve meses de alquiler. A cambio, Kenna arreglaría el lugar. Luego trajo algunos amigos, no todos los bitcoiners, les cobró tarifas por debajo del mercado, y utilizó el dinero del alquiler para arreglar el lugar, con la promesa de que mantendría su renta en el mismo nivel después de los nueve meses.

Todavía estaba en la ruina y vivía de poco más que una bolsa gigante de arroz y una bolsa gigante de frijoles mientras convertía el lugar en un lugar habitable. Él lijó pisos y pintó las paredes, haciendo todo el trabajo con la ayuda de un amigo. Diez personas se mudaron inicialmente. Varios meses después de su mudanza, la zapatería se mudó. Kenna ahora tenía el espacio de trabajo para estar de acuerdo con la sala de estar. La noticia se difundió de boca en boca.

Hoy se alquilan las cuarenta y una habitaciones, la mayoría a largo plazo. En una ciudad con gastos de vida tan altos como los de San Francisco, el edificio no tardó en llenarse. Es una mezcla ecléctica. Sí, se trata principalmente de hombres jóvenes y blancos, pero algunas mujeres jóvenes también viven allí, desde lugares tan lejanos como Australia, y algunos muchachos están incluso al norte de los cuarenta. Comparten el espacio de la cocina, una sala común e incluso el baño. Se puede describir mejor como un cruce entre un albergue y un dormitorio. La sala forma un gran cuadrado. Los tapices están en las paredes y los tubos fluorescentes de luz negra en el techo. Cada pasillo tiene su propia placa de calle, también: Litecoin Lane, por ejemplo. Dogecoin Drive. La mayoría de las puertas están cubiertas de carteles e imágenes como en un dormitorio de la universidad. Un par de docenas de bicicletas cuelgan de la pared de la amplia escalera que baja hacia la entrada de la calle.

Tienen noches de película y crespón y hacen fiestas locas con cientos de personas descendiendo en la casa. Y trabajan incesantemente en sus ideas. Incluso los más exitosos no se van. Allan Grant es cofundador de hired.com, un sitio de reclutamiento no relacionado con bitcoin que en mayo de 2014 recaudó $ 15 millones en fondos de riesgo. Todo el mundo suponía que se iría, que recaudar ese dinero representaba "hacerlo". En cambio, Grant simplemente invirtió algo de dinero en mejoras en su habitación a 20 millones de dólares.



Encuentro de bitcoin en 20Mission
(Cortesía de Paul Vigna)

La planta baja es un espacio luminoso y abierto, con un techo alto, paredes de color crema llenas de obras de artistas locales, escritorios en el piso abierto, salas de conferencias y una pequeña habitación en la parte posterior con "cabinas telefónicas", pequeñas, compartimientos amurallados para conversaciones privadas. Los sonidos apagados de la calle, los autobuses, los automóviles, la gente hablando e incluso gritando, agregan un zumbido de fondo constante. Puñados de muchachos jóvenes, principalmente blancos, techy siempre escriben código para algún proyecto, generalmente en jeans y camiseta, algunos descalzos, otros barbudos.

Kenna opera un pequeño centro de medios fuera del sótano para su última aventura, un sitio web llamado Money & Tech, atendido por un pequeño grupo de editores y productores, principalmente traductores independientes. Construyó un estudio completo allí, con un set de video, luces, cámaras, un mostrador de noticias y un telón de fondo. En otras esquinas del sótano hay un par de empresas diferentes. Un artista mayor usa un espacio para hacer sus artículos de cuero; otro espacio es para una compañía de bitcoin unipersonal llamada Piper.

Chris Cassano, un joven de veinticinco años de Florida con cabello largo y peludo negro, gafas y una barba rala, había estado trabajando como contratista de defensa en Mystic, Connecticut, cuando escuchó por primera vez sobre bitcoin en 2011. Después de superarlo su escepticismo inicial, se dio cuenta de que tenía un montón de computadoras que podrían poner a la minería. ¿Por qué no el mío, convertir el bitcoin en dólares, "y tomar su dinero loco, estafa"?

Al vivir sola, lejos de la familia y los amigos, en la pequeña ciudad de Connecticut, Cassano tenía mucho tiempo libre. Pronto, la mayor parte de ese tiempo se gastó en las salas de chat de Bitcoin o pensando en cómo mejorar su hashrate. Tenía experiencia en programación y sistemas de archivos, y su trabajo incluía algoritmos que eran similares a los utilizados en bitcoin. Explotó, pero dice que gastó la mayor parte de su dinero extraído en cosas aleatorias en Internet, sin pensar en cómo podría almacenar su valor para el crecimiento futuro. "Fue genial en ese momento poder gastar mi dinero falso en Internet en cosas del mundo real", dice entre risas. Pero se estaba consumiendo con una pregunta: ¿cuál es la mejor manera de proteger una billetera?

La palabra billetera se usa mucho en los círculos de bitcoins, y es una descripción evocadora, pero es solo una aplicación de usuario que le permite enviar y recibir bitcoins a través de la red de bitcoins. Puede descargar el software para crear su propia billetera, si realmente quiere ser su

propio banco, pero la mayoría de las personas recurre a un proveedor de billeteras como Coinbase o Blockchain, que las combina en sitios web fáciles de usar y aplicaciones para teléfonos inteligentes. De cualquier manera, la "billetera", al igual que una cuenta en un banco tradicional, es poco más que líneas de código, y debido a eso, la seguridad en línea es un problema. En teoría, siempre y cuando uno de los componentes más importantes de ese código -la clave privada más importante que desbloquea la capacidad de una dirección de bitcoin para enviar dinero- resida en algún lugar en línea, es vulnerable a los piratas informáticos. Las nuevas soluciones de cifrado y seguridad introducidas en 2014, especialmente el sistema multi-sig que requiere la coordinación de múltiples claves para acceder a una dirección, deberían hacer tales ataques virtualmente imposibles fuera de la extorsión o negligencia extrema de dos partes. Aún así, si desea mantener sus bitcoins 100 por ciento seguras, no puede dejar el código en línea en ninguna parte.

Así es como Cassano recurrió a una solución simple, no digital: la billetera de papel. Con su programa, el usuario imprimirá el código y lo almacenará fuera de línea. No tardó mucho tiempo en crear una impresora dedicada a prototipos basada en una Raspberry Pi, una placa madre pequeña y económica que venía con protecciones de seguridad incorporadas, que eran necesarias para evitar el problema de registrar inadvertidamente tu código en tu disco duro. cada vez que se comunique con una impresora menos protegida. Publicó una descripción en Kickstarter e inmediatamente vendió veinticinco. Eso le reportó alrededor de $ 4,000. En septiembre de 2013, recibió una llamada de Kenna, invitándolo a 20 Misiones. El trato inusual fue que Cassano podía vivir y trabajar en 20Mission a cambio de una pequeña participación en su compañía; Kenna actuaría esencialmente como un ángel inversor para Cassano. Entonces el floridiano se mudó a la hacker house en diciembre. Tenía vivienda, espacio de oficina, un producto y un patrocinador. Todo lo que necesitaba era un nombre.

"Seguí diciendo: Raspberry Pi, billetera de papel, billetera de papel Pi, billetera de papel Pi", dijo. Finalmente, las palabras se mezclaron en una: Piper.

"El dinero también es bueno", dice Nathan Lands, sentado en un reservado en el restaurante de su esposa, Ramen Underground, que se ha convertido en un lugar frecuentado por los bitcoiners en San Francisco, una alternativa a 20Mission. "Estoy entusiasmado con eso, pero esto es algo del tipo de cambio mundial".

El desertor de la escuela secundaria de treinta años es el cofundador de QuickCoin, el creador de una billetera que apunta directamente a encontrar la ruta más rápida y fácil para la adopción masiva. La idea, que soñó con su compañero de bitcoiner, Marshall Hayner, una noche durante una cena en Ramen Underground, es darles a los novatos de bitcoin no técnicos acceso a una billetera móvil fácil de usar a través de las herramientas familiares de las redes sociales. Los usuarios pueden suscribirse a la billetera de QuickCoin a través de Facebook en sus dispositivos móviles y luego son dirigidos a una interfaz simple que prescinde de la gran cantidad de datos técnicos que se muestran en productos como Blockchain. Con el cabello rubio recortado y una risa fácil, Lands sigue pareciendo el jugador adolescente que era, aunque ahora es un marido y un padre que tiene fondos de riesgo cortejándolo como una reina del baile de graduación. Él ya construyó, vendió y perdió un puñado de negocios, ganó dinero y luego lo perdió, y ahora lo está haciendo nuevamente.

A los quince años, Lands había hecho su primer dinero serio, serio para un adolescente, es decir, dirigiendo un gran "gremio" conectado al videojuego EverQuest y vendiendo bienes virtuales con dinero real. Él ya era un emprendedor. Él simplemente no lo sabía todavía. "No sabía nada de negocios", dijo Lands. "Ni siquiera conocía a nadie que tuviera un negocio. Mi hoja de cálculo era una libreta ".

Esta fue la época del tiroteo en Columbine, y un jugador con cabello largo que tenía predilección por vestirse de negro pronto se encontró en el foco de las autoridades de su escuela, que temía que pudiera tener inclinaciones similares a las de los dos jóvenes asesinos que orquestaron esa masacre. Tener dinero en su bolsillo le dio el coraje de simplemente dejar la escuela en lugar de lidiar con el acoso. Viajó por todo el país, se metió en bienes raíces en Florida, perdió todo y más en el accidente, volvió a los juegos, comenzó las empresas relacionadas con los juegos y se fortaleció nuevamente. Esas empresas lo trajeron regularmente a San Francisco. Finalmente, tenía sentido estar allí permanentemente.

Sus éxitos le permitieron a Lands recaudar $ 10 millones para una compañía, Gamestreamer. Comenzó a hacer investigaciones furtivas sobre un competidor, lo que lo puso en contacto con uno de sus empleados, Patrick Murck, ahora asesor general de la Fundación Bitcoin y una figura clave en los complicados pero esenciales esfuerzos de enlace de la industria bitcoin con los reguladores gubernamentales y los legisladores. Los dos competidores entablaron una amistad. Murck fue el primero en contarle a Lands sobre Bitcoin.

Gamestreamer nunca despegó, y en el verano de 2013, Lands silenciosamente lo cerró. Mientras mataba el tiempo ayudando a su esposa con el negocio de su restaurante, comenzó a pensar en lo que haría a continuación. Siguió volviendo a Bitcoin, que cada vez parecía una buena apuesta. Comenzó a comprar monedas en línea, donde se encontró con su posible socio de negocios, Hayner (con quien más tarde tuvo una pelea, y cuya participación compró). Se conocieron en persona, en Ramen Underground, y comenzaron a esbozar ideas. Una de esas ideas se convirtió en QuickCoin.

Lands es típico de la mayoría de los empresarios itinerantes que conocimos. Brillantes y motivados, poseen, o al menos creen que poseen, varillas de adivinación internas que les permiten detectar la próxima gran cosa e irán donde señale la barra. Mientras hablábamos con Lands, mencionó al menos media docena de negocios que había construido y perdido o vendido; mencionó tener $ 10 millones y estar en la ruina. En un momento dado, él comparó inconscientemente su pequeña puesta en marcha con Apple y Google. Los empresarios también tienen una extraña relación con el dinero. Todos parecen tratar el dinero como si no importara en lo más mínimo. No es algo de lo que preocuparse. A veces lo tienen, otras no. Sin embargo, todos parecen esperar llegar a ser asquerosamente ricos algún día, cuando alcanzan el grande.

"Casi tienes que estar loco", dice Lands, "pero no puedes estar realmente loco". Sin embargo, lleva un poco de nuez ".

Los capitalistas de riesgo de Silicon Valley no comenzaron a meterse en Bitcoin de manera seria hasta bien entrado 2013, más de cuatro años después de su lanzamiento y después de que varias empresas, como Kenne's Tradehill, ya habían llegado y se habían ido. Pero desde entonces, el soporte ha aumentado exponencialmente. El Valle ahora está poniendo dinero detrás de muchos jóvenes innovadores como los que hemos conocido, brindándoles una insignia crítica de legitimidad y garantizando la criptomoneda. Es posible que los capitalistas de riesgo aún no estén desembolsando rondas de financiación de $ 100 millones en nuevas empresas de bitcoin, pero un número cada vez mayor de ellas ha entregado grandes cantidades de dinero.

Por supuesto, se genera mucho dinero de VC como parte de una estrategia de scattershot, con la esperanza de que si solo algunas de las muchas apuestas lo hacen grande, los inversores pueden recuperar su dinero. De manera sensata, muchos capitalistas de riesgo ven sus apuestas de bitcoin en este contexto. Sin embargo, llama la atención cómo muchos parecen estar entusiasmados con la tecnología; en el Valle, casi hay una sensación de que tienes que estar en Bitcoin para que no te pierdas una revolución. El conteo de dinero proveniente de capitalistas de riesgo se ha convertido

en una especie de obsesión con los bitcoiners, y por una buena razón. Es una medida tangible del interés de estos actores influyentes en el campo de la criptomoneda y, por lo tanto, de cuán lejos se ha movido en el camino hacia la aceptación y la legitimidad. Según las encuestas realizadas por el sitio de noticias CoinDesk, el capital de riesgo invertido en empresas de bitcoin saltó de $ 2 millones en 2012 a $ 88 millones en 2013. A mediados de 2014, se habían recaudado más de $ 113 millones solo en la primera mitad. Si continúa en la segunda mitad a esa tasa de expansión del 30 por ciento en seis meses, el aumento anual se habría triplicado desde 2013. Sin duda, la cantidad total dedicada a bitcoin es solo una porción del dinero global de capital de riesgo; Dow Jones VentureSource contabilizó $ 33 mil millones en fondos de capital de riesgo en 2013. Pero la tasa de crecimiento es difícil de ignorar. No está lejos de la recaudación de fondos que se arremolinó en torno a las nuevas empresas de Internet en la segunda mitad de la década de 1990, y sugiere que las afirmaciones de la desaparición de Bitcoin eran prematuras.

Sobre todo, son los nombres de los inversores los que captan la atención de las personas. La lista incluye una selección de jugadores clave del auge temprano del comercio electrónico en la década de 1990, incluido un hombre con un derecho tan grande como cualquiera a haber popularizado Internet: Marc Andreessen. El fundador de Mosaic, el primer navegador de distribución masiva, así como su sucesor más conocido, Netscape, Andreessen es ahora un toro bitcoin de alto perfil. Su firma, Andreessen Horowitz, ha realizado grandes inversiones en el sector de las criptomonedas, incluso en el procesador de bitcoin Coinbase y en el proveedor de pagos Ripple. No es el único techie convertido en inversor de esa época que ahora se lanza a las start-ups de criptografía. Jerry Yang, quien creó el primer motor de búsqueda exitoso, Yahoo, invirtió dinero de AME Ventures en una ronda de financiación de $ 30 millones para el procesador BitPay y en una de las dos rondas de $ 20 millones recaudadas por el proveedor de cartera y billetero Xapo, que ofrece seguro a los depositantes y se llama a sí mismo una "bóveda de bitcoin". Stratton Sclavos, el ex CEO de Verisign, la empresa de clasificación de seguridad del sitio web que convirtió la promesa del comercio electrónico basado en tarjetas en una realidad, tomó una participación importante en la seguridad de billetera de alta tecnología especialista en BitGo a través de su firma Radar Capital. Otros toros de bitcoin prominentes del establecimiento de inversión del Valle incluyen a Jim Breyer de Accel Partners, quien tomó un papel principal en Circle, el servicio de intermediación y depósito de bitcoin fácil de usar lanzado por Jeremy Allaire, el creador del reproductor de video en línea Brightcove. El influyente padre de Adam Draper, Tim, invirtió dinero en Vaurum, un intercambio de bitcoins destinado a bancos e instituciones financieras. Jeremy Liew de Lightspeed Partners ha dirigido dinero en BTC China y Ripple, y la firma de Reid Hoffman Greylock Partners compartió el liderazgo en la segunda recaudación de fondos de $ 20 millones de Xapo, junto con Index Partners of London.

Mientras tanto, el fondo de cobertura Pantera Capital, con sede en San Francisco, pasó de invertir en bonos y divisas globales a convertirse en un vehículo de bitcoin totalmente dedicado, administrando dinero en nombre del fondo de megafondos con sede en Nueva York Fortress Capital. También en Nueva York, Union Square Partners ha asumido un rol clave en el aumento de bitcoins de la Costa Este, más comúnmente a través de la persona del cofundador Fred Wilson. Grandes nombres en negocios y entretenimientos también están apareciendo en bitcoin y otras fuentes de inversión en criptomonedas: el presidente del Virgin Group, Sir Richard Branson, el actor Ashton Kutcher a través de su fondo A-Grade Investments y el multimillonario de Hong Kong Li Ka-shing, que araron dinero en BitPay a través de su firma Horizons Ventures. Luego están aquellos inversionistas que se han involucrado tanto que ahora son parte de la comunidad bitcoin como pilares del circuito de conferencias de bitcoin: Matthew Roszak en Tally Capital en Chicago, Rik Willard de MintCombine en Nueva York y William Quigley de Santa. Con sede en Mónica Clearstone Venture Partners, por nombrar algunos. Además de esto, una comunidad activa de bitcoiners está poniendo su nueva riqueza en programas de aceleración y proyectos de inversión ángel, a menudo con fondos denominados en bitcoin y otras criptomonedas. Los más activos de

esta multitud pertenecen al grupo BitAngels que comprende personas como el agente de relaciones públicas Michael Terpin, el desarrollador de criptomonedas David Johnston y el empresario de moneda digital Brock Pierce.

Las ofertas por $ 20 millones y $ 30 millones son cada vez más comunes. BitPay, Blockchain, Coinbase, Xapo, el fabricante de equipos de minería BitFury, y Circle han llegado a eso, algunos en más de una ronda de recaudación de fondos, mientras cantidades dignas de varios millones de dólares se han destinado a Ripple, BitGo y San Francisco. intercambiar Kraken.

En caso de que esto parezca demasiado centrado en Estados Unidos, vale la pena señalar que el intercambio de alta tecnología Coinfloor con sede en Londres fue financiado en parte por Passion Capital de esa ciudad, el intercambio chino BTC China está respaldado por la unidad asiática de Lightspeed Ventures y la firma nórdica de VC Creandum una ronda de financiamiento de $ 14 millones para KnC Miner, fabricante de equipos de perforación con sede en Estocolmo.

No todo el mundo parece necesitar, o querer, este dinero de VC, que, como hemos mencionado, despierta sospechas entre los primeros utopistas de bitcoin que se preocupan de que los "trajes" se hagan cargo. Hasta que obtuvo $ 30 millones en fondos de VC en octubre de 2014, la gigantesca compañía de billeteras Blockchain llevó a cabo toda su operación en bitcoins. Eso requiere pagar al personal de Bitcoin y recurrir constantemente a los proveedores que aceptan la moneda digital, como CheapAir.com, que el CEO de Blockchain para el establecimiento de jets, Nicolas Cary, utiliza para vuelos. Pero también es más fácil porque el monedero no ofrece ningún servicio de intercambio de moneda fiduciaria. Bitstamp y BTC-e de Bulgaria deben negociar en dólares y euros, pero el par de intercambios centroeuropeos de gran éxito nunca se ha enganchado al flujo de capital de riesgo. Algunas empresas han podido mantener todo en la familia, aprovechando la riqueza de la comunidad bitcoin mediante el lanzamiento de operaciones de crowdfunding denominadas en su totalidad en monedas digitales. Esta es la ruta preferida para las muchas empresas "Bitcoin 2.0" que buscan convertir la cadena de bloques en una plataforma multifacética para intercambios de propiedad y contratos libres de intermediarios y para crear aplicaciones y organizaciones descentralizadas.

Ya sea que estas nuevas empresas llenen las cuentas bancarias tradicionales con dólares de los inversores o acepten las subvenciones de bitcoiners en sus billeteras digitales, el carrusel de dinero está teniendo un profundo efecto en el panorama de las criptomonedas. El aumento en el financiamiento solo rivaliza con el creciente interés de los reguladores gubernamentales como la principal fuerza que configura ese panorama. En su forma ad hoc, de auge y caída, estas empresas con derecho a voto y sus fundadores inteligentes, jóvenes y de ojos abiertos están construyendo y organizando una economía descentralizada que algún día definirá cómo vamos sobre nuestras vidas.

Antes de que la vieja guardia de la comunidad de Valley VC tomara Bitcoin, fueron liderados por un jugador más joven en su campo. Adam Draper, de 28 años, ha sido descrito como el "príncipe" financiero de la comunidad bitcoin, una referencia a la poderosa dinastía de capital de riesgo de la que él es oriundo. El padre de Draper es el ya mencionado Tim Draper, fundador de Draper Fisher Jurvetson y otro entusiasta creyente de Bitcoin. El abuelo de Adán, Bill Draper, y su bisabuelo, William H. Draper, también fueron ambos exitosos VCs de Silicon Valley, este último a menudo se conoce como el padre fundador de la industria. El más joven Draper, quien le dice a los visitantes de su sitio web personal que la ambición de su vida es ayudar en la creación de un traje de hombre de hierro, ha heredado claramente el impulso empresarial de su familia. En 2009, mientras estaba en su último año en la UCLA, Draper fundó Xpert Financial, una plataforma para comercializar acciones en compañías privadas que aún no se han hecho públicas. Funcionando de manera muy parecida a SecondMarket, la creación de cinco años de antigüedad del prominente

refuerzo de bitcoins Barry Silbert, Xpert ha obtenido la aprobación de la SEC. Un año después, el ahora graduado Draper fundó Enders Fund, un proyecto diseñado para financiar el desarrollo de juegos de teléfonos móviles. En junio de 2012, después de una reunión con Brian Armstrong de Coinbase abrió los ojos al entusiasmo de su comunidad, Draper estableció la empresa que lo lanzaría al mundo de bitcoin: Boost, un programa especial de "aceleración" para alimentar las primeras empresas .

Los aceleradores están hechos a medida para Silicon Valley. Esencialmente, los capitalistas de riesgo y los llamados inversionistas ángel reúnen el dinero y lo designan para ayudar a que comiencen las nuevas empresas. Pero no es solo dinero. Durante un período de aproximadamente tres meses, los financistas proporcionan a estas empresas en ciernes espacio de trabajo y espacio de vida y traen mentores para asesorarlos (la principal diferencia entre un acelerador y una casa de piratas informáticos, según parece, es el dinero). Es un curso intensivo sobre cómo convertir sus ideas en negocios, un campo de entrenamiento para nuevas empresas.

El acelerador de Draper fue el primero en enfocarse únicamente en proyectos de bitcoin, pero no comenzó de esa manera. "Estábamos tratando de ejecutar un buen programa de aceleración", dijo. Tomaron espacio en el sótano de otro acelerador, Hero City, un programa que forma parte de Draper University, una escuela de negocios que comenzó el padre de Adam en 2012, en una calle comercial arbolada en la próspera San Mateo. De un grupo de empresas a otro, Draper estaba buscando una tecnología de avanzada para quedarse atrás. Consideró la impresión 3D y los drones. Bitcoin siguió apareciendo, y pronto se convenció de su potencial, tanto desde el punto de vista tecnológico como comercial. "Terminamos realmente sumergidos en el bitcoin", dijo. "Vemos muchas oportunidades en el espacio". En ese momento, solo había un puñado de negocios de bitcoins. Draper pensó que podía duplicar eso.

Explicó que Boost tomaría entre 5 y 7 start-ups relacionadas con bitcoins y que recibiría rápidamente 150 aplicaciones. Los conoció a todos por más de un mes y lentamente reconstruyó la fotografía. "A fines de ese mes, fui una de las principales autoridades en bitcoin", dijo, solo medio en broma. Incluso otros VCs, esencialmente sus competidores, se estaban acercando a él, buscando información. Él se mudó primero, y emergió como el líder en el campo, lo que significaba que sus nuevas empresas podrían sacar dinero de los muchachos más grandes cuando llegó el momento de rondas de financiación más grandes. "Quieres ir a donde nadie más está dispuesto a ir, para que puedas encontrar las grandes cosas que se van a construir".

"Dimos un salto", dijo; "Fuimos los primeros en mostrar que había algún interés". Boost no estaba escribiendo enormes cheques, sino que estaba escribiendo cheques, y los negocios que estaban atravesando se hacían notar. En poco tiempo, el dinero de VC comenzó a verter en Bitcoin. "Nos hizo grandes peces en un pequeño estanque. Y luego se convirtió en un estanque realmente grande".

Scott Robinson es el director de marketing de Plug and Play Tech Center, una incubadora en Sunnyvale, entre Palo Alto y San José en el extremo sur de la Bahía de San Francisco. También es el evangelista de bitcoin residente de la operación. Se enteró de la criptomoneda en 2011, de un amigo que la había usado para comprar drogas en línea. Se sintió intrigado al notar más y más menciones en la prensa. A finales de 2012, comenzó a asistir a las reuniones de bitcoin en Sunnyvale organizadas por Roger Ver, un inversor de bitcoin y cofundador de la Fundación Bitcoin, que ahora también funciona como un tipo de orador motivacional en el circuito de conferencias de bitcoin. Cuando Ver se mudó a Tokio, le pidió a Robinson que se hiciera cargo de las reuniones. Lo hizo y, finalmente, comenzó a mantenerlos en las oficinas de Plug and Play.

Plug and Play es una creación de Saeed Amidi, un inmigrante iraní parlanchín que inició el acelerador en 2006 y ha convertido la exitosa idea en una franquicia global que recluta nuevas empresas en todo el mundo. Las unidades Plug and Play ahora se encuentran en Canadá, España, Singapur, Jordania, Daguestán, Rusia, Polonia y México, así como en otros cuatro sitios en los Estados Unidos. Varios de estos tipos de programas existen en todo el mundo y en el Valle: Boost, Hero City, Y Combinator, 500 Startups, todos con más o menos la misma idea. La diferencia entre "incubadora" y "acelerador" es algo vaga, pero la idea principal detrás de este último es moverse rápido. Facturado como "Silicon Valley in a box", Plug and Play reúne empresas de nueva creación, corporaciones, capital de riesgo y universidades, todo en un solo lugar y elimina a las empresas. Ha sido un modelo tremendamente exitoso y frenético. Cientos de nuevas empresas han recorrido el campus, unas 325 están allí en el verano de 2014, y varias se han convertido en operaciones de miles de millones de dólares.

El campus de Sunnyvale es masivo. Su pieza central es un espacio de oficina de planta abierta para las nuevas empresas que es del tamaño de un campo de fútbol. Muchas empresas se agrupan en torno a socios corporativos, como Volkswagen y Panasonic. Otros se agrupan alrededor de industrias y tecnologías; los bitcoiners, por ejemplo, estaban todos en el mismo cubículo grande. El centro tiene un auditorio, un espacio expo e incluso un gran patio con vistas a las montañas de Santa Clara.

Las mentorías se organizan, trayendo personas con experiencia en los mismos campos que las nuevas empresas. Los fundadores de las start-ups son presentados a capitalistas de riesgo, ejecutivos corporativos y representantes de universidades. A cambio de todo esto, Plug and Play obtiene una participación en el capital de cada uno, generalmente $ 25,000 por una participación del 5 por ciento. En el mejor de los casos, es un arreglo mutuamente beneficioso. Las empresas obtienen exposición y acceso a la experiencia y el capital que de otro modo nunca podrían tener, y el centro llega a disparar decenas de pozos, por así decirlo. Si uno paga-PayPal, Dropbox y Zoosk todos vinieron a través de este programa-vale la pena en grande.

En junio de 2014, Plug and Play organizó su "expo" trimestral de un día, un evento de networking en la culminación de un programa de aceleración que reúne a inversionistas y nuevas empresas para una serie de presentaciones y seminarios y que termina con un pitchfest, donde cada start-up envía a un miembro de su equipo al escenario frente a cientos de inversores interesados de todo el mundo. Este día maníaco viene después de meses de escribir, probar y reescribir el código del software durante meses y luego redactar y volver a redactar los planes de negocios. Al final, estos empresarios obtienen tres minutos en la exposición; tres minutos para destilar tres meses de esfuerzo, tres minutos para subir al escenario y actuar, para representar y vender su empresa, su idea, a una multitud con los bolsillos profundos, los bolsillos más profundos, que están acostumbrados a escuchar todo tipo de cosas fantásticas lanzamientos. Es una oportunidad de oro, lo que lo hace aún más estresante, sobre todo teniendo en cuenta que la mayoría de los técnicos no son aficionados naturales y carecen del carisma de su gerente de marketing promedio. Tres ganadores son elegidos por un panel de jueces. Robinson estaba especialmente orgulloso porque esta exposición incluía a sus bebés especiales: cinco nuevas empresas relacionadas con el bitcoin entre las dos docenas de pitcheo.

Todo tiene un sentimiento de American Idol, y al igual que muchos de los cantantes más populares que emergen de la fábrica de American Idol son los que no ganan: Daughtry, Katharine McPhee, Kellie Pickler, en la exhibición de Plug and Play es genial pero no el único premio. Haga un buen lanzamiento, e incluso si no gana, la gente comienza a prestarle atención, y el día de pago puede venir por el camino.

Las cinco empresas de bitcoin representaban una impresionante amplitud del tipo de innovación que se está llevando a cabo actualmente en este campo. CoinVox es un servicio de donaciones políticas basado en bitcoins; 37Coins es un producto para enviar moneda digital a través de mensajes SMS dirigidos a países en desarrollo; CoinsFriendly es una herramienta de análisis comercial y de comercio de bitcoins; Purse proporciona una puerta trasera para comprar bienes en Amazon con bitcoin; y PeerPal es un mercado en línea para que las personas intercambien bitcoins y dólares directamente entre sí en línea. Sus equipos vinieron de Texas, California y Maryland, y Ucrania, Corea del Sur y Alemania. En su mayor parte, estos bitcoiners eran jóvenes, con una excepción, ya pesar de sus diferentes antecedentes, todos tenían dos características en común. Todos eran increíblemente inteligentes, ya vinieran con una piel de oveja de la Ivy League o se habían enseñado a sí mismos a codificar, y todos eran fantásticamente ambiciosos.

Purse's Andrew Lee, que tiene experiencia en pagos en Merrill Lynch, había aprendido sobre bitcoin en 2011 y estaba lo suficientemente interesado en comprar en línea 5 dólares, que olvidó rápidamente. Había pasado más de un año cuando de repente notó que el precio del bitcoin subía exponencialmente y recordó su inversión de $ 5. "Una taza de café", explicó a modo de comparación, "se había convertido en una computadora portátil".

Lee comenzó a asistir a reuniones de bitcoin y en una conoció a Kent Liu, un científico informático de IBM. Un día de febrero de 2014, se reunieron en una cafetería alrededor del mediodía en el Distrito de la Misión en San Francisco. Para cuando terminaron su última taza de café, a las 11:00 p.m., habían elaborado una propuesta que pretendía resolver dos problemas de diferentes grupos de personas a la vez y que eventualmente los ubicaría en Plug and Play. En primer lugar, les permitiría a aquellos que quieran gastar bitcoins en productos en Amazon hacerlo aunque el sitio de comercio electrónico no acepte la moneda digital, y a un precio de descuento negociado para arrancar. En segundo lugar, permitiría que cualquiera que quiera comprar bitcoin lo haga con una tarjeta de crédito, una ventaja que la mayoría de los intercambios de bitcoin y corretaje de bolsa no permiten debido al riesgo de contracargos de los bancos emisores de tarjetas de crédito. La ingeniosa solución de Lee y Liu fue reunirlos a través de un mercado abierto, el titular de la tarjeta de crédito comprando los productos en nombre del comprador y obteniendo bitcoins como compensación. Era como una versión mecanizada y orientada al mercado del famoso reparto de pizza de Laszlo Hanyecz. Funcionaría como un mercado simultáneo para bitcoin y bienes, con ofertas para descuentos de productos de Amazon que representan ofertas de precios de bitcoin con primas impuestas para la conveniencia de usar una tarjeta de crédito. Y así nació Purse.

Ambos pronto renunciaron a sus trabajos. "Fue una decisión fácil", dice Liu.

El equipo detrás de PeerPal era notablemente diferente de los demás: eran el único grupo cuyos miembros obviamente estaban en el otro extremo de sus veinte años. O los treinta para ese asunto.

Cuando comenzaron a reunirse en agosto de 2013, James Jones, Joshua Schechter y Houston Frost fueron los únicos tres bitcoiners en San Antonio, Texas. "Tendríamos reuniones", explica Schechter, "y éramos los únicos allí". Los tres también caen en el molde del empresario. Frost es el CEO de Akimbo, que vende una tarjeta de débito prepaga que permite a los usuarios configurar una rama de varias subcarpetas para los miembros de la familia. Schechter construyó y vendió una empresa de procesamiento de pagos, y Jones inventó un producto llamado CubeSpawn, una impresora autorreplicante. Schechter aprendió acerca de bitcoin en 2009, después de leer el libro blanco de Nakamoto, pero no fue cortado del molde de Cypherpunk de los primeros fanáticos de bitcoin. "No soy anarquista ni libertario", dice Schechter. "Soy un capitalista". En bitcoin, vio su oportunidad de hacerse rico. Una reunión casual con Robinson en una conferencia de bitcoin en Las Vegas llevó a una oferta para venir a Sunnyvale. "¿Cómo se dice que no a una oportunidad en un acelerador de Silicon Valley?", Dijo retóricamente. Entonces, el hombre de cuarenta y ocho años

puso a su esposa, a su casa, a sus hijos, a sus peces y a su perro en espera por tres meses y salió a California.

Estos chicos tienen necesidades ligeramente diferentes de la mayoría de sus compañeros en la exposición. Aunque es fácil para un joven de veinticinco años cuyos únicos gastos son el alquiler y la cerveza no preocuparse por el dinero, los hombres de PeerPal tienen familias y bocas que alimentar. "No podemos hacerlo de forma gratuita", explica Schechter. Cuando nos conocimos, vivía de los ahorros y del trabajo de su esposa. En junio de 2014, se alojaba en Circuit House, una hacker house como 20Mission, en San José. "Es como estar en la universidad de nuevo", bromeó. Pero si PeerPal no despegaba, sabía que tendría que pivotar de nuevo, descubrir su próximo movimiento. Schechter representó al grupo en el escenario. Un extrovertido natural, dio una buena presentación, que tuvo una buena reacción. Las reacciones de la multitud durante todo el día no fueron diferentes a las de una obra de teatro de la escuela primaria, con miembros dispersos de la familia que gritaban con más fuerza cuando su hijo subía al escenario. Schechter terminó su discurso de manera inusual con una solicitud específica en dólares: $ 600,000. (Más tarde nos dijo que lo consideraba una figura conservadora).

Schechter reconoció que uno de sus objetivos era comprarse. (Ellos conscientemente eligieron su nombre, PeerPal, con la esperanza de atraer la atención de PayPal.) Pero al final no obtuvieron ninguna inversión nueva o compraron, y para el final del verano los tres estaban de vuelta en Texas, De regreso a sus viejos conciertos, sus sueños de riqueza de bitcoin se retrasaron, no se destruyeron. Frost tuvo a Akimbo. Schechter está ayudando a Jones con CubeSpawn, cuyas pequeñas máquinas autorreplicantes y descentralizadas están diseñadas para fomentar la "fabricación distribuida". Naturalmente, su negocio requiere bitcoin.

Prácticamente todos los innovadores tecnológicos y capitalistas de riesgo con los que hablamos dicen que están motivados por las perspectivas a largo plazo de Bitcoin. Con eso quieren decir que las oportunidades de ganar dinero que ven provienen de brindar a las personas herramientas de criptomoneda descentralizadas con las cuales cambiar las prácticas comerciales, no las ganancias a corto plazo de especular sobre su precio. Aún así, no es coincidencia que la recuperación del dinero de VC hacia el sector coincidiera con el aumento en el precio de Bitcoin en 2013, cuando la moneda digital subió un 8,400 por ciento en once meses hasta un máximo de $ 1,151 a principios de diciembre, un nivel mil seiscientas veces mayor de tres años antes. Un mercado en alza, especialmente uno que escala nuevas alturas a un ritmo como ese, puede crear rumores y atención alrededor de un activo. Más que eso, también libera el gasto y el poder de inversión entre quienes poseen ese activo.

Un ciclo de retroalimentación positiva es cómo lo describiría Silicon Valley, con los precios más altos generando más interés en las criptomonedas, más capital de inversión que fluye hacia Bitcoin, más innovación y más interés y beneficios para el sector, lo que debería impulsar el precio aún más. Los escépticos también podrían llamarlo una burbuja, y muchos buscaron hacerlo una vez que el precio retrocedió a menos de $ 500 en la primera mitad de 2014, usándolo para justificar sus representaciones de "manía de tulipanes" alrededor de bitcoin. Pero incluso en esos niveles más bajos, el bitcoin aún era más alto que cualquier nivel que hubiera tenido en toda su historia antes de mediados de noviembre de 2013. Eso dejó a muchos mineros, empresarios de bitcoins y empresas que se han ganado la criptomoneda durante un año o más marcadamente más rico . Las decisiones que toman al invertir esa riqueza han incentivado aún más la innovación en el sector y han impulsado los precios de las propiedades digitales relacionadas con bitcoin, al igual que el auge de las acciones de NASDAQ alimentó la manía de las empresas y emprendimientos de TI a fines de la década de 1990.

La historia serpenteante del nombre de dominio bitcoin.com, la pieza más valiosa de bienes inmuebles en línea de la criptomoneda, ilustra esto bien. Se registró por primera vez en el año 2000 por una compañía de telecomunicaciones sueca, lo que permitió que el registro caduque. Una compañía tecnológica de Corea del Sur la poseyó desde 2003 hasta 2005, luego también dejó que caduque. En 2008, un estudiante y empresario de la Universidad de Yale llamado Jesse Heitler lo registró, y luego lo vendió en 2010 por $ 2,000 a un empresario de Toronto llamado David Lowy. Lowy pasó al propietario actual, que permanece en el anonimato. Ese propietario ha alquilado el nombre a tres grupos diferentes: uno fue Kenna, que pagó $ 1 millón en capital de Tradehill en 2011 por el nombre. Después de que Tradehill cerró, el hombre lo arrendó primero a Coinbase, y luego en 2014 a Blockchain. No sabemos qué pagaron los últimos dos, pero si valió $ 1 millón en 2011, es una buena apuesta que vale mucho más que eso ahora.

Si bien puede parecer que todos en el Valle están interesados en bitcoin, así como puede sentir que todos los que están fuera del Valle están en contra o tienen poco interés, la verdad es que la camarilla de fervientes creyentes es todavía relativamente pequeña. Algunos en la comunidad de VC tienen serias dudas, simplemente no parecen expresarlos a menudo. En una publicación en el blog StrictlyVC de Connie Loizos titulada "Un oso Bitcoin en Silicon Valley, es cierto", Josh Stein, el director general de la firma Draper Fisher Jurvetson de Menlo Park de Tim Draper, se cita describiéndose a sí mismo como un "oso bitcoin". Stein, cuya firma invirtió en Twitter, Skype y Tesla, argumentó que los ahorros en los costos de transacción en bitcoin no eran mucho más competitivos que los cables electrónicos o las nuevas tecnologías de pago basadas en dólares, y que el bitcoin, a diferencia del oro, no tenía valor. "Sin embargo, en un giro revelador, Loizos escribió que Stein rápidamente acortó sus comentarios, afirmando que revelar públicamente sus puntos de vista" serviría de pista a los trolls ". Probablemente se estaba refiriendo a los zelotes bitcoin que rápidamente llevan a Reddit o Twitter a desacreditar cualquiera que desafíe la noción de que la criptomoneda es la respuesta a los problemas del mundo. Pero el comentario de Stein también lo hace sonar como si la comunidad de CV estuviera atrapada por su propio pensamiento grupal sobre bitcoin, mediante un tipo sutil de autocensura que evitara que cualquier miembro se salga de sus mensajes.

Según nuestra experiencia, los capitalistas de riesgo son mucho más reflexivos y de mente abierta que eso. Entonces, es probable que Stein aún pueda almorzar felizmente con su compañero Tim Draper. Pero fuera de los estrechos confines del Área de la Bahía, los bitcoiners son muy minoritarios. Las críticas de Stein resuenan allí mucho más fácilmente, especialmente su punto discutible sobre la falta de cualquier valor intrínseco. Sin importar cuán defectuosa sea esa visión, recuérdese nuestra discusión en el capítulo 1 sobre el mito del valor intrínseco de todas las monedas, es ampliamente sostenida por personas que viven fuera del Área de la Bahía.

La imagen que surge es de un mundo desequilibrado dividido entre una camarilla pequeña pero bien financiada que está convencida de que la criptomoneda va a cambiar el mundo y todos los demás, que no pueden ver de qué se trata todo este alboroto. Sin el apoyo del segundo grupo, la visión del primero no se hará realidad. Eso es tan cierto para Bitcoin como para cualquier nueva tecnología. Silicon Valley necesita pisar con cuidado. Mientras que los estadounidenses todavía ven en general las empresas emergentes de la región y sus inversores arriesgados en una luz positiva, como los hombres y mujeres jóvenes que promueven el sueño americano, el descontento puede potencialmente surgir. Con cada faceta de nuestra economía ahora depende de los tipos de software desarrollados y financiados en el Área de la Bahía, y con las comunidades adineradas del Valle convirtiéndose en un caladero vital para las donaciones políticas y el mecenazgo, estamos presenciando una migración de lo político y base de poder económico lejos de Wall Street a esta región. En medio de ese cambio, la omnisciencia de compañías gigantes como Google, Microsoft, Apple y Facebook y las revelaciones sobre la información privada que la gente les cede hace que muchas personas, incluidos algunos legisladores, se sientan incómodas. Ciertamente, su poder

abarcador crea una impresión mucho más negativa que la imagen romántica de geeks de la informática que hacen aparatos geniales en garajes. A medida que nuevas olas de tecnologías altamente disruptivas comienzan a despojar a más estadounidenses de sus trabajos, y como veremos más adelante, las criptomonedas podrían incluirse en ellas, el resentimiento hacia la "sabiduría" del establecimiento de Silicon Valley podría seguir creciendo. Por otro lado, los productos que salen del Valle han hecho contribuciones positivas a la sociedad, como las que surgieron de la llegada de Internet. De hecho, es su experiencia relativamente reciente con el desarrollo de Internet lo que ayuda a muchos tipos de Silicon Valley a entusiasmarse con las criptomonedas. No saben lo que depara el futuro para Bitcoin, pero debido a las impredecibles innovaciones derivadas de Internet, muchos sienten que esta nueva "plataforma" tiene perspectivas similares y liberadoras.

"Si volviste a 1993 y preguntaste a la gente qué pensaban que podrían hacer si conectaban en red todas las computadoras, mucha gente básicamente habría tomado cosas que ya estaban haciendo con las computadoras y habría imaginado que las harían más rápido y en mayor escala". dice Chris Dixon, socio de Andreessen Horowitz. "Por ejemplo, la gente decía: 'En casa, actualmente copio archivos colocándolos en un disco y caminando por la sala, pero ahora en la red puedo hacerlo instantáneamente'. Entonces, la gente imaginaba cosas como copiar archivos y chatear en los tablones de anuncios. Pero nadie imaginó Twitter o Wikipedia o YouTube o todos estos increíbles inventos que han sucedido en los últimos diez o veinte años. Sería muy difícil encontrar a alguien en 1993 que predijera todas esas cosas. "Dizon dice que esas posibilidades inimaginables existen con Bitcoin, porque" las plataformas extensibles de software que permiten a cualquiera construir sobre ellas son increíblemente poderosas y tienen todos estos usos inesperados . Lo interesante de arreglar el sistema de pago existente es interesante, pero lo superfino es que tienes esta nueva plataforma en la que puedes mover dinero y propiedades y potencialmente construir nuevas áreas de negocios ".

Si Dixon tiene razón acerca de que Bitcoin es Internet una vez más, una visión moldeada por la experiencia de su socio, el fundador de Netscape, Marc Andreessen, entonces muchas de las nuevas empresas que se han zambullido en este campo cumplirán sus sueños y bien podrían convertirse en el próximo PayPal, o al menos, comprado por PayPal. Para los capitalistas de riesgo, la esperanza es que su enfoque scattershot llegue solo a un par de grandes ganadores. Este enfoque inherentemente optimista se basa en la idea de que las oportunidades se encuentran en lugares múltiples sin explotar: no siempre sabemos cuáles.

Como veremos en el próximo capítulo, algunas de las grandes oportunidades, quizás las más importantes, se ven mucho más allá de los barrios bien cuidados de Palo Alto o los apartamentos bien amueblados de Nueva York o Londres. La gran promesa de la criptomoneda no es que los ricos se apresuren y aumenten su precio, sino que a los pobres les resultará extremadamente útil. Es hora de explorar una de las ideas más emocionantes de bitcoin: que puede liberar a los "no bancarizados".

Capítulo 8

LOS NO BANCARIZADOS

> El dinero, se ha dicho, es la causa de las cosas buenas para un hombre bueno y de las malas para un hombre malo.
>
> -Philo

Aproximadamente 2,500 millones de adultos en el mundo no tienen acceso a los bancos, lo que significa que alrededor del orden de 5.000 millones de personas pertenecen a hogares que están aislados de un sistema financiero que el resto de nosotros damos por sentado. No pueden iniciar cuentas de ahorro. Ellos no tienen cuentas de cheques. No pueden obtener tarjetas de crédito. Viven en lugares donde los bancos no quieren ir, y debido a esto, permanecen efectivamente amurallados de la economía global. Se llaman los no bancarizados. Pero no son inalcanzables, ni remotamente, y uno de los prospectos más grandes y emocionantes con los que bitcoiners habla es el uso de sus criptomonedas para llevar a estos miles de millones de personas rugiendo en el siglo veintiuno.

El dinero no es ni bueno ni malo. Es simplemente un sistema de intercambio y contabilidad: una forma en que la sociedad puede intercambiar bienes y servicios de manera eficiente y eficaz y realizar un seguimiento de todo ello a gran escala. Sin embargo, la gente lo ha investido de valores trascendentes. El "dinero" se ha convertido en una construcción mental como el "valor" mismo. Los bitcoiners no son diferentes en la forma en que describen su moneda. En sus mentes, Bitcoin es una fuerza en sí misma que remodelará y mejorará las vidas de las personas donde quiera que vaya, lo que les lleva a la idea de que ambos pueden hacerse ricos y hacer un gran bien. Es como el capitalismo con una inclinación radicalmente altruista. En ninguna parte esto es más evidente que en cómo se ofrece el bitcoin como una solución para los pobres del mundo, y en este caso tienen un caso convincente para obtener una forma de dinero mejor y más accesible.

Para ilustrar, volvamos brevemente a una de las start-ups que debutó en el día de la Exposición de Plug and Play en junio: 37Coins. La puesta en marcha es el trabajo combinado de sus tres fundadores, Songyi Lee, Johann Barbie y Jonathan Zobro. De los tres, Lee parecía el más fuera de lugar en el Valle. No codificadora, ni libertaria ni criptoanarquista, era trabajadora social. Barbie, su novio, era entusiasta de la tecnología y el bitcoin. Pero un día, los dos juntaron sus mundos separados y se dieron cuenta de que tenían la oportunidad de hacer algo grande.

En septiembre de 2013, Lee formó parte de un equipo de filmación en Mali, trabajando con World Vision, una organización sin fines de lucro contra la pobreza, en su primer viaje al campo. Mali acababa de pasar por una brutal guerra civil, y la gente se había vaciado del norte y había huido hacia los campamentos de refugiados en el sur. Allí, Songyi conoció a Fátima, una madre de cinco hijos que vivía en un "campamento" que se parecía más a una residencia permanente. Su esposo había inmigrado a Costa de Marfil para trabajar, como muchos malienses, y le enviarían dinero cuando pudiera. Cómo lo hizo causó una gran impresión en el joven Lee.

El esposo de Fátima le devolvió dinero a la gente. Personas aleatorias, personas que se dirigieron en la dirección de su esposa y familia. La familia de Fatima no tenía cuentas bancarias, ni siquiera identificaciones. A veces el dinero llegó. Algunas veces no. Para complementar esa frágil corriente de ingresos, Fatima trabajó como ama de llaves. Si eso no fuera suficiente, sus hijos mayores también trabajarían.

Ella, lo que es más importante, tiene un teléfono, un teléfono con funciones de $ 5. "No podía creerlo", dijo Lee. Este último punto es crítico. Sin cuentas de ahorro, sin acceso a servicios bancarios, las personas en los mercados emergentes, así como una buena cantidad en mercados avanzados como los Estados Unidos, tienen dificultades para acumular una riqueza duradera. Es solo un desafío más que deja a tantos atrapados en la pobreza. Para ellos, la búsqueda de otras libertades de expresión, por ejemplo, debe subordinarse a la tarea de abordar estos desafíos financieros y económicos. El escape de todo eso, conjeturan los bitcoiners, puede residir en esos teléfonos de $ 5 y en un nuevo y radical sistema de dinero móvil.

Malí es una de las naciones más pobres del planeta. Ocupó el lugar 175 entre 187 naciones en el Índice de Desarrollo Humano de la ONU. Más del 70 por ciento de la población vive por debajo del umbral de la pobreza. Depende en gran medida de la agricultura, y el ingreso per cápita tiene un promedio de $ 500 por año. Hay esfuerzos para impulsar el turismo, pero la historia de violencia del país, incluido el golpe en 2012 que expulsó a personas como Fátima de sus hogares, hace que sea una venta difícil.

Después de que Lee regresó a su casa en Seúl, le mostró a Barbie las imágenes que había tomado, y una bombilla se apagó en su cabeza. Barbie era una diseñadora de software que había trabajado para IBM y que se había fascinado con Bitcoin: "No dormí durante dos días", describió su primera reacción al descubrimiento de la criptomoneda e inmediatamente vio una forma de solucionarlo. El problema de Fatima: pagos móviles. Los bitcoins, después de todo, no son más que líneas de código. Si alguien tiene un teléfono, ni siquiera tiene que ser un teléfono inteligente, puede ser un teléfono que puede recibir mensajes de texto, puede engancharse en un sistema informático para entregar bitcoin. Es posible que los bancos no quieran extender su engorroso sistema bizantino a estos bolsillos de los mercados emergentes porque simplemente no es rentable. Pero eso no es un problema para bitcoin.

"Pensé que esto es todo", dijo Lee. "Esta es mi oportunidad de vida para intentar salvar el mundo y tratar de cambiar el mundo". Dejó su trabajo en World Vision y, junto con Barbie y Zobro, comenzó a construir 37Coins. (El nombre es una referencia a un comentario de Satoshi Nakamoto, quien opinó una vez en un tablero de mensajes que la minería bitcoin era "como intentar arrojar 37 monedas a la vez y hacer que todas salgan caras").

El servicio permite a cualquier persona que tenga un teléfono con funciones simples de vainilla, incluidos los teléfonos de gama baja utilizados por personas de países en desarrollo, enviar dinero a través de mensajes de texto, es decir, mensajes de texto. Todo lo que uno tiene que hacer es abrir una billetera con 37 Monedas. Es similar a un servicio popular llamado M-Pesa en Kenia, pero donde M-Pesa es operado por una compañía de telecomunicaciones, Safaricom, y está construido sobre la infraestructura bancaria tradicional, 37Coins funciona desde la red descentralizada de bitcoins. Utiliza personas en la región con la suerte de poder pagar los teléfonos inteligentes Android como "puertas de enlace" para transmitir los mensajes. A cambio, estos portales reciben una pequeña tarifa, que proporciona el beneficio corolario de brindarles a los locales la oportunidad de crear un pequeño negocio para ellos mismos moviendo el tráfico. El negocio todavía se encuentra en las primeras etapas, con pruebas en Asia y en otros países donde la población es más conocedora de la tecnología, antes de ser juzgada en lugares como Malí.

Los fundadores de 37Coins tienen energía y pasión, pero enfrentan grandes obstáculos. A pesar de la notable penetración de los teléfonos celulares en los barrios marginales del mundo, la tecnología tiende a moverse más lentamente en los lugares más pobres. Otros obstáculos son culturales, sociales y políticos, como las guerras civiles, o la lejanía de algunos clientes potenciales, o su resistencia a las nuevas formas de hacer las cosas. Además, 37Coins enfrenta presiones

competitivas. Cada vez más start-ups de criptomonedas apuntan a sus servicios en mercados emergentes, incluidos BitPesa en Kenia, BitPagos en América del Sur y Volabit en México. Algunos de ellos, 37Coins, BitPagos y Volabit, por ejemplo, han pasado por los programas de acelerador de Silicon Valley. Otros, como BitPesa, están bien conectados y financiados. Todos comparten la creencia de que pueden ganar un buen dinero y hacer que el dinero sea bueno.

Las personas en los países desarrollados a menudo no se dan cuenta de los costos ocultos y los problemas de privacidad de las tarjetas de crédito. Para ellos, las tarjetas de crédito funcionan muy bien: los comerciantes son golpeados con las tarifas de transacción y los contracargos, no los clientes, y no tienen que molestarse en buscar dinero en efectivo. Entonces, a menos que hayan sido quemados por el costo inesperado de usar su tarjeta de crédito en un país extranjero, tienden a ver las criptomonedas como una solución en busca de un problema. Pero en el mundo en desarrollo, donde los costos de un sistema financiero ineficaz y la carga de transferir fondos están demasiado claros, las criptomonedas tienen un argumento mucho más convincente. Los evangelistas de Bitcoin tienden a centrarse en dos áreas: las remesas de dinero de los países desarrollados a los países en desarrollo y los pagos y transferencias internos.

El Banco Mundial estima que el negocio global de remesas vale alrededor de $ 500 mil millones anuales en flujos transfronterizos. Países como Filipinas y los de América Central, que tienen grandes grupos de ciudadanos que trabajan en países más ricos, dependen en gran medida de estos fondos para llevar a casa sus economías. Sin embargo, nuestro sistema financiero internacional ineficiente asegura que solo una parte del dinero llegue a donde se supone que debe ir. Dependiendo del país receptor, las tarifas por el dinero enviado desde los Estados Unidos a menudo llegan al 10 por ciento; desde el Reino Unido y otros países puede ser el doble. Con los costos de la tasa de cambio, la "fricción" total en la transacción puede llegar hasta el 30 por ciento.

Dentro de los países en desarrollo, pueden existir desafíos igualmente grandes en la realización del comercio cotidiano. Para un comerciante cuyos clientes no tienen acceso al crédito, simplemente llevar todo ese efectivo puede ser peligroso. Para un cliente sin una cuenta bancaria, crear cualquier tipo de ahorro es prácticamente imposible. El problema no se limita a los mercados emergentes. En Canadá, el Reino Unido, Alemania y Australia, la proporción de personas mayores de quince años con una cuenta bancaria oscila entre el 96 y el 99 por ciento. Pero vaya a los Estados Unidos, y la cifra se reduce al 88 por ciento. Agregue una categoría separada "no bancarizada", es decir, aquellos que pueden tener una cuenta bancaria, pero también son dirigidos a fuentes bancarias "no tradicionales" tales como cobradores de cheques o préstamos de día de pago, y el porcentaje de la población estadounidense con acceso insuficiente a la el sistema financiero excede el 30 por ciento. Mientras que China ha entregado cuentas bancarias al 64 por ciento de su población, en Argentina, a pesar de la gran población educada e instruida de clase media de Buenos Aires, solo el 33 por ciento del país está bancarizado, una cifra menor que el 35 por ciento de la India. En Filipinas, donde las remesas son tan valiosas que los OFW (Trabajadores filipinos en el extranjero) que regresan están exentos de los impuestos aeroportuarios y reciben un procesamiento rápido de pasaportes en el aeropuerto de Manila, solo el 27 por ciento de la población tiene cuentas bancarias. En Pakistán, la cifra es del 10 por ciento.

Los bancos no darán servicio a estas personas por varias razones. En parte se debe a que los pobres no ofrecen ganancias tan abundantes como los ricos, y en parte es porque viven en lugares donde no existe la infraestructura y la seguridad necesarias para que los bancos construyan sucursales físicas. Pero principalmente se debe a instituciones legales débiles y leyes de titulación subdesarrolladas. Sin documentación para demostrar su identidad, presentar garantías y crear historiales crediticios, los pobres del mundo carecen de los cimientos básicos para participar en el sistema bancario mundial. Esto los limita a transacciones en efectivo. Todo un nivel de banca en la sombra ha surgido para satisfacer sus necesidades, pero por lo general implica transmisores

de dinero exorbitantes o, como en el caso de los trabajadores migrantes en Malí, se ponen a la merced de extraños.

A Bitcoin, como sabemos, no le importa quién es usted. No importa cuánto dinero está dispuesto a ahorrar, enviar o gastar. Usted, su identidad y su historial de crédito son irrelevantes. Necesitas una plataforma electrónica con la que conectarte a Internet. Pero si puede obtener eso, bitcoin le permite enviar o recibir dinero desde cualquier lugar. Si vive con $ 50 a la semana, los $ 5 que ahorrará importarán mucho.

Integrar financieramente a un tercio de la humanidad podría crear nuevas oportunidades para el comercio mundial y para atacar la pobreza. Ya hemos visto el gran impacto que la globalización y la digitalización han tenido en la vida de las personas, incluso sin reformar el sistema financiero. Esto ha significado que los jóvenes en la India con un dominio del inglés y una comprensión de una computadora de escritorio ahora pueden obtener trabajos para el mantenimiento de computadoras estadounidenses y europeas sin tener que abandonar sus hogares. Ha permitido que las empresas multinacionales obtengan sus productos de cualquier parte del mundo, creando trabajos de manufactura en regiones que nunca los tuvieron. Mientras que muchos han sido perdedores en los países ricos que han visto la fábrica y otros empleos subcontratados desaparecer, en un nivel macro los beneficios de la globalización son difíciles de ignorar, incluso si sus críticos a menudo lo hacen. Entre 1990 y 2010, el porcentaje de la población mundial que vive con menos de $ 1.25 al día bajó del 43.1 al 20.6 por ciento, lo que coloca al mundo por delante del Objetivo de Desarrollo del Milenio de la ONU para reducir a la mitad la pobreza extrema en 2015. La esperanza de vida aumentó en siete años en el mismo período, y las tasas de mortalidad infantil se redujeron casi a la mitad.

Esta mejora sin precedentes en la prosperidad del mundo en desarrollo no refleja una repentina emanación de la filantropía de los países ricos. Está directamente relacionado con el crecimiento del comercio posterior a la Guerra Fría con y entre los mercados emergentes de Asia, América Latina y África. Esto se muestra claramente en las correlaciones entre el avance del comercio en la región más poblada del mundo, Asia, y el rápido ascenso de una clase media allí. Pero incluso es evidente en las regiones más pobres de África, que se ha aprovechado del avance económico liderado por la globalización de China para convertirse en un proveedor de su insaciable apetito por los productos básicos y un imán para sus inversiones, todo lo cual fomenta centros pequeños pero en crecimiento. de la prosperidad en todo el continente. Cuanto más comercialice el mundo y cuanto más profunda y amplia sea su integración económica, mayor será la creación de riqueza agregada. La integración financiera global podría impulsar ese proceso en sobremarcha.

Por supuesto, Bitcoin no es la única herramienta para la integración económica, y los escépticos a menudo enfatizarán dos puntos, ninguno de los cuales es particularmente convincente. En primer lugar, argumentan que las poblaciones pobres, con diversos grados de alfabetización, no son capaces de manejar nuevas tecnologías complicadas como el bitcoin. Su segundo reclamo es que no cuentan con sistemas de telecomunicaciones lo suficientemente sofisticados como para permitir su uso. En realidad, estas áreas son posiblemente lo que hace que estas regiones estén listas para la adopción de Bitcoin.

Con respecto a la alfabetización, el mundo en desarrollo en su conjunto es significativamente más alfabetizado de lo que era hace solo una década y media. Entre 1999 y 2012, la alfabetización de los países de bajos ingresos medida por el Banco Mundial saltó al 71 por ciento desde el 50 por ciento, la alfabetización de los países de ingresos medianos pasó al 96 por ciento desde el 83 por ciento y para todo el mundo aumentó al 92 por ciento 81 por ciento. El punto clave es que a pesar de esos avances, la gran mayoría de aquellos en países pobres y una gran parte en países de ingresos medios no tienen acceso a servicios bancarios. Carecen de acceso a los bancos no porque

carezcan de educación, sino por los persistentes obstáculos estructurales y sistémicos a los que se enfrentan personas de escasos recursos: sistemas no desarrollados de documentación y titulación de propiedad, excesiva burocracia, esnobismo cultural y corrupción. El sistema bancario hace demandas que la gente pobre simplemente no puede cumplir.

Un punto más sobre el analfabetismo: los analfabetos son predominantemente mayores. En las regiones en desarrollo de Europa del Este, Asia Oriental, América Latina y el Caribe, la finalización de la educación primaria es ahora más o menos universal. Enormes olas de personas educadas en la escuela están ingresando a la fuerza de trabajo en estas regiones, donde la demografía es lo opuesto a las sociedades que envejecen en Occidente. Esta afluencia masiva de jóvenes escolarizados estará más que capacitada para manejar la tarea cada vez más simple de enviar y recibir moneda digital.

De hecho, las personas en los países en desarrollo pueden estar mejor preparadas mentalmente que las personas en Occidente para el dinero digital, en virtud de haberse arreglado con arreglos financieros complicados. Las personas que han sufrido olas de crisis financieras están acostumbradas a la volatilidad. Las personas que han pasado años confiando en los costosos intermediarios y moviéndose de un lado a otro entre dólares y su moneda de origen probablemente tengan más probabilidades de comprender las ventajas de bitcoin y superar sus fallas. "Recuerdo que una vez estuve en el Caribe cuando una anciana me sorprendió al negociar un precio en tres monedas diferentes", dice Pelle Braendgaard, cuya firma Kipochi ha desarrollado una billetera bitcoin móvil dirigida directamente a los países en desarrollo. "La gente común en estos mercados puede hacer cosas que nosotros aquí en los Estados Unidos, Europa o Canadá encontramos que son bastante difíciles".

Otra característica de las economías en desarrollo que los hace abiertos a este tipo de cambio es que tienen una proporción mucho mayor de personas que trabajan por cuenta propia, es decir, una clase empresarial mucho más activa. Desde operadores de puestos de comida hasta conductores de rickshaw, los propietarios de pequeñas empresas son un pilar de las economías de mercados emergentes, y para estas personas la capacidad de ahorrar costos en las transacciones financieras podría marcar una gran diferencia en su rentabilidad. Igualmente importante, crea oportunidades para la expansión. Una costurera que trabaja en los mercados locales en Dhaka, Bangladesh, puede ampliar su línea de productos si ahora puede enviar dinero a un productor de telas en Chittagong, a 160 millas de distancia. Y si puede encontrar compradores extranjeros dispuestos a pagarle en bitcoin, de repente tiene un medio para recibir ingresos de exportación.

Si bien las carreteras y otras formas de infraestructura deben desarrollarse también, bitcoin, al abordar el sistema de pago, promete abordar al menos un área defectuosa de la infraestructura. Eso a su vez podría impulsar el cambio en las otras áreas al liberar riqueza para lidiar con ellas. Lo más importante es que las tecnologías de comunicación han recorrido un largo camino en el mundo en desarrollo. Vaya a un cibercafé en un polvoriento pueblo del altiplano en Bolivia, el país más pobre de América del Sur, y puede que encuentre que la conexión es más rápida que en la mayoría de los hogares estadounidenses o europeos. En muchos casos, estos países omiten virtualmente la tecnología heredada, yendo directamente a los cables de fibra óptica de alta tecnología. Una explosión de la telefonía inalámbrica ha llevado la capacidad de las telecomunicaciones a las zonas rurales y barrios marginales que, de otro modo, quedarían excluidos de la instalación de esos cables. Ericsson ConsumerLab estima que África subsahariana por sí sola tenía 635 millones de suscripciones de teléfonos móviles a fines de 2014, o dos tercios de la población. En comparación, solo el 20 por ciento de los adultos africanos tienen cuentas bancarias. Como lo demuestra el proyecto 37Coins, y otros que exploraremos a continuación, incluso las versiones básicas de estos teléfonos ofrecen una plataforma rudimentaria con la que

ingresar a una red global de criptomonedas. Y la tecnología se está volviendo más accesible todo el tiempo: las billeteras bitcoin son cada vez más fáciles de usar y los teléfonos inteligentes más baratos. Mozilla, la compañía detrás del navegador Firefox, ahora está vendiendo teléfonos inteligentes muy básicos en países en desarrollo con precios tan bajos como $ 25.

Por lo tanto, hay muchas promesas aquí, pero como en los países desarrollados, las grandes barreras permanecen en los países en desarrollo para el despliegue de criptomonedas. Algunos tienen que ver con los defectos y riesgos de Bitcoin; algunos reflejan prácticas sociales y culturales que son difíciles de cambiar. Las personas sin mucho dinero desconfían naturalmente de una nueva forma de pago arriesgada en una moneda que no todos aceptan y de la que muchos nunca han oído hablar. Muchas personas favorecen los métodos probados y practicados para evitar la inestabilidad financiera: efectivo bajo colchones, joyas de oro, dólares. Pagar a Western Union hasta en un 11 por ciento para que transmita dinero a familiares en el extranjero puede ser molesto, pero siempre ha funcionado. Y hay desafíos regulatorios. Al igual que en los países desarrollados, los funcionarios podrían crear obstáculos de licencia para los intercambios de divisas digitales y otros servicios necesarios para una integración más fluida de las criptomonedas. La corrupción y el poder de cabildeo de los intereses de los amigos pueden hacer que ese proceso sea impredecible.

Todo eso fomenta el mismo problema de huevo y gallina que enfrentan las criptomonedas en los países desarrollados: si muy pocas personas están dispuestas a usar bitcoin, todos los demás estarán menos dispuestos a recibirlo. Al menos para empezar, las personas necesitarán una infraestructura que les permita convertir monedas digitales a monedas locales o dólares, lo que significa intercambios de bajo costo, corredoras de bolsa y cajeros automáticos bitcoin. Varias personas en la comunidad bitcoin están trabajando solo en estos temas. En ninguna parte, sin embargo, las promesas y las trampas de las criptomonedas son más duras que en la nación más poblada del mundo: China.

China es un mercado tentador para bitcoiners, como lo es para casi todos los empresarios. En teoría, el atractivo de las criptomonedas independientes para los ciudadanos chinos es convincente. Prometen una ruta de escape para su ahorro de $ 12 trillones de ahorros atrapados en los bancos chinos, donde obtienen tasas de interés demasiado bajas para cubrir la inflación. Las leyes chinas limitan su capacidad para comprar o vender divisas y les ofrecen vehículos de inversión alternativa limitados. Los ahorradores atrapados de China subsidian a los especuladores inmobiliarios y las empresas estatales corruptas, facilitando un tren de gracia de préstamos bancarios artificialmente baratos que está levantando el espectro de una crisis de deuda china para rivalizar con los de Estados Unidos y Europa. Con el bitcoin, según la teoría, la gente podría eludir ese sistema bancario injusto y sacar su dinero de China a bajo costo.

Si bien China tiene una comunidad grande y entusiasta de inversores y mineros de bitcoins, la demanda de bitcoin como herramienta práctica para el comercio o para transferir fondos simplemente no se ha materializado. Los pocos comerciantes que lo aceptan se concentran entre las empresas que prestan servicios a la comunidad bitcoin, como Cheku Café de Beijing, que alberga encuentros de bitcoin, y algunos fabricantes de equipos de minería de bitcoin con sede en Shenzhen. Bitcoin en China es puramente un juego de especuladores, una forma de apostar en su precio, ya sea a través de una de una serie de intercambios en China continental o mediante su explotación. Es popular: los volúmenes comerciales chinos superan a los que se ven en cualquier otro lugar del mundo. La demanda de China fue el principal factor detrás de la escalada vertical de bitcoin a un máximo de más de $ 1.100 en diciembre de 2013, y se ha estimado que la actividad minera en China representa el 30 por ciento de toda la potencia de hash. (Eso podría cambiar si se eliminan los subsidios a las centrales de carbón, lo que aumenta el costo de la electricidad). Pero, nuevamente, todo se trata de especular. Mientras que muchos capitalistas de riesgo miran a

China, y unos pocos están invirtiendo en intercambios locales de bitcoin y en operaciones mineras, casi no se invierte dinero de capital riesgo o VC en empresas comerciales o procesamiento de pagos.

Las reglas ambiguas del gobierno no ayudan. Bitcoin no está prohibido en China, pero tampoco se le otorga la legitimidad de la regulación, y se ha desalentado a los medios de comunicación para que lo escriban a través de un régimen de censura centralizado. Cuando se combina con las restricciones del banco central sobre las compañías financieras, eso crea un catch-22 para las empresas de bitcoin, dice Bobby Lee, CEO de BTC China, que se convirtió en el intercambio de bitcoin más largo del mundo después del colapso de Mt. Gox. "Pusieron a las compañías de pagos en la categoría de compañías financieras a las que no se les permite tocar Bitcoin", dice Lee. "Se nos permite tocar Bitcoin, pero por definición no podemos solicitar una licencia de pagos". ¿Debería seguir adelante y crear un procesador de pagos bitcoin sin licencia? "Eso no está claro", dice.

Pero no son solo las reglas que evitan que los chinos realicen pagos en bitcoin. También hay pocos incentivos financieros. La red de tarjetas de pago UnionPay controlada por el gobierno está diseñada deliberadamente para incurrir en tarifas de transacción bajas, por lo que los pagos con tarjeta son más atractivos desde el punto de vista financiero tanto para consumidores como para proveedores que Bitcoin, que conlleva el costo adicional de riesgo de volatilidad. Además, ya existe un sistema dinámico y conveniente de dinero digital en torno a los proveedores de comercio electrónico basados en renminbi. La omnipresente aplicación de mensajería WeChat de Tencent Holdings, que cuenta con alrededor de 400 millones de suscriptores de teléfonos inteligentes y que, según parece, todas las personas chinas que conoce lo consultan constantemente, tiene su propia herramienta de pagos digitales fácil de usar. Con WeChat, puede enviar dinero instantáneamente a sus amigos, pagarle a los taxistas o comprar cosas en máquinas expendedoras. Este servicio, así como la oferta competidora de Alipay de e-marketplace Alibaba, están ayudando a convertir a China en la economía de comercio electrónico más dinámica del mundo. ¿Cómo está compitiendo Bitcoin con eso?

Pero, ¿qué hay del potencial para evitar los controles que el gobierno impone a las transferencias de fondos transfronterizas? Bueno, existe una alternativa más conveniente que bitcoin para eso, también, personificada por un hombre que se presentó a nosotros como "Mr. Fei, "un cambista de mercado negro en el distrito de Gubei de Shanghai. El Sr. Fei pasa sus días con un colega acampado en una acera justo en frente de las sucursales del Banco Industrial y Comercial de China y el Banco de China. A la vista de los guardias de seguridad y el personal de los bancos comerciales estatales, el Sr. Fei abiertamente maneja su comercio ilegal, cambiando monedas por efectivo en la calle. Nos citó 6.16 renminbi por dólar para cambiar $ 200 por moneda local, una tasa mejor que la cifra de 6.12 que se cobra en el aeropuerto. Dijo que para una compra en renminbi de $ 150,000, la tasa sería de 6.18. En ese caso, transferiríamos el dinero a su asociado en Hong Kong, y él personalmente entregaría el equivalente en moneda china en la forma que prefiramos en Shanghai. También podría hacer lo contrario, si lo deseamos, aceptando renminbi en Shanghai para liberar dólares en Hong Kong. Mientras hablábamos, el socio del Sr. Fei completó un trato con una mujer bien arreglada que compró 720,000 won surcoreanos con aproximadamente 4,000 renminbi. Un contacto nuestro en Shanghai dijo que usa los servicios del Sr. Fei con frecuencia y que tiene absoluta confianza en él.

El valor que el Sr. Fei proporciona a sus clientes proviene no solo del mejor tipo de cambio, sino también de la conveniencia. El gobierno limita a cada ciudadano chino a compras de $ 50,000 en moneda extranjera por año. Eso puede parecer una cantidad decente, pero para decenas de millones de residentes chinos recientemente ricos que desean invertir en propiedades en Singapur o enviar niños a la universidad en los Estados Unidos, es una restricción onerosa.

Además, cada vez que quieren cambiar dinero, deben entregar montones de documentos para demostrar su identidad, nacionalidad, derecho al trabajo, recibos de impuestos y fuente de ingresos, todo para que el gobierno pueda controlar su moneda extranjera. actividad. El Sr. Fei hace que todo se vaya. Pobres vacíos bien conocidos como este -otros incluyen el uso de una tarjeta UnionPay para comprar fichas denominadas en dólares en los casinos de Macao- parecen ser tolerados por el gobierno. Miles de Sr. Feis están en todas las ciudades costeras de China. Con alternativas como esa, bitcoin en China comienza a parecer una solución en busca de un problema.

Un escenario que podría fomentar la aceptación china de la criptomoneda sería una crisis bancaria, una amenaza que los economistas toman en serio y que algunos ven como el mayor riesgo que enfrenta la economía global. Explotando el modelo de tasa de interés controlado que penaliza a los ahorradores, los bancos han acumulado imprudentemente billones de deudas en renminbi con los municipios y los desarrolladores que seguramente irán mal. Cuando eso suceda, el gobierno probablemente rescatará a los bancos más grandes del país como lo hizo cuando sus deudas se volvieron demasiado difíciles de manejar en el 2003, pero esta vez es probable que permita que algunos bancos pequeños y medianos y compañías fiduciarias fallen. Después de todo, el Banco Popular de China ha declarado planes para liberalizar las tasas de interés y abrir los bancos a la competencia extranjera. Ha marcado planes para un moderno plan de seguro de depósitos para facilitar esa reforma a un costo mínimo para los depositantes. Este cambio hacia un modelo más dirigido por el mercado es necesario para que China logre sus aspiraciones internacionales de que el renminbi rivalice algún día con el dólar, pero también significa que la rentabilidad de los bancos no tendrá que pagar y tendrá que pagar un precio por el mal. inversiones. La pregunta es, si se permite que un banco falle, ¿qué señal enviará a los ahorradores chinos sobre el sistema financiero basado en el renminbi de su país? ¿Podrían entonces calentar a Bitcoin?

"Muchas personas en los EE. UU. No confían en los bancos debido a la crisis de 2008. Saben que un banco puede hundirse. Pero en China es una atmósfera diferente ", dice Eric Gu, que dirige una reunión de bitcoins en Shanghai. "Si hay alguien que ha experimentado una falla bancaria, probablemente tenga más de setenta años. Pero personas como las de la generación de mi padre nunca vieron una quiebra bancaria. Y esta es la razón por la cual los chinos confían en los bancos. Creen que el dinero en el banco es el más seguro ". Gu sabe que cuando lleguen las quiebras bancarias" va a ser doloroso "y se pregunta si esto podría cambiar las actitudes de la gente hacia el sistema bancario y generar más interés en el bitcoin. Señala que aquellos que están interesados en bitcoin por algo más que una inversión especulativa son personas como él que han vivido en el extranjero (Gu vivió durante siete años en Toronto) o que al menos tienen un título universitario. "Lo entienden", dice.

El Caribe es otra área del mundo de los mercados emergentes donde se puede presentar un argumento sólido para que los locales utilicen el bitcoin para sortear un sistema financiero restrictivo. Pero al igual que en China, las criptomonedas enfrentan desafíos específicos, pero muy diferentes. Si pueden superar esas barreras hace que la región sea un caso de prueba útil.

"Intenté todo", dice Jamal Ifill, sentado en el escritorio que también funciona como su oficina y espacio de trabajo en su pequeño estudio de vidrio en Bridgetown, Barbados. "Tarjetas de crédito, PayPal, Western Union. Son muy caros ".

Ifill, una artista joven y de voz suave, con la cabeza llena de pelo rapado y una cálida sonrisa, ha estado soplando vidrio en Barbados durante once años y ha tenido su propio estudio / sala de exposición de una habitación durante cinco años. Él hace cosas absolutamente increíbles con el vidrio; él puede hacer estallar un colgante de mármol perfecto con una flor azul dentro con un pistilo rojo. Una de sus últimas piezas es una lámpara de celosía rectangular de dos pies de altura

que para nuestros ojos de Nueva York parecía una de las Torres Gemelas. Ifill llama a su perfección imperfecta y dice que si miras con cuidado, puedes ver las imperfecciones (no podríamos) en una capa externa y una capa interna. Él vende su obra de arte localmente y ha atraído algo de atención; una pieza que hizo fue presentada a la Princesa Anne cuando visitó la isla en 2011. Quiere expandirse internacionalmente al mercado de los EE. UU., pero la logística y los costos de trasladar el dinero desde allí hasta allí son prohibitivamente altos, por lo que la mayor parte de su negocio permanece local.

Barbados es relativamente acomodado. Con $ 25,000, el PIB per cápita de la isla es más alto que el de Grecia y no muy por debajo del de España. La alfabetización de Barbados es del 99 por ciento y su tasa de pobreza, del 14 por ciento, es un punto más baja que la de los Estados Unidos. Comparte mucho en común con Jamaica, Trinidad, Bermudas y otras naciones insulares de las Indias Occidentales Británicas. Hablan el mismo idioma y comparten un pasado colonial cuya historia volátil está repleta de batallas navales, piratas, esclavitud, comercio de ron y rebelión. Las Antillas incluso se unen para formar un equipo internacional de cricket cuando juegan contra Inglaterra, Australia y otros miembros de la Commonwealth. Lo que no tienen, sin embargo, es una moneda común que podría mejorar el comercio entre las islas.

Prácticamente todas las naciones de las Indias Occidentales Británicas tienen su propia moneda, impresa por separado, cada una llamada dólar, cada una fluctuando en valor frente a las demás y frente al dólar estadounidense más conocido. Y las antiguas colonias españolas, holandesas y francesas tienen sus propios pesos, florines y gourdes. Los gobiernos de la región han hablado durante mucho tiempo sobre la creación de una unión monetaria para profundizar el acuerdo de libre comercio de la región, el mercado común de Caricom. Pero al igual que con el desarrollo de esa zona de libre comercio, el avance hacia la construcción de una autoridad monetaria única y las otras instituciones necesarias para una moneda común ha sido irregular. Un dólar caribeño sigue siendo una quimera.

Debido a esto, transferir dinero a las naciones insulares de la región requiere intercambios monetarios constantes y costosos, lo que socava aún más las relaciones comerciales que ya están limitadas porque sus economías pesadas en turismo, finanzas y productos básicos compiten entre sí y no se complementan entre sí. Para empeorar las cosas, una serie de bancos centrales imponen controles de capital a sus ciudadanos. Los barbadenses como Ifill, por ejemplo, están limitados en la cantidad de divisas que pueden comprar. Que Barbados, las Islas Caimán, las Bahamas y otras naciones del Caribe sirvan como paraísos fiscales para fondos de cobertura y otras instituciones financieras extranjeras es una ironía que no se pierde en los residentes estrictamente controlados de la región. Esta mezcla de sistemas monetarios y regulaciones financieras, y la frustración que genera, hacen que las islas soleadas del Caribe maduren para el bitcoin, o eso dice Gabriel Abed.

Los amigos lo llaman el Sr. Bit, y no está claro si el sobrenombre es serio o como una broma juguetona. Educado en los Estados Unidos, Abed es un emprendedor itinerante, un joven con una energía ilimitada que dirige tres compañías diferentes mientras hace planes para otros y descarta planes para otros y que se concentra en una idea revolucionaria: llevar el bitcoin al Caribe.

Abed, de veintisiete años, proviene de una prominente familia barbadense de origen sirio. La mayoría de los miembros de su familia extendida han ido a empresas prósperas; no es raro ver a los compradores caminando por Swan Street en Bridgetown con bolsas colgando de sus brazos impresos con ABED, la tienda minorista del mismo nombre propiedad de un pariente. Hubiera sido fácil para él seguir esos pasos. Pero estudió TI en la universidad, con un enfoque en la criptografía. No estaba interesado en instalarse en un punto de apoyo tecnológico como Silicon Valley o Portland, aunque trabajó en este último por un corto tiempo. Él quiere estar en su querido Barbados, y quiere llevar su isla a la era digital.

Abed recurrió a las criptomonedas como la respuesta a un problema: cómo expandir el comercio electrónico. Él es el CEO de Web Designs, una empresa local que vende registros de dominios de Internet, diseños de sitios web, mantenimiento y plataformas de comercio electrónico. La última ha sido una venta particularmente difícil. Debido a los costos de divisas y tarjetas de crédito y PayPal, que pueden sumar hasta un 8 o 9 por ciento, dijo, la mayoría de los comerciantes simplemente evitan vender en el extranjero.

Abed se enteró de Bitcoin desde el principio y vio su potencial para resolver este problema. Comenzó con la idea de una criptomoneda caribeña, a la que apodó CaribCoin, pero se dio cuenta rápidamente de que era un proyecto más grande de lo que él quería asumir. Se centró en la idea de un intercambio de bitcoins, y un servicio comercial que podría combinar con su servicio de diseño web y alojamiento, y comenzó a construir Bitt (la URL es en realidad bi.tt, siendo el dominio .tt para la vecina Trinidad y Tobago). También comenzó a extraer sus propios bitcoins, en Trinidad, aprovechando los costos de electricidad relativamente bajos allí, y utilizando los beneficios de eso y de los diseños web para financiar a Bitt.

Bitt está diseñado como un servicio comercial y de intercambio en línea centrado en el Caribe, que ofrece transacciones entre diferentes monedas cifradas y monedas fiduciarias, así como un módulo para ayudar a las empresas locales a adoptar monedas digitales para el pago. Su atractivo para las empresas es simple: ¿qué pasa si puedo darle una opción de pago que cuesta solo 1 por ciento?

Es fácil en Bridgetown o en la Bahía de Mantego o en Puerto España recoger algo de fruta de un árbol -cocos o ackee, tal vez- establecer un puesto en la carretera, y vender sus productos. Es mucho más difícil establecer un negocio legítimo orientado al cliente, o incluso comercial, y ofrecer todo lo que un negocio moderno debería hacer. En los países desarrollados, los bancos suelen ofrecer estos servicios, desde el procesamiento de pagos hasta las líneas de crédito y la gestión del fraude. Pero en Barbados, dice el Dr. Leroy McClain, director general de Barbados Investment Development Corp., los bancos nos "venderán una tarjeta de crédito para que podamos gastar dinero, pero no nos darán servicios comerciales para que podamos". vender productos. "Se reunió con Abed para explorar formas de ayudar a la joven compañía y, esperaba, a la isla de manera más amplia. Desde el punto de vista de McClain, los grandes bancos internacionales están felices de proporcionar servicios de banca comercial a compañías en los Estados Unidos y Canadá, pero hacen que las empresas de la isla salten a través de muchos más obstáculos para los mismos servicios.

Jamal Ifill, el soplador de vidrio, entiende el problema demasiado bien. De hecho, él tiene todos los problemas de un negocio internacional. El vidrio particular que usa debe importarse de Ucrania. Sus clientes no solo están en la isla, sino en el extranjero. Está compitiendo con artistas extranjeros que no están paralizados por los costos que lo atan. Probó el comercio electrónico, a través de la empresa de diseños web de Abed, pero se dio por vencido porque no había suficientes clientes que lo usaran, lo que significaba que no estaba obteniendo ningún negocio de él. Un círculo vicioso. "Incluso probé Etsy", dice, el sitio de arte y artesanía en línea. Una vez más, no pudo competir en costos con artistas de los EE. UU.

Ifill está ansioso por expandir su negocio en el extranjero. Tiene grandes ideas sobre marketing y cómo obtener un poco de prensa para su marca. Pero su ambición está bloqueada. Entonces, cuando Abed entró en su discurso de bitcoins, los ojos de Ifill se iluminaron: ¿una tarifa de 1 por ciento por hacer negocios? ¿A diferencia del 5 por ciento, o el 8 por ciento o el 9 por ciento?

El truco es que la tarifa del 1 por ciento viene con bitcoins, que a partir de este momento no se puede comprar mucho en Barbados. Decir que las criptomonedas no son grandes en Barbados sería una subestimación. Efectivamente no existen en la isla, y tampoco lo hace el comercio móvil. Si bien prácticamente todo el mundo tiene un teléfono celular, la insignia proverbial de un ciudadano digital, la gente lo usa solo para enviar mensajes de texto y hablar. El comercio electrónico apenas está comenzando, al igual que la banca en línea.

La forma de superar el problema de la gallina y el huevo y fomentar la adopción, cree Abed, es centrarse en los comerciantes. Él cree que si puede ofrecerles un método de pago mucho más económico, se les puede convencer de que acepten ese método en sus tiendas. Pero él tiene su trabajo cortado para él.

David Simpson, director general de Prestige Accounting, una escuela comercial regional, y cliente de Web Designs, ve una curva pronunciada hacia la adopción generalizada de bitcoin. "En mi opinión, los bajans no se han acostumbrado a usar la tecnología para facilitarles la vida", dice. "Incluso transfiriendo dinero en línea, prefieren ir a un banco, hacer cola". Cuenta la historia de un banco local que intentó promover la banca en línea; instaló cajeros automáticos y redujo los cajeros en un intento de sacar a sus clientes de las líneas y en línea. Fue contraproducente. Los clientes se rebelaron; no querían conectarse a la banca en línea, en realidad querían esperar en una línea física para hablar con un cajero físico. Los barbadenses simplemente no están interesados en las nuevas tecnologías. Tales actitudes cambiarán, dice Simpson, cuya compañía ha adoptado el comercio electrónico, el uso de libros electrónicos y ofreciendo clases en línea. "La pregunta es cuánto tiempo lleva". En cuanto a su punto de vista sobre bitcoin, es pragmático: "Una vez que los clientes están dispuestos a usar Bitcoin y abrazarlo, soy flexible". Pollo y huevo.

El dilema de la gallina y el huevo requerirá incentivos. La promesa de ahorrar dinero es ciertamente una de ellas. Pero hay otros. Al igual que en el mundo desarrollado, una esperanza es que si las grandes empresas o instituciones cuyas relaciones se encuentran en lo más profundo de la economía comiencen a usar bitcoins, pueden crear incentivos para que sus proveedores y clientes las utilicen.

Patrick Byrne, CEO de Overstock.com, minorista en línea con sede en Salt Lake City, que comenzó a aceptar bitcoin a principios de 2014 para convertirse en el que era el mayor comerciante que gana ingresos, cree que su empresa puede desempeñar un papel tan catalizador creando una bitcoin "ecosistema" en el mundo en desarrollo. La creencia de Byrne en el bitcoin se forjó durante la crisis financiera, cuando los fondos de cobertura comenzaron a vender en corto las acciones de Overstock, una práctica en la que los valores prestados son objeto de dumping en el mercado para obtener ganancias cuando caen a un precio inferior. Los fondos de cobertura dijeron que no confiaban en la contabilidad de la compañía; Byrne lo vio como una especulación puramente manipuladora, todo facilitado y alentado por los sistemas centralizados de Wall Street para comprar, vender, prestar y tomar prestados valores. La criptomoneda, él cree, es un arma para combatir esto porque reúne compradores y vendedores dispuestos de activos, sin que los corredores y los bancos de inversión actúen como intermediarios que cobran honorarios. Es un instrumento, cree, para reformar un mundo que se ha vuelto demasiado dependiente de tales instituciones centralizadas y que, por lo tanto, se ha vuelto propenso al "autoritarismo" de élites privilegiadas en los mundos del gobierno y las finanzas. Overstock trabaja con proveedores en ochenta países diferentes, y entre sus proveedores hay cientos de pequeños empresarios de bajos ingresos que contribuyen a Worldstock, el sitio secundario de Overstock para productos artesanales de "comercio justo". Comprende artesanos, gente como el soplador de vidrio Jamal Ifill, que vive en cincuenta y cuatro países en desarrollo, que están ávidos de un sistema financiero más justo que el modelo de pago obsoleto y costoso al que están actualmente obligados.

Cuando nos reunimos en junio de 2014 en Utah, Byrne explicó que veía el bitcoin como una forma de ampliar las oportunidades económicas, si tan solo lograba que la gente lo aceptara. Todavía estaba descifrando las zanahorias que usaría, pero tenía algunas ideas. Él habló animadamente; un colgante de rueda de dharma que había obtenido de monjes tibetanos cerca de la residencia del Dalai Lama en el norte de la India se balanceaba hacia atrás y hacia adelante desde una correa de cuero alrededor de su cuello. "Si podemos hacer que los proveedores lo acepten, tal vez les demos un dos por ciento extra si les pagamos en bitcoin, o un uno por ciento extra, o tal vez los paguemos en diez días netos o quince días netos en lugar de treinta. Eso nos costaría quince días, pero el bitcoin permite esa liquidación rápida. Y usted sabe que en el mundo de los pagos y el trato con los vendedores, existe toda esta sensibilidad en torno a los términos de pago. Los vendedores a veces le darán un descuento del dos por ciento por afeitarse veinte días, porque para ellos es como un costo de dinero del treinta y seis por ciento durante el año. Eso afecta todo tipo de cosas. El solo hecho de que los proveedores ofrezcan esos términos significa que hay una enorme oportunidad para que bitcoin avance en esta área ". Unas semanas después, Byrne anunció que no solo pagaría a los proveedores que aceptaban bitcoin una semana antes, sino que también lo haría. pagar sus bonos de empleado en bitcoin.

Lo que las compañías como Overstock están tratando de hacer con los pagos en moneda digital tiene un paralelismo con lo que Walmart logró al innovar la tecnología de las comunicaciones para revolucionar la administración de la cadena de suministro en la década de 1990 y principios de la de 2000. El minorista con sede en Arkansas desarrolló una sofisticada red con la que conectar a todos sus proveedores en todo el mundo en una única base de datos integrada para administrar los bienes y servicios que entran y salen de los almacenes de Walmart. Junto con las grandes mejoras en la logística de envío, esto permitió a la compañía optimizar su administración de inventarios justo a tiempo, lo que redujo drásticamente sus costos. Walmart aprovechó esos ahorros en los precios más bajos en cualquier lugar de los Estados Unidos, lo que lo convirtió en el icónico y, para algunos, infame gigante que ahora domina los suburbios estadounidenses. Igualmente importante, su red de alta tecnología tuvo un efecto de retroalimentación en los proveedores, lo que contribuyó a la concentración de la fabricación en centros como el delta del río Perla en China. A medida que Walmart se convirtió en un cazador cada vez más poderoso pero implacable de las fuentes de fabricación más baratas, y mientras otros compradores occidentales alcanzaban su liderazgo en alta tecnología, las fábricas que pagaban bajos salarios en el mundo en desarrollo se congregarían en lugares donde era más eficiente acceder a Walmart. red. Byrne ahora ve oportunidades similares para que firmas como la suya generen influencia aprovechando el bitcoin en sus relaciones de pago internacionales y así creando un punto de inflexión desde el cual el cambio comienza a afectar la economía mundial. A medida que un grupo de empresas en una región comienza a adoptar la moneda, será más atractivo para otras personas con las que hacen negocios. Una vez que se construye una red de negocios entrelazados, nadie quiere ser excluido de ella. O eso dice la teoría.

"Así como el minorista estadounidense colapsó en Walmart, ¿quién sabe cuánto puede colapsar en nosotros? Y no me refiero a Overstock. Me refiero a bitcoin ", dijo Byrne. "Comienzas a obtener efectos de red. Está incentivando a todos, es como si tuviéramos la primera máquina de fax pero nadie más tiene una máquina de fax, por lo que no le sirve de nada. Pero comienzas a agregar otros nodos y a crear incentivos para agregar nodos y, finalmente, obtener una masa crítica. Ahora las personas no solo nos envían un fax, sino que se envían por fax ".

"No tengo compasión por estas mujeres en Afganistán", dice Francesco Rulli desde detrás del bar en el que entretiene a los visitantes del loft encalado de su empresa en un edificio del centro de Manhattan. "Solo tengo un enfoque matemático al respecto". No es cierto lo que dice sobre la compasión, al menos no en el sentido habitual de la palabra. A Rulli parece preocuparle profundamente el bienestar de las mujeres jóvenes en este país del Medio Oriente devastado por

la guerra que ahora está siendo educado en computación y medios a través de la fundación que estableció en conjunto con su compañía de medios. Pero con esta declaración enfática, Rulli está haciendo un punto filosófico sobre las cualidades de empoderamiento de bitcoin. Al igual que Byrne de Overstock, él está desempeñando un papel de activista, explotando su control sobre las cuerdas del bolsillo para alterar el comportamiento de las personas, animándolas a usar criptomonedas para liberarse.

El Women's Annex, con sede en Afganistán, es una filial sin fines de lucro de la firma con fines de lucro Rulli Film Annex, que ahora usa el nombre comercial Bitlanders, un sitio de contenido de video en línea que comparte sus ingresos publicitarios con un ejército mundial de bajos ingresos. cineastas de presupuesto. Rulli se inspiró para crear la fundación después de ver un video producido por la OTAN en su sitio sobre Roya Mahboob, el CEO de Afghan Citadel Software Company. Él se acercó a ella sobre la creación de una escuela, y ahora la empresaria diminuta, que en 2013 se incluyó en la lista de la revista Time de las cien personas más influyentes del mundo, encabeza la fundación Women's Annex. Con la cofundadora Fereshteh Forough, quien, al igual que Mahboob, nació en Irán como refugiada afgana, administra un incipiente cuerpo estudiantil de más de cincuenta mil adolescentes en once escuelas de Afganistán con un programa que ahora se está globalizando.

Muchas de las mujeres en el programa nunca habrían visto una computadora antes de unirse a la escuela; ahora están aprendiendo cómo publicar blogs, producir películas, escribir códigos de computadora y desarrollar estrategias de redes sociales. Su educación está en la moneda de diez centavos del Anexo de la Mujer, pero muchos estudiantes, más de seis mil de ellos, también obtienen ingresos del contenido que proporcionan a los bitlandeses con fines de lucro. Allí, su trabajo es juzgado, como el de cada colaborador, por los editores y se analiza en términos de qué tan ampliamente se ve y se comparte. Estos criterios forman su puntaje "Buzz", que determina la cantidad de ingresos que pueden ganar. Esas ganancias, como con cualquier otro colaborador de Bitlanders, se pagan en bitcoin. Conocimos a una de estas colaboradoras, Parisa Ahmadi, en la apertura de este libro.

La decisión de pagar a los contribuyentes de películas en una moneda digital inevitablemente provocó algunas quejas en todo el mundo entre las viejas manos del Film Annex. Pero tenía una lógica. La compañía hace millones de dólares en pagos en transferencias frecuentes de pequeña denominación. Con su capacidad de micropagos y bajas tarifas de transacción, bitcoin podría ahorrar dinero a la compañía en sus múltiples transferencias bancarias y costos de cambio, lo que a su vez dejaba más que compartir con los trescientos mil contribuyentes cinematográficos de Film Annex. Pero otro beneficio más profundo fue que este método de pago tuvo un profundo efecto de empoderamiento para las clientas afganas del servicio, que podrían usarlo para sortear las restricciones de su sociedad patriarcal.

"Pensamos que tal vez todos los estudiantes deberían tener una cuenta bancaria para poder transferir dinero de la cuenta bancaria de [Women's Annex], pero el problema era que las estudiantes no podían tener una cuenta bancaria hasta que tenían dieciocho años, y la mayoría de sus familias prefirieron que las chicas no tengan una cuenta bancaria en absoluto ", dijo Mahboob. Además, los viajes a sucursales bancarias y puntos de envío de remesas como Western Union estaban plagados de peligro y discriminación. La propia Mahboob no era inmune a esto. "Fue muy difícil en Afganistán cuando tenía dinero en efectivo, y especialmente cuando el dinero tenía que ir a su cuenta bancaria. La gente siempre se daría cuenta de que su cuenta bancaria tenía dinero entrando y saliendo; las personas que están en los bancos le dirían a las personas que están fuera de los bancos. Siempre tuve que ir al banco con algunos de mis colegas, con cuatro o cinco hombres para tomar el dinero y darles el dinero a los estudiantes ". Para las niñas afganas de las escuelas de Women's Annex, el bitcoin resolvió esos problemas, incluso si creado otros.

Rulli primero se interesó en Bitcoin a mediados de 2013 cuando se enteró de la inversión masiva en la moneda digital por Tyler y Cameron Winklevoss. La criptomoneda se convirtió rápidamente en una pasión permanente, un vehículo a través del cual Rulli pudo seguir la filosofía del empoderamiento personal que surgió de sus experiencias como maestro de judo de cinturón negro. A Rulli, el pelirrojo, le gusta hacer referencia a los banqueros renacentistas y de los Medici de su Florencia natal y cita con humor una cita de Spider-Man: "con gran poder, viene una gran responsabilidad", como un motivo para vivir. Desde esta perspectiva, ve el bitcoin como una fuerza para construir "ciudadanía digital", una nueva sociedad dedicada a la búsqueda personal de la excelencia, donde todos son valorados por lo que él o ella crea. Bitcoin permitió que Film Annex ajuste su concepto de puntaje de Buzz con tanta precisión, dice Rulli, que podría usarse como un motivador continuo de mejora personal. Con Bitcoin, "se puede desglosar claramente el valor de cada golpe en el teclado", dice. "Por lo tanto, incluso si crees que puedes producir contenido de baja calidad por un momento, decepcionarás a los moderadores, tu puntaje de Buzz disminuirá y dañarás tu reputación a largo plazo y, en consecuencia, tu largo ingreso a término ".

El problema básico, sin embargo, es que si las opciones para gastar bitcoin son limitadas en los Estados Unidos, Afganistán es un desafío de otro orden de magnitud. Una solución que el Film Annex ahora persigue junto con la plataforma de comercio de bitcoin Atlas ATS es una central con sede en Pakistán para intercambiar bitcoins en monedas tradicionales. Pero Rulli solo aceptó a regañadientes con esto; era una opción demasiado suave, sintió. Quería que el intercambio fuera únicamente en bitcoins para otras monedas digitales, sin opción de comprar rupias o dólares: "La creencia que tengo es que si encerras a estas personas en esta nueva economía, harán que esa nueva economía sea lo más eficiente posible . Si comienzas a darle a las personas la oportunidad de salir de la economía, simplemente lo reducirán, mientras que si la única forma de enriquecerte es intercambiando bitcoins por litecoins y dogecoins, te convertirás en un experto en eso ... se convertirá en el mejor comerciante en Pakistán ".

Rulli prefiere centrarse en otra ruta que Film Annex ha seguido para dar opciones de gasto a sus contribuyentes. Usando su tarjeta American Express personal, aprovechando así un historial de crédito que las niñas afganas nunca podrían tener, compra tarjetas de regalo de Amazon, minutos prepagos de teléfonos celulares y varios otros productos fáciles de entregar y luego los ofrece a la venta a través del sitio web de Film Annex. . La cuenta de cada colaborador no solo muestra el saldo ganado, sino también una selección de productos que tienen suficientes bitcoins para comprar. Él quiere que las chicas afganas lo gasten en tecnología como el próximo teléfono inteligente de $ 25 de Mozilla, que pueden convertir en una cámara y una herramienta para producir mejores videos y contenido de blogs. Está tratando de convertir el sitio web de Film Annex en su propia economía de bitcoin.

La imagen que muchos tienen de las niñas en Afganistán proviene de una única y famosa foto: Afghan Girl. Tomado en 1985 por el fotógrafo de National Geographic Steve McCurry, muestra a una niña de doce años con un pañuelo rojo hecho jirones en un campo de refugiados en Pakistán, sus ojos verdes en una expresión de desafío. La difícil situación de la mayoría de las mujeres afganas quizás ya no sea tan desesperada como la de esa niña refugiada, pero incluso con la expulsión de los misóginos, los talibanes medievales y la nueva estructura social introducida bajo la ocupación estadounidense, Afganistán sigue siendo una sociedad dominada por hombres. Las mujeres son ciudadanas de segunda clase. La mayoría no tiene dinero propio y no se les permite viajar afuera sin un miembro masculino de la familia que los acompañe. ¿Pueden liberarlos Francesco Rulli, Film Annex y Bitcoin?

"Estoy en contra del bienestar", dice Rulli. "Les estamos enseñando a ser sus propios empresarios". Y agrega: "Mi lógica es, ¿cómo puedo asegurarme de que las niñas estén a salvo? ...

[Si está ganando dinero], es más probable que sus hermanos la protejan porque ella es un activo para la familia en lugar de un ciudadano de segunda clase ... Entonces, finalmente, la prioridad de la familia no es solo protegerla sino también invertir en ella".

Según Mahboob, los miembros de la familia del Anexo Femenino están volviendo a esta forma de pensar: "Al principio, la mayoría de las familias no querían que las niñas aprendieran Internet; estaban en desacuerdo porque pensaban que Internet era algo muy malo. Pero cuando comenzaron a ganar dinero, las familias los apoyaron. Y luego otras familias apoyaron a sus hijas. Así que no solo tenemos a las niñas en la escuela, sino que tenemos a la comunidad detrás de ellas".

En los Estados Unidos, los procesadores de pago de bitcoin como BitPay y Coinbase generalmente encuentran que los comerciantes quieren que conviertan sus bitcoins entrantes en dólares, un servicio que proporcionan de forma gratuita. En Argentina, ocurre exactamente lo contrario. Las empresas como BitPagos con sede en San Francisco tomarán los dólares recibidos por los hoteles y otros clientes de la industria del turismo en Buenos Aires y les entregarán bitcoins a cambio. En casi todos los discursos que bitcoiners hacen sobre el potencial de las criptomonedas en el mundo en desarrollo, Argentina recibe la mejor facturación. La esperanza no es solo que el bitcoin tenga éxito allí; es que el país sudamericano demuestra cómo las criptomonedas pueden proporcionar una ruta de escape para las personas atrapadas por los controles de capital en el uso de monedas nacionales no confiables y no deseadas.

El servicio de BitPagos es tan atractivo para muchos empresarios en Argentina porque les da un tipo de cambio mucho más favorable. A mediados de junio de 2014, cada dólar recibido de las compras con tarjeta de crédito tenía que procesarse a través del sistema bancario argentino, donde pagaría 8.15 pesos, una tasa oficial que valora la moneda argentina en aproximadamente doce centavos. Por el contrario, un pago en efectivo podría convertirse a doce pesos por dólar en una cueva clandestina, o cueva, los prósperos negocios que manejan la moneda subterránea de Argentina en Buenos Aires y otras ciudades. En este mercado negro, el peso valía ocho centavos marcadamente más bajos; podrías obtener más de ellos con los dólares que obtienes de los turistas. El problema es que la mayoría de los viajeros en estos días pagan las facturas del hotel con una tarjeta de crédito. Así que bitcoin ofrece a los comerciantes un camino intermedio. En el sitio de intercambio de persona a persona Local Bitcoins Argentina, la tasa vigente para la venta de bitcoins fue de alrededor de 6.400 pesos a fines de junio de 2014. Con base en la tasa de cambio de bitcoin-dólar de alrededor de $ 560, eso se tradujo en un viaje de ida y vuelta de 11.42 pesos por dólar, una oferta 40 por ciento mejor que la tasa oficial.

En los últimos ocho años, cuando Argentina entró en la última etapa de un ciclo de crisis financieras que se repite cada diez años más o menos, su población ha buscado dólares como cobertura contra la inflación desenfrenada. A medida que la situación se deterioró y el gobierno luchó por obtener los dólares que necesitaba para pagar a los tenedores de bonos extranjeros y los proveedores de energía, la presidenta Cristina Fernández de Kirchner se dobló. Su gobierno hizo cada vez más difícil para los argentinos tener acceso a divisas, a menudo cambiando las reglas día a día para proteger sus reservas. Eso hizo la vida extremadamente difícil para cualquiera cuyo negocio se negoció regularmente en divisas. También es la razón por la cual surgió un mercado clandestino con una tasa mucho más baja para el peso.

Para Mike Abridello, un expatriado estadounidense que dirige Prodeo Hotel & Lounge en el barrio hipster de Palermo Soho, en Buenos Aires, los bitcoins que recibe de BitPagos proporcionan una forma de lidiar con estas regulaciones confusas y mercados de divisas bifurcados. "En este momento, si está trabajando en Argentina, Bitcoin simplemente le ofrece una solución de flujo de caja que es mucho más eficiente", dijo. Algunos de los clientes de BitPagos también ven los bitcoins como una reserva de valor superior al peso. Eso puede parecer una locura, dada la volatilidad del

tipo de cambio de Bitcoin. Pero con la inflación argentina en torno al 30 por ciento en los últimos años -según estadísticas no oficiales que obtuvieron mucho más crédito que los números manipulados por el gobierno- el peso ha sido una apuesta perdedora mucho mayor durante la última década. Tampoco es necesario que los argentinos sean tan viejos para recordar las tasas de más del 10,000 por ciento que ocurrieron durante la hiperinflación de fines de la década de 1980. Para esas personas, "bitcoin es una forma de protegerse contra la inflación", dice el CEO de BitPagos, Sebastián Serrano.

No hay forma segura de medir la adopción de bitcoins en ningún país, pero la evidencia sugiere que Argentina está superando a la mayoría. La cantidad de operadores que cotizan en Local Bitcoins Buenos Aires fue durante gran parte de 2014 tres veces mayor que la de Manhattan, y se sabe que la Fundación Bitcoin Argentina administra la mayor reunión de bitcoins en el mundo. BitPagos ha sido un beneficiario directo de esto. A mediados de 2014, la empresa había contratado a más de seiscientos comerciantes en América Latina, aunque no todos eran muy activos. Y después de haber duplicado sus volúmenes de transacción en tres meses desde marzo de ese año, la nueva empresa había captado una ronda de financiación de $ 600,000 con contribuciones de Pantera Capital Management, el CEO de SecondMarket Barry Silbert y el capitalista de riesgo Tim Draper. Otros también han percibido la oportunidad: el procesador BitPay, con sede en Atlanta, ha abierto una oficina en Buenos Aires, y un nuevo intercambio de bitcoin, Bitex.la, se lanzó en mayo de 2014.

Para estar seguros, la mayoría de los argentinos, recelosos de la crisis, aún deben ocuparse de esta extraña unidad digital, prefiriendo en cambio su refugio seguro durante mucho tiempo: dólares verdes fríos y duros. Aunque a mediados de 2014 el gobierno no tomó medidas regulatorias explícitas contra el bitcoin, el sitio web del banco central emitió una severa advertencia sobre sus peligros, señalando que "las denominadas monedas virtuales" no son emitidas por "este banco central ni por ninguna otra parte". de las otras autoridades monetarias internacionales y por lo tanto no tienen ningún recurso legal y no tienen respaldo ". El riesgo de una represión siempre estuvo ahí. Al igual que con las reacciones violentas en China y en otros lugares, las autoridades podrían hacer esto al impedir las conexiones con el sistema bancario tradicional, al dificultar que las personas vinculen sus cuentas bancarias con intercambios de pesos por bitcoins, por ejemplo. Aún así, al igual que con todo lo relacionado con las criptomonedas, las barreras a la adopción pueden sopesarse contra los costos de no adoptarlas. En Argentina, eso le da a bitcoiners como Serrano un tono aún más convincente que el que Abed hace sobre las tarifas de transacción a los barbadenses: ¿Estás seguro de que quieres seguir con esos pesos argentinos?

El negocio de las remesas, en el que los emigrantes y los expatriados que viven en el extranjero envían dinero a sus hogares, parece como si estuviera listo para la interrupción de las criptomonedas de bajo costo. El modelo comercial actual se basa en transferencias electrónicas a través de los antiguos rieles de la banca, y sus practicantes cobran altas tarifas por ese privilegio. A nivel mundial, es un gran negocio.

Se espera que los emigrantes envíen más de 500 mil millones de dólares a los países de origen en 2016, según el Banco Mundial. "Esos son solo los flujos oficiales", dice Dilip Ratha, un experto en el tema que lo rastrea para el Banco Mundial. Se envían otros $ 200 mil millones que el banco no rastrea, estima. Esos números empequeñecen los aproximadamente $ 125 mil millones que el mundo desarrollado envía anualmente en ayuda. Para muchos países, más dinero ingresa a través de las remesas que a través de las exportaciones. Además, los totales son netos de los cargos y tarifas que los emigrantes pagan a los agentes de transferencias como Western Union; en promedio, esos costos son alrededor del 8,5 por ciento a nivel mundial, pero en muchos países, es alrededor del 10 por ciento o más. En países donde los salarios anuales se pueden contar en cientos de dólares, esos costos son una carga seria.

Los kenianos que viven en el extranjero y desean enviar dinero a su país pueden elegir entre, digamos, Western Union y MoneyGram, pero ambos cobran tarifas altas. Aunque en el 42 por ciento la proporción de adultos kenianos con una relación bancaria formal excede la de muchos países, la mayoría en el país todavía no cuenta con servicios bancarios. Pero la experiencia de Kenia con las microfinanzas y las telecomunicaciones ha inspirado la imaginación de las personas sobre cómo abordar algunos de estos problemas. En particular, la emoción gira en torno a un producto clave: M-Pesa.

M-Pesa (la M es para "móvil" y "pesa" es swahili para "dinero") comenzó como un experimento de la mayor empresa de telecomunicaciones de Kenia, Safaricom. Debido a que muchos más kenianos tenían teléfonos que cuentas bancarias, los expertos en microfinanzas se dieron cuenta durante la década de 2000 que podían usar esos teléfonos para entregar préstamos a los prestatarios y recibir reembolsos de ellos. Por lo tanto, en 2007, Safaricom comenzó un programa piloto que permitía a los usuarios enviar dinero a través de sus teléfonos, convirtiendo de manera efectiva las unidades estándar de minutos de llamadas prepagas en una forma de moneda. El sistema demostró ser tremendamente popular. Hoy en día, dos tercios de los kenianos lo usan, y alrededor del 25 por ciento del PIB de Kenia lo atraviesa. Y Vodafone, que posee el 40 por ciento de Safaricom, ha lanzado el producto en Tanzania, Sudáfrica, Mozambique, Egipto, Fiji, India e incluso Rumania.

Para usar M-Pesa, las personas se registran para obtener una cuenta y obtienen una billetera electrónica en su teléfono. Para agregarle dinero, acude a su agente local de Safaricom -más de quince mil se distribuyen en Kenia- y le dan al agente efectivo por una cantidad equivalente de "e-float". Este dinero no se mantiene en forma de Chelines kenianos, pero como un reclamo separado sobre el e-float general de M-Pesa, todo lo cual está respaldado por depósitos en los bancos con los que cuenta Safaricom. Los usuarios pueden enviar dinero a otros titulares de cuentas de M-Pesa, comprar tiempo aire o pagar facturas. Para retirar dinero, los usuarios acuden al agente y lo retiran. Siempre que tengan una cantidad equivalente de e-float en su cuenta, el agente les entregará el dinero en ese momento.

M-Pesa tenía algunas cosas a su favor. En primer lugar, Safaricom ya contaba con una infraestructura masiva, no solo con los equipos de telecomunicaciones, sino con esos miles de agentes. M-Pesa también tuvo la suerte de escapar de la regulación gubernamental desde el principio. Por último, una forma diferente de política puede haber jugado un papel. Luego de las acaloradas elecciones del país en diciembre de 2007, la violencia estalló en todo Kenia. Se mataron a decenas, y todo el país fue empujado a una crisis. Con las instituciones de la nación esencialmente congeladas, la gente se dio cuenta de que había una forma de mover el dinero de manera efectiva: M-Pesa. Por ejemplo, un grupo de socorro, Concern Worldwide, evitado por la violencia y el costo de obtener ayuda para el remoto Kerio Valley de la región, encontró una solución en M-Pesa. Enviaron representantes al valle y le asignaron cuentas a las personas, dándoles a algunas familias teléfonos y cargadores solares. Dado que el agente más cercano estaba a unos ochenta kilómetros de distancia, también establecieron un agente en una estación de policía local. El gambito funcionó; el grupo pudo obtener ayuda para una comunidad aislada, y el costo de las tarifas de transacción de Safaricom fue mucho menor que el costo del transporte de alimentos y materiales. No solo eso, Concern Worldwide trajo a estos pueblos remotos la tecnología que resultaría útil más allá de la crisis, y la crisis misma mostró el verdadero valor de M-Pesa para sus clientes, que han sido firmemente leales desde entonces.

Un stand de M-Pesa
(© Tom Spender)

M-Pesa ha demostrado ser un salvavidas en otras formas inusuales, también. En su sitio web, Vodafone señala que en Tanzania, donde algunos ciudadanos no viven cerca de un hospital y no pueden pagar uno, una organización llamada Rehabilitación Integral Basada en la Comunidad envió dinero a los pacientes a través de M-Pesa para cubrir sus gastos de viaje. .

Pero aquí está el problema: M-Pesa no es un sistema sin fricción, y de alguna manera sus inconvenientes reflejan los que hemos delineado en el capítulo 4: lo que parece automático para el usuario tiene una infraestructura masiva, difícil de manejar y costosa. Los agentes de Safaricom deben lidiar con enormes cantidades de efectivo diariamente. Esto no solo es engorroso, sino que también puede ser peligroso. Cuando los agentes se quedan sin dinero, tienen que detener lo que están haciendo, cerrar la tienda e ir a un banco, o detener lo que están haciendo y enviar a alguien en su nombre. Los agentes en áreas rurales, donde es más probable que los clientes retiren dinero en lugar de depositarlo, se enfrentan a un desafío especial: no solo se agota más rápidamente su liquidez -su pila de efectivo literal-, sino que hay más probabilidades de que estén más lejos de una sucursal bancaria, lo que significa que un viaje lleva más tiempo y deja menos tiempo para hacer negocios reales.

Luego está la cuestión de cómo importar fondos al sistema M-Pesa desde el exterior. No es sin fronteras Su sistema móvil, vinculado a un teléfono, ofrece una "entrada" más fácil para las remesas que los sistemas financieros más tradicionales de otros países, pero todavía está atravesando oleoductos tradicionales. Vodafone tiene sociedades con MoneyGram, Western Union y otras redes de pago, con todas sus tarifas de rutina y costos dependientes del sistema bancario. Con Bitcoin, es posible enviar dinero a través de un teléfono móvil, directamente entre dos partes, para eludir todo ese sistema engorroso y costoso para las transferencias internacionales.

Quizás inevitablemente, entonces, alguien como Duncan Goldie-Scot, un veterano de las microfinanzas, llegaría a ver a Kenia como el lugar adecuado para comenzar un negocio de remesas a gran escala. Se acercó a la experta en microfinanzas Elizabeth Rossiello, oriunda de Queens, Nueva York, que trabajaba como consultora en Kenia, con una idea: ¿qué tal si combinamos M-Pesa con una moneda digital? Ofrecería todas las ventajas de M-Pesa, pero haría los costos a los usuarios aún más baratos para aquellos que importan dinero a ese sistema desde

el extranjero, porque esas remesas de parientes en Londres o Nueva York llegarían a través de bitcoin en lugar de la banca tradicional sistema. Llámalo BitPesa.

Comenzarían con un objetivo simple y alcanzable: tomar un solo "corredor" en el negocio de las remesas -entre el Reino Unido y Kenia- y construir un negocio de transferencia de dinero basado en bitcoins. Contrataron a un equipo de desarrollo para construir el prototipo inicial, luego un codificador para renovarlo. Luego, enviaron a un miembro del personal a Londres, para ir a los cafés en los vecindarios de Kenia y reclutar beta testers para las pruebas iniciales. Comenzaron su prueba beta en el verano de 2014 con aproximadamente dos docenas de emigrantes.

La idea no solo atraía a los kenianos que buscaban enviar dinero a su país de manera más económica. Rossiello recaudó rápidamente 700,000 dólares de inversionistas, incluido Barry Silbert de SecondMarket, quien también invirtió en BitPagos, la empresa emergente argentina, y cuya compañía está construyendo su propia plataforma de comercio de bitcoins. Ella podría haber criado más. "Tomamos treinta reuniones en dos semanas, hablando de vincular Bitcoin y M-Pesa, y vimos que los ojos se iluminaban", dijo. Los inversionistas entendieron que esta era una manera simple y potencialmente poderosa de socavar y tomar participación en el mercado de un puñado de compañías, las Uniones Occidentales del mundo que tenían un dominio sobre un gran negocio global. Después de que la compañía fuera perfilada en un artículo de Bloomberg en noviembre de 2013, antes de lanzar un solo producto, Rossiello comenzó a recibir llamadas de suscriptores de "alto valor neto" a la plataforma de información financiera de Bloomberg, y las firmas de California querían una parte de la acción . Pero ella no estaba preparada para ceder el control de la compañía. "Dije que no a muchos tipos grandes", dijo.

Rossiello ni siquiera había oído hablar de bitcoin hasta que Goldie-Scot se lo mencionó. Pero rápidamente se dio cuenta de las posibilidades y ahora tiene ambiciones para BitPesa que van más allá del bitcoin o las monedas digitales. Por todo lo bueno que ha hecho, la industria de las microfinanzas promovida por el Grameen Bank, galardonado con el Premio Nobel de la Paz, Muhammad Yunus todavía opera dentro de lo que describió como "un sistema financiero arruinado". Una alternativa basada en criptomonedas podría evitar muchos de los costos de la sistema existente, y ofrecía la promesa de hacer más que solo permitir remesas baratas.

Rossiello ve el bitcoin como una forma de generar no solo una revolución financiera en Kenia, sino también una revolución tecnológica. La idea es que la criptomoneda fomente la innovación, como hemos visto en San Francisco y otros lugares. Ella ha comenzado una cultura de encuentro y enseña la codificación a los escolares. Cinco personas estaban en su primera reunión; seis meses después, eran cuarenta, y estaban haciendo la codificación y creando sus propias aplicaciones. "Las personas están respondiendo, la gente está entusiasmada con eso", dice.

M-Pesa, ahora combinado con una comunidad naciente de bitcoin, está demostrando ser la puerta de entrada de Kenia a una revolución tecnológica más amplia, ya que el dinero móvil y la Internet generan una ola de creatividad y espíritu empresarial. Nairobi se ha convertido en uno de los centros tecnológicos más importantes de África, si no el más grande. A veces se llama Silicon Savannah. La ciudad incluso tiene su propia versión de 20Mission, una hacker house llamada iHub que no está lejos del centro de ciencias de la Universidad de Nairobi. Ocupa un espacio espacioso y moderno en el cuarto piso de un edificio de oficinas que sería como estar en casa en Silicon Valley, con mucha luz, espacio para charlas y presentaciones, sofás y espacio de descanso (incluyendo una mesa de futbolín) y un café bar. También tiene espacio de trabajo para las personas que crean cosas, aquellos que están impulsando el crecimiento de Silicon Savannah. El lugar está conectado, literal y figurativamente, y lleno de niños jóvenes, enérgicos y brillantes. Tienen reuniones, y charlas "al lado de la chimenea", y atraen grandes talentos: Joi Ito, el director

del MIT Media Lab en Massachusetts, habló en iHub en mayo de 2014. También visitó Eric Schmidt de Google.

Los objetivos del centro son similares a los de Silicon Valley: fomentar el espíritu empresarial, construir una red y hacer que los jóvenes y las mentes jóvenes participen y creen; casi se puede escuchar a Steve Jobs diciendo cosas "mágicas". Pero mientras que en los Estados Unidos los expertos en tecnología suelen idear dispositivos genéticos para satisfacer necesidades que no sabíamos que teníamos-¿de verdad necesita un robot para barrer su piso? -en Nairobi, los objetivos tienden a necesidades más inmediatas, por ejemplo, hacia productos que mejoran la gobernanza o hacen que el sistema de atención de la salud sea más efectivo o que el suministro de agua sea más seguro y esté mejor distribuido. Un grupo llamado Geeks in Gumboots, por ejemplo, está tratando de enfocar a la comunidad tecnológica en temas ambientales.

Como es el caso con todos los esfuerzos de personas ajenas que intentan mejorar las vidas de personas distantes, existe una conciencia incómoda del legado del colonialismo y la delgada línea entre asistencia y paternalismo. Rossiello es muy consciente de estos problemas y se enfada con la noción, a veces escuchada en las conferencias de Bitcoin, de que BitPesa está "salvando África". Ella no quiere nada del paternalismo subconsciente colonial que la idea implica. "En realidad, hay muchos africanos aquí haciendo cosas", dice.

Es importante resistir el impulso de ver la tecnología de las criptomonedas o cualquier tecnología como una panacea. A pesar de la promesa que tiene la tecnología, esta idea de que las naciones en desarrollo van a "saltar" décadas de desarrollo gracias a la tecnología descentralizada, barata y distribuida, la realidad sobre el terreno resiste a las soluciones fáciles. Lo que M-Pesa ha logrado, y lo que BitPesa promete, es importante porque son herramientas efectivas para promover la actividad económica y, por ende, el desarrollo. Esta es la razón por la cual las historias que salen de Silicon Savannah son importantes, no solo para Kenia sino también para el mundo en desarrollo en general. "Aquí hay una historia mucho más grande", dice Rossiello. "Recién estamos comenzando".

Las causas principales del aislamiento financiero en los países pobres van más allá de la falta de cuentas bancarias y de cuánto cuesta enviar dinero. Comienzan con los desfavorecidos, que típicamente están aislados de lo que el economista peruano Hernando de Soto llama el "misterio del capital", la idea de que el crecimiento económico y la creación de riqueza dependen de derechos de propiedad claramente definidos y documentados. De Soto ha hecho tanto como cualquier otra persona para promover la idea de que el desarrollo económico debe enfocarse en la documentación de los bienes de los pobres: los hogares que los habitantes de barrios marginales poseen por derecho pero para los cuales no tienen título; las empresas sin licencia que operan; los trabajos debajo de la mesa para los que se les paga. En Occidente, los documentos adjuntos a estos activos pueden presentarse como garantía a un banco para pedir dinero prestado o para convencer a un inversor de que invierta dinero en un proyecto que valga la pena. Pero sin esa documentación, los pobres a menudo son condenados a una existencia de la mano a la boca. Es por eso que Soto y otros de su Instituto para la Democracia Liberal, con sede en Lima, pasan tiempo en los barrios marginales de Perú, Haití, Egipto y otros lugares inspeccionando y documentando las propiedades de las personas y entregando hipotecas. Pero con este trabajo, simplemente están rascando la superficie. En conjunto, esta economía informal global, o el Sistema D, como el periodista Robert Neuwirth ha elegido llamarla, vale 10 billones de dólares según sus estimaciones. Si fuera su propio país, Neuwirth sugiere los nombres de Bazaaristán o la URSS, la República de los Vendedores de United Street, esta economía de los indocumentados sería la segunda después de la de los Estados Unidos.

Como sugiere Rossiello de BitPesa, las mayores oportunidades pueden no estar en las monedas digitales en sí, sino en la tecnología que las respalda. El potencial de la gente de la economía informal es grande para explotar la forma libre de intermediarios de Blockchain de intercambiar activos e información y su irrefutable registro público que está libre del control de cualquier institución central. Estas características crean oportunidades únicas para que esas personas superen las barreras legales e institucionales para el avance. La reducción de los costos de pago es solo el comienzo. Como mencionamos, las instituciones débiles y corruptas son la causa principal de la exclusión de los pobres del sistema bancario porque niegan a las personas la oportunidad de demostrar su integridad y valor neto a los banqueros. Bien, la cadena de bloques, si se toma en la medida en que una nueva ola de innovadores de bitcoin cree posible, podría reemplazar a muchas de esas instituciones con una autoridad descentralizada para probar las obligaciones y el estado legal de las personas. Al hacerlo, podría ensanchar dramáticamente la red de inclusión.

Discutiremos la miríada de nuevas ideas en el examen del siguiente capítulo de estos llamados inventos de Bitcoin 2.0. En teoría, el innovador modelo de blockchain para autenticar información podría liberar a los pobres de la incompetencia y corrupción de burócratas y jueces. Se podrían crear registros digitalizados de escrituras inmobiliarias, totalmente administrados por una red informática de criptomonedas sin el compromiso de una agencia del gobierno central, para administrar de manera económica y confiable los derechos de propiedad de las personas, administrando documentos digitales que podrían usarse para obtener préstamos en formato digital o moneda fiduciaria. Mientras que la corrupción judicial significa que las personas de bajos ingresos en un país en desarrollo no pueden depender de contratos estancos para apuntalar sus negocios y desbloquear el misterio de capital de Soto, someter tales acuerdos a la infalibilidad del blockchain podría terminar con todo eso.

Jonathan Mohan, que trabaja en Ethereum, la nueva plataforma Bitcoin 2.0 que busca interrumpir todo tipo de acuerdos legales y contractuales, ofrece una explicación convincente de cómo estos "contratos inteligentes", cada uno diseñado para ejecutarse en el blockchain a través de una pieza automatizada de software, beneficiaría a la economía informal. "Mientras prestes garantía para un contrato y Blockchain reconozca el contrato, entonces sabes que no hay fraude y sabes que no hay necesidad de tener que confiar en un tercero", dijo en una conferencia Inside Bitcoins en Nueva York. "Entonces el contrato es simple y todas estas otras cosas se solucionan por sí mismas". Si se encuentra en lugares como África, en China (demonios, incluso en Estados Unidos), sabe que se hará justicia porque la entidad ejecutará el contrato exactamente como se programó para ejecutarlo ".

Si bien puede que no sea tan simple como que "todas estas otras cosas" se clasifiquen a sí mismas, el verdadero potencial está aquí. Para entender cómo podría funcionar, debemos regresar a la cadena de bloques y explorar la gran variedad de formas en que se puede usar.

Capítulo 9

TODO DEL BLOCKCHAIN

> Cada hombre toma los límites de su propio campo de visión para los límites del mundo.
>
> -Arthur Schopenhauer

Te hemos llevado al movimiento Cypherpunk y las proto-monedas que precedieron al bitcoin, y a la mecánica de la cadena de bloques. Te hemos llevado a la formación de la comunidad y a la escena de alta tecnología en San Francisco. Les hemos mostrado mineros en Utah y bitcoin en el Caribe. Le mostramos cómo la moneda puede empoderar a las mujeres en Afganistán. Ahora es el momento de sumergirnos en las aguas criptográficas para mirar el futuro de Bitcoin en cosas que están a la vanguardia de la vanguardia. Es hora de hablar sobre el potencial para construir cosas encima de bitcoin. Estos pueden ir desde proyectos tan mundanos como los sitios de juegos de azar hasta aquellos tan trascendentes como la base de corporaciones autónomas completamente automáticas. El vínculo común es que todos ellos están tomando la base fundamental de bitcoin, un sistema descentralizado que utiliza la cadena de bloques incontrovertible para su legitimidad y verificación. Como todo lo demás en el mundo de la criptomoneda, el objetivo es descentralizar, quitarle el poder a los intermediarios. Sin embargo, como veremos, los innovadores que buscan alentar el crecimiento de negocios rentables a través de estos sistemas descentralizados pueden encontrar que los puristas de criptomonedas a veces los acusan, a menudo injustamente, de actuar como "centralizadores". "Cada hombre toma los límites de su propio campo de visión para los límites del mundo ", escribió el filósofo Arthur Schopenhauer. Sin embargo, para la gente que estamos por conocer, los límites de su campo de visión son sus puntos de partida.

Los jugadores de casino históricamente han estado a merced de los establecimientos que frecuentan. Antes del advenimiento de la regulación, no se podía verificar que los bandidos con un solo brazo no estuvieran razonablemente programados a favor de la casa. ¿Quién iba a decir que la bola de la rueda de la ruleta no estaba guiada por imanes o que la máquina barajadora de cartas de blackjack no había apilado la baraja? En la mayoría de los países, los casinos ahora están estrictamente regulados y esas leyes son en su mayoría aplicadas, pero todavía no hay garantía. Ahora que los juegos en línea han despegado, es posiblemente aún más difícil. Las cartas de tu juego de blackjack en línea promedio se reparten entre lo que se supone que es un generador de números completamente aleatorio, pero debido a que reside en el servidor del sitio de apuestas, podría manipularse fácilmente.

Un entusiasta de los bitcoins vio este dilema como una oportunidad, se hizo rico resolviéndolo, y sin querer demostró el poder de la cadena de bloques bitcoin para crear un reino inviolable de transparencia, uno que resultó ser extremadamente comercializable. Si bien la historia de un tipo que ganó algunos millones con un casino en línea podría no ser tan inspirador como un proyecto para liberar a los no bancarizados del mundo, su empresa reveló elementos clave del potencial de gran alcance de la criptomoneda.

Joseph Gleason, mejor conocido como Fireduck en los foros sociales de Bitcointalk.org y Reddit, pensó que podría usar la cadena de bloques de bitcoin para crear un sistema "provably fair" para las apuestas en línea. Gleason's era un concepto sencillo: la gente colocaría apuestas de corta duración cuyo resultado dependía de un número aleatorio derivado de los hash que aparecían en las transacciones enviadas a través de la cadena de bloques, es decir, una fuente probadamente

independiente. Los jugadores enviarían bitcoin a una de una selección de direcciones especiales asociadas a las apuestas de que un cierto "número de la suerte" de cinco dígitos de hasta 65.535 entraría por debajo del umbral elegido. Cuanto menor sea el límite superior elegido, menores serán las probabilidades de ganar y mayor será el posible pago. El programa de Gleason usaría un proceso de cifrado básico para encontrar un número de la suerte. Tomaría el código de transacción que el algoritmo de núcleo de bitcoin asignó al pago del jugador y lo combine con una clave diaria secreta separada conocida solo por su programa, creando así un nuevo código hash alfanumérico independiente. El número de la suerte se crearía al convertir los primeros cuatro caracteres de ese hash, que aparece como una combinación de letras y números, en un número regular. Debido a las convenciones matemáticas de este tipo particular de hash, este número siempre aparecería en 65.535 o menos. * La parte justa de la proposición fue que después de veinticuatro horas, el sistema divulgaría la clave secreta, que permitía a los usuarios Regrese y descomprima los números haciendo todos los cálculos al revés.

Para proporcionar este servicio, el casino basado en bitcoin de Gleason se adjudicó un margen de 1.9 por ciento declarado completamente sobre todas las apuestas. Una apuesta ganadora de diez bitcoins que el número de la suerte caería por debajo de 32.758, más o menos par, le pagaría al ganador 19.6 bitcoins, con Gleason reteniendo 0.4 de un bitcoin, o aproximadamente $ 2 en el momento en que concibió el proyecto por primera vez.

Después de poco más de una semana, Gleason se dio cuenta de que estaba sentado sobre algo explosivo. Él había invertido 45 bitcoins (alrededor de $ 225 en ese momento) y ya había hecho 146 bitcoins en ganancias. Pero ya podía ver las complicaciones legales: solo unos pocos estados habían legalizado los juegos de azar en línea, y esos estados habían adoptado estrictas leyes de licencias. Por lo tanto, el 17 de abril de 2012, puso un aviso en Reddit diciendo que entregaría su creación a cualquier persona preparada para enfrentar desafíos legales por parte del estado y contratarlo como consultor. Erik Voorhees, una voz libertaria emergente entre los entusiastas de los bitcoins, pronto tomó la oferta. Bautizando el servicio SatoshiDice, Voorhees lo convirtió en una mina de oro. Las transacciones de SatoshiDice pronto representarían la mitad de todas las transferencias de bitcoins en la red de la moneda digital. (La mayoría de las apuestas eran pequeñas y, por lo tanto, juntas representaban una porción mucho más pequeña del volumen total de las transacciones en términos de valor).

Durante el año que viene, Voorhees vendió acciones en el servicio a cambio de bitcoins, listando los valores en MPEx, una bolsa de valores rumana donde los activos digitales se cotizan y se negocian en monedas digitales. Luego, unos meses después de las ofertas de acciones, anunció que había vendido SatoshiDice a un comprador no revelado por 126,315 bitcoins, que luego valía $ 11,5 millones. Si bien eso significó que sus inversores disfrutaron de una gran ganancia, ya que la mayoría de los accionistas Voorhees terminaron con la mayor parte. No está mal por un año de propiedad.

SatoshiDice proporcionó una indicación temprana del potencial de lo que la industria llama Bitcoin 2.0, o, nuestra preferencia, aplicaciones de Blockchain 2.0: productos, servicios e incluso empresas en toda regla que se ejecutan de forma autónoma mediante una red de criptomoneda descentralizada.

Gleason y Voorhees no fueron las primeras personas en imaginar usos alternativos para la cadena de bloques. Si, pensaban algunas mentes aventureras, ahora dos partes podían intercambiar fondos de forma segura sin un honorario de confianza de terceros, entonces quizás este nuevo registro a prueba de falsificación de información verificada también podría usarse para otros intercambios "sin confianza". Los contratos pueden redactarse y ejecutarse sin la participación de abogados o tribunales; las escrituras de propiedad digitalizadas podrían ser transferidas y

verificadas por los agentes inmobiliarios de blockchain sans; los valores financieros se pueden negociar directamente entre los inversores, pasando por alto una central de intercambio o cámara de compensación.

Mike Hearn, que trabajó durante tres años en software de seguridad en Google antes de dejar de dedicarse al desarrollo de criptomonedas, ofrece quizás el pronóstico de mayor alcance sobre dicho potencial en la tecnología de blockchain. En un discurso en el Festival de Turing de agosto de 2013 en Edimburgo, Hearn imaginó una economía compuesta por agentes económicos autónomos. Utilizó el ejemplo de un taxi sin conductor, uno guiado solo por sensores y tecnología GPS. El servicio de taxi de un automóvil estaría a cargo de un programa de software inteligente conectado a un mercado electrónico automatizado que Hearn apodó el Tradenet. Allí, los posibles pasajeros podrían publicar solicitudes de viaje y recibir ofertas competitivas de varios automóviles sin conductor. Elegirían su taxi preferido según la tarifa, el tiempo de viaje y el modelo de automóvil, y podrían negociar la ruta en función de las duraciones y tarifas que el servicio obtuviera mediante pujas en un mercado de "espacio de carga" separado de Tradenet, donde las variaciones en las condiciones del tránsito ofrecerían diferentes precios de peaje basados en el mercado para cada ruta.

Si todo eso suena futurista pero factible, pruebe esta característica adicional del taxi imaginario de Hearn: no tiene dueño. El automóvil se posee a sí mismo, o más precisamente, es el programa de computadora que lo opera. Este programa pagaría los costos de funcionamiento del automóvil y tomaría sus propios ingresos; todo esto sería posible gracias a la criptomoneda y la invención de la cadena de bloques.

"Sospecho que si traté de ir al banco y abrir una cuenta bancaria que pertenece a un programa de computadora, me dirían que me perdiera o que pensarían que estoy loco y me reportarían a la policía", dijo Hearn. . "Pero Bitcoin no tiene intermediarios. Por lo tanto, no hay nada que impida que una computadora se conecte a Internet y participe [en la red bitcoin] por sí misma. Todo lo que necesita hacer para generar una billetera bitcoin es generar un gran número aleatorio, y prácticamente todo puede hacer eso ".

En este momento, probablemente se esté preguntando por qué le daríamos a una máquina esos derechos. Debido a que podríamos programarlo para proporcionar el servicio más económico y eficiente posible, el automóvil de Hearn se centraría en maximizar la productividad y sobrevivir, no acumulando una gran cantidad de ganancias retenidas para gastar en McMansiones y viajes a las Bahamas. Podría mantener sus márgenes de ganancia superthin y sus precios bajos. Dicho esto, si traía más ingresos que gastos, el automóvil podría programarse para "tener hijos", como lo expresa Hearn, invirtiendo sus bitcoins excesivos en nuevos autos sin conductor que "heredarían" un clon de su programa de software. Para adelantarse al juego, el automóvil también podría gastar su excedente contratando a un humano para que le escriba un código superior -después de buscar ofertas para estos servicios a través de la red de comercio- y luego aplique protocolos de prueba especiales para asegurarse de que el humano no lo estafa. de su competitividad. Si las condiciones económicas en su área se deterioran demasiado, el automóvil podría "irse a dormir" en un estacionamiento a largo plazo durante seis meses, dice Hearn, o podría irse a otra ciudad donde los datos de Tradenet indicaban una mayor demanda de servicios de taxi.

Por supuesto, un mundo de taxis sin conductor es un mundo sin empleos para los taxistas humanos. Si muchas de estas ideas de Blockchain 2.0 llegan a buen término, no son las únicas personas que se preocuparán por la obsolescencia: los abogados, los banqueros de inversión, los corredores de bolsa y una serie de otros servicios "basados en la confianza" podrían tener una menor demanda en una cadena de bloques. correr el mundo. Más adelante, en el capítulo 11, exploraremos cómo la sociedad puede tener que manejar el proceso doloroso que esto conlleva.

Pero por ahora solo profundizaremos en la mecánica de la tecnología y exploraremos las muchas formas disruptivas en que sus inventores la ven cambiar nuestra economía.

Los contratos de aseguramiento son solo una forma de una de las ideas más prevalentes de Blockchain 2.0: "contratos inteligentes", una idea que primero flotó Nick Szabo, que algunos investigadores creen que es Satoshi Nakamoto. En su punto crucial, esta idea sostiene que la cadena de bloques puede reemplazar el sistema legal, el último tercero confiable. En lugar de tener un bufete de abogados redactando un acuerdo escrito para ser ejecutado por un juez, si una parte no cumple con sus obligaciones -con todos los costos e incertidumbre que conlleva la participación de esas instituciones- la ejecución de esas obligaciones se automatiza mediante software. , con los criterios para hacerlo verificado por la cadena de bloques descentralizada. Piense en un acuerdo estándar de depósito en garantía en el que un propietario endeudado ahorra una cantidad mensual que garantiza que se pagarán los seguros e impuestos del hogar. Bueno, en este caso, esos pagos se realizarían con criptomoneda y se depositarían en una billetera neutral, todo se activará automáticamente una vez que vencen los pagos de impuestos y seguro. El blockchain mantiene a todos honestos, y se elimina toda una capa de burocracia bancaria, lo que reduce los costos.

Los mercados financieros están especialmente maduros para la innovación Blockchain 2.0. Muchos contratos de valores modernos ya están codificados, digitalizados y automatizados. Sin embargo, son administrados por los bancos de Wall Street y son escritos y litigados por abogados de alto poder que derriban retenedores de seis o siete cifras. Uno puede imaginar swaps de incumplimiento crediticio, una clase de derivado que ganó notoriedad durante la crisis financiera, establecida en una infraestructura descentralizada tipo blockchain. Los contratos de CDS, que funcionan como seguros, requieren que una de las partes, generalmente un banco de inversión o una compañía de seguros, realice un pago a la otra parte, generalmente un acreedor que ha prestado dinero a un deudor tercero, siempre y cuando ese deudor sea considerado en default. Las disputas ocurren a menudo sobre lo que constituye un "evento de crédito" para activar el pago, que a veces requiere resoluciones de organismos dominados por banqueros como la Asociación Internacional de Derivados e Intercambios (ISDA) y que con frecuencia involucra abogados y casos judiciales. Sin embargo, si el contrato de CDS se presentara en el blockchain, estos terceros intermediarios podrían, en teoría, ser eliminados de ese proceso de arbitraje. Cualquier falta de pago de la billetera del deudor provocaría un pago de bitcoin correspondiente de la billetera de la parte asegurada al inversor asegurado por CDS. Sin ambigüedades, sin desafíos legales, todo fácil y barato de instalar con algún software estandarizado.

Pero los "contratos inteligentes" no necesitan limitarse a las finanzas. Cuando se combina con "propiedad inteligente" -donde las escrituras, títulos y otras certificaciones de propiedad se ponen en forma digital para que el software actúe sobre ellos- estos contratos permiten la transferencia automática de la propiedad de un activo físico como una casa o un automóvil, o un activo intangible, como una patente. Del mismo modo, el software inicia la transferencia cuando se cumplen las obligaciones contractuales. Ahora que las empresas ponen codigos de barras, códigos QR, microchips y antenas Bluetooth en casi todos los artilugios y mercaderías, el emergente "Internet de las cosas" debería permitir transferir la propiedad en muchos tipos de propiedades físicas de esta manera.

Una solución creativa se aplica a los automóviles comprados a crédito. En este momento, si el propietario de un automóvil pierde sus pagos, es laborioso y costoso para la compañía financiera reclamar el título y la posesión física del automóvil, involucrando a abogados, agencias de cobro y, en el peor de los casos, a hombres de repo. Pero bajo un contrato inteligente, si los pagos no se cumplen, el título digitalizado se revertiría automáticamente a la billetera digital de la compañía financiera. Además, el encendido podría asociarse de forma inalámbrica a un sistema de encriptación en línea que requiere la presencia de una "clave" remota remota para que el

automóvil se encienda. En caso de incumplimiento, el sistema eliminaría esa clave y le negaría al prestatario el acceso al automóvil. Sin duda, esto suena intrusivo y parecido al Gran Hermano, pero tendría beneficios reales y generalizados. Al eliminar las ineficiencias, la burocracia y los costos del sistema, un enfoque tan automatizado para la incautación de activos podría reducir el costo del financiamiento. En teoría, abriría un financiamiento asequible a millones de personas con mal crédito que actualmente son negadas por las compañías financieras que no están seguras de que sus préstamos estén debidamente garantizados. Y los contratos no necesitan ser completamente restrictivos: podrían escribirse de tal manera que permitieran la negociación fuera de línea y / o la intervención del tribunal.

Otra aplicación para la propiedad inteligente: si las agencias de auto concesión de licencias del gobierno pudieran tomar la iniciativa de codificar los registros de automóviles y hacerlos viables para las transferencias aprobadas por la cadena de bloques, se podrían lograr grandes eficiencias. ¿Qué no le gusta de la desaparición del Departamento de Vehículos Motorizados? A menos que sea un empleado del DMV, por supuesto.

Existen obstáculos técnicos, legales, financieros y culturales formidables para la adopción generalizada de muchas de estas soluciones Blockchain 2.0. Cientos están en marcha en este momento, y muchos parecen medio cocidos y es probable que nunca despeguen del suelo. Pero la energía y la capacidad intelectual innovadora que se invierte en ellos es importante y se manifiesta en una serie de empresas de nueva creación y proyectos de desarrollo.

El pionero en el campo fue el proyecto Colored Coins, que se lanzó en la segunda mitad de 2012; su propósito: permitir a las personas intercambiar valores digitalizados y monedas fiduciarias directamente sobre la cadena de bloques bitcoin. (Dos personas podrían establecer un contrato para intercambiar directamente un reclamo digital en euros por un reclamo digital sobre oro, por ejemplo). Desde entonces, el campo se ha llenado de empresas y proyectos de lanzamiento de Blockchain 2.0, incluidos Next, Ripple, Mastercoin, Ethereum, BitShares, Counterparty y Stellar. Cada uno proporciona una plataforma especialmente diseñada basada en blockchain que permite a otras entidades crear contratos de igual a igual, emitir y permitir el comercio de activos digitales y digitalizados, o instalar aplicaciones especiales impulsadas por software, todas ellas con funcionamiento descentralizado. Cada uno también emite una moneda única o token digital-nextcoin, mastercoin, ether, bitshares y Counterparty's XCP-que facilita los muchos intercambios transaccionales que tienen que ocurrir entre las partes que usan estos protocolos para implementar las funciones de ida y vuelta de sus aplicaciones descentralizadas. Estos son intercambiables para bitcoins y otras criptomonedas en intercambios especiales de altcoins como Cryptsy, donde se espera que su valor aumente o disminuya según el éxito o el fracaso del protocolo al que pertenecen. Sin embargo, tales "monedas" de Blockchain 2.0 probablemente son mejor consideradas como recipientes digitales en los que la información incrustada se puede pasar alrededor de la cadena de bloques en lugar de como monedas. Son los vehículos a través de los cuales se implementan los contratos inteligentes, se intercambian activos digitales y pueden ocurrir todo tipo de otras acciones descentralizadas.

Los expertos en tecnología tienen un punto débil para las aplicaciones más arriesgadas, las últimas tecnologías disruptivas, y cuando se llevan al extremo, las ideas que impulsan cada una de estas empresas son tan perturbadoras como uno se puede imaginar. David Johnston es miembro directivo de la Fundación Mastercoin, el organismo que coordina los fondos para el proyecto Mastercoin, que ofrece una plataforma de software especial para que los desarrolladores diseñen aplicaciones descentralizadas especiales que puedan ejecutarse sobre la cadena de bloques de bitcoin. Él dice que la tecnología de blockchain "aumentará la economía de intercambio", esa tendencia emergente en la que los propietarios de apartamentos usan Airbnb.com para alquilar habitaciones cuasi hoteleras y los propietarios de automóviles se inscriben como taxistas

autónomos para Uber y Lyft basados en teléfonos inteligentes. La idea es que si podemos descentralizar la economía y fomentar múltiples formas de intercambios P2P, las personas descubrirán formas rentables de convertir gran parte de lo que poseen o controlan en un servicio comercializable. Johnston es conocido por haber acuñado el término DApp, por "aplicación autónoma descentralizada", para describir el tipo de programas de software especializados que podrían prosperar en entornos basados en blockchain. Él entusiasmado lanza varios ejemplos de tales DApps: una bolsa de valores completamente descentralizada; una red de computadoras interconectadas que contribuyen y extraen de un conjunto colectivo de espacio en el disco duro, todo pagado con criptomoneda; una "red mallada", en la que se paga a los usuarios para que aporten ancho de banda a una red de usuarios conectados a Wi-Fi de bajo costo que pasan por alto a las compañías de cable y telefónicas que actualmente funcionan como proveedores centralizados de servicios de Internet.

Las empresas nuevas y los proyectos sin fines de lucro que buscan llevar a cabo esta interrupción masiva vienen esencialmente en dos formas diferentes. Algunos utilizan directamente la cadena de bloques bitcoin para sus actividades, incluidas monedas coloreadas, contraparte y Mastercoin. Así como Bitcoin tiene su propio protocolo central, que, como vimos en capítulos anteriores, es el programa de software que establece las reglas básicas para la red de computadoras de bitcoin, también estos proyectos vienen con sus propios protocolos fundacionales. Eso los convierte en una plataforma de segunda capa, sobre la que se puede construir una tercera capa de servicios y aplicaciones. Estas plataformas de proveedores de Blockchain 2.0 les permiten a sus clientes acceder al poder de la cadena de bloques bitcoin descentralizada y subyacente para hacer cosas completamente diferentes de simplemente intercambiar bitcoins: contratos inteligentes, transacciones de propiedad inteligente, intercambios de activos digitales, etc. Bajo su modelo, el bitcoin subyacente las transacciones suelen ser de poco valor, tan bajas como un "Satoshi" (BTC0.00000001). Esto se debe a que el valor de bitcoin es esencialmente irrelevante frente al propósito más importante de transmitir los metadatos críticos de la aplicación descentralizada a través de la red, aunque se necesita algún intercambio de valor para hacer que la comunicación de la información se realice. Estos proveedores han decidido apostar por Bitcoin, apostando a que su ventaja como primer jugador, que la ha convertido en la criptomoneda más comercializada, minada y líquida, con una red global de prodigiosa potencia informática, asegura a sus usuarios de una red robusta y confiable para autenticar la integridad de sus operaciones.

Otros proyectos de Blockchain 2.0 han adoptado una filosofía diferente. No querían obligar al protocolo de bitcoin a hacer cosas para las que no estaba diseñado. ¿Por qué los mineros comprometen recursos para respaldar la instalación de un reclamo digital de propiedad, por ejemplo, cuando todo su sistema de incentivos se basa en recompensas por confirmar transacciones en moneda de bitcoins? Aunque algunos desarrolladores están buscando modificar el software central de bitcoins para hacerlo más versátil, estas personas sintieron que la capacidad del núcleo de la blockchain para manejar esta nueva y diferente carga de trabajo tenía limitaciones estructurales. Sentían que era mejor irse y construir una red completamente nueva, una cadena de bloques completamente nueva. Eso les permitió repensar el sistema de incentivos de la red, ajustarlo para que los nodos informáticos se animen a confirmar las transacciones que están diseñadas para tener grandes cantidades de información adicional incrustada en ellos. El proyecto Next, cuyo concepto de "prueba de juego" que discutimos en el capítulo 6, fue un líder en este impulso. Pero los nuevos y más audaces proyectos de blockchain también se han presentado. Uno de ellos cree que su tecnología puede reinventar la idea misma de una empresa.

Para Daniel Larimer, un obstáculo conceptual básico para expandir las ideas de Blockchain 2.0 se deriva de la nomenclatura. A las personas les cuesta etiquetar las criptomonedas: ¿son valores digitalizados, monedas virtuales o algún tipo de token o software que se usa en una aplicación? Por su parte, el fundador de BitShares cree que si Satoshi Nakamoto hubiera descrito Bitcoin como

una especie de compañía que ejecuta un sistema de pago y cuyas participaciones también funcionan como la moneda de ese sistema, la gente comprendería mejor tanto el proyecto original como el Blockchain 2.0 proyectos que se avecinan. En cambio, se fijan erróneamente en bitcoin como dinero, dice, en lugar de simplemente como una forma de dinero. "Es realmente difícil explicar qué es Bitcoin porque la gente no entiende el dinero. Incluso los expertos no están de acuerdo ", dice Larimer. "Pero el hecho es que los bitcoins no dejan de ser parte de una empresa solo porque se utilizan como dinero. El oro no deja de ser un metal duro y duradero solo porque se usa como moneda. El dinero se define por la forma en que se usa, no por lo que es. "Bitcoin, como él lo define, es una" compañía [que] obtiene sus ingresos de las tarifas de transacción ". Tiene que pagar para asegurar el sistema" y para que emplea subcontratistas, que son los mineros ... pagados con las nuevas acciones de bitcoin en sí mismas ". Una vez que Larimer comenzó a pensar en bitcoin de esta manera, comenzó a ver innumerables posibilidades de crear otras compañías que emitan su propia" moneda "digital como acciones y ejecutar sus negocios en la parte superior de una cadena de bloques.

Mientras que David Johnston y otros se centran en diseñar DApps, Larimer y BitShares tratan de DAC, "corporaciones autónomas descentralizadas". (Otros usan el acrónimo DAO, organización autónoma descentralizada). Estas son entidades propiedad de múltiples accionistas para las cuales las decisiones financieras rutinarias- cuándo liberar los fondos para pagar los gastos, qué tan grande es el dividendo a pagar; están automatizados por el software de orientación de la empresa y se han confiado a un sistema inviolable que ha sido verificado por la cadena de bloques. Cualquier cambio en la estrategia que requiera una alteración del software se somete a votación de los accionistas, todo hecho de manera verificable sobre la cadena de bloques incontrovertible. Pero el resto del tiempo esta entidad corporativa funciona con piloto automático, no es necesario que los empleados de confianza como un tesorero o un empleado de nómina manejen efectivo, no es necesario que una junta directiva mantenga a la gerencia bajo control. El taxi sin conductor de Mike Hearn podía funcionar así; es solo que el automóvil no se compraría solo, sino que sería propiedad de los criptopartidarios del servicio de taxi.

Larimer se anima mientras explica idea tras idea para los DAC construidos en la plataforma de BitShares. El esbelto desarrollador de Blacksburg, Virginia, habla sobre los músicos que fundan DAC que emiten acciones en sus canciones. Los fanáticos en lugar de las compañías discográficas se convierten en los financistas del trabajo de estudio. Cuando una canción se convierte en un éxito, la cantidad de bits digitales de los fans en esa canción aumentará en valor. "Convierte el concepto de copyright al revés", dice Larimer. También está entusiasmado con los "contratos por diferencia" automatizados, que permiten a las personas especular sobre la diferencia entre los precios de dos activos y recibir un pago automático si ese "spread" cruza un umbral predeterminado de acuerdo con un feed de datos de mercado que está hablando con un blockchain -programa de software instalado. Incluso ve surgir mercados de reputación basados en blockchain, donde todos, desde restauradores hasta contratistas, pasando por periodistas independientes, pueden promocionarse a sí mismos basados en las métricas matemáticas y las fuerzas del mercado. El irrefutable conjunto de recomendaciones del blockchain no solo crearía un sistema mucho más honesto que el de los "Me gusta" de Facebook o de TripAdvisor, sino que podría permitir a las empresas y autónomos crear valores basados en esas reputaciones, una forma de monetizar automáticamente lo que los contables llaman buena voluntad .

Una idea favorita de Larimer es la votación a prueba de corrupción, basada en cadena de bloques. Bajo este modelo, cada votante usaría una clave privada encriptada para enviar una pequeña cantidad de criptomoneda, esencialmente inútil, a una billetera de votación designada, creando un voto permanente e irrefutable con sello de tiempo en la cadena de bloques para evitar el fraude. "Nuestro objetivo es mejorar la democracia", dice Larimer con total naturalidad. Ideas similares a las suyas ya están entrando en práctica, muchas motivadas por el aumento de la votación

computarizada que, si bien prometen eficiencia y, si se amplía a votación en línea, una participación más amplia, también aumentan el espectro del fraude electoral por quienes tienen acceso al conteo de votos software propietario de sistemas. El municipio de Takoma Park, Maryland, durante los últimos cinco años ha estado utilizando diferentes versiones de un sistema de votación remota encriptado que permite a los votantes comprobar que sus votos fueron contados correctamente sin perder su anonimato. En los últimos años, el legendario criptógrafo y fundador de DigiCash, David Chaum, ha trabajado en tales proyectos.

A mediados de 2013, el periodista Vitalik Buterin también comenzó a pensar en cómo se creó Bitcoin. En su opinión, su protocolo central era demasiado torpe para que los desarrolladores de software crearan interfaces de programación de aplicaciones (API) robustas pero fáciles de usar. Todos los protocolos secundarios que se construyeron sobre él fueron igualmente estrechos. En esencia, decía que era como DOS, antes de que se creara Windows.

¿Qué pasaría si construyera un protocolo y una cadena de bloques completamente independientes que pudieran sustentar cualquier tipo de aplicación escrita en cualquier lenguaje de programación, que fuera, como dicen los desarrolladores, "Turing completa"? ¿Qué pasaría si pudiera soportar cualquier servicio descentralizado -sistemas de negociación de divisas, contratos inteligentes, registros de accionistas, sistemas de votación, DApps, DAC, DAO, lo que sea- y permitir a los desarrolladores construir una interfaz tan bonita como la que su mercado necesitaba? La solución que ideó rápidamente tomó por sorpresa el mundo de las criptomonedas: un blockchain completamente rediseñado, completamente versátil y descentralizado que podría funcionar como una plataforma abierta sobre la cual se podrían instalar todo tipo de contratos y aplicaciones descentralizadas. Él lo llamó Ethereum.

"Esperamos ser como el Android de la criptomoneda", dice Buterin, refiriéndose al sistema operativo móvil diseñado por Google que es utilizado por múltiples modelos de teléfonos inteligentes y que para 2014 había inspirado más de un millón de aplicaciones. "En Android puedes instalar Google Maps, puedes instalar Gmail, puedes instalar lo que quieras. Ahí es donde queremos que vaya la criptomoneda. Ethereum proporciona la capa base, y si desea instalar una billetera, hay una aplicación para eso; si desea instalar un explorador de bloques, puede diseñar uno; o una solución de pagos comerciales o lo que sea ".

Un geek informático y hacker autodidacta sin antecedentes criptográficos formales, Buterin expuso por primera vez su visión en un libro blanco. En noviembre de 2013, lo publicó en GitHub, un repositorio de claves para proyectos de código abierto en el que los codificadores intercambian ideas y colaboran en el desarrollo de software. "Esperaba seriamente que unos cinco criptógrafos lo descartaran inmediatamente y explicaran las razones por las que esto no puede funcionar de ninguna forma, o para decir: 'Aquí están los diez proyectos que ya están haciendo esto'", dice. . Pero tuvo un efecto bastante opuesto, provocando una chispa de imaginación entre los criptógrafos y los ingenieros de software. En enero de 2014, cuando alcanzamos a Buterin en el marco de una conferencia de bitcoin en Miami, Ethereum, que había sido concebido solo unos meses antes, ya contaba con un equipo de quince desarrolladores a tiempo completo dirigidos por Gavin Wood, un destacado británico. el programador aprendió el lenguaje de programación C ++ y tuvo casi cien desarrolladores de medio tiempo que agregaron sus comentarios. Se establecieron en Zug, Suiza, y se pusieron a construir una nueva y versátil plataforma de blockchain.

El equipo también planeó una recaudación de fondos. Descrito como una "preventa" de éter, la moneda interna especial de Ethereum -que en conformidad con la ley suiza se describía en la recaudación de fondos no como una divisa o una garantía, sino como una pieza de software necesaria para ejecutar futuras aplicaciones- la oferta recaudó más de veintinueve mil bitcoins, por valor de más de $ 14.5 millones a finales de agosto. Con esa medida, y considerando el

relativamente corto período de seis semanas, es justo decir que fue el ejercicio de crowdfunding más exitoso de la historia, superando cualquier otra cosa que se haya hecho incluso en plataformas como Kickstarter.

No hace falta decir que Buterin, una canadiense de nacimiento ruso, no era su adolescente promedio. Todavía no veinte cuando nos conocimos en Miami, explicó cómo se interesó por primera vez en bitcoins en marzo de 2011, y cómo en septiembre de ese año, todavía en la escuela secundaria, fue contratado por el empresario suizo de bitcoin Mihai Alisie (más tarde un cofundador temprano de la Proyecto Ethereum) para ser el escritor principal de la Revista Bitcoin. Le pagaron únicamente en bitcoin. El año siguiente, Buterin ingresó a la Universidad de Waterloo en Ontario para estudiar informática. Pero mientras estaba en la escuela, se distraía constantemente con empresas de criptomonedas: leía y escribía sobre el tema con voracidad y ganaba recompensas realizando trabajos de desarrollo independientes para el proyecto Colored Coins de Alex Mizrahi, el temprano esquema de Blockchain 2.0 para incorporar información sobre activos y contratos en bitcoin. actas. Con el aumento vertiginoso del precio del bitcoin y el interés en el tema en expansión, el adolescente canadiense abandonó la universidad para dedicar su tiempo a las criptomonedas. (Cuando Buterin nos contó esto, el evangelista de bitcoin Roger Ver, escuchando desde la barrera, dijo, "¡Buena llamada!")

Buterin realizó una gira de escucha por comunidades de bitcoins de todo el mundo, pagada con el bitcoin que recibía por sus continuas contribuciones a la Revista Bitcoin, artículos que se estaban convirtiendo en una lectura vital para los recién llegados de criptomonedas y los veteranos. Visitó el proyecto Free State en New Hampshire, dedicado a los ideales libertarios, asistió a las reuniones de bitcoin en toda Europa, se enganchó con un grupo hactivista clandestino liderado por el legendario codificador londinense Amir Taaki y estuvo un par de meses en lo que describió como una comuna "anarco-izquierdista" en España. Todo el tiempo recogió pensamientos y conceptos que lo ayudarían a desarrollar su idea maestra.

Siendo un ingeniero financiero calificado en MBA, Buterin extrae los conceptos de las aplicaciones que podrían ejecutarse en Ethereum y ayudan a reinventar Wall Street: los contratos derivados denominados en moneda digital a través de los cuales las monedas tradicionales y las materias primas cotizan como tokens digitales de IOU; Ofertas de seguridad basadas en Ethereum que funcionan sin necesidad de los servicios de suscripción y gestión de libros de un banco de inversión; algoritmos descentralizados para desafiar los siniestros vehículos de inversión del "grupo oscuro" y las máquinas de negociación de alta frecuencia con las cuales los fondos de alto riesgo, los bancos de inversión y los grandes apostadores de Wall Street obtienen una ventaja en el mercado. Pero él admite que solo está lanzando ideas.

Por ahora, Ethereum es un proyecto no probado. El modelo de compensación basado en el éter para los mineros y el sistema de prueba por el cual obtendrían su compensación todavía era un trabajo en progreso al momento de escribir. Nadie podría decir con certeza si la red será estable, si asegurará una base lo suficientemente amplia de mineros comprometidos para evitar la amenaza del poder de concentración concentrada que discutimos en el capítulo 6. Aún así, el personal talentoso y grande de Ethereum y su guerra sólida el cofre existe precisamente para hacer frente a estos desafíos, para obtener la arquitectura correcta. Se está dedicando mucho cerebro a la creación de la plataforma descentralizada definitiva.

En algún momento antes de que Buterin pusiera su mirada en una cadena de bloques completamente nueva, otra escuela de desarrolladores de Blockchain 2.0 comenzó a llevar los libros contables descentrados de criptomonedas en otra dirección. Creían que no era necesario modificar por completo la economía tradicional de las monedas fiduciarias para recortar los

costos de la transferencia de fondos en esas monedas. Simplemente tenía que simplificar la oficina administrativa del sistema financiero.

Aquí, una vez más a la vanguardia, estaba Jed McCaleb, el mercurial y solitario innovador que fundó el intercambio de Mt Gox y así, casi por sí solo, creó un medio para que las personas pasaran a las economías de fiat y bitcoin. El nuevo proyecto de McCaleb, que cofundó con el emprendedor de Internet Arthur Britto y Chris Larsen, fundador de varios proyectos financieros de igual a igual, se llamó Ripple. Audazmente apuntaba a suplantar muchas partes de la infraestructura de intermediación a través de la cual las instituciones financieras se enviaban dinero entre sí.

Al igual que los otros proyectos de Blockchain 2.0, Ripple tiene su propia moneda interna, XRP, a menudo coloquialmente llamada ondas, que funciona como un recipiente para transferir información y como un almacén de valor para los participantes y los inversionistas en la red, ya sean usuarios que quieran a bajo costo. intercambie euros por yenes o especuladores apostando a Ripple. Pero el sistema difiere de casi todas las criptomonedas en que su red para confirmar transacciones no depende de recompensas monetarias o tarifas de transacción como incentivos. Ningún minero casero que vive en el sótano maneja sus computadoras las 24 horas del día, los 7 días de la semana, en una obsesiva búsqueda de ondas. Por el contrario, el libro mayor de las transacciones suele ser confirmado por las mismas instituciones que lo utilizan, las "puertas de entrada" como lo llaman Ripple Labs, la compañía administradora de la red, y los creadores de documentos y contratos digitales que operan en la red Ripple. Las puertas de enlace son bancos, servicios de envío de remesas, transmisores de dinero y casas de cambio, y se espera que contribuyan libremente con recursos informáticos a la red. Los operadores de activos digitales son diseñadores de altcoin respaldados por oro o de contratos denominados en monedas fiduciarias. Confirman las transacciones mediante un sistema de consenso que, a diferencia de los bloques de diez minutos de bitcoin, es virtualmente instantáneo y consume una energía mínima. Están motivados a hacerlo puramente por un interés común en que el sistema funcione bien.

Los clientes externos pueden dirigirse a una de las instituciones de puerta de enlace y solicitar el envío de dinero -o cualquier otro activo que pueda recibir una representación digitalizada dentro de una transacción de XRP- a otra persona, que reciba el pago en su moneda de elección de un beneficiario recíproco puerta de enlace en cualquier otro lugar. Las puertas de enlace no entregan moneda física entre sí. Por el contrario, crean un libro mayor de pagarés negociables, donde el titular de ese pagaré puede reclamar el pago de una puerta de enlace a un cliente para satisfacer las reclamaciones de otro cliente en otro lugar. Si las dos puertas de enlace correspondientes en un intercambio confían entre sí, no hay necesidad de utilizar la red descentralizada "sin confianza" sobre la cual se intercambia XRP; en cambio, es un intercambio contractual directo. En algunos aspectos, entonces, imita el sistema hawala del mundo musulmán: la red mundial de distribuidores de dinero de siglos de antigüedad que utiliza relaciones de confianza de larga data y transfronterizas para enviar dinero a los clientes en todo el mundo bajo el acuerdo de que las deudas serán correspondido, mientras que está modelado en parte en bitcoin.

Una vez que la red Ripple esté completamente desarrollada, podrá intercambiar tokens de IOU denominados en moneda fiduciaria entre sí, creando tipos de cambio de facto. Ripple Labs espera atraer suficientes pasarelas de intercambio de divisas para que su intercambio global descentralizado sea lo suficientemente líquido como para ofrecer tasas más atractivas que las del actual sistema centralizado de cambio de divisas, que se ejecuta a través de las mesas de negociación de los grandes bancos internacionales. Se espera que su estructura descentralizada otorgue a los compradores y vendedores acceso a una selección de precios mucho más amplia y justa, reduciendo la brecha entre los precios de compra y venta, el llamado spread que genera ganancias para los bancos. Para darle una idea de la oportunidad, ese mercado monetario global

centrado en el banco valía más de $ 5 billones en facturación diaria en 2013. Es el mercado financiero más grande del mundo.

Pero Ripple trata tanto de eliminar a los intermediarios como de estrechar los diferenciales cambiarios. Elimina la necesidad de procesadores de pagos, agentes de liquidación, bancos de divisas, servicios de custodia y la red ACH (Automated Clearing House). Al igual que Bitcoin, apunta a los trillones de dólares en comisiones de intermediarios que actualmente se añaden anualmente a las transferencias monetarias nacionales e internacionales, particularmente en los servicios de banca corresponsal que los bancos de Wall Street ofrecen a costos elevados para bancos pequeños o regionales. No en vano, Ripple está promocionando agresivamente a estos bancos más pequeños. David Andolfatto, el economista jefe del Banco de la Reserva Federal de St. Louis, ha cantado las alabanzas de Ripple por reducir el desperdicio en el sistema financiero. A mediados de 2014, el concepto recién comenzaba a resonar con algunos de los primeros usuarios. AstroPay, con sede en el Reino Unido, que afirmaba administrar la mayor red de pagos transfronterizos de América Latina, firmó como una puerta de acceso para sus seiscientos mil clientes comerciales en la región, y Fidor Bank de Alemania, ya pionero en la prestación de servicios a bitcoin empresas, dijo que planeaba utilizar Ripple para ofrecer transferencias internacionales superdeportivas, al igual que CBW Bank y Cross River Bank en los Estados Unidos. Mientras tanto, Ripple Labs había atraído ya $ 6.5 millones en inversiones de importantes firmas de Silicon Valley como Andreessen Horowitz, el vehículo de capital de riesgo del pionero de Netscape Marc Andreessen, Google Ventures y Lightspeed Venture Partners. Sorprendentemente, la nueva empresa afirmó estar involucrada en discusiones intensas con los bancos internacionales más grandes, ofreciéndoles la oportunidad de reducir los costos de sus transferencias de dinero globales y obtener una ventaja competitiva. Es un prospecto potencialmente atractivo para cualquier banco que no esté fuertemente invertido en las funciones intermedias de la infraestructura de pago que Ripple haría redundantes. Es mucho menos atractivo para aquellos que constituyen esa infraestructura.

Aún así, a partir de mediados de 2014, parecía que Ripple había generado más entusiasmo entre técnicos e individuos que entre los banqueros. El proyecto tenía seguidores fanáticos, nada del orden de Bitcoin, pero sí una comunidad distintiva y apasionada. En ocasiones, estos fanáticos han sido arrastrados a chocar con bitcoiners, algunos de los cuales han criticado a Ripple por trabajar con, y no en contra del sistema financiero. En parte porque la red Ripple es administrada por una empresa privada con fines de lucro, en lugar de asumir una estructura descentralizada y sin propietario como la de bitcoin, despierta la sospecha de los puristas de criptomonedas, que a menudo lo definen erróneamente como un sistema centralizado. A pesar de los elaborados esfuerzos de la compañía para crear reglas transparentes y en condiciones de igualdad para emitir y diseminar su moneda XRP, inevitablemente se presenta como una trampa en Reddit y en otros foros favorecidos por la criptobomba.

El tema de los motivos de lucro de Ripple llegó a un punto crítico en mayo de 2014, cuando McCaleb hizo el asombroso anuncio de que vendería todas sus tenencias de XRP. En un breve mensaje publicado en Reddit, el cofundador dijo que después de regalar algunos de sus 9 mil millones de XRP a la caridad, ahora planeaba vender el resto en dos semanas. Eso representó aproximadamente el 9 por ciento de los 100 mil millones iniciales de suministro de dinero de XRP, que a diferencia de la emisión prolongada de bitcoins de 130 años, se creó en un solo lote en 2012. Los comentarios de McCaleb aludieron de paso a la decisión de que él y sus cofundadores Larsen y Britto había decidido asignarles el 20 por ciento de esa emisión inicial. (El 80 por ciento restante se otorgó a la fundación OpenCoin de Ripple, que coordinaba la liberación gradual de la moneda a lo largo del tiempo para optimizar su valor y utilidad como vehículo de transacciones). Pero no se dieron explicaciones reales sobre sus acciones en un asunto que de otro modo de hecho: "Debido a que tengo un gran respeto por los miembros de la comunidad y quiero ser transparente,

estoy anunciando públicamente esto antes de comenzar. Así que solo fyi ... las ventas de XRP entrantes ".

Inevitablemente, con una cantidad tan grande de monedas que se espera llegue al mercado, el precio del XRP se desplomó, perdiendo el 45 por ciento de su valor en bitcoins, la moneda contra la que cotiza en los mercados de altcoin, en dos días. El hilo de Reddit que McCaleb había iniciado se iluminó. Algunos comentaristas aplaudieron a McCaleb por ser tan abierto acerca de sus ventas; otros lo condenaron por generar FUD (miedo, incertidumbre y duda) alrededor de Ripple. Ripple Labs declaró que la venta no tenía ninguna consecuencia ya que el precio de XRP no tendría ningún impacto en la capacidad de la criptomoneda para transmitir pagos a través de la red. Pero luego las cosas se pusieron feas cuando Jesse Powell, el CEO de criptomonedas Kraken, anunció en el foro abierto de Ripple que renunciaba al directorio de Ripple Labs porque el CEO Chris Larsen había rechazado la solicitud de Powell de que los fundadores transfirieran sus asignaciones XRP personales a la compañía . (El hecho de que se realice tal solicitud habla de la relación incómoda que tienen los fundadores de criptomonedas con las personas que tienen la nueva divisa que crean. Mientras que los inversores en empresas regulares dejan que los fundadores se enriquezcan, la expectativa es que aquellos que emiten una la criptomoneda no explotará el poder único de ese papel, no se involucrará en las mismas prácticas de señoriaje que los bancos centrales tradicionales y ganará dinero por sí mismo simplemente haciendo dinero.) La administración de Ripple respondió acusando a Powell de mentir y le envió un carta de cese y desistimiento, que también exigía una retractación. Powell luego publicó la carta, que había sido marcada como "confidencial", en línea, junto con anotaciones que defendían sus declaraciones como verdaderas. La feliz comunidad de Ripplers se consumió repentinamente con mala sangre. Un poco lo llamó Jedmageddon.

Las cercas se repararon tres meses después cuando la administración de Ripple llegó a un acuerdo con McCaleb para extender su venta de XRP durante un período de siete años. Larsen, por su parte, aceptó hacer una donación de 7 mil millones de XRP (por un valor de $ 33 millones en ese momento) a una fundación independiente comprometida con los marginados financieramente. El precio de XRP se estabilizó.

Larsen no minimiza que Ripple Labs está dispuesto a ganar dinero. Mientras que "el mundo de la criptografía" a veces es sospechoso de estructuras de propiedad con fines de lucro, "cuando nos reunimos con los bancos para hablar sobre nuestro servicio, no les importa", dice. "Quieren saber qué puede hacer, y ven los beneficios". Sin embargo, al igual que con varios lanzamientos de altcoin que subieron de precio desde un principio, para posteriormente sumergirse cuando los inversores comenzaron a sospechar que los fundadores de la bomba y "estafa", es difícil disipar la sensación de conflicto de intereses cada vez que se crean nuevas criptomonedas. Volvemos al problema del señoreaje que discutimos en el capítulo 5 y que Nakamoto eligió abordar a través de la competencia de bitcoins.

Jed McCaleb utilizaría un proyecto completamente nuevo para destacar la importancia de evitar estas percepciones de interés propio. Llamado Stellar y lanzado en julio de 2014 con el respaldo y el dinero de algunos inversores clave, incluidos Keith Rabois, de Khosla Ventures, uno de los primeros fundadores de PayPal y Stripe, un fabricante de software de última generación para procesadores de pagos, el proyecto era principalmente de carbono copia de Ripple con un par de diferencias clave. De la emisión inicial de 100 mil millones de monedas, conocida como estelar, el 95 por ciento simplemente se regalaría, la mitad de aquellos a los primeros solicitantes que se registran a través de Facebook y la mitad a causas caritativas que se centran en el alivio de la pobreza y el desarrollo económico y / o los adoptantes de las criptomonedas. Mientras que el 5 por ciento todavía se reservaba para los fundadores y los primeros inversores, el lanzamiento de

otro modo gigante parecía necesario para ganarse la confianza de las poderosas hordas de entusiastas de criptografía que dominan Reddit, Bitcointalk y Twitter.

Las experiencias de uno de los clientes más importantes de Mastercoin, MaidSafe, resaltan aún más las dificultades que enfrentan los proyectos Blockchain 2.0 para recaudar dinero a través de sus monedas internas. Como producto que facilita la agrupación de almacenamiento en disco y recursos informáticos, MaidSafe es simplemente ingenioso. Como recaudador de fondos, ha demostrado ser mucho menos inteligente. Las experiencias de MaidSafe recaudando dinero demostraron los desafíos de emitir criptomonedas recién acuñadas en condiciones de igualdad, en particular, los desafíos que enfrentan los fundadores para asegurar a sus inversores que no otorgan el señoreaje injustificado a ellos mismos o a sus socios comerciales.

MaidSafe se basa en la idea de que muchas personas, incluida la mayoría de los usuarios de computadoras hogareñas, son "largas" en almacenamiento -tienen un exceso de espacio en disco no utilizado en sus computadoras y unidades externas- y podrían prestarlo a aquellos que son "deficientes" en almacenamiento . Hacer coincidir esos dos grupos a través de una red podría hacer que los recursos de computación estén disponibles a bajo costo para los programadores que escribirán el código para todas las cosas geniales de nuestro futuro descentralizado. Mientras tanto, el resto de nosotros puede convertir nuestro espacio en disco no utilizado en un generador de dinero. Las matemáticas funcionan si comparas un disco duro externo de terabyte a $ 100 con las tarifas premium en almacenamiento en la nube de Dropbox, Google Drive y Amazon Cloud, que en 2014 oscilaron entre $ 120 y $ 500 por año por la misma cantidad de almacenamiento.

MaidSafe, cuyo nombre significa Massive Array of Internet Disks, Secure Access for Everyone, pretende evitar el "desastre ecológico" que se está gestando bajo el actual paradigma basado en centros de datos para almacenamiento externo, dijo David Irvine, el ingeniero escocés que fundó MaidSafe. Los centros de datos, dice, son un desperdicio enorme de electricidad porque almacenan grandes cantidades de potencia informática infrautilizada en grandes almacenes que necesitan aire acondicionado y costoso mantenimiento. Es una forma muy ineficiente de asignar recursos en la red. Para aprender a optimizar realmente los recursos de red, Irvine estudió las colonias de hormigas y otros elementos del ecosistema natural. El mundo natural, dice, es en esencia un gigantesco sistema descentralizado de coexistencia dentro y entre especies. No tiene una organización central. Descubrió que las hormigas, por ejemplo, cambian constantemente el rol que le dan a la colonia, cambiando de trabajo dependiendo de lo que el grupo más necesita en cualquier momento. Su objetivo era diseñar una red informática para hacer lo mismo, de modo que cada nodo pudiera cambiar entre consumir y ofrecer espacio de almacenamiento en el grupo gigante de la red.

Para una moneda interna que los participantes de MaidSafe podrían usar para pagar y ganar fondos para recursos informáticos compartidos, Irvine recurrió a Mastercoin, la plataforma basada en bitcoins para aplicaciones descentralizadas. Mastercoin diseñaría una recaudación de fondos descentralizada, ejecutada de manera transparente sin un intermediario sobre la plataforma Mastercoin y la cadena de bloques bitcoin, que simultáneamente generaría las nuevas monedas seguras para la circulación de divisas, y recaudar dinero para pagar el desarrollo continuo de MaidSafe. La oferta fue diseñada para permitir a los inversores comprar Safecoins con bitcoins o con la moneda interna propia de Mastercoin, naturalmente llamadas mastercoins. La buena noticia es que la oferta recaudó la friolera de $ 7 millones en cinco horas, al menos según las tasas de cambio en ese momento. La mala noticia es que este aumento en la demanda provocó un gran colapso en la entrega de Safecoins, en parte porque los organizadores habían creado precios favorables para los titulares de Mastercoin dos semanas antes de que se lanzara la oferta. Esto significaba que por un tiempo corto la cantidad de safecoins que podía comprar con mastercoins era mayor que la cantidad que podía comprar con el equivalente derivado del

mercado en bitcoins. En efecto, implicaba un precio para Mastercoin dos veces más alto que su tasa de mercado en Cryptsy. Los inversores inteligentes lo vieron como una oportunidad clásica de arbitraje y se embarcaron en una estrategia para sacar provecho de ella. Sabiendo que muchos desarrolladores e inversores a largo plazo en el proyecto de MaidSafe comprarían mastercoins como una ruta para obtener safecoins, estos especuladores arrinconaron el mercado y aumentaron el precio hasta que desapareció la brecha de arbitraje. Pero esto dejó muy pocas mastercoins disponibles para aquellos que querían Safecoins. Inevitablemente, una vez que la oferta terminó, el precio artificialmente sostenido de las mastercoins se desplomó, dejando una horda de inversionistas enojados que tenían participaciones en una altcoin altamente ilíquida y sin garantías. MaidSafe y Mastercoin trataron de enmendarse comprando algunas de las nuevas Safecoins y revendiéndolas con un descuento para bitcoins, pero todo el asunto dejó una mala impresión, con algunos inversionistas hastiados pronosticando mal como un esquema de bombeo y volcado en tableros de mensajes de bitcoin. Era más probable solo un caso de mala planificación. Después de todo, MaidSafe también tenía el extremo corto del bote, ya que la caída del precio de la mastercoin lo obligó a rebajar su cuenta de recaudación de fondos a $ 5.5 millones. No solo eso, sino que un nuevo producto por lo demás ingenioso ahora, lamentablemente, se asociaría con una desastrosa recaudación de fondos.

Este problema de MaidSafe sin duda ha influido en el pensamiento de otros innovadores de Blockchain 2.0 sobre cómo emitir una nueva moneda, recaudar dinero para sí mismos y mantener la fe en la comunidad. Pero también tuvieron que descubrir cómo mantenerse en el lado correcto de la ley. Esta preocupación se destacó en 2014 cuando la Comisión de Bolsa y Valores impuso una multa de $ 35,000 al ex propietario de SatoshiDice Erik Voorhees y lo forzó a renunciar a $ 15,000 en ganancias por haber vendido acciones de ese proyecto a través de una oferta no registrada. Los grandes proyectos, como Ethereum, no solo han atraído al sólido talento de los desarrolladores, sino que también han contratado a algunos abogados e ingenieros financieros con experiencia que están tratando de redactar reglas de compromiso para mantener a todos contentos.

Aún así, "todos" en este sentido incluye un electorado que es especialmente difícil de complacer: los reguladores. Los abogados que actualmente actúan como enlaces entre los innovadores de criptomonedas y los reguladores del gobierno están luchando para lograr que estos últimos formen las reglas en torno a un concepto que el sistema legal existente nunca contempló. "Crees que es difícil descubrir qué es Bitcoin desde el punto de vista de la regulación, bueno, ahora estamos hablando de averiguar qué es una corporación autónoma", dice Jacob Farber, abogado principal de Perkins Coie en Washington. "Para ellos es como algo de The Matrix".

Los desarrolladores también podrían adelantarse tecnológicamente. Si la cadena de bloques de Bitcoin termina como el protocolo predeterminado para estas nuevas aplicaciones, va a necesitar una actualización seria antes de que pueda cumplir con todas estas arrolladoras promesas que alteran la vida. Bitcoin solo puede manejar siete transacciones por segundo (contra los diez mil de Visa), por ejemplo, todo debido a un límite explícito de la cantidad de datos que pueden entrar en un bloque de transacción. Ese límite deberá aumentarse significativamente si el sistema se va a expandir para incluir todos estos otros intercambios de valor además de los pagos de bitcoin. Algunos también se preocupan de que los mineros se desincentiven para confirmar las transacciones si están integrados con contratos de propiedad de alto valor, con la idea de que la compensación de los mineros no será acorde con el valor contenido en el bloque. También existen problemas con las tarifas que bitcoin impone a la transacción más pequeña, una política, como el límite de datos, diseñada para desalentar el correo no deseado y hacer que sea prohibitivamente costoso para un actor nefasto lanzar un ataque de denegación distribuida masiva o DDOS. El problema es que estas tarifas también hacen que resulte prohibitivamente costoso desarrollar ciertas aplicaciones Blockchain 2.0 que implican grandes cantidades de intercambios de datos

individuales de poco o ningún valor monetario, como la votación basada en cadenas de bloques o mensajes encriptados. La buena noticia es que entre la comunidad global de desarrolladores dispersos que trabajan en Bitcoin, muchos están abordando estos problemas y están buscando modificar el protocolo central o encontrar alternativas para las nuevas aplicaciones.

Pero incluso más allá de arreglar los aspectos técnicos, aún quedan algunos retos serios de mercadeo si estos proyectos van a lograr la adopción general. Considera la idea de contratos inteligentes. Los contratos tradicionales a menudo deben ser adjudicados por abogados porque la vida es más complicada de lo que se puede describir en un contrato o en un código de software. Si alguien incumple con un préstamo, puede ser beneficioso para el acreedor a largo plazo reducir un poco al deudor. ¿Puede un contrato automatizado, ejecutado por una máquina, descubrir eso? Recurrir a un tribunal en el que los seres humanos puedan ordenar todos los matices e intereses en competencia es de gran valor para la sociedad en general. Sabemos que la bancarrota, por ejemplo, una institución consagrada por el tiempo para alentar la renovación y ofrecer segundas oportunidades, ha ayudado a la economía de EE. UU. A recuperarse más exitosamente de las crisis que los lugares que son menos amables con los deudores. La gente puede negarse a abandonar estas opciones; pueden sentirse incómodos con la finalidad de un contrato inteligente automatizado. Sin embargo, las eficiencias de las soluciones basadas en blockchain prometen reducir drásticamente los precios si pueden consolidarse. Entonces, tal vez haya una necesidad de modelos híbridos, con una vía judicial asociada a un contrato inteligente de cadena de bloques, o algún otro medio de arbitraje fuera de línea.

Híbridos, compromisos, soluciones pragmáticas. Debe haber espacio para este tipo de pensamiento si las ideas de Blockchain 2.0 van a salir del mundo hipotético y entrar en el mundo real. Algunas de las posiciones ideológicas rígidas tendrán que ser moderadas. Eso ya está sucediendo. Algunos proyectos nuevos se están aprovechando de la estructura descentralizada y distribuida de bitcoins, pero también están utilizando la potencia y la eficiencia de un sistema centralizado interno para crear valor para los usuarios.

Uno que salió a la luz en el verano de 2014 se llama Realcoin, fundado por el prolífico inversor de bitcoin Brock Pierce y el ex ejecutivo publicitario Reeve Collins. Realcoin es una nueva criptomoneda que promete al titular el derecho a canjearla por el equivalente en dólares en cualquier momento. Los tokens digitales se pueden comercializar a través de la cadena de bloques de bitcoin, lo que permite a las personas enviar de manera económica y sencilla un bien que, en teoría, es tan bueno como un dólar para cualquier persona en cualquier parte del mundo. El problema con esta idea aparentemente simple es que para que la moneda digital conserve su valor, se requiere confianza en Realcoin para cumplir su compromiso. Reintroduce la confianza y el riesgo de contraparte central en lo que se supone que es un entorno descentralizado y sin confianza. Realcoin lo soluciona inteligentemente prometiendo llevar una reserva permanente de activos en dólares y publicitar sus tenencias en tiempo real y, de la mejor manera posible, usar blockchain para demostrar la exactitud de su contabilidad. Está centralizado, lo que muchos bitcoiners no pueden soportar, pero es transparente.

Una versión aún más centralizada de un concepto similar es Bitreserve. Esta start-up, lanzada por Halsey Minor, fundadora del servicio de tecnología de noticias y noticias CNET, permite a las personas importar bitcoins de una billetera digital en una única cuenta de Bitreserve donde pueden usar el sistema internalizado del servicio para convertirlo instantáneamente en una cuenta en dólares, euros o yenes a los tipos de cambio vigentes. Una vez dentro de ese sistema interno, también pueden realizar transferencias económicas, transparentes e instantáneas dentro y a través de las cuentas de otros usuarios de Bitreserve en cualquier parte del mundo. Al igual que con Ripple, las tenencias de Bitreserve expresadas en estas monedas fiduciarias son, en efecto, pagarés negociables en lugar de derechos reales sobre dólares. Pero a diferencia de Ripple, y al

igual que Realcoin, están respaldados por reservas de monedas fiduciarias reales que son propiedad de la empresa y cuyos saldos se actualizan y publican en tiempo real. La ventaja es que con el sistema centralizado de servidor de Bitreserve que respalda todo ese valor, los usuarios obtienen una reserva de valor garantizada denominada en la moneda de su elección. La centralización aquí ofrece una solución a la volatilidad de la celebración de bitcoins en la cadena de bloques descentralizada, pero conserva la capacidad de transferir fondos de forma rápida y económica de forma digital.

La viabilidad de Bitreserve aún no se ha probado, pero la idea de Minor vale la pena considerarla como una lección general sobre cómo los enfoques tradicionales como las reservas de moneda fiduciaria y los servidores centralizados pueden dar a los aspectos revolucionarios de la criptomoneda una aplicación práctica. Es una desviación de los principios de la descentralización a toda costa detrás de la mayoría de las ideas de criptomonedas grandes, pero no sería una sorpresa ver el lanzamiento de más start-ups como Bitreserve.

"Es como si fuéramos Henry Ford y estamos trabajando con esta nueva e increíble invención, el automóvil, pero ni siquiera hemos empezado a comenzar la producción del Modelo T y ahora estamos diciendo: 'Oye, salgamos'. y construye un cohete ", dice Nicolas Cary, CEO de Blockchain.info. Él quiere que la comunidad de desarrolladores, cuyos servicios están limitados, se concentre en obtener bitcoin justo antes de pasar a todas estas nuevas aplicaciones.

Pero es imposible evitar que los soñadores sueñen. La creación de la cadena de bloques, con sus oportunidades para reorganizar la forma en que los seres humanos interactúan y hacen comercio, ha desatado una lluvia de imaginación entre los geeks de la computación. Sienten una revolución y ya están fijando sus objetivos, independientemente de si estamos listos.

No solo las nuevas empresas, como Ethereum y MaidSafe, lanzan recaudaciones de fondos denominadas en criptomonedas, sino que incubadoras especiales como Swarm están creando vehículos de inversión denominados en criptomonedas para fomentar el desarrollo de otras start-ups descentralizadas financiadas con criptomonedas. Con capas sobre capas y plataformas sobre plataformas, esto puede ser confuso, pero la idea clave es que las nuevas aplicaciones de software pueden convertir plataformas extensibles como Bitcoin en poderosos agentes de cambio.

Las nuevas empresas están tratando de lidiar con la afluencia de innovaciones en este campo y darle sentido. Una compañía llamada Chain proporciona servicios altamente especializados de administración de redes y software para empresas que desean crear aplicaciones descentralizadas sobre bitcoin o cualquiera de los otros blockchains y protocolos. Coinist se ha establecido como una agencia de calificación para la afluencia de activos digitales y criptomonedas que llegan al mercado en las plataformas Blockchain 2.0, como Next y Ripple. El fundador John Whelan está posicionando a la empresa como el Servicio de Inversores Moody's de criptomonedas. Si hay un mercado para sus servicios, se reconocerá que, aparte de las propias transacciones descentralizadas de blockchain, los emisores de esos nuevos activos son inherentemente instituciones centralizadas que requieren confianza y, por lo tanto, exigen evaluaciones objetivas de su confiabilidad. Mientras tanto, la firma de capital de riesgo Aleph, con sede en Tel Aviv, está incubando proyectos de Blockchain 2.0 ofreciendo bonificaciones de $ 50,000 -una especie de premio a la inversión- para empresas nuevas que ideen soluciones a algunos de los obstáculos al desarrollo de estos proyectos. Al menos una consultora, Humint, asesora a empresas e incluso a personas sobre cómo crear sus propias monedas digitales corporativas y personalizadas.

Para colmo de males, Open Transactions, con sede en Zurich, está compitiendo por que el metaproyecto finalice todos los metaproyectos. Está desarrollando un programa de software que

instruye a los servidores a conectar todos estos blockchains, protocolos y monedas de la competencia dentro de una estructura descentralizada e interconectada. Para simplificar en exceso una idea muy compleja, busca crear pasarelas entre distintas plataformas sin confiar a los guardianes información valiosa ni pagarles ninguna tarifa. Si tiene éxito, el proyecto creará un intercambio descentralizado único, sin interrupciones, que funciona por sí mismo, un gigantesco bazar de Internet en el que casi todo puede ser intercambiado, transferido y valorado en tiempo real. El fundador de Open Transactions, Chris Odom, quiere invertir la tendencia donde las rutas para conectar Bitcoin con otras plataformas, ya sea con criptomonedas alternativas o con la economía de moneda fiduciaria, se han ejecutado a través de entidades de terceros confiables, el intercambio fallido de Bitcoin siendo el caso de Mt Gox que destaca los peligros de este enfoque. "Este no es el sueño de Satoshi", dice Odom.

No sabemos si el sueño de Satoshi incluía todas las aplicaciones de Blockchain 2.0 que ahora se están construyendo sobre su moneda y sistema de pago más estrechamente definidos. Pero al abrir la puerta a todas estas nuevas formas de organizar negocios y la sociedad, tal vez inevitablemente desencadenó el tipo de tensión que implica el comentario de Odom. Satoshi inició un movimiento de descentralización que ahora está chocando con un sistema preexistente de negocios y leyes que busca perturbar, dando lugar a tensiones dentro de la sociedad en general, pero también dentro de las mismas comunidades de criptomonedas. Este frente de batalla es el tema del próximo capítulo. *

Capítulo 10

COSAS QUE NO ENCAJAN

> La insolencia de la autoridad se esfuerza por sustituir el dinero por ideas.
>
> -Frank Lloyd Wright

Gavin Andresen abrió la puerta de su raída oficina de subarrendamiento, ubicada en un edificio anodino encima de un Dunkin 'Donuts en la ciudad universitaria de Amherst, Massachusetts. La habitación contenía poco más que un escritorio de plástico improvisado y su computadora, una Apple iMac. Una semana antes había limpiado su oficina en la casa que comparte con su esposa, Michele, profesora de geología en la Universidad de Massachusetts, y dos niños. Había decidido que un hombre esencialmente, si no fuera titular, a cargo de administrar una economía de $ 8 mil millones necesitaba algo más que una oficina en casa. Si la nueva oficina estaba escasamente amueblada, tenía la virtud de la privacidad ininterrumpida. Hoy, lo necesitaría.

Era el 10 de febrero de 2014. Cuando revisó su correo electrónico esa mañana, descubrió que su bandeja de entrada rebosaba de mensajes de pánico de todo el mundo. De la noche a la mañana, el cambiante intercambio de divisas digital Mt Gox, esta vez verdaderamente en su lecho de muerte, había advertido de un error peligroso en el software subyacente de bitcoin que permitía a los piratas informáticos crear códigos de transacción falsos y exigir pagos injustificados. Ahora, personas con todo tipo de participación en la moneda buscaban ayuda de Andresen. La versatilidad que ofrece la estructura no regulada y sin líder de bitcoins ha sido una de sus grandes fortalezas, pero ahora los defectos en esa falta de supervisión se hacían evidentes.

Si bien el código básico de fuente abierta de bitcoin permitió que cualquiera lo examinara y sugiriera adiciones y mejoras, solo unas pocas personas, esencialmente cinco hombres asignados al equipo de desarrollo central, tenían acceso mediante contraseña al código en vivo dentro del protocolo central. De ellos, el que tenía la mayor responsabilidad de supervisar el programa era Andresen, el científico jefe de cuarenta y siete años del principal grupo representativo de bitcoin, la Fundación Bitcoin. La fundación le paga para coordinar la aportación de los cientos de técnicos remotos que manipulan el software con licencia abierta. En este momento, la comunidad de bitcoin necesitaba respuestas, y en ausencia de un CEO, un CTO o cualquier autoridad central a la que recurrir, Andresen era su mejor esperanza. ¿Cuál era esta falla de "maleabilidad de transacción" de la que hablaba Mt Gox? ¿Qué tan malo fue? ¿Estaba la cadena de bloques comprometida? ¿Era seguro el dinero de las personas?

Después de llegar a su oficina, Andresen pasó un tiempo leyendo los mensajes, tratando de determinar la naturaleza del problema. Para él, la línea de "maleabilidad transaccional" en la declaración de Mt Gox era sospechosa. Este problema ya se había identificado en el 2011 y se discutió mucho en los foros de desarrolladores. Se refirió a una característica del software de billetera suplementario que se creó junto con el código de protocolo central original y que dentro de una breve ventana después de una transacción permitió a alguien alterar una identificación de transacción para agrupar más de uno. En teoría, esto significaba que un defraudador podría engañar a un intercambio como Mt Gox para que creyera que nunca se había producido un pago intencionado, esencialmente haciendo que pareciera que la transacción nunca había caído en la billetera del estafador, y pedir que se lo reenviara. Pero esta "peculiaridad", como le gustaba llamar a Andresen -la maleabilidad de los códigos de transacción era una característica deliberada,

aunque cuestionable, no necesariamente un error o un error- se resolvió fácilmente si una divisa usaba procedimientos contables básicos para controlar su registros internos de bitcoins salientes. Andresen se sorprendió al escuchar que el CEO de Mt Gox, Mark Karpelès, un participante activo en los foros de desarrolladores de bitcoin en el que la maleabilidad de las transacciones había sido discutida extensamente, no lo conocía o tenía precauciones.

Andresen llegó a la conclusión de que Mt Gox había malinterpretado y / o tergiversado intencionalmente sus problemas internos y había culpado injusta y erróneamente a Bitcoin por esos problemas. Él preparó un post para el blog de la Fundación Bitcoin que decía eso. Llevaba el título "Al contrario de la afirmación de Mt Gox, Bitcoin no tiene la culpa" y declaró que el protocolo era sólido y simplemente recordó a las empresas que usaran "mejores prácticas" para administrar sus billeteras.

El tema animó a Andresen a trabajar de una vez por todas en una solución para poner fin a la función de maleabilidad de las transacciones, que se pospuso por un tiempo a favor de tareas más apremiantes. Por amplio acuerdo, era una molestia, pero su eliminación implicaba una ingeniería complicada. Aun así, por lo que él sabía, nada en el código central se veía amenazado de inmediato. Utilizando una sala de IRC, discutió el asunto con algunos de sus colegas, dos de los cuales están en Europa, dos en Estados Unidos, y algunos otros desarrolladores, pero no tenía sentido de urgencia. Es decir, hasta que llegó un nuevo mensaje, de Gregory Maxwell, un codificador de bitcoin voluntario de Mountain View, California.

Maxwell había hablado con Karpelès de la noche a la mañana, había hecho algunas excavaciones y se había dado cuenta de que efectivamente había un problema, potencialmente grande, en el código subyacente del software estándar de billetera. Creía que podría permitir que un actor deshonesto pirateara los registros de transacciones y causara daños. Esencialmente, un pirata informático podría convertir el error de maleabilidad de la transacción en un tipo de ataque DDOS (denegación de servicio distribuida) e inundar la red con códigos de transacción falsos. Andresen diría más tarde que una de esas cosas era "simplemente esconderse a la vista". La integridad de la blockchain en sí misma no se vio comprometida, ya que tanto la característica de maleabilidad de transacción como la falla residían en el software suplementario de billetera, no en el protocolo central que dictaba las funciones críticas de gestión de minería de datos y blockchain. Sin embargo, los intercambios y otras entidades que realizan transacciones frecuentes eran vulnerables a múltiples solicitudes fraudulentas de pago. La red bitcoin era segura, pero el ecosistema bitcoin a su alrededor estaba en peligro, todo por un error que estaba al acecho en el software original presentado por Satoshi Nakamoto. El fundador, nos dijo Andresen, era un brillante codificador de "lobo solitario", pero un operador un poco descuidado que nunca sometería su código al tipo de prueba que es rutina en la mayoría del trabajo de desarrollo.

El propio Nakamoto, o quienquiera que representara el usuario anónimo de la sala de chat, había elegido a Andresen con gafas para su trabajo actual. En los primeros días de Bitcoin, el desarrollador de software nacido en Australia había tenido un intercambio con el fundador de incógnito de Bitcoin sobre un problema mucho más grande que este. En 2010, alguien silenciosamente les dijo a los dos que un error en el software permitiría que la gente gastara el bitcoin de otras personas. Manteniendo el problema en secreto, Nakamoto simplemente lo solucionó y anunció a la incipiente comunidad que deberían usar una nueva versión del código. No mucho después de eso, Nakamoto, en consulta con otro codificador principal, Jeff Garzik, decidió que Andresen debería ser el líder en la coordinación del pequeño equipo de desarrolladores principales con acceso al código. Nakamoto le dijo que fue elegido, dice Andresen, por su actitud calmada.

Ahora, el ingeniero informático descubrió que su nivel de estrés aumentaba. Estaba preocupado de que con toda la atención que Mt Gox había atraído al problema de la maleabilidad de las transacciones, alguien intervendría y explotaría el error que Maxwell había identificado. Pero el problema profundamente arraigado no se eliminaría fácilmente del programa; tomaría nuevas codificaciones y pruebas significativas. Mientras tanto, la comunidad mundial de bitcoins estaba nerviosa; el reclamo de Gox sobre el error no solo era confuso, sino que además de haber congelado el acceso de los clientes a sus bitcoins, le entró el pánico a algunos. Andresen trabajó hasta tarde en la consulta con otros desarrolladores en la sala de chat sobre cómo proteger la red. A las 2:00 a.m., envió órdenes de marcha para el trabajo de reparación del día siguiente a los otros cuatro miembros de su equipo, uno en Mountain View, Atlanta, Zurich y Eindhoven en los Países Bajos. Por fin, pudo dormir.

Pero la mañana no restableció la calma. De la noche a la mañana, cuando se corrió la voz sobre la vulnerabilidad, la gente ya se había ocupado de intentar explotarla. Se despertó y descubrió que los intercambios Bitstamp y BTC-e, junto con otros intermediarios y servicios de bitcoin, se habían visto obligados a detener las operaciones, ya que cedieron bajo un aluvión de reclamos falsos que explotaban el error de maleabilidad de la transacción. Estos usuarios pesados y comerciales del software genérico de billetera bitcoin habían sido incluidos en el mismo evento tipo DDOS que los desarrolladores temían. El precio del bitcoin, a $ 703 apenas veinticuatro horas antes, había caído a un mínimo de $ 535 durante la noche.

Andresen regresó a los desarrolladores principales. Ahora no solo tenían que abordar el error sino que también tenían que ayudar a que los intercambios volvieran a funcionar. Garzik, a quien el procesador de pagos BitPay le paga en Atlanta pero se lo considera un miembro permanente del equipo de desarrollo de bitcoin, se centraría atentamente en la redacción de "parches", soluciones prácticas que Bitstamp, BTC-e y otros operadores afectados podrían instalar mientras se diseñó una solución permanente. Wladimir van der Laan, residente de Ámsterdam, que también está en la nómina de pago de la Fundación Bitcoin, trabajaría con Andresen en una solución más duradera. Harían una profunda inmersión en el código de software de bitcoin, identificarían los errores y pasarían por el laborioso proceso de escribirlos y luego probar todo el sistema. Los dos desarrolladores voluntarios, Maxwell, empleado de la Fundación XIPH para mantener Internet libre de intereses especiales, y Pieter Wuille, que trabaja para Google en Zurich, harían lo que pudieran con el tiempo que pudieran ahorrar en sus trabajos diarios. Mientras tanto, las demandas seguían llegando de desarrolladores de software, mineros, inversores de bitcoins y comerciantes. ¿Estaba seguro Bitcoin? ¿Por qué estaba pasando esto?

Hablamos con Andresen una noche en medio de la crisis. "Tengo que irme a la cama", dijo. "Tengo que mantener mi cordura. Tengo que decirme a mí mismo, 'No es todo sobre mí.' Sabes, parte de la filosofía del código abierto se supone que es que si tienes problemas, no esperes que alguien te lo arregle, soluciónalo tú mismo. Tal vez hemos hecho un buen trabajo y la gente se ha vuelto complaciente y espera que el equipo de desarrollo central arregle cualquier cosa desgarradora. Esa es una expectativa irracional. Somos cinco personas y solo tres de ellas son de tiempo completo ".

Imagínese una crisis monetaria de la misma magnitud para un gobierno: una cuarta parte de la riqueza nacional, medida en términos de dólares, desapareció en dos semanas. Es el tipo de cosas que sucede de vez en cuando en los mercados emergentes. Imagine el ejército de personal que el ministerio de finanzas nacional y el banco central ordenarían en acción para estabilizar la economía; Imagine también los refuerzos de apoyo técnico y financiero que provendrían de los equipos SWAT en el Fondo Monetario Internacional. Compare eso con lo que estos cinco hombres, dos de ellos voluntarios, se enfrentaron, y usted tendrá una idea de qué tan diferente está

estructurada la economía de Bitcoin, así como los desafíos particulares de mantener un modelo de código abierto como este.

El arreglo minimalista para el equipo central de bitcoin, hasta las paredes desnudas y expuestas y el escritorio endeble de Andresen en la oficina de doce por doce pies que subarrienda de una firma de inversión de Nueva Inglaterra, refleja una estructura organizativa que está fundamentalmente descentralizada. Las instituciones estatales que manejan nuestros sistemas monetarios y las corporaciones públicas que administran efectivamente nuestras economías capitalistas son jerárquicas; se supone que el dinero se detiene con el CEO. Entonces, ¿qué significa esto para Bitcoin, donde nadie está realmente a cargo? Andresen es un sustituto de algo que no existe.

El equipo de Andresen tardaría casi un mes en corregir el error, aunque la solución de parches de Garzik aseguró que la mayoría de los intercambios, aparte de los condenados Mt Gox, volvieran a funcionar para el final de la semana. En el peor momento de esta crisis, el precio de la moneda digital caería un 32 por ciento, destruyendo $ 3 mil millones en riqueza, antes de recuperar algo de terreno en la última parte de febrero.

Pero algo positivo también había surgido. A pesar del lamento del codificador jefe por tener el peso del mundo sobre sus hombros esa noche, al final la configuración de fuente abierta sirvió bien al software de bitcoin después de la debacle del Monte Gox, porque puso a muchas mentes a trabajar, todo con un interés creado en la solución del problema. Los cinco desarrolladores principales hicieron la mayor parte del trabajo pesado, pero legiones de codificadores talentosos en la comunidad aportaron soluciones de pensamiento y codificación, y pusieron a prueba el trabajo del equipo central. Entonces, aunque la falta de liderazgo centralizado de Bitcoin crea el problema de no tener a nadie con quien se suponga que se detenga, su banco de talento profundo y global a menudo significa que sale de crisis como esta con un software notablemente mejorado.

"Probablemente diez mil de los mejores desarrolladores del mundo están trabajando en este proyecto", dice Chris Dixon, socio de la firma de capital de riesgo Andreessen Horowitz. "Debido a que no están sentados en un edificio llamado Bitcoin Incorporated, la gente parece perderse ese punto". Dixon dice que su equipo "apuesta por la innovación informática, y dado que [la colaboración de código abierto] es la forma en que la innovación informática ocurre hoy, esto es el tipo de cosas en las que apostamos Ciertamente, no me gustaría apostar contra las diez mil personas más inteligentes. "Esta confianza cerebral gigante es una razón clave por la que no está preocupado por los diversos errores que aún se encuentran en el software de bitcoin y por qué cree que las mayores innovaciones aún se construyen esta por venir. "Usted lee estas críticas de que 'bitcoin tiene este defecto y Bitcoin tiene ese defecto', y nosotros pensamos 'Bueno, genial'. Bitcoin tiene a diez mil personas trabajando duro en eso '".

No es un proceso sencillo, pero esta vasta comunidad de desarrolladores de software en todo el mundo se confunde para llegar a una solución de consenso. Tampoco es exactamente democrático, ya que los cinco miembros principales deben decidir finalmente qué hacer. Pero el propio equipo central utiliza un proceso de consulta y presta mucha atención a las sugerencias de la comunidad en general con la que se comunica frecuentemente con los mensajes transmitidos. De esta manera, el programa de código abierto de bitcoins, un modelo de desarrollo colaborativo que es utilizado por innumerables otros proyectos de software actualmente, explota elegantemente la sabiduría inherente de una multitud. Es por eso que el colapso de Mt Gox fomentó, y rápidamente, algunas de las soluciones criptográficas más brillantes para la seguridad de bitcoin, si no para la seguridad financiera en general. El acuerdo de código abierto descentralizado significa que el caos descenderá sobre el proyecto de vez en cuando, pero también significa que el progreso y la mejora pueden ocurrir rápidamente.

El colapso de Mt Gox y la quiebra de la Ruta de la Seda antes de ayudar a impulsar un movimiento dentro de Bitcoin, uno dirigido por una facción creciente de empresarios y empresarios, para tener una visión más acogedora de la regulación en lo que había sido un dominio sin ley. Era hora, algunos bromistas, para que este adolescente rebelde creciera. Yendo contra los puntos de vista de algunos de los primeros adoptantes de mentalidad libertaria, que veían al gobierno como una presencia entrometida que destruiría este proyecto de laissez-faire, estos recién llegados con menos inversión en la misión filosófica de bitcoin vieron ahora la regulación como la ruta hacia la salvación de bitcoin. Sin él, creían, la criptomoneda continuaría siendo percibida por el público en general como un producto marginal arriesgado y, por lo tanto, nunca cumpliría su potencial como tecnología disruptiva. Naturalmente, tales puntos de vista alimentaron la división dentro de las categorías de bitcoins, con los primeros adoptantes ideológicamente impulsados por un lado y una nueva ola de "trajes" más pragmáticos por el otro.

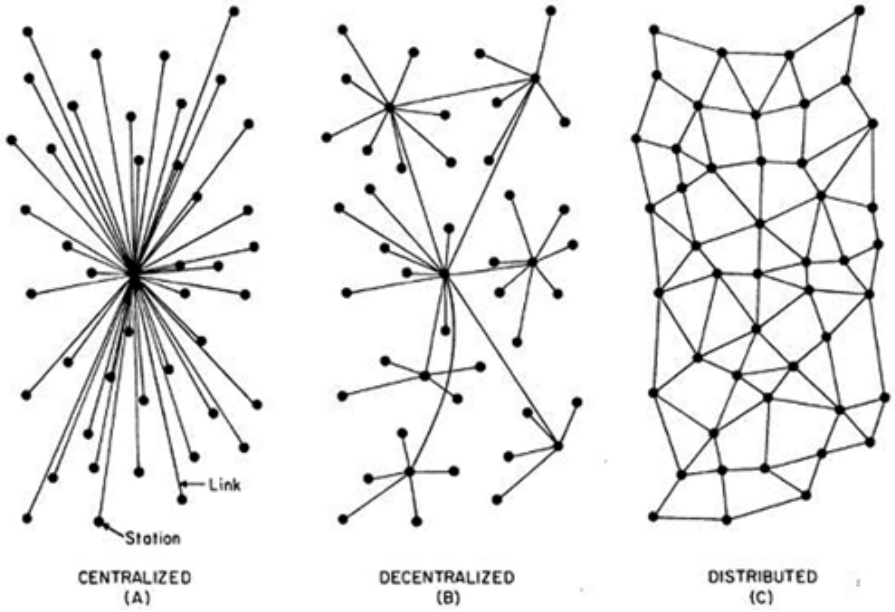
Mientras tanto, las fuerzas de seguridad tenían preocupaciones reales sobre los delincuentes atraídos por el anonimato inicial de la criptomoneda, y los reguladores financieros estaban preocupados de que los inversores en bitcoin y productos de bitcoins fueran vulnerables al fraude. Pero regular las criptomonedas fue más fácil decirlo que hacerlo debido a lo que podría llamarse el desafío de las estrellas de mar.

En su libro de 2006, The Starfish and the Spider: El poder imparable de las organizaciones sin líderes, Ori Brafman y Rod Beckstrom desarrollaron una metáfora para explicar el poder del tipo de colaboración de código abierto y toma de decisiones descentralizada que define el bitcoin. Si te cortas una pata de araña, queda lisiada y si te cortas la cabeza, muere, nos dicen los autores. Pero si le cortas la pierna a una estrella de mar, crece una nueva, y la pierna desalojada puede convertirse en una estrella de mar completamente nueva. En cuanto a una cabeza o cerebro, no tiene ninguno. Del mismo modo, una organización descentralizada no tiene un punto central de vulnerabilidad y, por lo tanto, es prácticamente imposible cerrarla o destruirla. Brafman y Beckstrom exploran algunas organizaciones contemporáneas de Internet que prosperaron bajo las ventajas de la descentralización como las estrellas de mar: Wikipedia, Craigslist y Skype, por ejemplo. También citan casos de fuera de la red: los alcohólicos anónimos sin líder, la tribu apache y la institución descentralizada máxima de nuestra era, al-Qaeda.

Las experiencias de Napster y BitTorrent también son instructivas. Si bien el innovador servicio de intercambio de archivos del primero representaba un desafío para el control del negocio de la música por parte de las compañías discográficas, su red estaba centralizada y controlada en un servidor identificable. Por lo tanto, los agentes del gobierno, armados con sentencias de infracción de derechos de autor, finalmente pudieron cerrarlo. BitTorrent, por el contrario, no reside en ninguna parte en particular. Es imposible cerrar, por lo que su servicio de intercambio de archivos ha sobrevivido.

Lo que hace que esto sea posible para BitTorrent, como lo es para Bitcoin, es una red distribuida, la última forma de descentralización, según un esquema de estructura de red establecido por el pionero de la informática Paul Baran en un influyente documento de 1964. Con Bitcoin, siempre que ningún minero obtenga el control del 51 por ciento de la potencia de hash, la red de minería que administra el sistema monetario tiene una estructura de poder totalmente distribuida. Ninguna entidad en ninguna parte tiene control sobre el sistema, lo que significa que no tiene un punto vulnerable de ataque. Esto no quiere decir que no haya vulnerabilidades en el ecosistema que se haya construido alrededor de esa red, en intercambios defectuosos como Mt Gox, cuyos problemas de control recentralizado exploraremos más adelante, o en errores asociados al software que interactúa con ese ecosistema como el descrito anteriormente. Pero la red distribuida en sí misma, el grupo ad hoc de computadoras que colectivamente decide sobre qué es Bitcoin y cómo debería funcionar, es virtualmente imposible de cerrar.

¿Cómo fueron los reguladores para enfrentar este dilema? Sin un CEO a cargo de la moneda o alguien a quien citar, ¿cómo se controla la economía de bitcoin? La ley está diseñada para tratar con instituciones centralizadas en las cuales los gerentes identificables son considerados responsables de la conducta de una organización.



Grados de centralización / descentralización de redes de Paul Baran
(Como se ve en el artículo de Paul Baran de 1964 "Sobre redes de comunicaciones distribuidas" en ComputerHistoryMuseum.com, imagen cortesía del Computer History Museum)

Un incidente cuyo recuento tiende a provocar risas engreídas del público en las conferencias de bitcoin ilustra el problema. En junio de 2013, la División de Instituciones Financieras de California presentó una carta de cese en la Fundación Bitcoin diciendo que necesitaba una licencia de transmisión de dinero del estado. Pero la fundación en realidad no hace ningún negocio; su misión es promover la adopción de bitcoin, ponerse en contacto con los gobiernos en asuntos regulatorios y financiar el trabajo de desarrollo para salvaguardar el protocolo de fuente abierta de la criptomoneda. Pero si no ellos, ¿quién?

A menudo, para muchos legisladores es difícil darse cuenta de la naturaleza del desafío al que se enfrentan. En febrero de 2014, el senador demócrata de West Virginia Joe Manchin pidió que se prohibiera el uso de bitcoins. Pero, ¿qué implicaría esto? Podrías hacerlo ilegal, pero eso surgiría para desafíos constitucionales inmediatos. ¿Qué está prohibiendo exactamente que las personas posean? Código digital? En esencia, es una forma de comunicación. Eso implica derechos de la Primera Enmienda. ¿O es una mercancía, algo que se puede cambiar a cambio de otra cosa? De ser así, eso plantearía problemas con los derechos comerciales y de propiedad. Es difícil ver cómo podría capturarse Bitcoin bajo una definición legal de bienes controlados como pornografía infantil o drogas ilegales. Aún así, el punto más importante de todos: ¿cómo lo controlas? Es el problema de BitTorrent nuevamente. No hay un servidor central para que los federales cierren.

Sin embargo, a pesar de la creencia de bitcoiners en la invencibilidad de su dominio de criptomonedas, los gobiernos están equipados con un inmenso poder legal. Tienen todo tipo de formas de dificultar la vida de la criptomoneda. Como dijo Gareth Murphy, director de supervisión de mercados en el Banco Central de Irlanda, en una conferencia de bitcoin en Dublín, la audiencia "no debería sorprenderse si Moisés bajó de la montaña con la ley".

En los Estados Unidos, el primer descenso desde la cima de la montaña fue el busto del FBI de Silk Road en 2013. Si bien esto marcó un grave golpe para la reputación del bitcoin y dejó una impresión negativa en las mentes tanto de los funcionarios del gobierno como del público en general, posiblemente allanó el camino para que los reguladores se relacionaran con la comunidad bitcoin de una manera más constructiva. Dado que el FBI se había apoderado de los bitcoins y planeaba mantenerlos en subasta, reconoció implícitamente que estas cadenas de código digital tenían algún valor real. De manera indirecta, era un sello de legitimidad. Además, el aparente éxito de la operación hizo que bitcoin fuera menos desalentador para la aplicación de la ley en los Estados Unidos. Los funcionarios descubrieron que podrían usar blockchain como una herramienta para rastrear transacciones y controlar a los usuarios, si no los identifican fácilmente.

Un mes después de la caída, la Red de Control de Delitos Financieros del Departamento del Tesoro, o FinCEN, adoptó un enfoque sorprendentemente complaciente con la criptomoneda. La FinCEN emitió directrices que trataban a los procesadores de pagos de bitcoin y las bolsas de valores como entidades legales que tendrían que registrarse y tendrían que cumplir con las normas estado-por-estado sobre las licencias de transmisores de dinero. Esto preparó el terreno para una audiencia del Senado muy esperada en noviembre de 2013, donde la directora de FinCEN, Jennifer Shasky Calvery, pronunció unas palabras que entusiasmaron a todos menos a los más doctrinarios de bitcoiners: "La decisión de llevar moneda virtual dentro del marco regulatorio debe ser vista por aquellos que respetan y obedecen el estado de derecho básico como un desarrollo positivo para este sector. Reconoce la innovación que brindan las monedas virtuales y los beneficios que pueden ofrecer a la sociedad ".

El gobierno había hablado. No solo no estaba demasiado preocupado por la criptomoneda, sino que también tenía ventajas. Y si los bitcoiners no eran grandes admiradores de la regulación gubernamental, las reglas de FinCEN eran simplemente una extensión de aquellas que por mucho tiempo se habían aplicado a los proveedores de remesas en dólares, los procesadores de pagos y los servicios de divisas. Fue, al menos en papel, el mismo trato. Las empresas de Bitcoin habían recibido legitimidad.

Pero esto fue solo el comienzo. La legitimidad necesitaba más que la bendición de una agencia federal, especialmente en los Estados Unidos, donde el negocio de la transmisión de dinero es una preocupación estatal y federal. Los negocios de Bitcoin aún tenían que obtener una licencia de estos estados, lo que a su vez requería que explicaran sus actividades desconocidas a la agencia de cada estado y probaran que tenían procedimientos de cumplimiento para prevenir el lavado de dinero y otros usos nefastos de los sistemas de transferencia de dinero. Obtener una licencia fue laborioso, impredecible, burocrático y prolongado.

Algunos estados, como Texas, adoptaron una postura deliberadamente acomodaticia y decidieron que las criptomonedas no estaban dentro de los límites de sus reglas y, por lo tanto, se les podía permitir funcionar sin una licencia. Eso llevó a un montón de escaparates en entornos texanos amigables con la tecnología como Austin para configurar cajeros automáticos bitcoin para permitir a las personas convertir dentro o fuera de bitcoin y efectivo en el acto. Mientras tanto, muchas empresas seguían operando en otros lugares con la suposición de que eventualmente obtendrían licencias en los estados que importaban. Aun así, gran parte del alcance de los clientes para start-ups de Bitcoin se estancó, incluso si esas empresas continuaron emprendiendo la innovación y el desarrollo a un ritmo vertiginoso, ya que sin licencias de la mayoría de los estados sus equipos de gestión no estaban seguros de si serían enjuiciados. Estas demoras burocráticas significaron que los intercambios de bitcoins basados en los EE. UU. Como Kraken y CoinMKT lucharon por competir con competidores mucho menos regulados en Europa como Bitstamp y BTC-e.

Alrededor del tiempo de la aparición en el Senado de Shasky Calvery, el ambicioso superintendente del Departamento de Servicios Financieros de Nueva York, Benjamin Lawsky, dijo que estaba explorando la idea de una "BitLicense" especial para establecer reglas adaptadas a la industria de las monedas digitales. Dada la prominencia de Nueva York en el mundo de las finanzas, muchos en la comunidad de bitcoin esperaban que esto se convirtiera en una plantilla para otros estados. Lawsky tomó un enfoque proactivo. En febrero del año siguiente, celebró audiencias sobre la regulación de bitcoins, en la que llegaron a testificar algunos de los recién llegados más adinerados y mejor conectados al emprendimiento bitcoin, incluidos Tyler y Cameron Winklevoss, el CEO de SecondMarket Barry Silbert y Jeremy Allaire de Circle Financiero. Después de las audiencias, Lawsky llevó a Reddit para dirigir una de las sesiones AMA (Ask Me Anything) de ese foro social. Este fue un movimiento audaz pero estratégicamente astuto. La comunidad bitcoin de Reddit puede ser un grupo duro e ingobernable, y no son conocidos por su deferencia a la autoridad.

A Lawsky le fue bastante bien en ese foro. Rompió el hielo al admitir que era un neófito de Reddit. Los bitcoiners fueron en su mayoría educados en respuesta, haciendo preguntas difíciles pero prácticas. Una persona citó al banco británico HSBC, que acababa de acordar un acuerdo sin culpabilidad de 1.900 millones de dólares con el gobierno de Estados Unidos por cargos de negocios con carteles mexicanos de la droga, y preguntó: "¿Por qué Bitcoin recibe el martillo cuando todo lo demás simplemente se desliza? ¿el radar cuando se trata de lavado de dinero? "Pero la mayoría de las preguntas sobre qué tipo de transacciones de bitcoin entrarían bajo las reglas de la emisora de dinero y las definiciones de Lawsky de" moneda virtual ". Sus respuestas sugirieron que estaría abierto a un diálogo constructivo con la comunidad en estos asuntos.

A medida que las empresas de bitcoin esperaban las nuevas reglas de licencia en Nueva York, continuaron enfrentando obstáculos para ganar legitimidad, entre ellas la cautela que raya en la paranoia de los banqueros. Desde la Ley Patriótica posterior al 11/9 y otras iniciativas lanzadas para matar de hambre a los terroristas y otros tipos de fondos malos (con un éxito limitado), los bancos reforzaron sus equipos de cumplimiento, cuyos funcionarios fueron acusados de implementar un nuevo y resistente lavado de dinero. (AML) y conozca a su cliente (KYC). Su poder se incrementó aún más a raíz de la crisis financiera, ya que la reforma multifacética del Dodd-Frank Act del sistema financiero de los Estados Unidos hizo que los bancos se preocupen aún más por la caída de sus supervisores del gobierno. Las primeras respuestas de los oficiales de cumplimiento a un cliente cuyo modelo de negocios fue ligeramente fuera de lo común fueron decir que no y luego quizás tratar de resolver las cosas más adelante. En este entorno, la palabra bitcoin era como una etiqueta de leproso. Muchos en la industria de la criptomoneda tuvieron que establecer relaciones bancarias en el extranjero y encontrar otras formas de organizar sus operaciones con jurado.

Fue difícil moverse sin tener una cuenta bancaria. No todos podrían ser como Blockchain, la firma analítica de billetera y bitcoin que pagaba personal y proveedores en bitcoin y no tenía una cuenta bancaria regular. La compañía con sede en Londres representaba el ideal sin bancos con el que soñaban los bitcoiners, pero por ahora a la mayoría de las empresas les resultaba extremadamente difícil replicar. ¿Cómo interactuarían con los proveedores y clientes que esperaban pagar o ser pagados en moneda fiduciaria? Fue especialmente difícil para los intercambios de bitcoin, que sin una cuenta bancaria se redujeron a tomar, almacenar y pagar en efectivo a cambio de la comercialización de bitcoins. Esta no era una forma de aumentar las operaciones.

Tampoco se puede culpar por completo al exceso de celo en los oficiales de cumplimiento bancario. Las señales que los bancos recibieron del gobierno fueron ambiguas y contradictorias.

FinCEN se estaba adaptando al bitcoin, y la Reserva Federal era ambivalente: la presidenta de la Fed, Janet Yellen, señaló durante una audiencia en Capitol Hill que la Fed no tenía autoridad para supervisar el bitcoin y que los legisladores lo resolvieron. Sin embargo, los bitcoiners reportarían que los agentes de la Federal Deposit Insurance Corporation, el organismo encargado de limpiar los bancos en quiebra para que los depositantes asegurados puedan mantenerse enteros, estaban presionando a los oficiales de cumplimiento bancario para que no trabajen con bitcoiners. Es difícil verificar este reclamo. La FDIC había comunicado sus inquietudes a los banqueros por categorías de comerciantes supuestamente de alto riesgo, y los agentes de cumplimiento bancario le dijeron a las empresas de bitcoin que estaban incluidas en esos grupos. Pero no hay una política general; Los supervisores de FDIC usan su discreción en cada caso. Sin embargo, a raíz de la bancarrota de $ 500 millones de Mt Gox, cuya relevancia para este debate veremos más adelante, no habría sido sorprendente que el bitcoin pareciera ser de alto riesgo para la FDIC. A diferencia de los acreedores de Mt Gox, su banco japonés, Mizuho, evitó grandes pérdidas, pero su participación en ese lío le habría recordado a los funcionarios de la FDIC los riesgos cuando los bancos se involucraron con negocios de bitcoins.

El Departamento de Justicia de Estados Unidos también envió mensajes a los bancos que contradecían el mensaje complaciente de la FinCEN. En 2013, el DOJ lanzó una iniciativa conocida como Operation Choke Point, en la que investigó bancos que trataban con comerciantes en negocios que no eran necesariamente ilegales pero que se consideraban de alto riesgo de fraude. El abogado con sede en Miami Andrew Ittleman, que se ha convertido en un experto accidental en el tema, nos dijo que Operation Choke Point ahora ocupaba la mayor parte de su tiempo y que principalmente sus clientes eran proveedores legales de servicios de bitcoin y marihuana medicinal, junto con algunos pornógrafos y traficantes de armas. La ley estaba teniendo un efecto escalofriante: los bancos podrían no estar violando la ley al dar servicio a tales negocios, pero el riesgo de una auditoría del Departamento de Justicia era suficiente para disuadirlos de hacerlo. Ittleman luchó arduamente por sus clientes, a quienes se les negó un instrumento vital de acceso financiero, pero fue una batalla cuesta arriba. El asunto, dijo, debe ser llevado a la Corte Suprema por activistas de derechos civiles como la Unión de Libertades Civiles de Estados Unidos.

Casi al mismo tiempo que el debate regulatorio de EE. UU. Se calentó, lo mismo comenzó a suceder en otros países. El Banco Popular de China también comenzó a usar los bancos para mantener el bitcoin bajo control, aunque de una manera más directa. Eventualmente, un fallo formal cayó en abril de 2014 impidiendo explícitamente a los bancos chinos tratar con negocios de bitcoins. Después de eso, la Autoridad Bancaria Europea, el organismo de supervisión continental creado después de la crisis del euro, intervino; en julio recomendó a la agencia de supervisión bancaria de cada país miembro "desalentar a las instituciones de crédito, instituciones de pago y dinero electrónico de comprar, mantener o vender monedas virtuales" hasta que se elaborase un "cuerpo sustancial de regulación" para abordar los riesgos asociados con ellos. Jim Harper, principal oficial de enlace del gobierno de la Fundación Bitcoin, dijo que la EBA había ido más allá de su propia promesa de "identificar los riesgos que surgen de las actividades financieras, priorizarlos y tomar medidas de mitigación, de ser necesario". En lugar de mitigarlos, dijo: había tomado medidas preventivas que enfatizaban "detener la integración de la moneda digital en el sistema de servicios financieros de Europa".

Harper, un miembro del equipo de investigación libertario Cato Institute, con base en D.C., había sido contratado por la fundación en marzo de 2014; pronto estaría muy ocupado. Más allá de las medidas adoptadas en los Estados Unidos, Beijing y Bruselas, varios países de mercados emergentes emitieron declaraciones rigurosas. Bolivia dijo que prohibiría el bitcoin directamente; Bangladesh advirtió a los comerciantes de bitcoins que podrían ser encarcelados bajo las leyes contra el blanqueo de dinero; Los reguladores rusos emitieron una declaración condenatoria que

declaraba que el rublo era la única moneda legal en Rusia; y mientras Ecuador abrió la puerta al dinero digital, dijo que solo podría ser emitido por su banco central.

De regreso en los Estados Unidos, el 25 de marzo, justo a tiempo para la fecha límite del 15 de abril para la presentación de impuestos, el Servicio de Rentas Internas salió con una guía muy anticipada, declarando que el bitcoin no era una moneda en el sentido legal. Tampoco era una mercancía. Más bien, era "propiedad", como bienes raíces o acciones, y estaba sujeta a los mismos impuestos sobre plusvalías si cambiaba su valor. Fue la primera oferta para aclarar cómo deben contabilizarse las transacciones de bitcoin a efectos fiscales.

En cierto sentido, este movimiento codificó bitcoin dentro del marco legal. Algunos, especialmente aquellos que estaban tratando de crear un vehículo de inversión con bitcoin, estaban felices de que se trataría como cualquier otra inversión y no estarían sujetos a impuestos sobre la renta, que generalmente son más altos que los impuestos sobre ganancias de capital. Pero el objetivo declarado de la comunidad en general no era hacer de bitcoin un vehículo especulativo sino más bien un medio de pago. Las reglas del impuesto a las ganancias de capital podrían hacer que usar Bitcoin como moneda sea una pesadilla logística. Significaba que cuando los ciudadanos estadounidenses presentaban impuestos, debían contabilizar cada bitcoin adquirido, vendido o usado para compras, y los precios y fechas en que ocurrían esas transacciones. Si compraste 0.5 bitcoins a $ 360 en abril de 2014 y las vendiste por $ 645 el 9 de junio, deberías declarar esa ganancia como un evento imponible en 2015. Bastante justo. ¿Pero tenía que dar cuenta de los cambios en el valor si usaba su bitcoin para comprar unas vacaciones en Expedia o para pedir una pizza? El movimiento del IRS pareció minar el potencial de Bitcoin como moneda.

En el lado positivo, el IRS al menos había eliminado la incertidumbre sobre cómo se tratarían las monedas digitales a efectos fiscales, y había razones para creer que después de una revisión se presentarían exenciones para aliviar la carga de cumplimiento. Además, los tecnólogos de Bitcoin siempre inventivos hicieron lo que muchos hacen cuando llegan las regulaciones: lo vieron como una nueva oportunidad para la innovación. Los expertos en tecnología comenzaron a idear aplicaciones que rastrearan permanentemente las transacciones de bitcoin de una persona y escupieran una ganancia o pérdida neta para el año y un registro permanente de impuestos.

Unos meses más tarde, en julio, Lawsky en el NYDFS finalmente presentó su propuesta de BitLicense. Cualquier entidad en el negocio de almacenar, intercambiar o enviar "moneda virtual" en Nueva York requeriría una licencia, decía el esbozo, y tendría que cumplir varios criterios diseñados para proteger contra el lavado de dinero, el financiamiento del terrorismo y otras actividades ilícitas. Estos incluían oficiales de cumplimiento para evaluar los perfiles de los clientes tanto en moneda digital como en moneda fiduciaria, manteniendo una cantidad aún no especificada de capital de respaldo, actualizaciones con el departamento cada vez que la empresa cambiaba su modelo de negocio (que a veces era mensual para nuevas empresas que cambian rápidamente) y, lo que es más difícil, una tienda de "moneda virtual" equivalente a cualquier monto que la empresa posea en nombre de los clientes. Fue una carga pesada.

Algunos de los peces más grandes de bitcoin al principio elogiaron el anuncio, quizás prematuramente. "Nos complace que el Superintendente Lawsky y el Departamento de Servicios Financieros hayan adoptado Bitcoin y los activos digitales y hayan creado un marco regulatorio que proteja a los consumidores", dijo Cameron Winklevoss en un correo electrónico. De hecho, estas reglas no eran un gran problema para las empresas bien capitalizadas que ya mantenían una infraestructura de cumplimiento -el fondo fiduciario de bitcoins de los gemelos Winklevoss, por ejemplo- e incluso podían darles una ventaja competitiva. Pero la mayoría de los bitcoiners estaban alarmados por lo que vieron. El borrador parecía arrojar una red mucho más allá de los intercambios y los procesadores de pagos, lo que sugiere que cualquier pequeña empresa

emergente en un garaje de San Francisco podría ser sofocada de repente con la burocracia. Muchos sintieron que sus cargas eran mucho más onerosas que aquellas con las que los bancos debían cumplir: los bancos necesitaban solo un grupo de oficiales de cumplimiento, no dos, y podían salirse con la simple segregación de las cuentas de propietario y cliente en lugar de tener que mantener uno solo. un capital contra las tenencias de sus clientes. Mientras tanto, Perianne Boring, fundadora de la recientemente creada Cámara de Comercio Digital, argumentó que la ausencia de una distinción entre activos digitales y moneda digital en las reglas propuestas podría sofocar las nuevas aplicaciones de blockchain. Lo que esto significaba para todos los proyectos de Bitcoin 2.0 simplemente no estaba claro. Muchos bitcoiners sintieron que la propuesta de BitLicense era deliberadamente discriminatoria porque había incumplido un principio regulador de larga data de no hacer las leyes "tecnológicas específicas", es decir, que las autoridades deberían regular la actividad comercial particular, no la tecnología que maneja esa actividad.

La respuesta de la comunidad bitcoin fue rápida, lo que demuestra cuán bien organizado se había convertido este grupo ad hoc y global. Una petición circuló rápidamente y fue firmada por cientos, incluido un quién es quién de bitcoin. Pidió una extensión del período de comentarios de cuarenta y cinco días que Lawsky había establecido, argumentando que este era un período excesivamente corto para firmas de tecnología con poca financiación y experiencia limitada en Wall Street. Algunos sugirieron acciones más drásticas y comenzaron a presionar a los legisladores del estado de Nueva York en Albany para controlar a Lawsky, enmarcándolo como un asesino de la innovación y la creación de nuevos empleos en Nueva York. Más dramáticamente, el CEO de Circle Jeremy Allaire, quizás el bitcoiner con las mejores conexiones con el establishment político, * escribió una poderosa publicación de blog argumentando que su servicio de bitcoin minorista de alto perfil y bien financiado podría tener que excluir a las personas con direcciones ISP de Nueva York . Allaire postuló que sería "devastador" para Bitcoin si la BitLicense de Nueva York se convirtiera en una plantilla para otros estados.

La presión claramente tuvo algún efecto. Lawsky acordó otra extensión de cuarenta y cinco días y dijo que la propuesta no tenía la intención de atrapar pequeños equipos tecnológicos. Reconociendo que el NYDFS no tenía "el monopolio de la verdad", dijo que la agencia estaba "seriamente" considerando algunas de las contrapropuestas que entraban. En el momento de escribir esto, el proceso todavía estaba en curso, y no estaba claro. cuál sería el resultado, pero vale la pena reflexionar sobre si algunas de las implicaciones radicales que los bitcoiners presentaron se habían hundido. La idea de los "geofencing" ISP, insinuados por Allaire, captó la magnitud de la fragmentación geográfica que estas reglas podrían generar. También se discutió otra noción en las salas de chat de Bitcoin: que las bitcoins procesadas por firmas sin licencia en Nueva York serían consideradas inferiores a las autorizadas, creando un mercado bifurcado donde las monedas "sucias" sospechosas serían cotizadas a un precio rebajado. precio en comparación con los "limpios". Eso sería contraproducente para la idea de un precio global fluido y global para una moneda digital. Como señala Harper of the Bitcoin Foundation, también sería contraproducente para los reguladores que buscan controlar el flujo de dinero, ya que empujaría el negocio de bitcoins a áreas no reguladas fuera del ámbito regulatorio de las agencias de los EE. UU. De hecho, como el júbilo generado por las audiencias FinCEN en noviembre dio paso a la consternación ante el manejo inicial de New York de BitLicense, algunos negocios de bitcoins iniciados en los Estados Unidos comenzaron a hacer que esto suceda. Se movieron.

Es un axioma de las finanzas que en una economía globalizada, las empresas responderán a la regulación y las cargas impositivas trasladando las operaciones a un lugar donde sean menos inhibidoras. El fenómeno se conoce como arbitraje regulatorio, porque permite a las empresas aprovechar la postura laxa de una ubicación para extraer una postura más fácil de otra. En 2014, el problema se convirtió en un pararrayos político en los Estados Unidos cuando una compañía tras otra diseñó fusiones de "inversión", adquiriendo competidores en el extranjero y luego

cooptando sus oficinas corporativas para reducir su factura de impuestos corporativos en Estados Unidos. Las naciones insulares en el Caribe y los territorios británicos autónomos en el Canal de la Mancha han construido modelos económicos completos alrededor de tales ideas, con entre $ 5 billones y $ 32 billones de dólares que se dice que se mantienen en alta mar en tales paraísos fiscales.

Las mismas reacciones oportunistas a la regulación ya están ocurriendo en el mundo de la criptomoneda. Con sus redes descentralizadas y distribuidas, las criptomonedas son el epítome de las instituciones sin ataduras de nuestra era digital y global. Entonces, como es lógico, a medida que el panorama regulatorio del mundo toma forma, se están fundando los equivalentes de criptomoneda de las Islas Caimán.

Ciertos países de Europa Central y del Este han adoptado una postura acomodaticia hacia la moneda digital y se han convertido en el hogar de intercambios de bitcoins como resultado. BTC-e, uno de los intercambios de bitcoins más grandes, tiene su sede en Bulgaria, cuya agencia fiscal reconoció formalmente la moneda digital y estableció una baja tasa impositiva del 10 por ciento sobre las ganancias en el ingreso de bitcoin. Su rival, Bitstamp, reside en Eslovenia, mientras que MPEx, la bolsa de valores denominada en moneda digital, se ha establecido en Rumania. Pero las empresas también se están aprovechando de más políticas de puertas abiertas en economías mucho más grandes y establecidas.

Una de ellas es Suiza, situada convenientemente fuera del alcance de los nuevos organismos reguladores de la Unión Europea, pero con todas las características de una economía avanzada de Europa occidental y de industrias financieras y tecnológicas muy sofisticadas. La Autoridad de Supervisión del Mercado Financiero de Suiza anunció en junio que no tenía la intención de redactar reglas especiales para el bitcoin porque, por el momento, las normas existentes impuestas a las firmas financieras serían suficientes. Este enfoque de no intervención ha convertido al país en una meca para proyectos de criptografía financiera, de acuerdo con Chris Odom, quien dirige el proyecto de redes descentralizadas Open Transactions fuera de la ciudad alpina de Zug. Entre los vecinos de Open Transactions en lo que Odom llama Crypto Valley están Ethereum, el operador de alto perfil Blockchain 2.0, Bitcoin ATM proveedor Bitcoin Suisse y varios proyectos de criptografía no financiera como ProtonMail y Silent Circle, que proporcionan servicios telefónicos y de correo electrónico cifrados de forma segura.

Incluso en el Reino Unido, que se encuentra dentro de la Unión Europea pero a menudo sigue su propio camino con respecto a las normas impositivas y reglamentarias, la perspectiva es una mano más fácil para la criptomoneda. En agosto de 2014, el ministro de Hacienda, George Osborne, dijo que el Reino Unido lanzaría un estudio exhaustivo para descubrir cómo aprovechar la tecnología de criptomonedas e idear reglas para convertir a Gran Bretaña en "el centro global para la innovación financiera". Aunque algunos estaban preocupados por Repetición de la decepción de BitLicense en Nueva York, las palabras de Osborne ciertamente sonaron alentadoras. Dijo que los "sistemas de pago alternativos basados en monedas digitales son populares ya que son rápidos, baratos y convenientes" y que quiere "ver si podemos hacer un mayor uso de ellos para el beneficio de la economía del Reino Unido". Incluso antes de esa fecha Varias firmas de bitcoins optaron por hacer de Londres su hogar, incluyendo Blockchain y Coinfloor, un intercambio de bitcoins completamente regulado y de alta tecnología. Además, varias islas de paraíso fiscal de los Estados Unidos compiten para convertirse en las localidades más amigables con las criptomonedas del mundo. El primer fondo de inversión de bitcoin totalmente regulado se lanzó en la Isla del Canal de Jersey, y la Isla de Man anunció que los intercambios de bitcoins eran libres de operar allí sin una licencia.

De la misma manera que Suiza y las Islas del Canal presentan alternativas a la mano más pesada del resto de Europa, México y Canadá pueden atraer empresas de criptomonedas de los Estados Unidos. El gobierno canadiense rompió su silencio sobre la regulación de bitcoins en junio de 2014, aunque vagamente, ya que incluía una referencia a "monedas virtuales" en un proyecto de ley diseñado para actualizar las leyes sobre la transmisión de dinero y las protecciones contra el blanqueo de dinero. Si bien eso implicaba que una era de oportunidad de laissez faire en Canadá podría estar cerrándose para las empresas bitcoin, muchos lo vieron como un signo alentador, uno que legitimó su industria y le dio el mismo trato que los servicios financieros existentes. Las ciudades más grandes de Canadá se estaban convirtiendo en pequeños centros de monedas digitales. Toronto cuenta con un acelerador agresivo conocido como Bitcoin Decentral y es el hogar del proveedor de monedero digital KryptoKit. Mientras tanto, VirtEx, que opera un intercambio de divisas digitales y fabrica tarjetas de débito Bitcoin, tiene su sede en Calgary, y el primer cajero automático bitcoin del mundo se instaló en un café del centro de Vancouver. En cuanto a México, en julio su gobierno anunció que estudiaría la posibilidad de crear un peso digital basado en blockchain y exploraría cómo el país podría aprovechar los beneficios de las redes de criptomonedas descentralizadas para atacar la corrupción. A pesar de que era escaso en detalles, esta fue una declaración sin precedentes, lo que sugiere una visión prospectiva del potencial de la cadena de bloques para mantener a los funcionarios y sus socios comerciales responsables.

Después de las directivas de antibitcoin del Banco Popular de China a sus bancos, varias empresas de criptomonedas de la nación se trasladaron a Hong Kong, donde la carta que dejó el traspaso del Reino Unido en 1997 a China y su condición de centro financiero casi garantiza un mercado abierto. mercado, postura de laissez-faire. ANX y Bitfinex, dos de los intercambios de bitcoin de más alta tecnología en el mundo, se basan allí. El único problema es que los bancos de Hong Kong, que hacen una gran cantidad de negocios con contrapartes en los Estados Unidos y China, a menudo desconfían de las nuevas empresas de bitcoins. "Todos los bancos están realmente asustados por este cumplimiento", afirma Aurélien Menant, cofundador y CEO de Bitcoin Exchange Gatecoin, que también dirige un programa para organizaciones benéficas basadas en Bitcoin en Asia. "Realmente puede abrir y registrar una empresa fácilmente". Usted puede obtener una licencia fácilmente. Pero luego ... tan pronto como esté registrado como un negocio de servicios monetarios, los bancos lo incluirán en la lista negra, nos dijo durante una visita al territorio. Es un recordatorio de la vasta e indirecta influencia que Washington y Nueva York tienen sobre el mundo financiero.

Con los bancos de Hong Kong preocupados por mantener contentos a Beijing y Nueva York, Singapur, con su mezcla bastante contradictoria de gobierno autoritario y principios económicos de libre mercado, representa un territorio más amigable para llevar negocios de bitcoins fuera de Asia. El procesador GoCoin de pagos internacionales de bitcoin, que incluye al fundador de transacciones en serie de Brock Pierce, fundador de Bitcoin, tiene su sede en la ciudad-estado. Al igual que cualquier centro acreditado de criptomonedas, Singapur tiene algunos intercambios de bitcoin establecidos, incluidos FYB-SG y First Meta, aunque este último ha sido objeto de cierto escrutinio tras la prematura muerte de su director general estadounidense de veintiocho años, Autumn Radtke, en marzo. 2014. Después de declarar explícitamente en 2013 que no intervendría en las empresas que eligen comercializar bitcoin, la Autoridad Monetaria de Singapur dijo en marzo del año siguiente que los intercambios de bitcoins tendrían que cumplir con los requisitos de cumplimiento regulares contra el blanqueo de dinero. Pero en general, el gobierno de Singapur se ha mostrado cautelosamente interesado en fomentar la innovación de criptomonedas. Según un informe, el gigantesco conglomerado estatal Temasek Holdings, un pilar del sistema financiero de Singapur, ha estado experimentando con inversiones de bitcoin en su cartera de activos de inversión de $ 300 mil millones.

La movida de marzo de 2014 de Singapur para regular el bitcoin se produjo a raíz de un período difícil para la criptomoneda. Los titulares de malas noticias llegaron con fuerza a finales del invierno boreal, dando a los escépticos y extraños lo que vieron como "prueba" de que Bitcoin era un mundo de traficantes de drogas, hackers e intercambios en línea mal regulados que podrían correr con su dinero en un momento de aviso. Para aquellos que apostaron fuerte por construir esta tecnología, los hombres de negocios arando dinero en ella, los desarrollos equivalieron a una crisis existencial para su amada criptomoneda, una que ellos sentían exigía una infraestructura de regulación más ordenada.

Comenzó a fines de enero con el arresto de Charlie Shrem, jefe de bitcoin de Bitcoin con sede en Nueva York y vicepresidente de la Fundación Bitcoin, de veinticuatro años, bajo cargos, luego reducidos en un acuerdo de culpabilidad, de que él había conspirado con un cliente de Silk Road para lavar dinero de drogas. Pero aún más importantes fueron los desarrollos posteriores en Mt Gox, que simplemente se descontrolaron. Detuvo las retiradas de los clientes y culpó a sus problemas de un problema universal de bitcoin, invitando al ataque DDOS que le negó a Gavin Andresen una buena noche de sueño, todo antes de colapsar en bancarrota total el 28 de febrero con un anuncio de que había "perdido" 850,000 monedas por valor de $ 500 millones. Doscientas mil de esas monedas fueron luego "encontradas" después de que algunos miembros de la comunidad de bitcoin dijeron que habían rastreado las transacciones de blockchain a las billeteras propiedad de Mt Gox que misteriosamente no habían incluido en su declaración de bancarrota. Hasta el momento de escribir, el resto aún no se ha tenido en cuenta.

Es difícil imaginar un mayor abuso de inversionistas que el de los 127,000 que se quedaron en la estacada cuando Mt Gox colapsó. Su experiencia captura los problemas inherentes a la fusión del mundo desregulado, descentralizado y de laissez-faire de bitcoin con el mundo ordenado y centralizado de las monedas tradicionales y el derecho comercial. Para los inversores, Mt Gox representaba lo peor de ambos mundos. Por un lado, no estaba regulado, ya que ni las leyes de comercio financiero ni de valores de Japón ni de los Estados Unidos podían en ese momento ubicar adecuadamente a las empresas de bitcoin en su marco para la regulación. Después de que el intercambio colapsó y un tribunal de quiebras japonés comenzó a procesar la multitud de reclamaciones de todo el mundo, se enfrentó a un dilema fundamental: ¿cuál, desde la perspectiva de la ley japonesa, es un bitcoin? Y sobre esa base, ¿qué vale realmente? Otros intercambios no regulados como Bitstamp y BTC-e podrían haber estado diciendo que un bitcoin valía $ 600, pero si no podemos definir legalmente un bitcoin, ¿cómo podemos confiar en esos precios? ¿Valían absolutamente todas las afirmaciones de estos acreedores?

Por otro lado, aunque pueda parecer extraño decirlo, Mt Gox era una institución tradicional del viejo mundo en el sentido de que asumía el control centralizado de los fondos de las personas. Al permitir que las personas intercambien dólares y otras monedas tradicionales por bitcoin, le dio a la gente una "entrada" en el entorno "sin confianza", transparente y descentralizado de la cadena de bloques, pero para llevarlos allí los llevó a través del tipo de confianza entorno centralizado y dependiente que Bitcoin fue diseñado para dejar de lado. No hubo forma de evitar esto, dado que la mitad de cada compra o venta de bitcoins involucraba una moneda no criptográfica, como el dólar o el yen, y estas no residían en una cadena de bloques descentralizada. Pero el resultado fue que tenía que confiar en Mt Gox con su dinero. Incluso después de haber completado una operación para comprar bitcoin, aún no tenía control basado en la cadena de bloques sobre esas monedas hasta que Mt Gox cumplió con una solicitud para transferirlas a su billetera personal. No era muy diferente de tener una cuenta en una correduría de Wall Street. Si se hundía, no tenía control automático y directo sobre sus activos; simplemente tenía un reclamo sobre la institución en bancarrota, uno que esperaba que un tribunal hiciera cumplir.

Muchos desarrolladores de criptomonedas se han sentido incómodos con esta reversión a modelos centralizados. Algunos, como Odom en Open Transactions, ahora están trabajando en soluciones de software basadas en principios de descentralización que permitirían a las personas entrar y salir de estos diferentes criptomonedas y reinos fiduciarios sin tener que invertir confianza en servidores centralizados. Ya sea que se necesite una solución cripto-tecnológica, o si la regulación más estricta de estos intercambios centralizados es el camino a seguir, está abierto al debate. De cualquier manera, es difícil imaginar un abuso más atroz de la confianza centralizada que el de Mt Gox. Eso no se debe a que su propietario haya robado las monedas -no existen afirmaciones fundamentadas al respecto-, sino porque toda la operación se estableció sin ninguna de las obligaciones fiduciarias de cuidado que normalmente se requieren para las empresas financieras reguladas. Cuando MF Global, el ex gobernador de Nueva Jersey, John Corzine, colapsó en 2011, sus inversores descubrieron con consternación que la correduría se había sumergido en las cuentas segregadas que se suponía que protegerían sus fondos para que no fueran utilizados por la propia cuenta de la empresa. Pero si eso fue malo, parece que Mt Gox no tenía segregación de cuentas en absoluto. Todos los bitcoins fueron controlados por el intercambio en sus propias billeteras.

Entonces, Mt Gox estaba centralizado y no regulado. En este entorno, prácticamente toda la responsabilidad de la toma de decisiones en esta compañía de unas tres docenas de empleados residía en el CEO Mark Karpelès. Reuters informó que solo Karpelès conocía las contraseñas de las carteras de Mt Gox y que rechazó una solicitud de 2012 de los empleados para ampliar el acceso en caso de que quedara incapacitado. Además de eso, al menos para algunos, él no se presenta como el tipo de persona que desea ejecutar el mayor intercambio de divisas digitales del mundo con tanta autoridad concentrada.

Durante el ataque de hacking de junio de 2011, cuando el precio bajó a casi cero y el intercambio tuvo que cancelar, o revertir, montañas de pedidos pendientes, Roger Ver y su amigo de escuela secundaria Jesse Powell obtuvieron información sobre esto. Se instalaron en las oficinas de Mt Gox en Tokio para tratar de resolver el problema y revivir el intercambio, una parte crucial de la economía de Bitcoin. Trabajando y reconciliando diez mil boletos cancelados o estancados, se marcharon con otros empleados de Mt Gox durante el fin de semana, solo para descubrir que Karpelès se tomó esos dos días libres. "Fue un poco desconcertante", recuerda Powell, ahora el gerente general de intercambio de bitcoin Kraken, con sede en San Francisco, quien también dice que Karpelès le reconoció entonces que Mt Gox había perdido cuatro mil bitcoins en el ataque de piratería informática. "En retrospectiva", dice Powell, "no puedo evitar preguntarme si descubrió que perdió mucho más que eso y tuvo que tomarse el fin de semana para recuperarse".

Para ser justos, mientras Ver y Powell estaban ocupados recuperando Mt Gox, Karpelès estaba haciendo su parte para restaurar la confianza en el intercambio, aunque de una manera que parecería extraña para las instituciones financieras modernas con procedimientos normales de auditoría. Al interactuar en foros de bitcoin con otros bitcoiners a través de su nombre de usuario de MagicalTux, Karpelès realizó un truco para demostrar la solvencia de Mt Gox. Le dijo a sus corresponsales en línea que mantuvieran sus ojos en dos direcciones particulares de bitcoins a través de un monitor de cadena de bloques en línea, y que transfiriera 424,242.424242 * bitcoins entre ellos. Era el equivalente de la criptomoneda de la antigua "pared de dinero" que los administradores bancarios de años anteriores pondrían detrás de sus cajeros para disuadir a los depositantes en pánico de participar en una operación bancaria. Después de mover una cantidad tan grande de monedas, la maniobra tuvo su efecto deseado. Tal traspaso masivo de bitcoins sugirió que Mt Gox estaba más al rojo de lo que todos temían. Tres años más tarde, la historia de este ejercicio, integrada por blockchain, en la que Karpelès identificó efectivamente esas direcciones como pertenecientes a las billeteras Mt Gox, proporcionó el punto de partida desde el

cual un grupo de bitcoiners trazaría la cadena de bloques para descubrir doscientas mil monedas que aún estaban presentes en las cuentas de Mt Gox.

Muchas teorías se desarrollarían más tarde relacionando esos eventos con la desaparición de los 650,000 bitcoins restantes en 2014. Una de las más elaboradas sostiene que Mt Gox perdió muchos más bitcoins de los que dejó pasar durante el truco de 2011, y que Karpelès confió en un siempre creciente precio de bitcoin después de eso para que parezca como si todo fuera normal. Si es así, era como un esquema Ponzi para deshacer las pérdidas en lugar de obtener un beneficio personal. Significaría que a medida que aumentara el valor de las tenencias de bitcoin no segregados de Mt Gox a medida que más y más inversores firmaran, Karpelès canjeó la cuenta de Mt Gox por esas tenencias restantes, luego reservó ganancias para cumplir con los reembolsos de los inversores que no sabían lo que había pasado . Pero cuando las cosas se pusieron difíciles en 2013, cuando el gobierno de EE. UU. Congeló las cuentas de Estados Unidos de Mt Gox, por ejemplo, mover fondos se hizo difícil, y se hizo cada vez más difícil permanecer en la cinta Ponzi. Finalmente, el colapso del precio de 2014 hizo que todo el juego fuera imposible, o al menos eso es lo que sostiene la teoría. Otra teoría sostiene que Karpelès, con su completo control sobre las llaves privadas de las billeteras, simplemente las perdió, haciendo que los bitcoins sean irrecuperables. Una tercera teoría es la que Mt Gox defiende: que perdió sus monedas como resultado del error de maleabilidad de la transacción, que su sistema simplemente respondió repetidas veces y erróneamente a las solicitudes fraudulentas de los operadores deshonestos de volver a enviar dinero. Pero para muchos, parecía inverosímil que Mt Gox no hubiera notado una estafa de tales proporciones. Adam Levine, un presentador de programa de entrevistas de bitcoin y desarrollador que estaba en la búsqueda para encontrar las monedas de Mt Gox que faltan, dijo que era como si "alguien llega y roba tu casa debajo de ti mientras trabajas en tu negocio". y nunca lo notas ".

Es posible que nunca sepamos lo que sucedió. Nuestros repetidos intentos para lograr que Karpelès respondiera a las diversas acusaciones y teorías provocaron algunas respuestas limitadas por correo electrónico cuyo contenido era insuficiente para permitir una caracterización clara de su posición. A veces explicaba que la investigación llevada a cabo por el tribunal de quiebras limitaba su capacidad de respuesta. Pero, claramente, la estructura de gestión de Mt Gox era inviable para una institución financiera de este tamaño. Karpelès fue efectivamente CEO, CTO, CFO y director de cumplimiento en uno. Su transferencia de billetera en 2011 pudo haber tenido el efecto impresionante de un truco parecido a George Bailey en la interpretación clásica de Jimmy Stewart de una corrida bancaria en It's a Wonderful Life, pero esa no era forma de realizar un intercambio financiero moderno. Los clientes tenían cero protección, su confianza se alojó por completo en este hombre. Casarse con el Wild West descentralizado de Bitcoin a un modelo de confianza excesivamente centralizado fue un desastre que estaba por ocurrir. Cuando lo hizo, la presión para regular el bitcoin se volvió imparable y creó tensiones dentro de la comunidad bitcoin.

Los "trajes" de Bitcoin comenzaron a ser serios: la regulación, la seguridad, el cumplimiento y la participación del know-how de Wall Street de repente cobró sentido. La billetera multi-sig altamente segura de BitGo salió en este momento, ofreciendo una versión digital del sistema de doble llave utilizado por los banqueros suizos para brindar a los clientes acceso a sus objetos de valor en cajas de depósito. Firmas como Circle y Xapo implementaron sus servicios de depósito asegurados para brindar tranquilidad a los clientes.

Mientras tanto, los gemelos Winklevoss progresaron con una solicitud en la Comisión de Bolsa y Valores de EE. UU. Para que su Fideicomiso Winklevoss Bitcoin sea autorizado como el primer fondo negociado en bolsa enfocado en bitcoin, una medida que permitiría a las personas invertir en bitcoin sin tener que poseer el monedas directamente. Más tarde, Atlas ATS lanzó una red de

intercambios interconectados a nivel mundial con tecnología de Perseus Telecom que satisfacía las demandas de gran ancho de banda de las firmas comerciales de alta frecuencia y proporcionaba un cumplimiento sofisticado e impulsado por computadora para administrar relaciones sensibles con los clientes. El entusiasta de Bitcoin, Barry Silbert, lanzó su propio fondo de bitcoin, que reclamaba una ruta de acceso a la aprobación regulatoria federal que supuestamente venció a los "Winklevii" en la carrera por ofrecer un fondo regulado de bitcoin a los estadounidenses de bajos ingresos. Silbert también comenzó a construir su propio intercambio, uno diseñado para tener capacidades de cámara de compensación tradicional, asientos de propiedad de corretaje y la misma estructura de autorregulación que es fundamental para el funcionamiento de Wall Street. Sería, dijo, "parecería la Bolsa de Nueva York" y "nada como Mt Gox".

Sin embargo, una bolsa de intercambio de información, que tiene un fondo común para asegurarse de que todas las transacciones se liquiden dentro de un tiempo específico, implica la estructura de centros y radios de una institución centralizada. Este tipo de soluciones, todas orientadas a la construcción de la confianza de los inversores, no son una salida en absoluto del problema de Mt Gox. Los usuarios todavía están obligados a confiar en una sola contraparte. La pregunta es si tales instituciones son necesarias para conquistar a la gente común y mantener a raya a los reguladores.

El hecho de que la comunidad de negocios de bitcoins emergentes estuviese argumentando a favor de esto era profundamente perturbador para los tipos anarquistas puritanos que abrazaron inquebrantablemente la mentalidad de un segundo escenario. Con una gran cantidad de técnicos inteligentes en medio de ellos, esta facción rebelde fue en busca de nuevas herramientas criptográficas para que sea aún más difícil para los reguladores para influir y controlar una red de bitcoin descentralizada. Su solución más radical se llamó Dark Wallet. La creación de un criptoanarquista estadounidense llamado Cody Wilson y su colega hacker iraní británico, Amir Taaki, Dark Wallet es un servicio de "mezcla". Toma transacciones, las divide en pedazos más pequeños y las ejecuta a través de múltiples billeteras y direcciones para crear una matriz indescifrable de datos densos. Para Wilson, esto significaba ser fiel a una filosofía de protección de la privacidad y reflejaba un profundo deseo de devolver Bitcoin a lo que él veía como su razón principal de ser: un instrumento de libertad personal.

Wilson cree que las personas que una vez creyeron en las cualidades de búsqueda de la libertad de Bitcoin han sido seducidas por el dinero y el poder. "Un grupo de nuevas empresas están entrando, aparentemente libertarias, y diciendo [al gobierno]: 'Mira, podemos hacer esto por ti'", nos dijo. "Es el dinero fácil". Y eso es crear una narrativa sobre bitcoin, una conversación que es fácil de entender, una que dice: 'En realidad, Bitcoin al final es tu compañero. Es tu amigo. Mire, ayudará al sistema bancario; ayudará al sistema regulador. '... Las personas que hace tres años eran bastante radicales ahora se están poniendo un traje y corbata y simplemente tiran la toalla y dicen:' Incluso si el bitcoin no puede ser algo que cambie el mundo, Puedo ganar mucho dinero. Puedo entrar al reino".

Dark Wallet fue una respuesta a eso. En otro lugar, Wilson fue citado describiéndolo como una forma de "burlarse de todos los intentos de rociar [bitcoin] con la regulación", y decirle al gobierno: "'Te has configurado para regular el bitcoin. Regula esto. '"Wilson, quien previamente se había hecho un nombre al diseñar el primer arma 3-D-impresa, no tuvo reparos, dijo, acerca de que su proyecto se convirtiera en un vehículo para lavado de dinero, tráfico de drogas, pornografía infantil, o terrorismo Su respuesta: "La libertad es algo peligroso". Esta no era una forma de llevar el bitcoin a la corriente principal, pero ese no era su objetivo. Si Dark Wallet logró la libertad solo para aquellos que están en los márgenes de la sociedad, que así sea.

La respuesta en la comunidad bitcoin a Dark Wallet fue dividida. A los libertarios incondicionales les encantó. Algunos técnicos estaban impresionados: Gavin Andresen, el científico en jefe de la Fundación Bitcoin, calificó la tecnología de "fantástica" y dijo que más "privacidad es mejor", aunque también esperaba que las regulaciones se pusieran al día. El elogio de Andresen fue algo irónico dado que Wilson y su cofundador, Amir Taaki, se habían burlado repetidamente de la fundación como un vehículo para los intereses comerciales de bitcoins para congraciarse con el establecimiento de Washington. Sin embargo, el periodista independiente, comentarista y empresario de bitcoin Ryan Selkis articuló lo que debe haber preocupado a muchos de esos empresarios. Dark Wallet abrió "una pesadilla reglamentaria" para Bitcoin. "Decirle al gobierno más poderoso del mundo que se vaya a la mierda cuando estás en tu infancia ciertamente lo convierte en un excelente teatro, pero también quema a todos los demás en la comunidad bitcoin", escribió Selkis, cuyo blog lleva el sobrenombre TwoBitIdiot. . "El gran problema es si las billeteras oscuras y los mercados oscuros harán que todos los bitcoiners parezcan culpables por asociación".

Por lo tanto, las tensiones entre los intereses centralizadores de los empresarios bitcoin y la visión pura de una utopía descentralizada volvieron a incrustarse en la ruidosa arena pública en la que esta comunidad discute y debate sus ideas. Una división similar surge cuando los emprendedores de Blockchain 2.0 lanzan nuevas aplicaciones inteligentes que explotan la infraestructura descentralizada de bitcoin solo para que los fanáticos las etiqueten en Reddit como esquemas de bombeo y volcado ejecutados por los especuladores que centralizan. Mucho está en juego en este debate, ya que dictará el enfoque que toma la criptomoneda en su intento por ser ampliamente relevante. ¿Tratará de lograr ese objetivo como un grupo guerrillero rebelde desafiando abiertamente al establecimiento? ¿O desempeñará el papel de intermediario, un negociador que incorpora parte del sistema existente en su modelo y que aún aporta algo nuevo y valioso al mercado? Este último ofrece una ruta mucho más libre de fricción para una afirmación significativa en la sociedad, pero la pregunta es si hacerlo socavaría bitcoin de su significado y su verdadera capacidad para interrumpir la economía política actual. Si este enfoque de medio término tiene éxito, tal vez servicios como Dark Wallet simplemente se convertirían en dominios subterráneos donde la actividad ilícita continúa y los bitcoins en su circulación permanecen aislados de una economía más amplia de criptomonedas, que es más o menos lo que buscan las leyes gubernamentales de lavado de dinero para lograr con drogas y dólares terroristas. Pero es evidente que algunos temen que si el bitcoin se diluye y regula demasiado, pierde su poder, su propósito y su valor para la sociedad.

Este no es un debate que la comunidad bitcoin puede o resolverá por sí mismo. Estas cuestiones serán abordadas por la sociedad más amplia en la que se están desarrollando. Y la sociedad misma ya está experimentando un cambio profundo, el resultado de amplios cambios tecnológicos, demográficos y económicos globales. En este entorno en evolución, las criptomonedas están preparadas para desempeñar un papel altamente disruptivo. Depende de nosotros, los ciudadanos, los votantes y los agentes económicos de esta sociedad futura, determinar cuán importante es el rol que queremos que tenga esta tecnología y, por lo tanto, cuál de los dos modelos de criptomonedas termina siendo dominante.

Capítulo 11

UNA NUEVA ECONOMÍA

El progreso es una enfermedad confortable.

-MI. E. Cummings

Hasta ahora, nos hemos centrado principalmente en cómo se han desarrollado las criptomonedas y los beneficios y desafíos que representan para la sociedad. Pero estas nuevas formas de dinero y formas de organizar la actividad comercial no están aterrizando en una sociedad estática y adormecida, como si los seres humanos estuvieran esperando ser despertados por una nueva idea monetaria. La sociedad misma está cambiando rápidamente. La tecnología digital y la informática en línea están en el centro de este cambio, cambiando la forma en que formamos comunidades, relaciones sociales y vínculos comerciales, ya que cada aspecto de nuestras vidas está cada vez más sujeto al poder de la informática y las conexiones de red. También influyen otros factores: los cambios demográficos de un Occidente que envejece, el crecimiento sin precedentes de una clase media en los países en desarrollo, el aumento del terrorismo en lugar del conflicto internacional como la mayor preocupación de seguridad de nuestro tiempo y el legado de la Crisis financiera de 2008 con su daño a la confianza de las personas en el sistema financiero tradicional. Todo esto crea oportunidades y desafíos para las criptomonedas ya que buscan imponer algunos cambios incluso mayores en las sociedades a las que se comercializan.

En este confuso período, no faltan personas que afirman haberlo descifrado. Innumerables libros han aparecido sobre la era digital y lo que significa, sobre el "final del trabajo" o el impacto de la deuda que quedó de la crisis financiera. Este libro encaja bien en ese género. Pero es importante reconocer que el pensamiento lineal que hace que las personas reconozcan una tendencia u otra a menudo puede evitar que reconozcan una tendencia simultánea contradictoria. A continuación, exploraremos algunas de estas contradicciones y veremos qué significan para la forma en que las sociedades luchan contra la introducción de tecnologías disruptivas como la criptomoneda. Examinamos la tensión que crea y las demandas de que las tensiones se resuelvan mediante el compromiso y la negociación, generalmente a través de la intervención del gobierno.

Una de las contradicciones más grandes ocurre a lo largo del continuo descrito en el capítulo anterior: el de la descentralización versus la centralización. Las fuerzas en conflicto en cualquiera de sus extremos son evidentes no solo en el ámbito de las criptomonedas, sino también en toda la sociedad.

Puede parecer que vivimos en una era de über centralización. La concentración de poder y control que contribuyó al colapso financiero de 2008, más importante aún en forma de bancos excesivamente poderosos y demasiado grandes para quebrar, se ha intensificado en muchas medidas solo desde la crisis. Aunque las nuevas reglamentaciones buscaban reducir el poder de los bancos, la solución preferida por los responsables de las políticas a la vorágine económica y financiera era duplicar el antiguo sistema de poder concentrado. Los bancos centrales se volvieron aún más importantes, inyectando billones de dólares en moneda fiduciaria en la economía global a través de sus antiguos socios, los bancos. Esto puede haber evitado el desastre al evitar un colapso total en el sistema financiero, pero jugó en manos de las grandes instituciones y quienes las administran y dejaron al pequeño individuo atrás. Las grandes empresas públicas pudieron obtener préstamos a bajo precio a través del mercado de bonos corporativos en esta era de tasas de interés cero y así crecieron aún más, ya que crearon incentivos para las fusiones corporativas.

Sin embargo, las pequeñas y medianas empresas descubrieron que su principal fuente de financiación -los bancos comerciales- se había vuelto mucho más estricta con el crédito, lo que limitaba su capacidad de crecer y contratar. Mientras tanto, la demanda subyacente continuó disminuyendo, lo que significaba que las empresas más grandes tampoco tenían incentivos para invertir en nuevas contrataciones, no cuando podían explotar costos financieros más bajos para mantener los márgenes de ganancia y recurrir a la contratación externa y robots para reemplazar a los trabajadores locales.

Esta gran solución es mejor para los pocos y frena a muchos. Mientras que la riqueza de los gestores de fondos de cobertura y otras élites aumentó gracias a las ganancias incesantes del mercado bursátil después de que la crisis financiera disminuyó en 2009, los ingresos de la mayoría de los hogares en las sociedades occidentales se estancaron, creando la mayor brecha de riqueza desde la Gran Depresión. Es una historia de grandes bancos, grandes compañías y grandes casas para el 1 por ciento, con casi nada para el resto. Esa es una de las características de nuestra economía del siglo XXI, y habla de una tendencia de centralización, no de descentralización.

Sin embargo, al mismo tiempo, los signos de descentralización son claros, principalmente a causa de las nuevas tecnologías que han dado a las personas las herramientas y la motivación para liberarse de la dependencia de esas grandes instituciones centralizadas. Por ejemplo, toma energía. La utilidad moderna, con sus plantas de energía y líneas de transmisión, tiene una licencia estatal para operar; está sujeto a controles estatales de fijación de precios; es una empresa privada que sirve una necesidad pública. Pero cada vez es más posible que los propietarios configuren sus propiedades con suficiente capacidad de energía solar y eólica para reducir significativamente la dependencia de los servicios públicos o para salir de la red por completo. Como dijo el ex vicepresidente estadounidense Al Gore en un ensayo publicado por Rolling Stone en el verano de 2014, "Estamos presenciando el comienzo de un cambio masivo hacia un nuevo modelo de distribución de energía: desde el modelo de red de servicios públicos de la 'estación central' que se remonta a la década de 1880 a un modelo "ampliamente distribuido" con células solares en la azotea, almacenamiento de baterías en la instalación y en la red, y microrredes ".

Más allá de la energía, muchas otras industrias están experimentando cambios hacia modelos descentralizados que pasan por alto intermediarios guardianes: alojamiento turístico sin hoteles, servicios de taxis propiedad de los conductores sin servicios centrales de despacho, e-marketplaces para alquiler de herramientas para vecinos que quitan negocios de ferreterías. Esto está sucediendo incluso sin el uso de cryptocurrencies o blockchains. Las personas han descubierto que si tienen activos inactivos, pueden prestarlos a las personas que los necesitan, mientras que esas personas a su vez se han dado cuenta de que no necesitan pasar por costosos puntos de distribución central para encontrar esos activos. Este nuevo sistema se llama varias cosas: la economía colaborativa, la economía de malla, la economía colaborativa. ¿Tienes algo de poder de cómputo extra sentado en tu escritorio? Compártalo con quienes lo necesitan. ¿Tienes un auto sentado inactivo en tu entrada? Comparte eso. ¿Tienes una gran idea? Compártalo en línea y recaudar dinero en línea para financiarlo. Hasta ahora, los símbolos empresariales de esta era incluyen el sitio de alquiler de apartamentos personales Airbnb, el sitio de crowdfunding Kickstarter, la red de préstamos peer-to-peer Lending Club y los servicios de taxis controlados por los propietarios de automóviles individuales Uber y Lyft.

En algunos aspectos, estos nuevos modelos comerciales son extensiones de un proceso que comenzó mucho antes con el advenimiento de Internet. Si bien ningún bitcoiner que se respete describiría a Google o Facebook como instituciones descentralizadas, no con sus servidores controlados por corporaciones y vastas bases de datos personales de los clientes, estas gigantes empresas de Internet de nuestros días llegaron alentando a los pares y a los intermediarios. -actividades gratuitas. GoogleAds permitió a las pequeñas empresas eludir a las grandes

organizaciones de medios y comercializar más directamente a los posibles clientes; Facebook permitió a las personas formar orgánicamente grupos, comunidades y asociaciones que no estaban vinculadas por la geografía o las estructuras sociales y nacionales; Twitter significaba que las personas podían diseñar sus propios canales de noticias.

La importancia de la descentralización va más allá del surgimiento de nuevos modelos de negocios o incluso de que las personas están encontrando formas de ahorrar unos pocos dólares aquí o hacer unos pocos allí. Al desatar este enfoque de bricolaje para el comercio, los cambios en la tecnología y la cultura están conduciendo a nuevos métodos de interacción, tanto social como económicamente. Tanto las organizaciones sin fines de lucro como las sin fines de lucro ahora evitan las jerarquías verticales a favor de líneas de comando más horizontales y democráticas. (Para una representación visual de cómo funciona esto, compare los diseños de oficina de planificación abierta en el programa de televisión contemporáneo Silicon Valley con las oficinas cerradas de los Mad Men de los años sesenta). Muy parecido a los equipos de desarrollo de software de código abierto que parecen después de Bitcoin y un sinnúmero de otros proyectos de computación, las comunidades se están formando, en su mayoría en línea, sin titular y sin centro central. Se mantienen unidos por la convención comúnmente reconocida de que el consenso de la multitud prevalece sobre todo lo demás.

¿Se está formando un choque entre estos dos movimientos, la concentración de riqueza y poder del mundo corporativo y el reforzamiento del individuo de Silicon Valley? Quizás estas tendencias puedan seguir coexistiendo si el movimiento de descentralización sigue limitado a áreas de la economía que no se desangran en los sectores más amplios que domina Big Business. Pero eso no es lo que los defensores de esta tecnología prevén, especialmente aquellos en el sector de criptomonedas. Creen que la descentralización recién está comenzando y que los estamentos económicos y políticos centralizados -incluso los gobiernos y las naciones-estado, esos últimos loci de poder centralizados- se verán afectados por ella. Si es así, las criptomonedas y la tecnología blockchain podrían montar esa ola triunfalmente. Una frase de David Johnston de Mastercoin que algunos en la comunidad de criptomonedas llaman la ley de Johnston podría hacerse realidad: "Todo lo que se puede descentralizar se descentralizará".

Esta visión especialmente optimista del potencial de la tecnología de criptomoneda choca con los muchos obstáculos que enfrenta. Pero si reservamos criptomonedas por un momento, es difícil no creer que la tendencia descentralizado tenga impulso. Cuando lo enfrentamos contra la consolidación del poder concentrado de Wall Street y Washington en el período posterior a la crisis, estas tendencias gemelas comienzan a verse menos como movimientos paralelos y más como dos trenes en curso de colisión. Bien podemos estar al borde de una profunda agitación social, tal vez la más significativa desde el siglo XVI, cuando, en la segunda mitad del Renacimiento, la banca y el Estado-nación se establecieron como las fuerzas centrales del poder alrededor del cual el mundo los sistemas monetarios y económicos girarían.

Cuando se enfrentan a este tipo de desafíos disruptivos a partir de la nueva tecnología y las nuevas formas de organización de la sociedad, las empresas y las instituciones que ocupan el centro -las que representan el establecimiento económico y político- tienen tres opciones. Una es simplemente ignorar la nueva idea, desechar la nueva idea y continuar como siempre. Una segunda es luchar contra ella, tal vez a través del cabildeo político, o mediante el uso de campañas publicitarias o campañas de desprestigio para destruir la naciente amenaza a través de asociaciones negativas en el ojo público. Un tercero es tratar de adaptarse, incorporar, cooperar o trabajar con la nueva tecnología o concepto.

Los innovadores de Silicon Valley a menudo advierten contra los peligros del primer enfoque, pero la historia sugiere que a menudo no es una mala idea dejar que una nueva tecnología caiga víctima

de su propia exageración. La burbuja de las puntocom de finales de la década de 1990, en la que la exuberancia detrás de los precios de las acciones reflejaba la creencia permanente de que los primeros minoristas de sitios web en cada sector ganarían simplemente creando un nicho y comercializándola, lo demuestra. Neighborhood Pets no mató a las tiendas de mascotas del vecindario, no más que los planificadores de bodas fueron despedidos por OurBeginning.com, cuyos representantes se unieron a la marioneta calceta parlante de Pets.com entre una serie de publicidades Super Bowl XXXIV en 2000, pero cuyo nombre de dominio desde entonces ha pasado a una guardería de Seattle. Recuerde también la amenaza Y2K, que alcanzó su anticlímax semanas antes de ese Super Bowl. Nunca sabremos si fue en vano porque las firmas de consultoría informática convencieron con éxito a todos para que actualizaran sus mainframes o si promocionaron brillantemente un nonevent. Mucho antes, la historia estaba llena de otras ideas tecnológicas fallidas: el Apple Newton, las cintas de audio digitales y el formato de video Betamax, por nombrar algunos que nuestra generación podría recordar. Aún así, ignorar el cambio es arriesgado, por lo que Eastman Kodak proporciona una historia de advertencia. El centenario fabricante de películas análogas con sede en Rochester, Nueva York, no pudo captar la invención de imagen digital de uno de sus propios ingenieros en la década de 1970, solo para verse abrumado en la década de 2000 por la llegada de la masa. cámaras digitales comercializadas.

La opción de stand-and-fight típicamente requiere dinero, valentía y conexiones políticas. Wall Street, que tiene los tres, es el practicante más efectivo de esto. Uno hubiera pensado que la reacción al desastre de 2008 habría garantizado que los bancos se verían obligados a enumerar los valores derivados no transparentes que ayudaron a explotar el sistema financiero en nuevos intercambios en línea diseñados para permitir precios transparentes e información sobre productos como el incumplimiento crediticio intercambios Pero los cabilderos de Wall Street lucharon contra varios legisladores reformistas que intentaron que eso ocurriera y lograron diluir sus cuentas de tal manera que muchos derivados continuaron comerciando en opacos "mercados extrabursátiles", dejándonos en la oscuridad sobre los problemas financieros. riesgos que contienen Aún así, la estrategia de stand-and-fight es costosa y no se garantiza que gane. De hecho, incluso los bancos de Wall Street no han podido frenar por completo los vientos de cambio en su industria desde la crisis, incluidas las reglamentaciones que les exigen llevar un capital mucho más alto que absorbe los riesgos en sus libros.

Siguiendo con Wall Street, también podemos ver los méritos de la estrategia de cooptación. Los sistemas de comercio electrónico surgieron a fines de la década de 1990 como una gran amenaza para el negocio tradicional de Street de negociar bonos y otros valores fuera de bolsa al cotizar precios por teléfono. Al difundir ampliamente los precios, los nuevos sistemas dieron poder a los inversionistas e hicieron que a los bancos les resultara más difícil ganar dinero cotizando amplios diferenciales de oferta y demanda sobre esas inversiones. Pero la tecnología nunca dañó seriamente el poder de Wall Street en ninguno de estos mercados, en parte porque los bancos pensaron que en este caso el mejor enfoque no era luchar contra sus rivales, sino unirse a ellos. Se formaron varios consorcios bancarios para ofrecer mercados en línea en bonos, divisas y otras clases de activos, y aunque los márgenes de ganancia en cada operación se redujeron a medida que la luz de la transparencia brillaba en sus negocios, esto fue más que compensado por los ingresos que llegaron de nuevos negocios dirigidos hacia ellos.

Ahora, con la economía compartida y el poder de la "multitud" que amenaza con volver a poner en tela de juicio los modelos comerciales tradicionales, otras empresas de la vieja escuela están buscando cooptar algunas de estas nuevas ideas y adaptarse a ellas. U-Haul, la venerable empresa de alquiler de camiones, tan vieja como usted, está tomando esta táctica. Adoptando una visión de las finanzas similar a la criptomoneda, ha comenzado un programa de inversión que permite a las personas invertir directamente en la empresa, comprando notas respaldadas por activos duros específicos, como tiendas individuales, camiones e incluso colchones. No hay ningún banco de

inversión involucrado, ningún intermediario. Los inversionistas simplemente están prestando dinero de U-Haul, peer-to-peer, y, a cambio, obtienen un pagaré con pagos de intereses fijos suscritos por los activos de la compañía. A diferencia de un modelo de cadena de bloques, el préstamo se realiza de forma centralizada en la que el inversor debe confiar en la empresa misma, pero el mecanismo sin intermediarios tiene algunos de los mismos efectos que los proyectos promocionados por los defensores de la criptomoneda.

Otras grandes compañías también están buscando una respuesta adaptativa a la aparición de nuevos modelos de negocios basados en el intercambio y el crowdfunding, como los empleados por Uber, Airbnb y Lyft. Crowd Companies, con sede en Silicon Valley, que asesora a compañías del viejo mundo sobre cómo sobrevivir en esta nueva economía, cuenta con una impresionante lista de clientes, entre ellos Visa, Home Depot, Hyatt, General Electric, Walmart, Coca-Cola y FedEx. Todos están tratando de descubrir cómo adaptar sus negocios a una economía sin centros.

¿Y la industria de pagos? Bueno, parece estar metiéndose en las tres estrategias en respuesta al desafío de las criptomonedas. Empleando la postura de ignorar y despedir en una entrevista a principios de 2014 con los editores y reporteros del Wall Street Journal, el CEO de MasterCard, Ajay Banga, dijo sobre bitcoin: "El mundo no está corto de monedas, ¿para qué sirve esta divisa?". realidad, MasterCard, con Banga a la cabeza, es uno de los compradores más dinámicos de la industria de pagos en la industria digital. La compañía también está adoptando la estrategia de stand-and-fight, al haber contratado a cinco empleados de la firma de cabildeo de D.C. Peck Madigan Jones para presionar al Congreso sobre el bitcoin y las monedas virtuales. Pero la respuesta más poderosa de MasterCard a Bitcoin reside en su propio compromiso con las nuevas tecnologías. Su fuerte inversión en su programa MasterPass para pagos de teléfonos inteligentes ha dado sus frutos hasta el punto de que la compañía, junto con American Express, fue un socio clave en la decisión de Apple de incorporar pagos digitales en el iPhone 6.

Jason Oxman, el CEO de la Asociación de Transacciones Electrónicas, cuyos miembros incluyen algunos de los pesos pesados en pagos, comercio electrónico y telecomunicaciones móviles -como MasterCard, PayPal, Amazon, Google y AT & T- le gusta distinguir su industria de la industria de la música. Mientras que los productores de discos "hicieron todo lo posible para matar" a Napster y la tecnología para compartir archivos, la industria de pagos está "adoptando nueva tecnología", afirma. De hecho, lo que está sucediendo allí, incluso dejando de lado la criptomoneda, es vertiginoso. Como dice Oxman, la industria atraviesa "el período de innovación más importante desde la invención de la banda magnética [hace cincuenta años]. Realmente es un momento revolucionario para los pagos ". Esto plantea un verdadero desafío para los esfuerzos de la industria de la criptomoneda para obtener un punto de apoyo en los pagos. Incluso si las criptomonedas parecen hechas a la medida de la edad actual, con los amplios cambios descentralizadores discutidos anteriormente, sus principales competidores en la industria de pagos están ideando alternativas que podrían evitar que el público en general cambie al modelo criptográfico.

De hecho, en la era del Internet de las cosas, las tecnologías que aprovechan el viejo sistema de dinero soberano están encontrando diversas formas de impresionar a los clientes con mejoras en la experiencia de pago. El teléfono inteligente, la herramienta preferida del intercambio de bitcoin móvil, también está siendo aprovechado por una serie de compañías de tecnología financiera que buscan revolucionar la forma en que hacemos los pagos. PayPal, que fue la primera empresa en la década de 1990 en descubrir cómo enviar dinero digitalmente antes de que los sitios web comenzaran a aceptar tarjetas de crédito directamente, ahora se está reorganizando agresivamente como una empresa de pagos móviles con una aplicación que admite pagos en puntos de venta a través de códigos QR y otras tecnologías inalámbricas como Bluetooth y comunicación de campo cercano, o NFC. Con la misma aplicación, los usuarios que precargan su

cuenta de PayPal con dólares pueden enviar dinero a otros usuarios de PayPal a través de la red. Productos similares basados en teléfonos inteligentes incluyen Google Wallet y Softcard, una empresa conjunta de los operadores estadounidenses AT & T, Verizon y T-Mobile que llevaba el nombre de ISIS hasta septiembre de 2014, cuando se movió para disociarse del grupo extremista islámico del mismo nombre. . Se cree que Facebook está trabajando en algo similar, después de haber solicitado una licencia de dinero electrónico en lo que podría ser el lugar experimental de Irlanda. Y como se mencionó, el iPhone 6 de Apple, con su billetera digital incorporada, finalmente podría abrir los Estados Unidos a esta nueva forma de pago.

En muchos lugares fuera de los Estados Unidos, los pagos de teléfonos inteligentes ya están bien establecidos, y los países con mercados emergentes que saltan la tecnología a menudo toman la delantera. Los ciudadanos chinos realizan pagos móviles a través del omnipresente servicio de mensajería WeChat y con Alipay, un servicio del gigante e-marketplace Alibaba. Y no olvidemos que la idea del teléfono como dinero tuvo su génesis en Kenia, con el exitoso M-Pesa, que ahora se ramifica en los mercados de Europa del Este.

Luego están los cambios dramáticos vistos en la antigua tecnología de pagos con tarjeta. El pase de tarjeta portátil de Square ha permitido que millones de propietarios de pequeñas empresas, como taxistas y vendedores de alimentos, conviertan sus teléfonos inteligentes y tabletas en procesadores de pagos móviles. Por mucho que los bitcoiners se quejen legítimamente sobre los riesgos de seguridad que conllevan las tarjetas de crédito y débito, cuyo sistema depende de la transmisión de información sobre la identidad del usuario, la seguridad en las redes que los usan ha mejorado drásticamente. En particular, eso viene con el advenimiento del estándar EMV (Europay, MasterCard y Visa) para microchips incrustados en tarjetas, una tecnología que recién ahora llega a los Estados Unidos, más de un año después de que se introdujera en casi todos los demás. El uso de datos biométricos como los escáneres de huellas dactilares y la tecnología de reconocimiento facial también deberían hacer que el sistema sea más seguro, siempre que se puedan abordar las cuestiones de privacidad.

Todas estas tecnologías prometen hacer que la experiencia de compra sea prácticamente perfecta. Si bien es posible que no eliminen a los bancos y procesadores de pagos, que aún coordinarán la infraestructura de back-office del sistema monetario, estas tecnologías podrían dejar a los cajeros sin trabajo. Una idea es que después de que haya llenado su carrito de compras en el supermercado, camine a través de un escáner que lea las señales de cada uno de los artículos en su carrito y cargue automáticamente en su bolsillo la tarjeta de débito o el teléfono. Estos sistemas hacen que el uso del dinero sea cada vez más automatizado. Estas nuevas formas de explotar el muy antiguo sistema de dinero soberano ayudarán a mejorar ese sistema y dificultarán que Bitcoin y otras criptomonedas incursionen en el comercio convencional, al menos a nivel minorista.

Pero aquí está el problema: debido a que se aprovechan de ese sistema heredado, estas nuevas tecnologías cargan con todos los costos de transferir dinero dentro de él. Los proveedores de la tecnología no tienen más remedio que pagarle a los bancos y otros jugadores en ese sistema para procesar y asumir el riesgo de crédito. Los comerciantes que usan PayPal, por ejemplo, reciben un arancel de 2.7 por ciento por esos costos. Y a pesar de su rápido crecimiento, las tarifas de back-end están dificultando que Square, que registró una pérdida de $ 100 millones en 2013, genere ganancias. La carga de esas tarifas plantea dudas sobre la viabilidad a largo plazo del producto generalizado. En comparación, los procesadores de bitcoin como BitPay, Coinbase y GoCoin dicen que han sido rentables más o menos desde el primer día, dados sus bajos gastos generales y las tarifas comparativamente pequeñas que cobran los mineros en la cadena de bloques. Incluso si los consumidores no sienten esos costos, las empresas que deben incurrir en ellos pueden comenzar a insistir en que el back-end de sus transacciones sea manejado por algún tipo de

procesamiento basado en criptomonedas. La capacidad está ahí para hacer que esto suceda con los consumidores y comerciantes que todavía están felices de ver sus pagos y recibos denominados en monedas fiduciarias.

Las cosas son diferentes en China, el único lugar donde tanto los consumidores como los comerciantes pagan casi cero tarifas en los pagos móviles. Ahí, el problema es que se necesita la influencia excesiva del estado para lograr eso. Los bancos de propiedad estatal, claramente bajo instrucciones de Pekín, cobran tasas de casi cero en el procesamiento de pagos. Ese subsidio de facto deja bitcoin sin ventaja competitiva sobre WeChat y Alipay o la red nacional de tarjetas de crédito, UnionPay, pero también significa que el sistema basado en renminbi depende de la generosidad del estado, que puede ser quitado en cualquier tiempo o usado como una forma de extorsión oficial.

Estos nuevos mecanismos de pago, aunque tecnológicamente avanzados, siguen atrapados en el modelo quinquenal de gestión financiera centralizada. Eso puede no importar ni un ápice a la persona promedio que los utiliza, cuya ambivalencia podría ser suficiente para garantizar que el dinero soberano sobreviva, incluso cuando la economía colaborativa del futuro continúe su impulso hacia el empoderamiento individual en todos los demás ámbitos de la economía. Pero su supervivencia sería intrínsecamente inconsistente con todos los demás cambios descendentes y en marcha. Es difícil alejarse de la idea de que estas tendencias apuntan inevitablemente a una era de criptomoneda, si no de inmediato, luego una década más o menos en el futuro.

Eso nos lleva a una pregunta importante: ¿qué sucede con los bancos como proveedores de crédito si llega esa edad? Cualquier amenaza a este rol podría ser un chip de negociación para los bancos en su batalla de marketing con la nueva tecnología. Podrían argumentar que un sistema de criptomonedas que reemplace el papel moneda soberano dejaría a los bancos incapaces de generar crédito y, por lo tanto, cumplirían su papel sancionado singularmente como creadores de dinero privado. (Nos referimos aquí al concepto crítico de la banca de reserva fraccionaria, discutido en el capítulo 1.) Demasiado malo, dirían muchos bitcoiners. Para las facciones libertarias dentro de la comunidad de criptomonedas, que tienden a ver su modelo monetario como un sistema transaccional de suma cero en el que un suministro finito de moneda simplemente se comparte de ida y vuelta, el crédito bancario sin fin es solo una receta para la degradación de divisas y la crisis financiera . Pero, ¿qué harían todas las empresas que dependen de los préstamos bancarios para pagar a sus empleados o para dirigir sus operaciones o expandirse a nuevos mercados? Es posible que el crédito no se cree tan fácilmente en una economía basada en criptomonedas. No se puede simplemente crear dinero de bitcoin de la nada como lo hace el crédito bancario en el sistema de moneda fiduciaria. Sí, eso elimina los riesgos inflacionarios y significa que los bancos centrales ya no necesitan administrar la oferta monetaria con herramientas políticas imperfectas como las tasas de interés, pero los críticos de bitcoin contrarrestarán, con algún mérito, que el crédito con grilletes dejaría sin fondos a las economías de crecimiento.

Aún así, puede que no tenga que ser tan crudo. Si consideramos que los bancos simplemente actúan como intermediarios que agregan los fondos de aquellos que buscan prestar sus excedentes de ahorro y entregárselos a aquellos a los que les falta dinero y necesitan pedir prestado, no hay nada que decir que no puede haber coincidencia entre prestamistas y prestatarios. una moda desintermediada con criptomonedas. La nueva tendencia de los préstamos punto a punto, ejemplificada por Lending Club, ofrece un modelo que escala fácilmente a los sistemas de criptomoneda, con los controles y equilibrios de la cadena de bloques que potencialmente ayudan a mejorar un sistema de verificación de crédito y reputación crediticia. De cualquier manera, el flujo de crédito y dinero en un sistema financiero liderado por criptomonedas tomaría una forma muy diferente si los bancos fueran eliminados de esos flujos.

¿Qué pasa con el estado nación en sí? ¿Cómo responderá? Ignorar, pelear o cooptar? El sistema de dinero soberano, y especialmente el dinero fiduciario que le da al estado el poder sin control para imprimir moneda como lo considere conveniente, ha sido posiblemente el arma más poderosa en el arsenal del estado nación. Más que generar seigniorage, la seductora idea de que cada dólar impreso es un préstamo sin intereses que fluye de la gente al estado, controlar el dinero de la nación ha permitido a los gobiernos controlar el aparato de poder. Con el papel moneda pueden comprar armas, lanzar guerras, aumentar la deuda para financiar esos conflictos y luego exigir pagos de impuestos en esa misma moneda para pagar esas deudas. Una democracia funcional debería, en teoría, poner límites a todo eso. Pero en realidad este sistema monetario permite la extensión del poder. Financia burocracias y agencias cuyos empleados ponen su propia supervivencia por encima de todo. En los peores Estados-nación (piense en Corea del Norte), financia los instrumentos del terror y la represión que destruyen la dignidad de las personas.

Si ese sistema desapareciera, el Estado-nación, cuyos intereses se encuentran como todos los nuestros en la supervivencia, tendría que descubrir cómo responder. El estado-nación ha demostrado ser adaptable en los últimos quinientos años, por lo que no dudamos de que podría volver a encontrar formas de adaptarse y sobrevivir. Como veremos en la conclusión, un enfoque de cooptación podría ser comenzar a emitir criptomonedas soberanas. Otro podría ser que los Estados-nación se unan y fortalezcan su cooperación internacional en dinero. No tenemos idea de cómo todo esto desaparecerá. Todo puede no ser nada. Pero por primera vez en siglos, estas preguntas al menos ahora deben formularse.

Como hemos destacado antes, depende de lo que las personas hagan, de cómo voten con los pies. Desde Silicon Valley, la impresión es que la sociedad humana está ahora lista para deshacerse por completo del sistema centralizado y adoptar un modelo descentralizado dirigido por "la multitud".

"Ahora la multitud tiene su propio modelo de negocios", dice Jeremiah Owyang, fundador del servicio de consultoría Crowd Companies. Al ofrecer una definición amplia de la economía colaborativa que abarca todo, desde el trueque hasta los préstamos, Owyang sugiere que toda la población humana se está haciendo cargo de los medios de producción y cambiando las reglas del juego. "Están haciendo sus propias malditas monedas, por el amor de Dios", agrega enfáticamente Owyang.

Pero más allá de estas frases, la imagen es más matizada. El lenguaje del Valle sobre estas nuevas tecnologías hace que parezca que las personas ahora tienen una utopía al alcance de la mano, si tan solo pudieran abandonar las viejas formas, alcanzar esa aplicación en el teléfono inteligente y hacer que el poder de la multitud se apodere. Pero incluso la generación del milenio, un grupo rutinariamente descrito como los impulsores de estas nuevas aplicaciones y el más comprometido con las nuevas formas de socializar y hacer negocios, parece temeroso de abandonar una estructura social centenaria. Un exhaustivo estudio de 2011 de la sociedad estadounidense realizado por el Pew Research Center descubrió que los millennials -típicamente definidos como aquellos nacidos después de 1981- eran la única generación de cada cuatro en que la mayoría quería que el gobierno brindara más servicios, no menos. Otros estudios de Pew han demostrado que es más probable que esta cohorte defina al gobierno como un proveedor de servicios "eficiente" que las generaciones anteriores. Esto no quiere decir que este grupo, que en perspectivas de empleo y poder adquisitivo ha sido posiblemente más dañado que cualquier otro por las políticas defectuosas que condujeron a la crisis financiera, espera que el gobierno esté ahí para ayudarlos. Los datos separados de Pew del mismo estudio también muestran que al menos el 50 por ciento de los millennials dudan de que alguna vez recibirán un solo pago de beneficios de su cuenta de la Seguridad Social. Podría ser que los millennials son simplemente realistas: les gustaría más gobierno; simplemente no lo esperan.

Si toda esta nueva tecnología interrumpe el empleo como se esperaba, la sociedad inevitablemente pedirá al gobierno que suavice el golpe. Esto podría ser especialmente así si las tecnologías de criptomoneda se integran correctamente, no solo en los pagos sino en las formas disruptivas y descentralizadoras previstas en el examen del capítulo 9 de las tecnologías Blockchain 2.0. Gil Luria, un analista de Wedbush Securities que ha analizado en profundidad el potencial de las criptomonedas, sostiene que el 21 por ciento del PIB de Estados Unidos se basa en industrias de "confianza", aquellas que realizan tareas de intermediarios que las cadenas de bloques pueden digitalizar y automatizar. Extraído de las cuentas nacionales del Departamento de Comercio, el cálculo de Luria engloba banca comercial, empresas de la industria de valores, fondos y fideicomisos, proveedores de seguros, agentes de bienes raíces y servicios legales, un grupo que empleó a 10 millones de personas a mediados de 2014, según la Oficina de Estadísticas laborales. Nadie espera que estas industrias desaparezcan de la noche a la mañana, pero incluso un deslizamiento gradual hacia la obsolescencia parcial será doloroso para cualquiera que trabaje dentro de ellas.

Glorivee Caban sabe una cosa o dos sobre cómo es trabajar en una industria de servicios financieros y verse perturbado por las nuevas tecnologías. Entre 2009 y 2013, sus horas como cajera de Banco Popular en la ciudad de Nueva York disminuyeron de un trabajo a tiempo completo a las 35 horas a la semana a veinticuatro horas, todas pagadas a $ 11 por hora, una tasa que nunca se levantó Si bien las pérdidas sufridas durante la crisis financiera contribuyeron a la necesidad del Banco Popular de reducir los costos de la nómina, el verdadero facilitador de estos recortes fueron los cajeros automáticos más avanzados, que permitieron depósitos y servicios de banca en línea. "Cuando comencé en el Banco, veíamos que tal vez doscientas cincuenta personas pasaban por la sucursal. Cuando me fui, había bajado a ciento veinte ", dice. Esto minó su capacidad para lograr uno de los principales objetivos de desempeño de su trabajo, que consistía en hacer de diez a quince referencias de nuevos negocios por día. "Si los clientes no vienen físicamente al banco, ¿cómo vamos a hacer referencias?", Preguntaba. Con su salario neto reducido, Caban no tenía suficientes ingresos para cubrir el alquiler de $ 1,380 por mes en su apartamento de Brooklyn y criar a su hija pequeña, incluso con la ayuda de una contribución mensual del Departamento de Asuntos de Veteranos que surgió de su despliegue de tres veces con la Marina de los EE. UU. en Medio Oriente. Ella no tuvo más remedio que presentar una solicitud al gobierno de la ciudad de Nueva York para obtener asistencia social. Considéralo una señal de los tiempos: un empleado de un banco en la capital financiera mundial que necesita ayuda financiera del gobierno.

La posición de un cajero fue una vez un trabajo seguro y decente, que a menudo establecía el camino hacia posiciones más lucrativas en la administración del banco. En estos días es un símbolo de cuánto ha cambiado el negocio. Si bien la interrupción del trabajo por cajeros automáticos y otras tecnologías bancarias no es nueva, vale la pena considerar qué presagia para otros empleos en los servicios financieros y sectores legales si la tecnología de criptomonedas logra la interrupción que buscan sus defensores: personas que trabajan en el procesamiento de pagos, en custodia servicios, en defensa de bienes raíces, en firmas de transmisión de dinero, todos podrían verse afectados. Visa, MasterCard y Western Union se combinaron -para nombrar solo tres jugadores cuyos negocios podrían ser significativamente reformados- tenía veintisiete mil empleados en 2013.

Es poco probable que Western Union, por ejemplo, se quede en sus manos, al estilo Kodak, frente al desafío de las criptomonedas para sus negocios internacionales de remesas. La compañía de 163 años de edad ya está promoviendo herramientas en línea para reducir los costos, y sus ejecutivos están bien informados sobre las perspectivas de las monedas digitales. De hecho, muchas empresas en este campo finalmente optarán por incorporar el procesamiento basado en

blockchain para ahorrar costos. Pero eso no protegerá todos los trabajos de ingreso de datos y servicio al cliente para los cuales esta tecnología no tiene ningún uso.

Una vez que alcanzan una escala lo suficientemente grande, la pérdida de empleos generará tensiones políticas. Mientras que los beneficios para la sociedad derivados del avance tecnológico a menudo se comparten ampliamente, los perdedores se concentrarán en áreas geográficas o en industrias específicas fácilmente identificables. Como dice el viejo adagio, toda política es local. Así que espere una reacción violenta una vez que los bancos comiencen a cerrar centros administrativos administrativos en el centro de Manhattan o en Canary Wharf en Londres cuando sus clientes comerciales comiencen a reservar más ventas de clientes a través de sistemas de criptomoneda para evitar las tarifas de transacción del 3 por ciento.

El desafío para los tecnólogos y sus partidarios del capitalismo de riesgo es enmarcar la interrupción dentro de una narración políticamente digerible del progreso general, dice el capitalista de riesgo de Andreessen Horowitz, Chris Dixon. "Por un lado, tiene al banco que pierde su trabajo, y todos se sienten mal por esa persona, y por otro lado, todos los demás ahorran el tres por ciento, lo que económicamente puede tener un gran impacto porque significa que las pequeñas empresas amplían sus ganancias márgenes. Pero desde una perspectiva narrativa, no se siente tan bien. Hay pérdidas individuales y ganancias socializadas ".

Cuando se le pide que describa el mercado de trabajo si los tipos de compañías autónomas descentralizadas previstas por su empresa se vuelven prevalentes, el CEO de BitShares Daniel Larimer predice con confianza que estos proyectos "pueden crear millones de empleos basados en la información". Además, dice, blockchain- los mercados de predicción basados, donde las personas compran y venden contratos que pagan según la precisión con que pronostican un evento, crearán nuevas oportunidades de generación de dinero en las industrias intermediarias destinadas a la interrupción. "Si usted es un intermediario en la industria de préstamos o un intermediario en materias primas, o tiene conocimientos médicos, conoce esa industria mejor que nadie, lo que significa que puede tomar el conocimiento que tiene y convertirlo en valor", dice Larimer. "Al mismo tiempo que está ganando dinero, está brindando información al mercado, lo que hace que todos sean más productivos". Esto, insiste, no son "trabajos de preparación" en los que las personas "cavan agujeros y los llenan". "; son "trabajos de alto valor que producen valor".

El utopismo de los trabajos para todos de Larimer -el espíritu predominante de Silicon Valley, compartido por muchos bitcoiners- aclara cuántas personas, si no la mayoría, encuentran difícil el cambio. No todos, y tal vez no muchos, trabajadores despedidos pueden levantarse fácilmente y utilizar sus conocimientos para obtener un ingreso del comercio especulativo en un mercado de predicción de BitShares. Para muchos parecerá una forma de juego. Someter sus vidas a tal incertidumbre es anatema para las personas que han esperado que un trabajo asalariado dure toda la vida y para proporcionar seguridad y permanencia.

Las personas tendrán que descubrir cómo aplicar sus habilidades particulares a este Mundo Feliz y, si no pueden aplicarlas, cómo adquirir rápidamente las habilidades correctas. Como señaló Tyler Cowen en su libro Average Is Over, "Las preguntas clave serán: ¿Eres bueno trabajando con máquinas inteligentes o no? ¿Son sus habilidades un complemento de las habilidades de la computadora, o la computadora está mejorando sin usted? Lo peor de todo es que compites contra la computadora ". La tesis de Cowen, que se basó en parte en la teoría de que" el trabajo ha terminado ", no fue una rosa para Mesoamérica. Atribuyó gran parte del reciente estancamiento económico de ese sector social a la velocidad cada vez mayor del cambio tecnológico, que por primera vez parece desplazar empleos más rápido de lo que la economía puede aprovechar el crecimiento desatado por esa tecnología para crear nuevos empleos.

Estas preguntas serán especialmente relevantes en la era de la criptomoneda, sin duda para todos aquellos que trabajan en industrias de "confianza" desafiadas por la automatización de blockchain. Podrían esperar ciegamente que esta nueva y extraña forma de manejar las finanzas nunca llegue a ser nada, al igual que Eastman Kodak equivocadamente hizo con la cámara digital. Pero probablemente ya se haya dado cuenta de que creemos que es un punto de vista peligrosamente ingenuo. Si bien es cierto que algunos economistas prominentes ven el bitcoin como una moda pasajera -Robert Shiller, de Yale, y Nouriel Roubini, de la Universidad de Nueva York- aún estaban en ese campo a mediados de 2014-mientras más tiempo la moneda digital desafíe estas expectativas y más a lo largo de la curva de innovación las empresas de bitcoins van, cuanto más desactualizadas parezcan esas vistas. El ex secretario del Tesoro de Estados Unidos Larry Summers, una de las mentes económicas más influyentes del planeta, reconoce los riesgos de ignorar esta tecnología para un sector financiero que está "listo para la interrupción". Como lo expresó en una entrevista, "Las personas que rechazaron el Internet como curiosidad para los científicos estaba en el lado equivocado de la historia, las personas que rechazaban la fotografía digital como algo realmente artificial estaban en el lado equivocado de la historia, y las personas que sentían que raquetas de tenis no estratégicas estaban hechas con madera estaban equivocadas lado de la historia. Así que me parece que las personas que rechazan con confianza toda la innovación aquí [en pagos basados en blockchain y sistemas monetarios] están en el lado equivocado de la historia ".

Dado lo que eso supone, incumbe a la sociedad determinar la combinación correcta de provisiones de redes de seguridad y apoyo transitorio para suavizar el golpe para los millones que podrían estar sin trabajo. En contraste con la idea de un mundo casi anárquico en el que el gobierno se reduce a un debilitamiento frente a una "multitud" resurgente, y donde las naciones-estado tienen su relevancia desafiada por criptomonedas sin estado, las personas a quienes elegimos dirigir la sociedad tendrá un gran trabajo importante por delante. Los planes de educación pública deben desarrollarse para que las personas puedan estar debidamente capacitadas para los trabajos del futuro. A los niños se les debe enseñar a codificar, pero también a usar sus talentos creativos para concebir formas nuevas y emocionantes en las que los sistemas descentralizados se puedan utilizar para mejorar las vidas de las personas. Mientras tanto, los adultos deben recibir el tipo de reentrenamiento vocacional necesario para prepararlos para un entorno de trabajo muy diferente. Para aquellos que no lo hacen, porque, contrariamente a las previsiones de Larimer, la evidencia sugiere que simplemente no habrá suficientes empleos para todos, se necesita un estado de bienestar más fuerte y más justo. Reducir el bienestar podría haber estado de moda en la era del pequeño gobierno que surgió con Reagan, pero a medida que crecen las filas de desempleados y subempleados, su influencia política también lo hará. No importa qué tecnología de criptomoneda pueda hacer para eludir a los gobiernos, los intereses de personas como estas determinarán las leyes y políticas del futuro.

En los Estados Unidos, todo esto tendrá lugar dentro de la política monetaria altamente cargada de Washington, una arena en la que la industria de las criptomonedas apenas está comenzando a ingresar como una fuerza de presión. Mientras que sus rivales en la industria tradicional de servicios financieros han hecho donaciones políticas cuantiosas, siempre útiles para dar forma a una legislación favorable, los bitcoiners se han ganado recientemente una entrada en este mundo. En 2014, la Comisión Federal de Elecciones de los EE. UU. Acordó por unanimidad permitir las contribuciones de bitcoin a políticos y organizaciones políticas de hasta $ 100 en valor, el mismo máximo permitido para donaciones en efectivo en dólares. Más importante aún, la FEC de seis miembros dividió repetidamente las líneas partidarias, con los republicanos del lado pro-bitcoin, sobre si se deberían permitir donaciones significativamente mayores en virtud de los términos existentes para las contribuciones no en efectivo a través de cheque y tarjeta de crédito. Esto llevó al presidente republicano de la FEC, Lee Goodman, que había apoyado el enfoque más generoso, a argumentar polémicamente que los donantes de monedas digitales efectivamente tenían luz

verde para llegar hasta el final ya que los tres demócratas no podían reunir una mayoría para detenerlos. . Nadie en la comunidad bitcoin iba a discutir eso. Entonces, las donaciones empezaron a fluir. Según Make Your Laws, un PAC sin fines de lucro que se enfoca en la reforma financiera, decenas de candidatos aceptaron donaciones de bitcoin a septiembre de 2014, incluido el congresista republicano de Texas Steve Stockman y su homólogo demócrata de Colorado. Jared Polis, junto con varias organizaciones del Partido Libertario y una serie de PAC.

A medida que Bitcoin gana lentamente una voz financiera en Washington y comienza a competir en los márgenes con los gigantes en el sector financiero tradicional, tendrá cierta influencia en el proceso regulatorio presentado en el capítulo anterior. Pero, irónicamente, si la industria de las criptomonedas tiene el éxito que desea, podría enfrentarse a un oponente aún más formidable de los grupos que representan a las personas que enfrentan el desplazamiento laboral. Para que la sociedad llegue a un medio feliz donde los grandes beneficios liberadores del empoderamiento comunitario se logran a través de aplicaciones de criptomonedas descentralizadas pero a un costo mínimo para aquellos seres humanos que son desplazados, todas estas partes deberán unirse para encontrar una solución negociada.

Este no es un momento para que el gobierno sea dejado de lado e irrelevante por esta tecnología. A pesar de todos los sueños utópicos de una sociedad de autoayuda que no necesita una autoridad centralizada, es difícil imaginar cómo se pueden negociar todos estos conflictos e intereses divergentes sin un árbitro central.

No se trata solo de proteger a los trabajadores desplazados. Las empresas de Bitcoin también pueden beneficiarse del apoyo de un gobierno que busca mantener el nivel de campo de juego. En la era de la criptomoneda, será igual de importante insistir en que se respeten las leyes antimonopolio, las reglas de transparencia y las agencias de protección del consumidor, ya que garantizarán que las regulaciones excesivamente onerosas no anulen la innovación. Esto no quiere decir que el modelo actual del gobierno para contener monopolios y fideicomisos y para promover la competencia no haya sido abusado de múltiples maneras. Pero descartar completamente al gobierno podría ser invitar a nuevos monopolizadores, otra forma de decir fuerzas "centralizadoras" para tomar el control de la economía del futuro, incluso si su infraestructura subyacente está construida sobre tecnología de criptomoneda descentralizada.

Mientras que los entusiastas de las criptomonedas tienden a pensar ahora en Google, Facebook, Twitter, Apple, Microsoft, etc., como el establecimiento centralizado, el enemigo, vale la pena recordar que ellos también, una vez solo existieron como ideas radicales y disruptivas de un comienzo inaudito. -UPS. Debido a que el sistema legal estaba estructurado de manera tal que permitía que esas nuevas empresas florezcan y busquen beneficios, el mundo ha cambiado, y para mejor, diríamos. Si no fuera por un marco político y regulatorio diseñado deliberadamente para alentar la innovación y la competencia, estas entidades no tendrían ninguna oportunidad contra los medios establecidos y las industrias de comunicaciones a cuyos mercados apuntaban.

Contrariamente a la mentalidad de los criptoanarquistas, todavía hay libertad y progreso en los compromisos a medio camino que se realizan tanto con el gobierno como con empresas financiadas por capital de riesgo que buscan obtener ganancias sobre las criptomonedas. El ideal libertario detrás de las criptomonedas puede ser noble en espíritu, y debemos abrazar los elementos clave de esa batalla por la libertad. Pero, para tomar prestada una idea de un editor nuestro, tales proyectos utópicos a menudo terminan como competiciones Ultimate Frisbee, que por diseño no tienen árbitros -sólo "observadores" que arbitran llamadas- y donde las disputas sobre violaciones a las reglas a menudo se convierten en gritos que se ganan con el jugador que grite más fuerte, adopta la postura más intransigente y persuade al observador.

Un día, las nuevas start-ups criptográficas que actualmente son la batuta en la continua lucha de la sociedad por la libertad se convertirán en parte del propio establecimiento, al igual que lo son ahora Google y Facebook. Esperamos que en ese momento nuestras redes de criptomonedas estén lo suficientemente descentralizadas y que nuestros gobiernos hayan redactado leyes acomodaticias que permitan que la próxima ola de innovadores interrumpa esos futuros Googles y Facebook. Esperemos también una red de seguridad social suficientemente solidaria y constructiva para que todos puedan beneficiarse de las profundas mejoras que estos recién llegados pueden aportar a nuestra forma de vida.

Conclusión

PASE LO QUE PASE

La realidad es un proceso histórico.

-Georg Hegel

Para todo lo que acabamos de exponer, a pesar de la promesa y el potencial de la criptomoneda, sigue siendo un producto de nicho. Digamos que hay 12 millones de billeteras, e incluso cien mil comerciantes que lo aceptan, e incluso $ 500 millones en dinero de VC ahora invertidos en proyectos de criptomonedas. Esos números palidecen junto a los 6 mil millones de personas en el mundo, o los 23 millones de negocios en los Estados Unidos solamente. Nadie ha estudiado a fondo cuánto les está yendo a los negocios comerciales con bitcoin y criptomonedas, pero los informes reales y anecdóticos tienden a vincularlo a un número bajo, alrededor del 1 por ciento de las ventas totales de los pocos que los aceptan.

Eso está muy por debajo de lo que podría sugerir el bombo. Si Bitcoin va a ser esta fuerza revolucionaria y global para el cambio que sus defensores creen fervientemente que es, algunas cosas evolutivas van a tener que suceder primero. Por un lado, la mancha de asociación que tienen las criptomonedas con el sitio Silk Road y Mt Gox aún es visible; La mayoría de la gente simplemente asume que todo es una estafa. Como mínimo, la gente debe sentir que las criptomonedas son seguras y no pueden perder valor repentinamente. No están ni cerca de eso en este momento. Una encuesta de mediados de 2014 descubrió que solo la mitad de los ciudadanos estadounidenses conocía el bitcoin, solo el 3% lo había usado y el 65% dijo que era improbable que lo usara (y esas cifras fueron una mejora de una encuesta varios meses antes).) Las criptomonedas, como solía decir Ricky Ricardo a Lucy, tienen algo que hacer antes de que las personas las adopten.

Un segundo problema es que, si Bitcoin se convirtiera realmente en una potencia monetaria dominante, podría crear fuerzas económicas que conmocionarían a la mayoría de los ciudadanos del mundo. Con la creación de nuevos bitcoins con un límite de 21 millones, Bitcoin es una moneda deflacionaria. Nuestra economía global tal como se construye actualmente se basa en las monedas inflacionarias. Los bitcoiners señalan acertadamente que esto puede tener un efecto destructivo para cualquiera que tenga un ahorro decente, ya que significa que esos dólares y euros pierden valor con el tiempo. Pero al menos en tiempos de crisis económica, estas monedas fiduciarias ilimitadas les permiten a los bancos centrales emitir tantas como sea necesario para evitar que la gente acumule dinero y liberar crédito para que se creen empleos. Bitcoin, en comparación, sería como una gran cucharada de aceite de ricino. Algunos defensores de Bitcoin argumentan que no tendríamos que tomar el medicamento porque las instituciones financieras interesadas y los bancos centrales que no rinden cuentas ya no podrían precipitar los tipos de crisis financieras como lo han hecho en el pasado. Pero no hay forma de probar eso. Para una economía global que funciona a crédito y que ya no está acostumbrada al rigor del control monetario, dicho sistema podría causar un gran daño si no se presenta adecuadamente. Economistas como Mark T. Williams de la Universidad de Boston y Paul Krugman, columnista del New York Times, advierten que en tiempos de pánico financiero y trastornos económicos, la gente acumulará la moneda digital de oferta limitada y muy codiciada. Esto restringiría el flujo de dinero a todos los demás y agravaría la recesión. Sin un banco central que actúe como prestamista de último recurso, todos nos moriríamos de hambre. Sería, en efecto, una repetición de la Gran Depresión, dicen estas personas.

Una tercera preocupación es la competencia, y olvidarse de competidores obvios como Visa y MasterCard. ¿Qué sucede si, digamos, hay un sistema de pago que ofrece todas las ventajas de los pagos digitales, sin ninguno de los inconvenientes reales o percibidos de Bitcoin? ¿Y si ese sistema ya estuviera instalado dentro de otro sistema en el que la gente confía? ¿Qué pasa si todo eso fue empaquetado y vendido por una compañía cuyo nombre y logotipo son ... una fruta? A Apple le resultará mucho más fácil encontrar conversiones a su sistema de pago móvil de lo que lo hará Bitcoin con su sistema de pago, sin importar sus cualidades.

El problema de seguridad / volatilidad puede y debe superarse con la innovación de criptomonedas desatada por su modelo de fuente abierta. La seguridad de bitcoin ya ha avanzado mucho desde la debacle de Mt Gox; ahora es prácticamente imposible imaginar que vuelva a ocurrir una pérdida tan masiva. La volatilidad en el precio de Bitcoin también eventualmente disminuirá a medida que más comerciantes ingresen al mercado y los intercambios se vuelvan más sofisticados. Además, es probable que el problema de deflación / inflación no sea un problema. Como señalamos a continuación en una discusión sobre lo que puede deparar el futuro, los analistas más serios de la criptomoneda no tienen el dominio mundial de bitcoin como caso base. Es casi seguro que los gobiernos mantendrán su poder para emitir monedas fiduciarias, que no tienen límites de emisión y ofrecerían una válvula de escape para las economías que se encuentran sin dinero. Además, varias altcoins que salen al mercado son más abiertas, con esquemas de emisión flexibles. Estos podrían un día plantear una alternativa a un sistema monetario bitcoin deflacionario. (Eso podría asustar a los partidarios libertarios de Bitcoin, que ven la deflación como una fortaleza, no como una debilidad, pero puede convertirse en una moneda práctica).

En cuanto a la competencia, es más difícil de tratar, y no porque las criptomonedas serán inferiores. El tipo de productos de pago con los que Apple y otros están jugando se basan en el viejo sistema centrado en los bancos y están cargados con los mismos costos subyacentes e ineficiencias, mientras que Bitcoin está libre de ellos. Pero la pregunta es, ¿qué quiere la gente? Eso nos lleva a la última medida de si la criptomoneda puede tener éxito: si, cuando se compara con la competencia, la gente puede convencerse de los beneficios de la criptomoneda, disuadida de temer sus trampas y dispuesta a abandonar las monedas emitidas por el gobierno con las que Fueron criados. Esa no es una tarea simple.

Aun así, vamos a dar un paso aquí y argumentar que las monedas digitales descentralizadas basadas en encriptación tienen un futuro. Podría ser bitcoin u otra criptomoneda, o una que aún no se haya creado, pero esta tecnología innovadora tiene un impulso detrás de ella que será difícil de detener. Mucho más importante, resuelve algunos grandes problemas que son imposibles de abordar dentro de la infraestructura de pago subyacente. Las criptomonedas prometen disipar gran parte del enorme costo que un modelo de pagos centrado en el banco impone a nuestra economía global; podrían llevar a miles de millones de personas excluidas de ese sistema a la economía global; y a través de múltiples aplicaciones basadas en blockchain, prometen responsabilizar a clases enteras de intermediarios, instituciones centralizadas y agencias gubernamentales como nunca antes.

Exactamente cómo la tecnología de criptomonedas se convierte en una parte importante de la infraestructura financiera mundial es la próxima gran incógnita que abordaremos. Sin embargo, algunas rutas son obvias. Uno o varios pueden jugar un papel, o esto podría estar dirigido por algún factor que nadie siquiera está pensando.

La forma más obvia en que las criptomonedas se incorporan es a través de la adopción continua, y nada aumentaría más rápido que el hecho de que un jugador importante las adopte y se convierta en un defensor eficaz. Una serie de grandes nombres se subieron al carro de bitcoin en

2014: Overstock, Expedia, Dish Network, Dell, PayPal a través de su filial Braintree, así como una serie de nombres más pequeños. Todo eso ayudó a construir la red, pero si un gran jugador, un jugador realmente grande, subiera a bordo, se podía ver que la criptomoneda llegaba al público en general mucho más rápidamente. Aquí no hablamos de una compañía que acepte Bitcoin de sus clientes minoristas en sí, sino de utilizar la criptomoneda en las transacciones de negocio a negocio para eliminar los intermediarios financieros, reducir los costos operativos y aumentar los resultados. Imagine cuánto más amplio sería el uso de criptomonedas si un minorista importante como Walmart cambiara a una red de pago basada en blockchain para recortar decenas de miles de millones de dólares en costos de transacción de los $ 350 mil millones que envía anualmente a decenas de miles de proveedores. en todo el mundo. ¿Y si, además, ese jugador realmente tiene religión, como lo hizo el CEO de Overstock, Patrick Byrne, con su plan de incentivar a los proveedores para que acepten Bitcoin? De esta forma, fomentaría cambios que van más allá de sus relaciones de pago directo. Con efectos de red como ese en mente, no es difícil imaginar que un jugador parecido a Walmart alimente la propagación de la adopción hasta que se alcance una masa crítica de auto-refuerzo. (Para el registro, no tenemos idea del pensamiento actual de Walmart sobre la criptomoneda).

El principal catalizador para la adopción podría ser un gobierno que busca reducir los costos de adquisición o aportar una mayor transparencia a la gobernanza. Ya sabemos que Canadá exploró la idea de un dólar canadiense digital con su MintChip, y Ecuador planea introducir una moneda digital emitida centralmente. ¿Qué pasa si el gobierno de México cumple con el plan aún más ambicioso que ha lanzado? (Recordemos que dijo que estaba estudiando la posibilidad de crear una criptomoneda propia y cómo usar la tecnología blockchain para mejorar la gobernabilidad.) Si México se convirtiera en el primer gobierno enfocado en criptografía, podría convertirse en un centro cripto-tecnológico, alentando a los gobiernos de las muchas otras naciones en desarrollo con las que comercian a seguir. Dado que casi todos los bitcoiners se obsesionan con la promesa de Bitcoin de solucionar los problemas de las naciones en desarrollo, como las remesas y las poblaciones no bancarizadas, un efecto de proliferación liderado por México en los mercados emergentes podría tener efectos de gran alcance.

¿O podría ser el conductor el descubrimiento de la proverbial "aplicación asesina"? En la década de 1990, el boom de Internet se inició con la creación del navegador web Netscape, que tenía características fáciles de usar que carecían de su predecesor, Mosaic, y que, por lo tanto, podía despegar como un producto de consumo. Un equivalente en criptomonedas podría ser una billetera que se adapta perfectamente a las plataformas de comercio electrónico y es tan segura que las personas no temen ser pirateada. El equivalente podría ser un servicio que hace que sea ridículamente simple para personas en mercados emergentes enviar y recibir criptomonedas y convertirlas dentro y fuera de sus monedas locales. Tendría que ser algo que todos consideraran imprescindible.

Por último, nada forja el carácter como una crisis. Cuando llegó el pánico de 2008, el bitcoin no existía. En cambio, los inversionistas se inundaron en ese antiguo refugio seguro, el oro, que triplicó su precio en dos años. Pero ahora Bitcoin ofrece una alternativa, una que es significativamente más útil que el oro. Tiene cualidades similares de suministro finito, lo que respalda su valor, y los bancos centrales no pueden meterse con él. Pero puede usar bitcoin mucho más fácilmente para comprar cosas que puede usar oro. La idea de otra crisis financiera es casi inconcebible. En un mundo inundado de deudas y sujeto a las intervenciones del banco central, los precios de los activos superados y las interconexiones del mercado cuyas fallas se revelaron hace seis años pero nunca se arreglaron, muchos analistas suponen que otra es inevitable. También hay un precedente de tecnología de pagos: M-Pesa en Kenia, que recordará obtuvo su gran oportunidad durante la crisis política de 2007 en ese país, cuando las personas descubrieron que podrían usarlo para transferir fondos cuando el sistema financiero tradicional se

descompuso. No es difícil imaginar que Bitcoin disfrute de una situación similar en el lugar correcto en el peor momento. Si las criptomonedas tienen la oportunidad de demostrar su valor en un mundo en llamas de financiación, es posible que encuentren una legión de conversos.

Con esos potenciales catalizadores para el cambio en mente, ahora podemos contemplar las formas en que esta tecnología podría desarrollarse y qué impacto podría tener. Nos involucraremos en un tipo de experimento mental para explorar los diversos escenarios sobre cómo podría desarrollarse este proceso. Sí, esto es completamente especulativo, pero al igual que con el ejercicio que acabamos de realizar, creemos que es útil. Se desarrollan líneas claras de lógica a medida que uno piensa a través de las relaciones de causa y efecto. Nadie sabe en qué dirección viajarán las criptomonedas, pero las personas inteligentes, las personas más inteligentes que nosotros, se inclinan por tratar de descubrir qué camino tomarán estas cosas.

Creemos que es más justo diseñar una gama de escenarios en lugar de hacer predicciones audaces. Como dijimos al comienzo de este libro, somos periodistas, no futuristas. A medida que exploramos esos escenarios, iremos deliberadamente más allá de la pregunta que hace la mayoría de la gente: ¿El bitcoin en sí tendrá éxito o fracasará? Siempre hemos subrayado que la tecnología subyacente presentada por la cadena de bloques de bitcoin importa mucho más que la moneda específica que lleva su nombre. Habiendo dicho eso, comencemos con los dos escenarios aludidos en la misma pregunta: si bitcoin domina el mundo o si se une a Betamax en el basurero de la historia. A partir de ahí veremos las posibilidades entre esas dos conclusiones contradictorias, así como algunas tangentes completamente diferentes sobre las cuales la criptomoneda podría llevar a la sociedad.

El caso "No"

El dinero tiene tres características generales: es una unidad de cuenta, un medio de intercambio y una reserva de valor. Para bitcoin, o cualquier criptomoneda, para alcanzar los tres, todo ese concepto va a necesitar un respaldo amplio, si no de los consumidores y de las empresas que usarán la tecnología para reducir costos. Es posible que no gane ese soporte, incluso si el producto es técnicamente sólido. Hasta el día de hoy, puede encontrar personas que explicarán por qué el videograbador Betamax fue técnicamente un producto mejor que el VHS. Pero la mayoría de la gente ahora ni siquiera sabe lo que era Betamax. La criptomoneda, a pesar de todas sus supuestas glorias, podría perder de manera similar a un competidor "lo suficientemente bueno", que funciona a través del sistema tradicional centrado en el banco pero que agrega suficientes ahorros de costos y conveniencia para darle una ventaja.

Si bien los que adoptan las empresas podrían ser los catalizadores más poderosos para el cambio, verán cómo los consumidores y el público en general ven el bitcoin y otras criptomonedas antes de saltar. La mayoría de los consumidores tal vez nunca muestren suficiente apoyo. Los servicios de depósito digital de cartera, procesamiento de pagos y bitcoin centrados en el consumidor, como Coinbase, Bitreserve, Circle Internet Financial y Xapo, facilitan el uso de criptomonedas y son más seguros para el público en general, tratando de borrar la memoria persistente de Mt Gox. Pero poca evidencia sugiere que hayan logrado llegar a la gente más allá de los pequeños grupos de adeptos a la tecnología y los entusiastas de las criptomonedas que actualmente lo usan. Tal vez la mala reputación haya arruinado para siempre la reputación de la criptomoneda. Agregue a esa imagen pública el dolor de cabeza del seguimiento del impuesto a las ganancias de capital ahora requerido en los Estados Unidos, así como las cargas regulatorias que dificultan que los proveedores de criptomonedas alcancen sin inconvenientes a los consumidores comunes, y es posible que esta nueva forma de dinero nunca ganes atractivo. En este escenario, las criptomonedas se atascan, para siempre, en el ciclo perpetuo de la gallina y el huevo: no hay

suficientes usuarios, no hay suficientes lugares para usarlos, no hay suficiente razón para poseerlos. La masa crítica nunca se alcanza y toda la idea se marchita y muere.

El caso "Sí"

(Nota: mientras que el caso "no" se refiere a un escenario en el que ninguna criptomoneda lo hace grande, aquí en el caso "sí" estamos hablando puramente de bitcoin. Como veremos más adelante, las criptomonedas podrían convertirse en otros escenarios imaginables atrincherado sin que bitcoin se vuelva dominante.)

El caso de que Bitcoin se convierta en el rey de las monedas puede parecer exagerado dadas las estadísticas de adopción que citamos arriba, pero todas las grandes cosas tuvieron que comenzar en algún lado. En 2009, pocos esperaban que Bitcoin llegara tan lejos como antes. Además, como ya hemos comentado, la red descentralizada de alta velocidad y bajo costo en la que se basa la cadena de bloques de Bitcoin tiene un beneficio real. Dado que Bitcoin es, con mucho, la más arraigada de todas las criptomonedas, con una clara ventaja de ser el primer jugador, si una nueva moneda es para capitalizar esos beneficios, podría ser también bitcoin.

Esta es una era digital, y bitcoin es dinero digital. En un mundo donde las personas viven con sus teléfonos, en un mundo donde se hace tanto comercio en línea, la simplicidad y el ahorro de costos están a su favor. Todo lo que se necesita es uno de esos catalizadores descritos anteriormente, y luego otro, y otro, y otro. Eventualmente, se vuelve tan popular que se cumplen las tres características del dinero y el bitcoin es tan grande como el dólar.

A pesar de su problema de imagen pública y las restricciones reglamentarias, el entorno no es del todo incómodo para que florezca el bitcoin. Algunos de los estados más amigables con las criptomonedas como Suiza, Singapur, el Reino Unido y Canadá podrían fomentar centros de innovación que le dan a la tecnología un impulso imparable. Incluso en los Estados Unidos, a pesar del rencor por la idea de BitLicense del superintendente del Departamento de Servicios Financieros de Nueva York, los reguladores reflexivos están dejando espacio para la innovación. Si bien los países en desarrollo han tardado en alcanzar el éxito, muchos han notado el atractivo del bitcoin allí. Si el bitcoin despegara como el principal vehículo para las remesas internacionales y las transferencias financieras dentro de los países en desarrollo, tan pronto como, digamos, WeChat despegó en China, podría convertirse rápidamente en la moneda elegida de los 2.500 millones sin bancarrota. No son súper ricos, pero representan un nuevo mercado que los inversores y vendedores de la frontera ahora quieren aprovechar. Para estar en eso, necesitas bitcoin. Este es el tipo de conflagración global gigante en torno a la cual es posible imaginar que Bitcoin se convierta en una fuerza global dominante.

¿Cómo se vería este mundo? No es solo un asunto cosmético. No se trata solo de que las personas toquen sus teléfonos para descargar los pagos de bitcoin en las cajas. Como sabrá por haber leído este libro, un mundo con bitcoin dominante tendría implicaciones mucho más amplias: por un lado, tanto los bancos como los gobiernos tendrían menos poder. Y si todas las otras aplicaciones descentralizadas de las que hemos hablado vienen con esto, este sería un mundo en el que la gente vivía mayoritariamente sola, en sus hogares alimentados por energía solar con sus automóviles sin conductor, propiedad de la comunidad, intercambiando dinero y valor directamente, peer-to-peer. Comienza a parecer ciencia ficción. Por supuesto, si hubieras descrito el mundo de hoy, tal como es, a alguien hace cien años, habrían pensado que sonaba como algo sacado de una historia de H. G. Wells, también.

A la gente le gusta hablar de bitcoin en los términos extremos planteados en los dos escenarios anteriores, sí o no, dominación o cubo de basura, pero no es una simple pregunta en blanco y negro. Lo que es probable es que el bitcoin continúe creciendo, no junto con el mundo "real", sino unido a él, la tecnología subyacente adoptada por una variedad de instituciones y empresas para satisfacer sus necesidades. Todo el proceso se asemeja a algo que verías en biología, evolución entre especies. Esto es lo que esperamos que suceda. El truco es intentar adivinar hacia dónde va esa trayectoria evolutiva. Una vez más, en lugar de hacer conjeturas directas, preferiríamos ofrecer otro conjunto de escenarios.

Un Cog vital, si no se ve,

Un escenario que los visionarios de Silicon Valley frecuentemente expresan es que las criptomonedas terminan desempeñando un papel vital dentro de la infraestructura de nuestros sistemas financieros, pero en un segundo plano, con monedas fiduciarias que continúan siendo las principales unidades de cuenta y medios de intercambio de las economías. En ese caso, los protocolos de criptomoneda y los sistemas basados en blockchain para confirmar las transacciones reemplazarían el engorroso sistema de pago que actualmente manejan los bancos, las compañías de tarjetas de crédito, los procesadores de pagos y los operadores de divisas. Algunos de esos intermediarios desaparecerían; otros simplemente usarían la tecnología de criptomoneda para sus propias transacciones de institución a institución. Debido a la conversión instantánea en monedas fiduciarias después de cada transacción, los consumidores y negocios de los usuarios finales seguirían sus vidas cotizando precios y entregando dinero en las mismas monedas que siempre han usado.

Si la cadena de bloques de bitcoin se convierte en la opción preferida en este escenario, su valor como moneda -o tal vez mejor concebido aquí como equidad en todo el "ecosistema" - aún se incrementaría considerablemente, ya que las bitcoins estarían constantemente en demanda. Si crees que este papel oculto es el futuro de Bitcoin, adelante e invierte en él. No necesita la aceptación de Mom y Pop para obtener ganancias impresionantes.

Pero también podemos imaginar varias alternativas altcoin convirtiéndose en la infraestructura de pago preferida. El sistema de Ripple Labs, por ejemplo, está diseñado deliberadamente para facilitar las transferencias internacionales en monedas fiduciarias y otras unidades de valor, al tiempo que elimina todos los pasos intermedios que encarecen la transmisión de dinero. Ripple también está comercializando activamente a bancos y otras instituciones financieras. Les ofrece una dulce sonrisa: una red financiera digitalizada que es mucho menos perjudicial para el sistema bancario que un escenario en el que todos cierran su cuenta bancaria para una billetera bitcoin. Si alguna de estas instituciones de "puerta de enlace" sospecha -como lo hacen algunos bitcoiners- de los motivos de lucro de Ripple, podrían probar Stellar, el clon que el ex cofundador de Ripple, Jed McCaleb, estableció con una agenda deliberadamente caritativa. Alternativamente, proyectos como Realcoin, un altcoin basado en la cadena de bloques bitcoin que está respaldado transparentemente por una reserva auditable de activos en dólares, convierten altcoins en un proxy para el dólar y un instrumento con el que las personas pueden enviar dinero entre ellos sin incurrir en los riesgos de los intercambios de Bitcoin. O está Bitreserve, el sistema interno de Halsey Minor en el que los titulares de cuentas pueden enviar dólares, yenes o euros digitales entre sí sin costo alguno. Cualquiera o todos estos podrían formar los componentes de un sistema financiero basado en criptomonedas.

Aún así, bitcoin es el claro favorito para convertirse en la plataforma de criptomonedas del sistema transaccional del mundo. Su capitalización de mercado empequeñece a todas las otras altcoins combinadas. Wences Casares, CEO de la firma de billetería y custodia de bitcoin Xapo, ve el futuro de Bitcoin como la "moneda nativa de Internet", donde se convertiría en la unidad de intercambio

preferida para el comercio en línea. Pero no ve ninguna razón por la cual los gobiernos abandonarían unilateralmente el poder de emitir monedas soberanas, que permanecerían como pilares clave en el sistema financiero y coexistirían con el bitcoin. Es otra razón para creer que las preocupaciones sobre una crisis de deflación inducida por Bitcoin son exageradas.

El mundo de Multicoin

No hay garantía de que bitcoin siga siendo la criptomoneda dominante. Si las criptomonedas sobreviven, más de una, o muchas, podrían terminar desempeñando un papel importante en el comercio. Dado que la cadena de bloques le permitirá a cualquier persona asociar un valor digital a cualquier cosa, es posible que pueda terminar con un mundo en el que todo es su propia moneda. En esa economía, las reclamaciones digitalizadas de los activos se crearían a través de la tecnología detrás de la cadena de bloques. Funciona con la idea de "propiedad inteligente" que discutimos en el capítulo 9, donde a todo tipo de propiedad se le asigna un token de propiedad digital, un título comerciable. Cada uno se puede dividir en las denominaciones de moneda que sean necesarias para permitir el intercambio fácil con otras reclamaciones de activos digitalizados. Estas monedas digitales, o tokens, se intercambiarían entre sí a través de intercambios interconectados basados en cadenas de bloques que establecerían justa y transparentemente los precios universalmente reconocidos. Este dinámico y dinámico intercambio digital de múltiples activos eliminaría por completo la necesidad de una moneda común. Se convierte, en efecto, en una forma de trueque, pero una forma cuya divisibilidad y flexibilidad supera las limitaciones originales de esa antigua forma de intercambio, porque ahora, literalmente, se puede vender medio caballo a cambio de un vuelo a Acapulco.

En este mundo, donde casi todo tiene una moneda, la moneda como la conocemos se vuelve mucho menos importante. Muchas formas de bienes y servicios se pueden comercializar sin necesidad de un medio de intercambio como un dólar o un bitcoin. Por extensión, terminamos con menos necesidad de bancos centrales y ciertamente no hay necesidad de tasas de interés centralizadas, ya que el precio de todo flotaría contra el de todo lo demás, lo que -si el mercado puede funcionar- significaría que todas las cosas finalmente encontrarían un equilibrio .

El gerente de inversiones e innovador financiero de alta tecnología con sede en Zurich, Richard Olsen, ha hablado de la perspectiva de esta "sociedad de trueque digital" con banqueros, gestores de fondos de cobertura y cualquier otra persona que los escuche. Él dice que, por extraño que parezca, resuena con mucha gente en Wall Street. ¿Por qué? "Porque es la única forma de salir del lío en el que nos hemos metido", dice. Olsen argumenta que debido a que no se ha permitido que los precios, especialmente los salarios, encuentren su nivel natural, han surgido distorsiones económicas que han provocado crisis como las de 2008 y la crisis del euro posterior. A su vez, esto llevó a los bancos centrales a inmiscuirse en las tasas de interés para tratar de encontrar un equilibrio económico deseado, y finalmente introdujo nuevas distorsiones que conducen a nuevas crisis. Los economistas de libre mercado a menudo han soñado con un mundo en el que todos estos precios se despeguen y las finanzas se vuelvan mucho menos propensas a las crisis. Un mundo de trueque digital basado en criptomonedas es la forma de llegar allí, dice Olsen.

Muchos factores podrían evitar que esto suceda. Una es la complejidad logística de un sistema de intercambio global para entregar valoraciones basadas en el mercado para un número infinito de activos digitalizados. Cómo llegamos de aquí para allá es casi incomprensible. Luego están las barreras políticas. Un mundo de precios totalmente flotantes podría poner fin a los salarios rígidos, que raramente se dejan caer en la mayoría de las economías. Si bien tal flexibilidad salarial debería ayudar a resolver el desempleo, es difícil ver cómo los trabajadores, los verdaderos perdedores en la última ronda de crisis, renunciarán a tales protecciones. Aun así, si los activos

digitalizados y los intercambios de blockchain se convierten en la norma, puede que empiece a surgir alguna forma de esta economía digital de trueque.

El dólar digital

Si un mundo de criptomonedas múltiples es el sueño de un profesional de la comercialización, a primera vista el escenario que presentamos a continuación parecería ser su antítesis. Dice así: decidiendo vivir según la máxima de "si no puedes vencerlos, únete a ellos", los gobiernos de todo el mundo comienzan a lanzar sus propias criptomonedas. La tecnología está ahí. Se ha demostrado que tiene muchas ventajas. ¿Por qué los gobiernos no lo adoptarían?

La gente podría comerciar estas monedas digitales estatales de igual a igual sin intermediarios. Sin embargo, existirían dentro de una estructura general centralizada -de hecho, el último sistema centralizado, con el estado operando como la contraparte central titular. La gente simplemente recibiría una versión digital de las mismas monedas en las que actualmente se les paga, aceptable allí donde se acepten esas monedas en papel. Eso daría a las criptomonedas fiduciarias una ventaja natural sobre sus advenedizos competidores independientes, una vez más, con la importante advertencia de que alguna crisis no lleva a millones al mismo campo que el lobby antifiduciano.

Las cosas realmente se ponen interesantes cuando el gobierno de los Estados Unidos emite un dólar digital. El dólar ya es la principal moneda de reserva y comercial del mundo, pero esto le daría una ventaja aún mayor. Esto se debe a que las personas en países cuyas monedas no son de confianza o que tienen prohibido o restringido la compra de monedas extranjeras -piensen que China, Argentina, Rusia- ahora podrían obtener fácilmente la única moneda que ha simbolizado por mucho tiempo la estabilidad internacional. Mientras que el movimiento internacional de dólares en papel puede controlarse (algo) con controles físicos en los cruces fronterizos y la regulación de las transferencias bancarias, los dólares digitales serían mucho más simples. Ellos invadirían las zonas monetarias de otras jurisdicciones. Si los ciudadanos de otros países pueden adquirir fácilmente dólares, la moneda más codiciada del mundo, y utilizarlos para comprar casi cualquier cosa, ¿por qué necesitarían renminbi o pesos o rublos? En este escenario, otras monedas se vuelven menos buscadas, el dólar más poderoso. Es la máxima expresión de la hegemonía de EE. UU. Y, para otros gobiernos, socava su soberanía de estado nación.

Si y cuando el dólar se vuelva digital, "las fronteras nacionales ya no tendrán mucho significado", dice el profesor de Cornell y ex economista del FMI, Eswar Prasad, que ha escrito extensamente sobre el sistema financiero global basado en el dólar. "Los muros que los países intentan establecer en torno a las entradas y salidas de capital, desaparecerán muy, muy rápido".

Un sistema monetario basado enteramente en moneda fiduciaria digital otorgaría poder a los gobiernos de varias otras maneras. Los bancos centrales podrían, por ejemplo, establecer tasas de interés negativas sobre los depósitos bancarios, ya que los ahorradores ya no podrían huir hacia el efectivo para evitar la penalización. Eso crearía un poderoso incentivo para que las personas gasten su dinero en lugar de ahorrarlo, una forma de inducir un estímulo económico. Para cualquiera que sospeche del exceso de poder del banco central, esto suena como una pesadilla. Es la antítesis de una utopía de criptomonedas.

Pero aquí está el problema: nada de esto es un juego de suma cero. En un mundo en el que cualquiera puede crear una criptomoneda, los emisores gubernamentales de monedas digitales fiduciarias enfrentarán la competencia como nunca antes. La Fed tendrá que rendir cuentas de una manera que es mucho más poderosa que cualquier regla del Congreso de que el presidente de la Fed deba ir de vez en cuando al Capitolio. El dólar digital tendrá que rendir cuentas en un

mercado global de monedas competidoras. Si el mercado percibe la administración de dólares digitales como confiscatorios o de otra manera destructivos para los medios de subsistencia de las personas, otras monedas ganarán al costo del dólar. Si, por otro lado, aumenta la confianza en la administración responsable de las políticas de la economía del dólar, el billete verde avanzará. Entonces, incluso si los gobiernos cooptan la tecnología de criptomonedas para sus propios fines, una fuerza poderosa limitará lo que pueden y no pueden hacer. Incluso en este escenario, las personas tienen poder.

Bretton Woods II

Como habrás notado, este ejercicio especulativo puede llevarte un largo camino. Cuando comienzas a contemplar ideas como un dólar digital, surgen efectos secundarios y otras implicaciones de largo alcance. Lo más profundo de esto es lo que significa para el Estado-nación, ese último árbitro de poder que define el orden económico y político global. Sin duda, si un dólar digital o cualquier otra criptomoneda llegara a tal dominio global que cruzara las fronteras y desafiara a las monedas nacionales, los estados lo verían como una amenaza. Mientras mayor sea el alcance de los controles de capital que ya existen, mayor será el peligro percibido para el gobierno, lo que significa que China, India, Corea del Sur, Taiwán, Argentina, Venezuela y varios otros países de mercados emergentes estarían entre los que reaccionarán más agresivamente . Pero todas las naciones, incluso las de Occidente con mercados de divisas internacionalizados, en cierta medida se verían perturbados por una situación monetaria tan fluida.

¿Cómo podrían reaccionar? La primera respuesta podría ser censurar Internet con firewalls que restringen el acceso a criptomonedas externas. Pero las herramientas de encriptación ya no solo facilitan a las personas eludir dichos controles, sino que las consecuencias involuntarias serían frenar la innovación, engordar el comercio e impulsar la actividad económica a más entornos de laissez-faire. No es difícil imaginar, entonces, que los gobiernos se unan. Los controles de criptomonedas y las soluciones comunes se convertirían en asuntos de importancia internacional, discutidos en acalorados debates en las reuniones anuales del Grupo de los 20 o en las reuniones semestrales del FMI. Nosotros, las naciones-estado, estamos todos juntos en esto, el estribillo iría. Necesitamos resolver juntos una solución.

¿Cuál sería esa solución? Bueno, manteniendo nuestros sombreros de imaginación, podríamos prever un conjunto de estándares internacionales para definir lo que los gobiernos pueden y no pueden hacer con dinero digital, tal vez algún tipo de junta internacional de reguladores de criptomonedas para alinear reglas y regulaciones que pertenecen a criptomonedas independientes tales como bitcoin Pero dado que las naciones-estado tienen problemas para mantener el control de las criptomonedas descentralizadas y sin líderes, es justo decir que la ley internacional sería aún más difícil de imponer. Después de todo, no existe un tribunal penal internacional plenamente respaldado; el que está en La Haya no es reconocido por Washington. El ámbito internacional existe en un estado de casi anarquía, un ajuste perfecto para las criptomonedas sin fronteras.

Algunos acuerdos internacionales sí se mantienen, como el sistema de Bretton Woods de monedas vinculadas establecido en 1944 en medio de la crisis de la Segunda Guerra Mundial (y terminó cuando el presidente Nixon sofocó el patrón oro en 1971). ¿Podría una crisis de criptomonedas incitar a los gobiernos a otro acuerdo tan radical? ¿Un Bretton Woods II? Aquellos que han soñado con que el FMI juegue un papel de intermediario en el comercio internacional, que hayan querido liberar al mundo de su dependencia no saludable del dólar y reducir la influencia excesiva de la Reserva Federal y el Tesoro de EE. UU., De repente podrían sentirse fortalecidos. Los chinos y los franceses, que han presionado para que los Derechos Especiales de Giro del FMI se eleven de su

papel actual como meras unidades de contabilidad a convertirse en una moneda de reserva internacional para almacenar depósitos del banco central, podrían tener una nueva causa. Dudamos que los funcionarios en París o Beijing estén concibiendo estas cosas en este momento, pero si la tecnología de criptomonedas cumple con su potencial, es posible que tengan que pensar en ello.

Bajo este imaginado Bretton Woods II, tal vez el FMI crearía su propia criptomoneda, con nodos para administrar el blockchain situados en números proporcionales dentro de todos los países miembros, donde ninguno podría tener poder de veto, para evitar un ataque estatal del 51 por ciento. Tal vez la criptomoneda estaría limitada a ser utilizada solo por los bancos centrales para invertir sus reservas. O tal vez una moneda digital así podría actuar como un intermediario de pagos para el comercio internacional, una especie de red Ripple autorizada por el gobierno. De esta forma, la comunidad internacional podría patrocinar una reducción enorme en el costo de las transferencias internacionales y así promover negocios, comercio, exportaciones e innovación.

Después de décadas en las que los países han luchado para llegar a acuerdos internacionales, y mucho menos hacerlos valer, tendrías razón en ver todo esto como descabellado. Pero el futuro de la criptomoneda tiene un aspecto binario: si falla, no pasa nada; si tiene éxito, es un cambio de juego. Si y cuando el juego cambia, también cambia mucho más sobre la estructura del mundo.

Esa es una gran cantidad de escenarios para lanzar allí. Quién sabe si alguno de ellos llegará incluso cerca de la realización. Sin embargo, algo de lo que estamos relativamente seguros es que los próximos años serán fundamentales. La mayoría de las personas con las que hablamos parecen pensar en criptomonedas y proyectos relacionados en términos de dos o tres años, o de cinco a diez años. Dudamos seriamente de que pueda haber un mundo de multinúcleos, un dólar digital o una criptomoneda del FMI en dos, tres o incluso cinco años. ¿Pero diez años? ¿Veinte años? Tal vez. Mucho dependerá de lo que ocurra con Bitcoin y sus imitadores en este período interino, y en particular sobre las acciones de aquellos que han invertido sus sueños en él, aquellos que lo ven como un vehículo para cambiar el mundo.

Bitcoin tiene solo seis años. Ha pasado de ser aparentemente el proyecto favorito de un codificador solitario a un fenómeno global que ha desatado la imaginación y el activismo de libertarios, anticorporativistas, criptoanarquistas, utopistas, empresarios y capitalistas de riesgo. Bitcoin ha pasado de ser esencialmente sin valor a ser muy valioso, solo para colapsar y subir de nuevo, un patrón de comercio salvaje que tiene pocos análogos en los mercados de capital. Ciertamente, se ha ido de la nada a algún lugar, y desde aquí puede ser tan desordenado y caótico como en el pasado.

Una forma de pensar en bitcoin es como un movimiento, pero un movimiento que está hecho de partes diferentes, a veces competidoras. Los criptoanarquistas y los tecnólogos libertarios construyeron el bitcoin y lo defendieron intelectualmente, y continuarán desempeñando un papel en promover su desarrollo como moneda y causa. Pero los capitalistas de riesgo y los empresarios que lo están sacando de la Web oscura y poniéndolo al frente de las masas también jugarán un papel fundamental en su desarrollo. Esta dicotomía refleja que, si bien la expansión de bitcoin se basa al menos en parte en una respuesta política a la crisis financiera, también se basa en la tecnología, que por definición la separa de la ideología. Eso lo hace muy diferente de cualquier otro movimiento político y crea contracorrientes que dan forma a su desarrollo de maneras impredecibles.

La sociedad en general también desempeñará un papel, en parte debido al impacto perturbador que la tecnología está teniendo en la vida de las personas. La criptomoneda es un nuevo elemento disruptivo potencialmente poderoso. Los dispositivos de cómputo interconectados brindan a las

personas un mayor control sobre sus vidas diarias, creando oportunidades para descubrir nuevas ideas, nuevos mercados para sus productos y mano de obra, y nuevas herramientas para organizarse políticamente. Pero la tecnología también alimenta la ansiedad. Algunos temen la vigilancia que permite; otros se sienten abrumados por el incesante aluvión de información; muchos reemplazarán sus empleos por máquinas y software nuevos. La tecnología siempre ha impulsado una reacción violenta, y las criptomonedas no serán diferentes.

Estas fuerzas en conflicto no pueden golpearse el uno al otro para siempre. Los creyentes apasionados y las masas amenazadas ya se están codeando en la plaza pública. Se van a encontrar y mezclar y mezclar y probar las ideas de los demás, y descubrir dónde va todo esto. Así es como realmente sucede el cambio, una evolución constante y lenta a través de la cual la sociedad humana se altera y se adapta. Es por eso que no vemos el extremo de la dicotomía bitcoin-dominación / falla de bitcoin jugando y en cambio esperamos que el terreno medio gane.

Los entusiastas de las criptomonedas inevitablemente tiran la palabra revolución, una de las más utilizadas en el idioma inglés. Pero las revoluciones reales, esos momentos en los que el orden existente está totalmente anulado, son raros, a pesar de su importancia en los libros de historia. Estos eventos violentos y cáusticos son el resultado ocasional de la tectónica de placas de las relaciones humanas, pero más a menudo el cambio ocurre a través de una negociación más ordenada. Este proceso evolutivo es lo que nos trajo a este momento, esta era de las criptomonedas. Es el mismo proceso que determinará cómo se desarrollará esa edad. El movimiento cultural que está detrás de bitcoin y criptomonedas se puede ver como una extensión de una larga línea multicéntrica de pensamiento evolutivo sobre cómo las personas deberían vivir mejor juntas. Eso es lo que establece las pruebas del mundo real que determinarán el futuro de las criptomonedas. Si los aspectos de la criptomoneda y el nuevo orden social que conlleva mejoran las vidas de las personas, serán adoptados. Aquellos que no lo hagan serán descartados. Compromisos serán ideados. La "realidad", como dijo Hegel, "es un proceso histórico".

Esto no es para negar hasta qué punto bitcoin ha llenado la imaginación de las personas sobre las perspectivas de un futuro mejor. La idea de que el bitcoin va a cambiar el mundo se ha convertido en un artículo de fe entre sus seguidores. Creen que esta es su oportunidad de ser parte de un cambio histórico. "Si de repente el mundo entero comienza a usar un dinero donde los gobiernos no pueden simplemente imprimir dinero extra porque les da la gana", dijo Roger Ver en una conferencia de bitcoin de Miami, "ya no podrán financiar estas gigantescas máquinas de guerra que están matando gente en todo el mundo. Así que veo el bitcoin como una palanca que puedo usar para mover el mundo en una dirección más pacífica ".

Curiosos paralelos de altruismo, avaricia y utopismo impulsan el fenómeno bitcoin. Esas diecinueve palabras que Satoshi Nakamoto usó para introducir el bitcoin en 2009 se han extendido para abarcar los sueños y esquemas de libertarios, tecnófilos, anarquistas y personas normales que buscan algo mejor. Algo sobre estas monedas digitales y sus patrocinadores es casi desesperadamente utópico, esta idea de que la gente puede hacer negocios, cualquier negocio, entre ellos, sin la necesidad de un intermediario. Esta idea es tan extravagante para la mente moderna como la idea del autogobierno debe haber sido para muchos en 1776. "Sostenemos que estas verdades son evidentes por sí mismas, que todos los hombres son creados iguales", escribió Thomas Jefferson, catorce palabras que hizo, de hecho, cambiar el mundo.

Pero las nociones jeffersonianas de democracia e igualdad de derechos no surgieron de la mente de un puñado de súbditos británicos que vivían en el Nuevo Mundo. Eran los productos de varios cientos de años de desarrollo humano, un período que abarcaba tanto el descubrimiento científico como una lucha constante por la libertad individual. Se remonta a 1215, el año en que el rey Juan firmó la Carta Magna con nobles ingleses, el primer documento que establece límites al poder de

un monarca. Más tarde recibió un impulso de la imprenta de Gutenberg, la última tecnología disruptiva, que haría redundantes a los escribanos y sus plumas, expandiría exponencialmente la difusión del conocimiento y estimularía el desarrollo de la educación moderna. Esos avances eventualmente darían lugar a la Ilustración, a las nuevas ideas de libertad y derechos individuales expuestas por Francis Bacon, John Locke y Voltaire. El largo período interino también implicó los grandes viajes de Colón, Vasco da Gama, James Cook y otros que abrieron los mares, mientras que Galileo, Leonardo da Vinci, Copérnico y Newton abrieron los cielos y nuestra comprensión de nuestro universo. Juntos, estos exploradores expandieron el mundo para los europeos. Una vez que sus descubrimientos se completaron, una vez que la verdadera naturaleza y amplitud del mundo quedaron claras, fue imposible volver a la vieja concepción de cómo eran las cosas. Nuestro punto es no comparar a Satoshi Nakamoto con esos gigantes. Es que, una vez más, nuestra visión del mundo se ha ampliado. No hay forma de volver a las viejas formas de pensar.

En estos días más que nunca, la tecnología está impulsando los procesos gemelos del descubrimiento humano y la lucha por la libertad. Fiel al espíritu de la invención de Gutenberg, la tecnología de la información ahora ocupa por completo la sala de máquinas. Para obtener información realmente es poder. El telégrafo, el teléfono y más tarde la televisión ayudaron a difundir ideas y cambiar el poder de aquellos que anteriormente monopolizaban la información. Luego vino Internet, que amplificó este efecto a nuevos extremos, dando a las personas más poder de lo que nunca tuvieron. Lo que sea que quiera llamar a esta nueva economía -la economía colaborativa, la economía colaborativa- está invirtiendo siglos de normas sociales aceptadas.

La criptomoneda, una forma pura de tecnología de la información, una forma deliberada y explícitamente disruptiva de tecnología de la información, promete llevar las cosas a un nuevo nivel. La red descentralizada de bitcoin y su libro de contabilidad público, el blockchain, son en esencia una nueva forma radical de manejar la información. En este caso, toma la información sobre las transacciones monetarias y los intercambios económicos fuera de las manos de las instituciones monopolistas y crea un mecanismo descentralizado para que la sociedad juzgue la validez de esa información. Por lo tanto, la criptomoneda puede afirmar que es la última de una larga lista de desarrollos tecnológicos que han desplazado el poder de las élites centralizadas y se lo han entregado a la gente.

Simplemente no esperes la revolución. Los libertarios todavía están allí en el movimiento bitcoin, al igual que los criptoanarquistas. Y está Dark Wallet, y la Web oscura, y todo ese mercado negro en línea para bitcoins. Esos no desaparecerán, pero si las criptomonedas van a hacer la diferencia, estos elementos radicales se convertirán en una parte menor de lo que los motiva, tal vez relegados a un rol secundario como agitadores o como idealistas cuyos estándares impiden que el medio se comprometa demasiado. La mayor parte de la composición cultural de la criptomoneda se encontrará en las partes de la economía más amplia en que se integra, tanto la economía tradicional como la economía de la nueva era. Eventualmente, creemos, esta transformación sucederá y todo cambiará. Bitcoin terminará siendo algo menos que el sueño utópico sin estado y sin terceros de sus partidarios más apasionados. Pero el estado bancario quebrado y quebrado tendrá una competencia muy necesaria y una disciplina forzada. Los costos bajarán, el comercio y la actividad económica crecerán a lo largo de líneas digitales que trascienden las líneas en un mapa, y el mundo parecerá aún más pequeño de lo que ya es.

Reconocimientos

Escribir un libro es un ejercicio de malabarismo, con múltiples bolas y objetos de formas extrañas en el aire en cualquier momento. No se trata solo de hacer malabares con la investigación, la escritura y la edición; también se trata de hacer malabarismos con la vida de las personas, equilibrar el trabajo con la familia, lidiar con las prioridades y demandas siempre cambiantes. En nuestro caso, con la fecha de presentación del manuscrito y el calendario de producción establecido en un plazo deliberadamente ajustado, ese ejercicio de malabarismo fue especialmente complicado. Nunca lo hubiéramos completado sin un pequeño ejército de ayudantes que nos incitaran y recogieran las piezas cuando cayeran. A través de su arduo trabajo y generosa provisión de información, consejo y apoyo moral, hicieron que este libro suceda. Este ejército es demasiado numeroso para nombrarlo por completo aquí. Pero esperamos que aquellos que no se mencionan entiendan la gratitud que sentimos.

Entre los que merecen nuestro agradecimiento están los muchos que actuaron como fuentes primarias para nuestro material, la mayoría de los cuales provienen de una comunidad vibrante de bitcoiners. Cuando se reduce a esto, esta comunidad es bitcoin. A pesar de todo lo que se habla de un deseo de secreto, privacidad y anonimato en los proyectos de criptomonedas, encontramos a muchas de estas personas dispuestas a compartir sus historias. La mayoría proporcionó sus nombres completos, con unos pocos que optaron por sus seudónimos en el foro en línea. A todos, expresamos nuestro agradecimiento. También agregamos que nosotros somos los únicos responsables del contenido de este libro, incluidos los errores inadvertidos que pueda contener.

Primero tenemos que elegir a nuestra agente, Gillian McKenzie, quien de inmediato comprendió el valor de este proyecto de libro cuando lo mencionamos y desde entonces se convirtió en un defensor entusiasta e incansable. Ella se aseguró de que este libro se pusiera delante del editor correcto, e incluso se le ocurrió el título.

Tim Bartlett, nuestro editor en St. Martin's Press, fue un duro capataz que nos mantuvo en el buen camino, puso nuestra prosa serpenteante en forma, y nos ayudó a encontrar el equilibrio justo de asombro y precaución que exige este tema polémico. Es difícil imaginar que alguien más pueda llevarnos a la meta. Claire Lampen era una editora asistente, tranquila pero trabajadora, que proporcionaba ideas nítidas sobre cómo mejorar el manuscrito y mantenía la máquina de producción en funcionamiento a su horario agitado. Gracias al resto del equipo de St. Martin's también por su enérgico abrazo a este libro y su disposición a ceñirse a ese apretado calendario.

Partes del manuscrito fueron revisadas por personas con mucho más conocimiento de los temas que cubrieron que nosotros, incluidos Jonathan Mohan, Emin Gün Sirer, Gil Luria y Félix Martín. Sus generosos consejos son muy apreciados.

Muchos en The Wall Street Journal proporcionaron un apoyo invaluable para este libro y para nuestra cobertura continua de criptomonedas en el periódico, en el blog MoneyBeat, y para WSJ Live. Algunos eran y siguen siendo escépticos sobre el futuro de las criptomonedas, pero mantuvieron la mente abierta y continuamente ofrecieron su aliento. Agradecemos al editor en jefe Gerry Baker y al editor de ética Neal Lipschutz por bendecir este proyecto desde el principio. Dentro de la sección Journal's Money & Investing, debemos mencionar el apoyo del editor gerente de la sección, Francesco Guerrera, y sus suplentes Emma Moody y Larry Edelman. El editor de MoneyBeat, Stephen Grocer, sufrió nuestro entusiasmo como editor principal de nuestra columna "BitBeat". Su cuestionamiento escéptico pero agudo ha mejorado nuestro trabajo. Un agradecimiento especial al suplente de Stephen, Erik Holm, al editor de mercados de WSJ Colin Barr y a los editores bancarios Rob Hunter y Aaron Lucchetti. Robin Sidel, un periodista pionero en la cobertura de bitcoin, fue generoso con los contactos, el tiempo, el apoyo y el buen humor. Y

Steven Russolillo, Maureen Farrell y Simon Constable fueron excelentes fuentes de consejos de noticias y consejos completos. Mientras tanto, varios empleados de las oficinas de Journal's San Francisco, Washington y Londres colaboraron con la cobertura de bitcoins hasta 2014. Desde WSJ Live, los productores Joanne Po y J. R. Whalen proporcionaron nuestra cobertura de bitcoins con una valiosa plataforma de video. Desde el equipo de Journal's China, el jefe de la oficina de Pekín Charles Hutzler y la investigadora Kersten Zhang ayudaron a suavizar las necesidades de visado de Michael, mientras que el periodista de Shanghai Chao Deng lo presentó a los contactos y compartió sus ideas durante su visita. En otras partes del WSJ, Vanessa O'Connell y Reed Albergotti proporcionaron consejos críticos sobre cómo coordinar a los autores de los pares, compartiendo las lecciones aprendidas al escribir su brillante libro sobre Lance Armstrong, Wheelmen. Dos colegas más para agradecer: a Gabriella Stein por, como siempre, una fuente de entusiasmo, apoyo y consejo y, finalmente, a David Benoit, cuyo comentario casual un día en la sala de prensa que el bitcoin sonaba como "algo que Michael Lewis escribiría un libro" sobre "fue el rayo que inspiró este.

Tenemos que destacar algunos nombres de una larga lista de miembros de la comunidad bitcoin que nos ayudaron. En la Fundación Bitcoin, el científico jefe Gavin Andresen nunca pareció cansarse de nuestras demandas de explicaciones sobre este o aquel aspecto del software de bitcoin, y el representante de prensa Jinyoung Englund haría todo lo posible para hacer presentaciones y proporcionar información. Estamos especialmente agradecidos con Fran Finney, quien hizo todo lo posible por obtener información para nosotros durante lo que debe haber sido un período extremadamente difícil. En San Francisco, Jered Kenna abrió 20 Misiones a Paul y fue generoso con su tiempo en medio de una mudanza; Erik Innocent, también de 20Mission, lo ayudó a navegar el sistema de transporte público de San Francisco; Dan Held, el fundador de ZeroBlock, proporcionó datos valiosos; y Scott Robinson en Plug and Play lo recibió el día de la exposición. En Barbados, Gabriel Abed pasó mucho más tiempo del que le había mostrado a Paul por la ciudad. En Shanghai, Bobby Lee abrió muchas puertas para Michael, y Zennon Kapron ayudó a poner todo en perspectiva. Y en Utah, Ravi Iyengar recibió a Michael en una reveladora gira de la operación de minería de bitcoin de CoinTerra.

Paul: Quiero agradecer a mi familia inmediata y extensa, todos los cuales han significado tanto para mí durante todos estos años: mi madre, Michele Vigna, y mi suegra, Sara Krischer, y mi tía, JoAnn Kulpeksa; mi hermana, Jeanne-Michele Vigna, y mi cuñado, Matt Anderson; así como a los primos David Kulpeksa y Christine Kulpeksa. Espacio no permite mencionar todas las Vignas de mi familia, pero gracias por su amistad y apoyo. Gracias también a Rob Copeck, un gran fotógrafo y mejor amigo que bien podría ser una familia. Ciertamente no olvidaría a mi difunto padre, Joseph Vigna, quien me enseñó temprano, importantes lecciones sobre el valor del dinero, y mucho más.

Luego está mi hijo, Robert. Tener a Robert en mi vida me inspiró a trabajar más duro de lo que nunca había trabajado antes. Especialmente quiero agradecer a mi esposa, Elizabeth, quien, literalmente, comenzó mi carrera de escritor en la escuela secundaria cuando me arrastró de la mano a una reunión de la revista literaria de la escuela. Ella vio algo en mí que yo no sabía que estaba allí, y ha sido mi mayor y mejor defensora desde entonces. Hay muchas maneras en que este libro no podría haber sucedido sin ella.

Michael: Quiero agradecer a varios amigos por su apoyo y consejo, incluidos Cameron Wilson, Phillip Chambers, Michael Ginn y Scott Robbins. A mi amada familia en Australia, madre, padre y cuatro hermanas, así como a sus parejas e hijos, agradezco su paciencia cada vez que desaparecía con mi computadora portátil durante una reunión de mitad de año en casa. Lo mismo ocurre con Isabel y mis otros parientes políticos en Long Island y Nueva York, quienes dejaron que esa computadora portátil ocupara una mesa de comedor durante un período emocionalmente difícil para la familia. Pete siempre será recordado como un suegro amoroso y siempre solidario.

También agradezco especialmente a mis hijas, Zoe y Analia, que ahora han vivido tres libros de su padre a veces ausente y, sin embargo, rara vez se quejan y siempre mantienen una actitud optimista y positiva sobre la vida. Para Alicia, mi amante esposa de dieciocho años, gracias, por todo.

Por último, de parte de los dos, un agradecimiento especial a Satoshi Nakamoto, quienquiera que seas.

Notas

Los números de página de las notas que aparecieron en la versión impresa de este título no están en su libro electrónico. Utilice la función de búsqueda en su dispositivo de lectura electrónica para buscar los pasajes relevantes documentados o discutidos.

Tenga en cuenta que algunos de los enlaces a los que se hace referencia en este trabajo ya no están activos.

Introducción: Dinero digital para una era digital

"Aquí en Afganistán la vida de una mujer está limitada por": Parisa Ahmadi, entrevistada por Paul Vigna por correo electrónico, 4 y 11 de julio de 2014.

Francesco Rulli, consciente de la dificultad que enfrentan mujeres como Ahmadi: Francesco Rulli, entrevistado por Michael J. Casey y Paul Vigna, el 19 de junio de 2014.

"Si piensas en qué se trata una economía moderna": Lawrence Summers, entrevista telefónica de Michael J. Casey, 30 de abril de 2014.

los "no bancarizados", los Parisa Ahmadis del mundo: Asli Demirguc-Kunt y Leora Klapper, "Midiendo la Inclusión Financiera", Documento de Trabajo de Investigación de Políticas del Banco Mundial 6025, abril de 2012.

"Cada vez que doy una charla, enfatizo": Gavin Andresen, entrevistado por Michael J. Casey, 11 de febrero de 2014.

"Una terrible reserva de valor": Jamie Dimon, entrevistado en CNBC, el 23 de enero de 2014.

el inversor Warren Buffett, que lo llamó simplemente un "espejismo": Warren Buffett, entrevistado en CNBC, el 14 de marzo de 2014.

1. De Babilonia a Bitcoin

En su reciente y provocador libro: Felix Martin, Money: The Unutorised Biography (Bodley Head, 2013).

él declara que "la moneda no es ella misma": Ibid., 14, 27.

Martin nos lleva a la isla Micronesia de Yap: Ibid., 3-8.

Este punto de vista del "metalismo": Distinciones entre el metalismo y el chartalismo informadas por Stephanie Bell, "The Hierarchy of Money" (Jerome Levy Economics Institute of Bard College, abril de 1998).

Aristóteles, que escribió: "Cuando los habitantes": B. J. Gordon, "Aristóteles, Schumpeter y la tradición metalista", Quarterly Journal of Economics 75 (4) (1961): 608-14.

Adam Smith en La riqueza de las naciones: Martin, Money, 8-10.

El antropólogo David Graeber plantea la hipótesis: David Graeber, "Sobre la invención del dinero: notas sobre el sexo, la aventura, la sociopatía monomaníaca y la verdadera función de la economía", http://www.nakedcapitalism.com/2011/09/david-graeber- on-the-invention-of-money-% E2% 80% 93-notes-on-sex-adventure-monomaniacal-sociopathy-and-the-true-function-of-economics.html.

El dinero, entonces, hizo que los asentamientos humanos fueran menos vulnerables: véase Martin, Money, 50-64.

empeorado por los intentos fallidos del Emperador Diocleciano de controlar los precios: Robert L. Schuettinger y Eamonn F. Butler, Cuarenta Siglos de Controles de Salarios y Precios, cap. 2, extraído por el blog del Instituto Ludwig von Mises, http://mises.org/daily/3498.

Como nos recuerda el historiador Niall Ferguson: Niall Ferguson, The Ascent of Money (Penguin, 2008), 42-49.

Staters, las monedas de aleación de oro y plata: Robert J. O'Hara, "Monedas griegas antiguas de Mileto", publicado en el blog Rjohara.net, http://rjohara.net/coins/lydia-electrum/.

Los emperadores chinos estaban llevando dinero a su siguiente fase: ver Martin, Money, 76-81.

Lo describieron como un medio para "preservar la riqueza": Richard von Glahn, Fuente de la fortuna: dinero y política monetaria en China, 1000-1700 (University of California Press, 1996), p 29.

El más impresionante de ellos fue el écu de marc: Marie-Thérèse Boyer-Xambeau, Ghislain Deleplace, y Lucien Gillard, Private Money & Public Currencies: The 16th Century Challenge (M. E. Sharpe, 1994)

Esta negociación entre el soberano: Martin, Money, 115-21.

Basado en las ideas de los pensadores liberales: Ibid., 122-36.

Encabezado por Walter Bagehot: Ibid., 196-204.

Pero al final, los Estados Unidos, como la única gran potencia: Véase Ben Steil, La batalla de Bretton Woods: John Maynard Keynes, Harry Dexter White, y La realización de un nuevo orden mundial (Princeton University Press, 2013).

2. Genesis

"He estado trabajando en un nuevo sistema electrónico de efectivo": Satoshi Nakamoto, "Bitcoin P2P e-Cash Paper", lista de correo de criptografía, 31 de octubre de 2008.

"Definimos una moneda electrónica como una cadena de firmas digitales": Ibid.

"La gente no tendrá activos en esta moneda altamente inflacionaria": Ray Dillinger, "Bitcoin P2P e-Cash Paper", lista de correo de criptografía, 6 de noviembre de 2008, http://www.metzdowd.com/pipermail/cryptography/2008- Noviembre / 014822.html.

para lograr el "viejo sueño de Cypherpunk": James A. Donald, "Secretos y teléfonos celulares", lista de correo de criptografía, 5 de noviembre de 2008, https://www.mail-archive.com/cryptography@metzdowd.com/msg09969. html.

los hackers serían en última instancia el "asesino" del sistema de Nakamoto: John Levine, "Bitcoin P2P e-Cash Paper", lista de correo de criptografía, 3 de noviembre de 2008, https://www.mail-archive.com/cryptography@metzdowd.com /msg09966.html.

Venga el Año Nuevo, él encendió: El primer bloque, el Bloque # 0, conocido como el Bloque Génesis, se extrajo el 3 de enero de 2008. https://www.biteasy.com/blockchain/blocks/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.

"Anunciando la primera versión de bitcoin": Satoshi Nakamoto, "Bitcoin V0.1 lanzado", lista de correo de criptografía, 9 de enero de 2009, http://www.metzdowd.com/pipermail/cryptography/2009- enero / 14994.html .

Jonathan Thornburg, profesor de astronomía en Indiana: Ibid.

"Todos estábamos diciendo 'Uh-huh, yeah'": John Levine, entrevistado por Paul Vigna, 8 de marzo de 2014.

"Era solo un nombre en una lista de correo": Russ Nelson, entrevistado por Paul Vigna, 7 de marzo de 2014.

la esencia de la criptografía, que toma su nombre de: Alfred Menezes, Paul van Oorschot y Scott Vanstone, Handbook of Applied Cryptography (CRC Press, 1996), http://cacr.uwaterloo.ca/hac/about/chap1.pdf .

Así, quizás, naturalmente, Finney estaba intrigado: Hal Finney, entrevistado por Paul Vigna, 18, 21 y 27 de marzo de 2014.

Los primeros intercambios de correo electrónico entre este par: los correos electrónicos Hal Finney y Satoshi Nakamoto proporcionados a los autores por Hal y Fran Finney, 21 de marzo de 2014.

"En retrospectiva, desearía haberlo mantenido por más tiempo": Hal Finney, "Bitcoin y yo (Hal Finney)," Bitcoin Forum, 19 de marzo de 2013, https://bitcointalk.org/index.php?topic=155054.0 .

El movimiento fue fundado en septiembre de 1992: detalles de las primeras reuniones de Cypherpunk y correspondencia tomada de una entrevista telefónica con Tim May por Michael J. Casey, 21 de abril de 2104; de los archivos de la correspondencia de la lista de correo de Cypherpunk administrados por cypherpunks@MHonArc.venona; y de cuentas en Andy Greenberg, This Machine Kills Secrets (Dutton, 2012), 49-137.

"Un espectro está inquietando el mundo moderno, el espectro de la criptoanarquía": Tim May, "The Crypto Anarchist Manifesto", http://www.activism.net/cypherpunk/crypto-anarchy.html.

Algunos productos fueron francamente aterradores: Jim Bell, "Assassination Politics", 3 de abril de 1997, http://www.jrbooksonline.com/PDF_Books/AP.pdf

un nuevo y encriptado mercado de asesinatos basado en sitios web: Andy Greenberg, "Conozca al 'Creador de Assassination Market' Quién está Crowdfunding Murder con Bitcoins", Forbes, 18 de noviembre de 2013, http://www.forbes.com/sites/andygreenberg / 2013/11/18 / meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins /.

Seis años después de esa primera reunión de Cypherpunks: Wei Dai, "B-Money", publicado en los archivos personales de Wei Dai y http://www.weidai.com/bmoney.txt.

Por la misma época, Adam Back, otro Cypherpunk: primero anunciado en la lista de correo de Cypherpunk por Adam Back el 28 de marzo de 1997, http://www.hashcash.org/papers/announce.txt.

Se exponen los amplios intereses de Szabo: blog no enumerado y artículos de Nick Szabo, http://unenumerated.blogspot.com/.

Pero aunque Wei dice que le dijo a Nakamoto: Per correos electrónicos entre Nakamoto y Wei Dai publicados por Gwern Branwen, un seudónimo utilizado por un investigador en criptografía y otros asuntos que publica en www.gwern.net, http: //www.gwern. net / docs / 2008-nakamoto.

David Chaum, el criptógrafo altamente innovador e influyente: Detalles de la biografía temprana de Chaum publicada por David Chaum en Chaum.com.

Chaum nos explicó la gran promesa: Detalles de la concepción, el desarrollo, la implementación y la desactivación de DigiCash parcialmente provistos en dos entrevistas telefónicas con Michael J. Casey el 18 y 23 de agosto de 2014.

Otro punto de vista, transmitido en un informe de 1999 en la revista holandesa ¡Siguiente !: Versión traducida publicada por Ian Grigg a la lista de correo dbs@philodox.com, http://cryptome.org/jya/digicrash.htm.

El hombre que condujo este proyecto fue Sholom Rosen: Detalles del proyecto de e-cash de Citibank de una entrevista con Sholom Rosen por Michael J. Casey, 23 de abril de 2014; y entrevistas de seguimiento con otras fuentes familiarizadas con el proyecto.

Esta "legislación histórica", Clinton dijo: William J. Clinton, "Declaración sobre la firma de la Ley Gramm-Leach-Bliley", 12 de noviembre de 1999, http://www.presidency.ucsb.edu/ws/?pid=56922 .

Mohamed El-Erian, entonces co-CEO del masivo administrador de activos: "Cuando Wall Street casi colapsa", Fortune, 14 de septiembre de 2009, http://archive.fortune.com/galleries/2009/fortune/0909/gallery. witnesses_meltdown.fortune /.

En una publicación del foro, Nakamoto dijo: Satoshi Nakamoto, "Re: Transacciones y guiones: DUP HASH160 ... EQUALVERIFY CHECKSIG," Bitcoin Forum, 18 de junio de 2010, https://bitcointalk.org/index.php?topic=195.msg1617 # msg1617.

En una publicación del 11 de febrero de 2009 en un foro: Satoshi Nakamoto, "Implementación de fuente abierta de Bitcoin de moneda P2P", Foro de la Fundación P2P, 11 de febrero de 2009, http://p2pfoundation.ning.com/forum/topics/bitcoin- fuente abierta.

Otra pista está incrustada en el código: Texto del mensaje visible en el monitor blockchain proporcionado por Biteasy, https://www.biteasy.com/blockchain/blocks/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.

Para octubre, una nueva sala de IRC enfocada en codificadores: tomada de la línea de tiempo de "History of Bitcoin", http://historyofbitcoin.org/.

Por lo tanto, para octubre de 2009, algunos en la comunidad: tasas de cambio históricas publicadas en el sitio web de New Liberty Standard, http://newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate.

Esto cambiaría en el Año Nuevo como Laszlo Hanyecz: Laszlo Hanyecz, entrevistado por Paul Vigna, 22 de abril de 2014.

3. Comunidad

El 12 de diciembre de 2010, la siguiente publicación: Satoshi Nakamoto, "Se agregaron algunos límites de DoS, se eliminó el modo seguro (0.3.19)," Foro de Bitcoin, 12 de diciembre de 2010, https://bitcointalk.org/index.php?topic = 2228.

Por lo que sabemos, el último fue para Gavin Andresen: Gavin Andresen, entrevistado por Michael J. Casey, 11 de febrero de 2014.

aunque los miembros de la comunidad han debatido: Nermin Hajdarbegovic, "Comité de formularios de la Fundación Bitcoin para crear el símbolo Bitcoin Unicode", CoinDesk, 19 de junio de 2014, http://www.coindesk.com/bitcoin-foundation-forms-committee-create-bitcoin-unicode-symbol /

"En los negocios, las historias de creación refuerzan el papel": Paul Vigna y Michael J. Casey, "BitBeat: El mito de la creación de Bitcoin también es diferente", Wall Street Journal, blog de MoneyBeat, 3 de marzo de 2014, http: //blogs.wsj .com / moneybeat / 2014/03/10 / bitbeat-bitcoins-creation-myth-is-different-too /.

"Misterioso en el caso del dinero": Tamara Audi, Robin Sidel y Michael J. Casey, "Bitcoin Report Sonata el mundo de la moneda", Wall Street Journal, 7 de marzo de 2014.

Esa es la estimación que el criptógrafo Sergio Lerner: Sergio Lerner, "La fortuna bien merecida de Satoshi Nakamoto, Creador de Bitcoin, Visionario y genio", Palabras sobre diseño de Bitcoin, Privacidad, Seguridad y Crypto blog, 17 de abril de 2013, http: // bitslog .wordpress.com / 2013/04/17 / the-well-merecido-fortuna-de-satoshi-nakamoto /.

El CEO de SecondMarket, Barry Silbert, describe: Comentarios realizados en la mesa redonda de medios patrocinada por Circle Internet Financial, Nueva York, 10 de diciembre de 2013.

Nick Szabo, cuyos escritos, los lingüistas forenses nos dicen: Paul Vigna, "Creador de Bitcoin 'Satoshi Nakamoto' Unmasked-Again '," Wall Street Journal, blog de MoneyBeat, 16 de abril de 2014, http://blogs.wsj.com/ moneybeat / 2014/04/16 / bitcoin-creator-satoshi-nakamoto-unmasked-again /.

Escribiendo para The New Yorker: Joshua Davis, "The Crypto-Currency: Bitcoin y su misterioso inventor", New Yorker, 10 de octubre de 2011.

El profesor de periodismo de la Universidad de Nueva York Adam Penenberg: Adam L. Penenberg, "El misterio de la criptodinámica de Bitcoin reabierto", Fast Company, 11 de octubre de 2011, http://www.fastcompany.com/1785445/bitcoin-crypto-currency-mystery reabrió

Luego vino Ted Nelson: Ted Nelson, "Creo que sé quién es Satoshi", YouTube, 17 de mayo de 2013, https://www.youtube.com/watch?v=emDJTGTrEm0.

Luego, el 6 de marzo de 2014, la revista semanal Newsweek: Leah McGrath Goodman, "The Face Behind Bitcoin", Newsweek, 6 de marzo de 2014.

"Me llamó la atención", dice Andresen: Gavin Andresen, entrevistado por Michael J. Casey, 11 de febrero de 2014.

Andresen comenzó un proyecto que llamó Bitcoin Faucet: Ibid.

El 21 de mayo de 2010, Hanyecz comió una pizza de queso. Los detalles de la oferta de pizza de Laszlo Hanyecz provienen de la entrevista telefónica de Paul Vigna con Hanyecz el 22 de abril de 2014, así como de la correspondencia de seguimiento del 1 de septiembre de 2014. También, Lazlo Hanyecz, "Pizza for Bitcoins?", Bitcoin Forum, 18 de mayo de 2010, https://bitcointalk.org/index.php?topic=137.0.

"Tenía mucho", dice, tantos: Hanyecz, entrevistado por Vigna.

"Pagaré 10.000 bitcoins por un par de pizzas": Hanyecz, "¿Pizza para Bitcoins?"

"Pizza fresca", dijo, "desde Londres": Hanyecz, entrevistada por Vigna.

En marzo de 2010, por ejemplo: Publicación de SmokeTooMuch, "Subasta de Bitcoin: oferta de arranque de 10.000 BTC 50.00 USD", Foro de Bitcoin, 30 de marzo de 2010, https://bitcointalk.org/index.php?topic=92.0.

"Entonces, finalmente conseguí que mi cliente comenzara a generar": Publicación de AgoraMutual, "¿Funciona correctamente mi segunda transacción?", Foro de Bitcoin, 1 de enero de 2010, https://bitcointalk.org/index.php?topic=17.0 ; wap2.

"En aquel entonces, había mucha gente ayudando": Hanyecz, entrevistada por Vigna.

"Sonaba como una aspiradora cuando estaban ocupados": Laszlo Hanyecz, entrevistado por Paul Vigna, 1 de septiembre de 2014.

"En una semana, la dificultad se disparó tanto": Hanyecz, entrevistada por Vigna, 22 de abril de 2014.

Más de cinco días, la tasa de cambio de bitcoin: a través de la bitcoin wiki "Historia", https://en.bitcoin.it/wiki/History.

"Hola a todos", escribió: Jed McCaleb, publicando como mtgox, "New Bitcoin Exchange (mtgox.com)," Bitcoin Forum, 18 de julio de 2010, https://bitcointalk.org/index.php?topic=444. msg3866 # msg3866.

En 2007, McCaleb había comenzado una plataforma en línea: Jed McCaleb, entrevistado sobre la historia de Mt Gox y los primeros días vía correo electrónico por Gwern Branwen, 16, 17 y 24 de febrero de 2014, http://www.gwern.net/docs / 2014-mccaleb.

En marzo de 2011, contó al foro: Jed McCaleb, publicando como mtgox, "Mt Gox está cambiando propietarios", Bitcoin Forum, 6 de marzo de 2011, https://bitcointalk.org/index.php?topic=4187.msg60610# msg60610.

Amante del manga y el cosplay japonés: Sophie Knight, "En Mt Gox Bitcoin Hub, el CEO de Geek Sought Both Control and Escape", Reuters, 21 de abril de 2014, http://in.reuters.com/article/2014/ 04/21 / uk-bitcoin-mtgox-karpeles-idINKBN0D700J20140421.

Mientras que el Foro de Bitcoin había agregado nuevos miembros: Tomado de la página de estadísticas en Bitcoin Forum, https://bitcointalk.org/index.php?action=stats.

Mt Gox aumentó de seis mil a sesenta mil: Mark Karpelès, publicando como MagicalTux, "Mt Gox: si sus monedas fueron robadas, por favor escriba aquí," Bitcoin Forum, 18 de junio de 2011, https://bitcointalk.org/index. php? topic = 18858.0; todos.

informes ponen la cantidad en cualquier lugar de dos mil a medio millón de monedas: para los dos mil de gama baja: Marc Bevand, "ataque mayor en el intercambio de bitcoin más grande del mundo", Zorinaq, 19 de junio de 2011, http: // blog. zorinaq.com/?e=55; para el medio millón de high-end: Jason Mick, "Inside the Mega-Hack of Bitcoin: The Full Story", DailyTech, 19 de junio de 2011, http://www.dailytech.com/Inside+the+MegaHack+of + Bitcoin + the + Full + Story / article21942.htm.

Los precios de Bitcoin se desplomaron para enfrentarlo: Jack Hough, "Bitcoin's Flash Crash", MarketWatch, 22 de junio de 2011, http://blogs.marketwatch.com/paydirt/2011/06/22/bitcoin%E2%80%99s-flash -choque/; también, Tyler Cowan, "The Bitcoin Crash", Marginal Revolution, http://marginalrevolution.com/marginalrevolution/2011/06/the-bitcoin-crash.html. Los intercambios fraudulentos se desenrollarán más tarde y no aparecerán en los gráficos de precios históricos, aunque un gráfico en Bitcoin Charts, http://bitcoincharts.com/charts/mtgoxUSD#tgCzm1g10zm2g25zv, muestra un "doble float" de 1.7e + 308 en las columnas de precios, durante seis días después del decimonoveno, el momento en que los intercambios se desenrollaron.

En julio de 2011, Mt Gox manejaba el 80 por ciento: esta cifra fue reportada por el propio intercambio y ampliamente citada; ver a Paul Vigna y Michael J. Casey, "BitBeat: Mt Gox detiene los retiros, el precio de Bitcoin cae", Wall Street Journal, blog de MoneyBeat, 7 de febrero de 2014, http://blogs.wsj.com/moneybeat/2014/02/ 07 / bitbeat-mt-gox-stops-retiros-bitcoin-precio-gotas /.

Las manifestaciones más extremas de esa idea: Publicar en silkroad, "Silk Road: Marketplace anónimo". Comentarios solicitados, "Bitcoin Forum, 1 de marzo de 2011, https://bitcointalk.org/index.php?topic=3984.msg57086#msg57086.

Con el foro de Bitcointalk ahora: tomado de la página de estadísticas en Bitcoin Forum, https://bitcointalk.org/index.php?action=stats.

El sitio web Gawker, en junio de 2011: Adrien Chen, "El sitio web subterráneo donde se puede comprar cualquier droga imaginable", Gawker, 1 de junio de 2011, http://gawker.com/the-underground-website-where-you- can-buy-any-drug-imag-30818160.

"El sitio se hizo popular": publicación de silkroad, "Silk Road: Marketplace anónimo". Comentarios solicitados, "Bitcoin Forum, 9 de junio de 2011, https://bitcointalk.org/index.php?topic=3984.msg189007#msg189007.

El senador Chuck Schumer del estado de Nueva York: "Schumer impulsa a cerrar el mercado de medicamentos en línea", NBC Nueva York, 5 de junio de 2011, http://www.nbcnewyork.com/news/local/Schumer-Calls-on-Feds-to -Shut-Down-Online-Drug-Marketplace-123187958.html.

La respuesta en el Foro de Bitcoin fue mixta: publicación de FatherMcGruder y otros, "Silk Road: Marketplace anónimo". Comentarios solicitados, "Bitcoin Forum, https://bitcointalk.org/index.php?topic=3984.260.

En agosto de 2012, Andy Greenberg de Forbes: Andy Greenberg, "El camino de la seda del mercado negro ', el camino de la seda': $ 22 millones en ventas anuales", Forbes, 6 de agosto de 2012.

El FBI calculó que entre el 6 de febrero de 2011 y la querella del FBI contra Ross Ulbricht, el 27 de septiembre de 2013, http://www.scribd.com/doc/172773561/Criminal-Complaint-Against-Silk-Road-and-Dread -Pirate-Roberts.

Comenzaron a aparecer plataformas de negociación para bitcoin: varios desarrollos en 2011-12 tomados de la línea de tiempo en http://historyofbitcoin.org/.

Charlie Shrem, una mujer de veintiún años con sede en Brooklyn: Adrianne Jeffries, "¿Aburrido con Bitcoin? BitInstant está a punto de perder el mercado haciendo que el comercio sea más rápido ", BetaBeat, 23 de agosto de 2011, http://betabeat.com/2011/08/bored-with-bitcoin-bitinstant-is-about-to-goose-the- market-by-making-trading-faster.

A mediados de 2012, SatoshiDice: Megan Geuss, "La firma dice cuentas de juego en línea para casi la mitad de todas las transacciones de Bitcoin", ArsTechnica, 24 de agosto de 2013, http://arstechnica.com/business/2013/08/firm-says- cuentas de juego en línea para casi la mitad de todas las transacciones de bitcoin.

Uno de los primeros fue Peter Vessenes: Publicación de blog, "Incubadora de inicio de Bitcoin, CoinLab, inicia en WA", red de noticias de Bitcoin, 25 de septiembre de 2011, http://www.btcnn.com/2011/09/bitcoin-startup- incubator-coinlab.html.

Revista Bitcoin, fundada por Mihai Alisie: Según la página de Bitcoin Magazine "About Us", http://bitcoinmagazine.com/about-us/.

En septiembre de 2012, se fundó la Fundación Bitcoin: Jon Matonis, "La Fundación Bitcoin se Lanza para Impulsar el Avance de Bitcoin", 9 de septiembre de 2012, http://www.forbes.com/sites/jonmatonis/2012/09/27/bitcoin- foundation-launches-to-drive-bitcoins-advancement /.

En ese momento, el Foro de Bitcoin tenía alrededor de sesenta y ocho mil miembros: Tomado de la página de estadísticas en Bitcoin Forum, https://bitcointalk.org/index.php?action=stats.

A partir de marzo de 2012, los robos totalizan: "Bitcoinica, dos veces pirateado en 2012, está siendo demandado", Infosecurity Magazine, 15 de agosto de 2012, http://www.infosecurity-magazine.com/news/bitcoinica-twice-hacked-in -2012-is-being-demandado /.

Intercambio de Kenne en Tradehill: Timothy B. Lee, "El mayor intercambio de Bitcoin se cierra, culpando a la regulación y la pérdida de fondos", ArsTechnica, 15 de febrero de 2012, http://arstechnica.com/tech-policy/2012/02/major-bitcoin -exchange-shuts-down-blaming-regulation-and-loss-of-funds /.

Sin embargo, todo el tiempo, el precio de bitcoin subió, subió y subió: Los precios se tomaron del gráfico del índice de precios de Bitcoin de CoinDesk, http://www.coindesk.com/price/.

Litecoin, la mayor y más antigua de las altcoins: datos de capitalización de mercado tomados del sitio web de CoinMarketCap, http://coinmarketcap.com/.

altcoin que comenzó como una broma de Billy Markus y Jackson Palmer: Patrick McGuire, "Such Weird: The Founders of Dogecoin Ver el punto de inflexión de Meme Currency", Motherboard, 23 de diciembre de 2013, http://motherboard.vice.com/ blog / dogecoins-fundadores-creen-en-el-poder-de-meme-monedas.

A través de las campañas lanzadas en Reddit: para obtener una descripción general de los esfuerzos de recaudación de fondos de dogecoin, The Dogesonian tiene una descripción general en http://thedogesonian.weebly.com/the-early-dogecoin-projects.html. También vea Roop Gill, "Manchester Co-op obtiene una mano de Dogecoin para aplastar los objetivos de recaudación de fondos", CoinDesk, 22 de abril de 2014, http://www.coindesk.com/manchester-co-op-gets-hand-dogecoin- smash-fundraising-target /.

Nuestro esfuerzo favorito de dogecoin: Paul Vigna, "BitBeat: Dogecoin hace su debut en NASCAR; Ripple Signs a Bank, "Wall Street Journal, blog de MoneyBeat, 5 de mayo de 2014, http://blogs.wsj.com/moneybeat/2014/05/05/bitbeat-dogecoin-makes-its-nascar-debut-ripple- signos-a-banco /.

Cuando GoCoin decidió que sería: Michael J. Casey, "BitBeat: Much Good, Dogecoin; So Hip, "Wall Street Journal, blog de MoneyBeat, 13 de marzo de 2014, http://blogs.wsj.com/moneybeat/2014/03/13/bitbeat-much-good-dogecoin-so-hip/.

aunque con la capitalización de mercado de bitcoins más de diez veces: según las capitalizaciones de mercado de las 100 criptomonedas más cotizadas en coinmarketcap.com.

Andreas Antonopoulos, jefe de seguridad del proveedor de billeteras Blockchain.info: Paul Vigna, "BitBeat: Dorian Nakamoto escribe una carta", Wall Street Journal, blog de MoneyBeat, 17 de marzo de 2014, http://blogs.wsj.com/moneybeat/ 2014/03/17 / bitbeat-dorian-nakamoto-escribe-una-carta /.

El escritor de Forbes, Andy Greenberg, comenzó un esfuerzo: Andy Greenberg, "El vecino de Nakamoto: Mi búsqueda del creador de Bitcoin llevó a un genio paralizado de Crypto", Forbes, 25 de marzo de 2013, http://www.forbes.com/sites/andygreenberg/2014 / 03/25 / satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt /.

"Oh, bitcoin, sé que vas a reinar, voy a reinar": John Barrett, "Oda a Satoshi (La canción oficial de Bitcoin)", YouTube, 13 de febrero de 2014, https://www.youtube.com/watch ? v = zEQ2nPSL5-0.

"10,000 Bitcoins": Laura Saggers, "10,000 Bitcoins", YouTube, 5 de marzo de 2014, https://www.youtube.com/watch?v=RIsZyg8OXlI.

"Bitcoin Barons": YTCracker, "Bitcoin Barons", YouTube, 4 de agosto de 2013, https://www.youtube.com/watch?v=RIsZyg8OXlI.

Mientras tanto, el artista alemán Kuno Goda: "BitBeat: el Banco Central de China significa negocios", Wall Street Journal, blog de MoneyBeat, 1 de abril de 2014, http://blogs.wsj.com/moneybeat/2014/04/01/bitbeat- chinas-central-bank-means-business /.

La fotógrafa de Los Ángeles Megan Miller: Paul Vigna, "BitBeat: Haciendo matemáticas en la minería", Wall Street Journal, blog de MoneyBeat, 16 de abril de 2014, http://blogs.wsj.com/moneybeat/2014/04/16/bitbeat-doing -math-on-mining /.

Los Craig eran improbables proselitistas: Austin y Beccy Craig, entrevistados por Paul Vigna el 20 de octubre de 2013 y el 28 de abril de 2014.

4. Montaña rusa

Estás en un Starbucks en Nueva York: precios de grandes lattes en Starbucks en Nueva York y Oslo tomados de "More or Less Brew for Your Buck", Wall Street Journal, 8 de marzo de 2013.

la enorme cantidad de $ 11 billones en pagos que Visa y MasterCard: Informes anuales, 2013, MasterCard Inc. y Visa Inc.

aproximadamente el 87 por ciento del mercado global: "Acciones de mercado de las transacciones de compra en todo el mundo en 2013", Informe Nilson, marzo de 2014.

Beneficiándose de una explosión global en el comercio electrónico: Will Craig, "Las oportunidades se expanden a medida que la Web extiende su alcance alrededor del mundo", Informe del 2º trimestre, 2014, Capital Group, http://capitalgrouppcs.com/opportunities-abound-as- the-web-extends-its-reach-around-the-world.html.

Al permitir que se desarrolle el sistema existente, permitimos: Gil Luria, entrevista telefónica de Michael J. Casey, 15 de abril de 2014.

los diez principales emisores de tarjetas de crédito en el mundo: "Los 10 mayores emisores de tarjetas de crédito del mundo", CNBC.com, 13 de abril de 2013, http://www.cnbc.com/id/36471668.

este proceso de compensación está coordinado por el servicio Fedwire de la Fed: estadísticas actualizadas disponibles de los Servicios del Banco de la Reserva Federal, http://www.frbservices.org/operations/fedwire/fedwire_funds_services_statistics.html.

Asegurar y distribuir todo este efectivo: Ajay Banga, "Reflexiones sobre FI2020-Parte 1", blog del Centro de Inclusión Financiera, 30 de octubre de 2013, http://cfi-blog.org/2013/10/30/ajay-banga- Reflections-on-fi2020-part-1 /.

una lista de comerciantes que aceptan bitcoin que, según el recuento de CoinDesk: "Informe del estado de Bitcoin Q2 2014 revela la expansión de la economía de Bitcoin", 10 de julio de 2014, http://www.coindesk.com/state-of-bitcoin-q2-2014- report-expanding-bitcoin-economy /.

El cofundador de Blockchain Peter Smith dice: Peter Smith, entrevistado por Michael J. Casey, 11 de agosto de 2014.

procesado diariamente por Visa y MasterCard en 2013: informes anuales, 2013, MasterCard Inc. y Visa Inc.

un hacker secuestró las computadoras de un proveedor de servicios de Internet: Swati Khandelwal, "Hacker piratea las redes de ISP para robar $ 83,000 de las piscinas mineras de Bitcoin", http://thehackernews.com/2014/08/hacker-hijacks-isp-networks-to-steal_7. html.

una botnet con sede en Grecia utilizó Facebook para infectar 250,000 computadoras: Mohit Kumar, "Facebook derriba la botnet que roba Bitcoin que infectó 250,000 computadoras", Hacker News, 9 de julio de 2014.

el ataque de $ 148 millones a Target en diciembre de 2013: Tom Gara, "Un ataque de hack costoso: incumplimiento de destino de $ 148 millones", 5 de agosto de 2014, http://blogs.wsj.com/corporate-intelligence/2014/08/05/ an-expensive-hack-attack-targets-148-million-breach /.

Comparemos el precio promedio de los EE. UU. De un galón de gasolina: Precios semanales promedio de la gasolina en los EE. UU. De la Administración de Información de Energía, http://www.eia.gov/dnav/pet/pet_pri_gnd_dcus_nus_w.htm; y precios de bitcoin del índice de precios CoinDesk Bitcoin, http://www.coindesk.com/price.

El profesor de la Universidad de Nueva York, David Yermack, concluyó que el bitcoin: David Yermack, "¿Bitcoin es una moneda real?", Documento de trabajo NBER 19747, diciembre de 2013.

No necesita buscar más: CoinDesk Bitcoin Price Index.

Esto incluyó un desastroso "flash crash": Paul Vigna, "BitBeat: un Flash Crash de Bitcoin" mientras Volume Spike toma el precio de $ 309, "Wall Street Journal, blog de MoneyBeat, 18 de agosto de 2014, http: //blogs.wsj .com / moneybeat / 2014/08/18 / bitbeat-a-bitcoin-flash-crash-como-volumen-pico-brevemente-toma-precio-a-309 /.

En una mordaz presentación en Nueva York: Mark T. Williams, "Testimonio de Mark T. Williams", Departamento de Servicios Financieros del Estado de Nueva York, 28-29 de enero de 2014, http://www.dfs.ny.gov/ about / hearing / vc_01282014 / williams.pdf.

"No diría que el acaparamiento es algo malo": Bobby Lee, entrevistado por Michael J. Casey en Shanghai, el 19 de julio de 2014.

Gil Luria, el analista de Wedbush: Gil Luria, "Abrazar la volatilidad: negociar como la primera aplicación de asesinos de Bitcoin", informe de investigación de Wedbush Securities, 20 de agosto de 2014.

"Si pueden hacer eso allí, pueden hacerlo en cualquier lugar": Mark McGowan, "El robo del gran banco de Chipre por terroristas financieros", 17 de marzo de 2013, https://www.youtube.com/watch?v=YDXtHsz2q6Q.

El precio pasó de $ 33 a fines de febrero a $ 230 el 9 de abril: CoinDesk Bitcoin Price Index.

El precio de bitcoin se desplomó a $ 68 el 16 de abril: Ibid.

A fines de junio de 2013, surgieron informes de que el FBI: John Biggs, "La DEA incautó Bitcoins en una redada antidrogas en Silk Road", TechCrunch, 27 de junio de 2013, http://techcrunch.com/2013/06/27/the- dea-seized-bitcoins-en-a-silk-road-drug-raid /.

Un mes después, la Comisión de Bolsa y Valores presentó cargos: Jessica B. Magee, abogada principal, Queja ante la SEC, 23 de julio de 2013, http://www.sec.gov/litigation/complaints/2013/comp-pr2013-132. pdf.

habían adquirido un stock masivo de bitcoins que valía entonces $ 11 millones: Nathaniel Popper y Peter Lattman, "Never Mind Facebook; Los gemelos Winklevoss gobiernan en dinero digital, "11 de abril de 2013, New York Times, blog de Dealbook, http://dealbook.nytimes.com/2013/04/11/as-big-investors-emerge-bitcoin-gets-ready- for-its-close-up /? _ php = true & _type = blogs & _r = 0; vea también a David Benoit y Andrew R. Johnson, "Los gemelos Winklevoss lanzan la oferta pública inicial para el inventario de seguimiento de bitcoin", Wall Street Journal, blog All Things Digital, 1 de julio de 2013, http://allthingsd.com/20130701/winklevoss-twins- launch-ipo-for-bitcoin-tracking-stock /.

Ni siquiera las dramáticas noticias del 2 de octubre: Danny Yadron, "El FBI Arresta, Se apodera del Mercado en Línea 'Ruta de la Seda'", Wall Street Journal, Blog de la Ley, 2 de octubre de 2013, http://blogs.wsj.com/law/2013 / 10/02 / fbi-makes-arrest-seizes-online-market-silk-road /.

"Reconoce la innovación que aportan las monedas virtuales": Jennifer Shasky Calvery, declaración ante el Subcomité de Política Económica del Senado de los Estados Unidos, 19 de noviembre de 2013, http://www.fincen.gov/news_room/testimony/html/20131119.html.

En enero de 2013, se cree que una de las primeras entregas fue una empresa china llamada Avalon: el desarrollador clave de Bitcoin, Jeff Garzik. Vitalik Buterin, "Avalon confirmado de Working Avalon, Hashing a 68 GH / s," Revista Bitcoin, 31 de enero de 2013, http://bitcoinmagazine.com/3231/working-avalon-asic-confirmed/.

En un momento decisivo, Bloomberg Businessweek presentó: Max Raskin, "Conozca a los millonarios de Bloomberg", Bloomberg Businessweek, 10 de abril de 2013, http://www.businessweek.com/articles/2013-04-10/meet-the-bitcoin -millonarios.

En diciembre, el bitcoin superaba los $ 1.100: por precio, CoinDesk Bitcoin Price Index; para la capitalización de mercado, CoinMarketCap.com, http://www.coinmarketcap.com.

Intercambio de BTC China, que en un momento incluso superó a Mt Gox en volumen: Emily Spaven, "BTC-China supera a MT Gox y Bitstamp se convertirá en el N º 1 del mundo en intercambio de bitcoins", CoinDesk, 4 de noviembre de 2013, http: // www .coindesk.com / btc-china-beats-mt-gox-bitstamp-become-worlds-1-bitcoin-exchange /.

el Banco Popular de China no estaba contento: Robin Sidel, Chao Deng y William Horobin, "Los bancos centrales advierten sobre los riesgos de Bitcoin", Wall Street Journal, 5 de diciembre de 2013, http://online.wsj.com/news/articles / SB10001424052702303497804579239451297424842.

En enero de 2014, el precio bajó a $ 770: el índice de precios de CoinDesk Bitcoin.

El día después de la conferencia, Charlie Shrem, uno de los "millonarios del bitcoin" de Businessweek: Christopher M. Matthews y Robin Sidel, "Dos acusados en un supuesto plan de lavado de bitcoin", Wall Street Journal, 27 de enero de 2014.

anunció que también dejaría de permitir clientes: Michael Carney, "Mt Gox suspende los retiros de Bitcoin (¿Temporalmente?), Market Falls en medio de preocupaciones de imprudencia", Pando Daily, 7 de febrero de 2014, http://pando.com/2014/ 02/07 / mt-gox-suspends-bitcoin-retiros-temporalmente-mercado-cae-en-preocupaciones-de-impropriety /.

el 28 de febrero anunció que se declararía en quiebra: Robin Sidel, Eleanor Warnock y Takashi Mochizuki, "Casi medio millón de dólares de Bitcoins desaparecen", Wall Street Journal, 28 de febrero de 2014.

China consolidó esa preocupación con un dictamen más formal en abril que prohíbe a los bancos: Michael J. Casey, "BitBeat: China Dings Bitcoin Again", Wall Street Journal, blog de MoneyBeat, 25 de abril de 2014, http://blogs.wsj.com/ moneybeat / 2014/04/25 / bitbeat-china-dings-bitcoin-again /.

El Servicio de Rentas Internas emitió un fallo muy esperado: John D. McKinnon y Ryan Tracy, "IRS dice que Bitcoin es propiedad, no moneda", Wall Street Journal, 25 de marzo de 2014.

Aunque el superintendente de Servicios Financieros Benjamin Lawsky: Paul Vigna, "NY Financial Regulator Lanza un Borrador de 'BitLicense' para Negocios Bitcoin," Wall Street Journal, blog MoneyBeat, 17 de julio de 2014, http://blogs.wsj.com/moneybeat/2014 / 07/17 / ny-financial-regulator-releases-draft-of-bitlicense-for-bitcoin-businesses /.

Lawsky indicó que estaba dispuesto a cambiar: Paul Vigna, "BitBeat: BitLicense obtiene extensión; Lawsky: 'No tenemos el monopolio de la verdad' ", Wall Street Journal, blog de MoneyBeat, 21 de agosto de 2014, http://blogs.wsj.com/moneybeat/2014/08/21/bitbeat-bitlicense- gets-extension-lawsky-we-dont-have-a-monopoly-on-the-truth /.

Bolsas chinas, instalaciones de negociación de márgenes presentadas: Michael J. Casey, "BitBeat: Mucho para ese aburrido mercado de Bitcoin", Wall Street Journal, blog de MoneyBeat, 13 de agosto de 2014, http://blogs.wsj.com/moneybeat/ 2014/08/13 / bitbeat-tan-mucho-para-eso-aburrido-bitcoin-market /.

5. Construyendo el Blockchain

tomaremos prestada una idea desarrollada por el ingeniero de software: Yevgeniy Brikman, "Bitcoin by Analogy", en el blog de Brikman Do not Panic, 24 de abril de 2014, http://brikis98.blogspot.com/2014/04/bitcoin-by -analogy.html.

El blockchain está gestionado: gran parte de lo explicado está tomado del wiki de Bitcoin en bitcoin.org y de las conversaciones con múltiples desarrolladores.

nonce se deriva de un pasaje de Lewis Carroll: ver a Angela Tung, "10 palabras caprichosas acuñadas por Lewis Carroll", Semana, 25 de enero de 2013, http://theweek.com/article/index/239253/10-whimsical-words -coined-by-lewis-carroll.

En el momento exacto en que estas palabras fueron escritas: Por la página de inicio en el momento de Blockchain.info, http://blockchain.info.

incluyendo uno de BlockCypher de nueva creación: Michael J. Casey, "BitBeat: ¿una solución a esa espera de 10 minutos?" The Wall Street Journal, blog de MoneyBeat, 5 de septiembre de 2014, http://blogs.wsj.com / moneybeat / 2014/09/05 / bitbeat-a-solution-to-that-10-minute-transaction-wait /.

6. La carrera de las armas

Uno de esos recién llegados fue Jason Whelan: Detalles de la experiencia de Whelan tomados de la correspondencia por correo electrónico, el 29 de mayo de 2014 y el 2 de junio de 2014.

En un centro de datos en las afueras: material sobre las operaciones de CoinTerra en Utah tomado de una visita a las instalaciones por Michael J. Casey, 7 de junio de 2014.

En ese momento, la red, que entonces estaba produciendo: datos de Hashrate de Blockchain.info, https://blockchain.info/charts/hash-rate; la comparación informática-potencia usa la estimación total de petaflop en http://www.bitcoinwatch.com/ y se compara con la potencia total de quinientas supercomputadoras principales detalladas en http://www.top500.org.

En abril de 2013, varios informes de prensa: por ejemplo, vea a Mark Gimein, "La minería virtual de Bitcoin es un desastre ambiental real", Bloomberg, 12 de abril de 2013, http://www.bloomberg.com/news/2013- 04-12 / virtual-bitcoin-mining-is-a-real-world-environmental-disaster.html.

Meses más tarde, Guy Lane: la metodología BitCarbon de Lane se explica en http://www.bitcarbon.org/bitcarbon/.

Si cada minero usara estas plataformas: Discusión de estimaciones obsoletas de consumo de energía en http://rationalwiki.org/wiki/Talk:Bitcoin/Archive1#Outdated_energy_consumption_estimate.

los consultores del centro de datos aconsejaban a los mineros de bitcoin: Michael J. Casey, "BitBeat: para los mineros de Bitcoin, un problema candente este verano", Wall Street Journal, blog de MoneyBeat, 29 de abril de 2014, http://blogs.wsj.com/ moneybeat / 2014/04/29 / bitbeat-for-bitcoin-miners-a-hot-problem-this-summer /.

Adam Smith opinó sobre un asunto similar en el siglo dieciocho: Paul Krugman, "Adam Smith odia a Bitcoin", New York Times, Conscience of a Liberal blog, 12 de abril de 2013, http://krugman.blogs.nytimes.com/2013 / 04/12 / adam-smith-hate-bitcoin /.

Una de estas vulnerabilidades fue decisiva: la cuenta del hardfork en el blockchain proviene de un hilo en la lista # bitcoin-dev en el Bitcoin Forum, 11 de marzo de 2013, http://bitcoinstats.com/irc/bitcoin-dev/logs/ 2013/03/11.

Un caso de gasto de $ 10,000: Vitalik Buterin, "Red Bitcoin sacudida por Blockchain Fork", Revista Bitcoin, 12 de marzo de 2013, http://bitcoinmagazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/ .

Según coinometrics.com: el costo de un ataque del 51 por ciento se actualiza regularmente en el sitio web de Coinometrics, http://www.coinometrics.com/bitcoin/brix.

en junio de 2014, el grupo GHash.IO: Michael J. Casey, "BitBeat: Mining Pool rechaza las soluciones a corto plazo para evitar '51% de ataque'", Wall Street Journal, blog de MoneyBeat, 16 de junio de 2014, http: // blogs.wsj.com/moneybeat/2014/06/16/bitbeat-a-51-attack-what-is-it-and-could-it-happen/.

En un artículo polémico: Ittay Eyal y Emin Gün Sirer, "La mayoría no es suficiente: la minería de Bitcoin es vulnerable", documento de investigación publicado por arXiv.org de la Universidad de Cornell, 15 de noviembre de 2013, http://arxiv.org/pdf/ 1311.0243v5.pdf.

El periódico molestó a muchos en la comunidad bitcoin: entrevista telefónica con Sirer por Michael J. Casey, 9 de marzo de 2014.

Como explicó Nakamoto en su libro blanco: Satoshi Nakamoto, "Bitcoin: un sistema de efectivo electrónico punto a punto", agosto de 2008, bitcoin.org, https://bitcoin.org/bitcoin.pdf.

CEX.IO tiene a veces: Casey, "BitBeat: Mining Pool rechaza reparaciones a corto plazo".

A finales de agosto de 2014: por "Top 100" en bitcoinrichlist.com, http://bitcoinrichlist.com/top100.

De ahí los informes de ostentosos basados en bitcoin: ver Robin Sidel, "Bitcoins Buy a Villa in Bali", Wall Street Journal, 19 de marzo de 2014; y Michael J. Casey y Paul Vigna, "Del viaje espacial a la pizza, su bitcoin va lejos estos días", Wall Street Journal, blog de MoneyBeat, 16 de enero de 2014, http://blogs.wsj.com/moneybeat/2014/ 01/16 / from-space-travel-to-pizza-your-bitcoin-goes-quite-far-these-days /.

Billeteras "multi-sig" de innovadores como BitGo: Michael J. Casey, "Bitcoin Security Startup BitGo obtiene más fondos; El CEO de Ex-Verisign se une al equipo, "Wall Street Journal, blog de MoneyBeat, 16 de junio de 2014, http://blogs.wsj.com/moneybeat/2014/06/16/bitcoin-security-startup-bitgo-gets-more- fondos-ex-verisign-ceo-join-team /.

El desarrollador principal de bitcoins Jeff Garzik: Vea a Daniel Cawrey, "Jeff Garzik anuncia una sociedad para lanzar satélites de Bitcoin al espacio", CoinDesk, 23 de abril de 2014, http://www.coindesk.com/jeff-garzik-announces-partnership-launch- bitcoin-satellites-space /; también vea a Catherine Bleish, "Entrevista con Jeff Garzik, Bitcoin in Space", revista Bitcoin, 17 de junio de 2014, http://bitcoinmagazine.com/14069/interview-jeff-garzik-bitcoin-space/.

De estas altcoins, litecoin: explicaciones de Litecoin tomadas de varias fuentes, incluyendo https://litecoin.org/.

En el caso de nextcoin: explicaciones de Nextcoin tomadas de varias fuentes, incluyendo http://nxt.org.

"Armas financieras de destrucción masiva", como las llamó Warren Buffett: del Informe Anual 2002 de Berkshire Hathaway Inc., extractos editados, http://www.fintools.com/docs/Warren%20Buffet%20on%20Derivatives.pdf.

7. Escuela de Satoshi

Stanford luego donaría la tierra que poseía: la Universidad de Stanford, Historia de Stanford, http://www.stanford.edu/about/history/.

Décadas más tarde, dos jóvenes estudiantes en esa escuela: David Jacobson, "Padres Fundadores", Revista Stanford, julio / agosto de 1998.

Entramos en una tienda especializada: Sarah Needleman, "Más pequeñas empresas adoptan Bitcoin", Wall Street Journal, 26 de junio de 2013.

Si el Área de la Bahía es la región más importante: muchos de los detalles en este capítulo provienen de un viaje a 20 Misiones y entrevistas realizadas por Paul Vigna en junio de 2014.

"Hay una sensación de que eres parte de un movimiento": Taariq Lewis, entrevistado por Paul Vigna, 15 de junio de 2014.

Dan Held tenía veinticinco años cuando asistió a su primera reunión de bitcoin: Dan Held, entrevistado por Paul Vigna, el 14 de junio de 2014.

"Es un tipo muy específico de cerebro obsesionado con el bitcoin": Adam Draper, entrevistado por Paul Vigna, 13 de junio de 2014.

Es Kenna, el fundador de 20Mission, quien mejor: Jered Kenna, entrevistado por Paul Vigna, 15 de junio de 2014.

que luego demandó por $ 2 millones sobre lo que Tradehill reclamó: Jeremy Quittner, "Dwolla nos sacó del negocio, Bitcoin Exchange dice en traje", American Banker, 6 de marzo de 2012, http://www.americanbanker.com/issues/ 177_45 / tradehill-dwolla-bitcoin-exchange-digital-currency-lawsuit-1047273-1.html.

Allan Grant es cofundador de hired.com: Billy Gallagher, "Hired plantea $ 15M en la serie A en la valoración de alrededor de $ 60M", TechCrunch, 24 de marzo de 2014, http://techcrunch.com/2014/03/24/hired -raises-15m-series-a /.

Chris Cassano, un joven de veinticinco años de Florida: Chris Cassano, entrevistado por Paul Vigna, 12 de junio de 2014.

Publicó una descripción de esto en Kickstarter: Chris Cassano, "Piper: una impresora de billetera de papel basada en hardware y más", Kickstarter, 10 de julio de 2013, https://www.kickstarter.com/projects/299052466/piper-a -hardware-based-paper-wallet-printer-and-mo.

"El dinero también es fantástico": Nathan Lands, entrevistado por Paul Vigna, 13 de junio de 2014.

De acuerdo con encuestas realizadas por el sitio de noticias CoinDesk: "El estado del informe Bitcoin Q2 2014 revela la expansión de la economía de Bitcoin", CoinDesk, 10 de julio de 2014, http://www.coindesk.com/state-of-bitcoin-q2-2014-report -expanding-bitcoin-economy /.

Andreessen Horowitz ha realizado grandes inversiones: Gregory Zuckerman, "Web Pioneer Keeps Faith, y Cash, en Bitcoin", Wall Street Journal, 21 de marzo de 2014.

poner dinero de sus AME Ventures en: Michael J. Casey, "Procesador de Bitcoin recauda $ 30 millones", Wall Street Journal, 13 de mayo de 2014.

Stratton Sclavos, ex CEO de Verisign: Michael J. Casey, "Bitcoin Security Startup BitGo obtiene más fondos; El CEO de Ex-Verisign se une al equipo, "Wall Street Journal, blog de MoneyBeat, 16 de junio de 2014, http://blogs.wsj.com/moneybeat/2014/06/16/bitcoin-security-startup-bitgo-gets-more- fondos-ex-verisign-ceo-join-team /.

Jim Breyer de Accel Partners: Emily Spaven, "Circle se lanza con $ 9M de Jim Breyer, Accel y General Catalyst en el mayor financiamiento de Bitcoin", CoinDesk, 31 de octubre de 2013, http://www.coindesk.com/circle- 9m-jim-breyer-accel-general-catalyst-biggest-bitcoin-funding /.

Blockchain, una compañía de billeteras con sede en Londres, manejó todo: Kim Lachance Shandrow, "CEO de Blockchain.info: Pagamos a nuestros empleados en Bitcoin. Y Algún día también podría ser, "Empresario, 2 de junio de 2014, http://www.entrepreneur.com/article/234463.

Antes de la vieja guardia de la comunidad Valley VC: Draper, entrevistado por Vigna.

Scott Robinson es el director de marketing: las entrevistas con Scott Robinson, Andrew Lee, Kent Liu, Joshua Schechter, así como los detalles del día expo de Plug and Play fueron recopiladas por Paul Vigna el 12 de junio de 2014.

La historia serpenteante del nombre de dominio: Paul Vigna y Michael J. Casey, "BitBeat: Los hombres que poseían Bitcoin.com", Wall Street Journal, blog de MoneyBeat, http://blogs.wsj.com/moneybeat/2014/04 / 22 / bitbeat-the-men-quien-poseía-bitcoin-com /.

En una publicación en el blog de StrictlyVC: Connie Loizos, "Un oso Bitcoin en Silicon Valley, es cierto", StrictlyVC, 7 de marzo de 2014, http://www.strictlyvc.com/2014/03/07/bitcoin-bear-silicon-valley-true /.

"Si volviste a 1993 y preguntaste": Chris Dixon, entrevista telefónica con Michael J. Casey, 25 de junio de 2014.

8. Los no bancarizados

Aproximadamente 2.500 millones de personas en el mundo: Asli Demirguc-Kunt y Leora Klapper, "Measuring Financial Inclusion", Documento de trabajo de investigación sobre políticas del Banco Mundial 6025, abril de 2012.

Para ilustrar, volvamos brevemente: Songyi Lee, Johann Barbie y Jonathan Zobro, entrevistados por Paul Vigna, 12 de junio de 2014, así como la posterior entrevista con Songyi Lee, 23 de junio de 2014.

Mali es una de las naciones más pobres del planeta: The Statesman's Yearbook (2014).

El Banco Mundial estima que el negocio global de remesas: "Informe sobre la migración y el desarrollo", Banco Mundial, 11 de abril de 2014, http://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1288990760745/MigrationandDevelopmentBrief22.pdf.

tarifas por dinero enviado desde los Estados Unidos: los precios de una gran cantidad de "corredores" se pueden encontrar en http://remittanceprices.worldbank.org/en.

El problema no se limita a los mercados emergentes: los datos sobre la inclusión financiera por país se pueden encontrar en el índice de inclusión financiera del Banco Mundial, llamado Global Findex, http://datatopics.worldbank.org/financialinclusion/.

Entre 1990 y 2010, el porcentaje de: "Poverty Overview", Banco Mundial, 7 de abril de 2014, http://www.worldbank.org/en/topic/poverty/overview.

Con respecto a la alfabetización, el mundo en desarrollo: "World Development Indicators, 2014", Banco Mundial, http://wdi.worldbank.org/table/2.13.

"Recuerdo que una vez estuve en el Caribe": Pelle Braendgaard, en la conferencia Inside Bitcoins, Nueva York, 7 de abril de 2014.

Ericsson ConsumerLab pronostica que: "África subsahariana, Apéndice de Ericsson Mobility Report", Ericsson ConsumerLab, http://www.ericsson.com/res/docs/2014/emr-june2014-regional-appendices-ssa.pdf.

ahora está vendiendo teléfonos inteligentes muy básicos: Lorraine Luke, "India, Indonesia, para obtener smartphones de $ 25", Wall Street Journal, http://online.wsj.com/articles/mozilla-to-sell-25-smartphones-1402466959.

una ruta de escape para su ahorro de $ 12 trillones de ahorros: Grace Zhu, "firmas de tecnología de los bancos de los bancos chinos en carrera por los depósitos", Wall Street Journal, 24 de febrero de 2014, http://online.wsj.com/news/articles/SB10001424052702304834704579402573128666330 .

Cuando se combina con el banco central: Bobby Lee, entrevistado por Michael J. Casey en Shanghai el 19 de julio de 2014.

"Mucha gente en los EE. UU. No": Eric Gu, entrevistado por Michael J. Casey en Shanghai el 20 de julio de 2014.

"Intenté todo": Jamal Ifill, entrevistado por Paul Vigna, 27 de junio de 2014.
A $ 25,000, el PIB per cápita de la isla: The Statesman's Yearbook (2014).

Sus amigos lo llaman Mr. Bit, y no está claro: gran parte de la información para esta sección, incluidas entrevistas con Gabriel Abed, el Dr. Leroy McClain, David Simpson y Jamal Ifill, fue recopilada por Paul Vigna en Barbados, del 24 al 28 de junio , 2014

aprovechando los costos de electricidad relativamente bajos allí: Mark Lyndersay, "En Bitcoin and Beyond", Tech News T & T, 24 de junio de 2014, http://technewstt.com/bd942/.

Patrick Byrne, CEO de Salt Lake City: Patrick Byrne, entrevistado por Michael J. Casey, 8 de junio de 2014.

"No tengo compasión por estas mujeres": Francesco Rulli, Fereshteh Forough, y Roya Mahboob, entrevistadas por Michael J. Casey y Paul Vigna, el 19 de junio de 2014.

El servicio de BitPagos es tan atractivo: Basado en entrevistas con el CEO de BitPagos, Sebastian Serrano, por Michael J. Casey, 25 de enero y 2 de junio de 2014.

A Mike Abridello, un expatriado de EE. UU .: Basado en una entrevista telefónica con Mike Abridello de Michael J. Casey, 13 de junio de 2014.

"Esos son solo los flujos oficiales": Dilip Ratha, entrevistado por Paul Vigna, 22 de mayo de 2014.

Para usar M-Pesa, las personas se registran: Frederik Eijkman, Jake Kendall e Ignacio Mas, "Puentes al contado: el fin minorista de M-Pesa", ahorros y desarrollo, http://aisberg.unibg.it/bitstream/ 10446/27458/1 / EIJKMAN% 202-2010.pdf.

un grupo de ayuda, Concern Worldwide: Dipankar Datta, Anne Ejakait y Monica Odak, "Transferencias monetarias basadas en teléfonos móviles: lecciones de la respuesta de emergencia de Kenia", Humanitarian Exchange Magazine, octubre de 2008, http://www.odihpn.org/ human-exchange-magazine / issue-40 / mobile-phone-based-cash-transfers-lessons-from-the-kenya-emergency-response.

Quizás inevitablemente, entonces, alguien como Duncan: Elizabeth Rossiello, entrevistada por Paul Vigna, 9 y 18 de mayo de 2014.

una casa de hackers llamada iHub: http://www.ihub.co.ke/.

de lo que el economista peruano Hernando de Soto llama: Hernando de Soto, El Misterio del Capital (Basic Books, 2000).

Jonathan Mohan, que trabaja en Ethereum: Jonathan Mohan, hablando en la conferencia Inside Bitcoins, Nueva York, 7 de abril de 2014.

9. Todo del Blockchain

Joseph Gleason, mejor conocido como Fireduck: Joseph Gleason, "Cualquiera quiere ejecutar mi Casino de Bitcoin", Foro de Bitcoin, 17 de abril de 2012, publicado en "fireduck", http://www.reddit.com/r/Bitcoin/comments / segz0 / anyone_want_to_run_my_bitcoin_casino; identificado como Joseph Gleason a través del sitio web de Gleason, http://1209k.com/bitcoin/faq.php.

Los jugadores enviarían bitcoins a uno: Jon Matonis, "Bitcoin Casinos Report 2012 Earnings", Forbes, 22 de enero de 2013, http://www.forbes.com/sites/jonmatonis/2013/01/22/bitcoin-casinos-release -2012-ganancias /.

Luego, unos meses después de las ofertas de acciones: Erik Voorhees, "Re: S.DICE-SatoshiDICE 100% activo que paga dividendos en PMEx", Bitcoin Forum, 17 de julio de 2013, https://bitcointalk.org/index.php ? topic = 101902.msg2751536 # msg2751536.

Mike Hearn, que trabajó durante tres años en seguridad: Mike Hearn, "El futuro del dinero", discurso del Festival de Turing, YouTube, 23 de agosto de 2013, https://www.youtube.com/watch?v=Pu4PAMFPo5Y.

"Contratos inteligentes", una idea que primero flotó Nick Szabo: Nick Szabo, "Formalizando y Asegurando Relaciones en Redes Públicas", septiembre de 1997, http://szabo.best.vwh.net/formalize.html.

David Johnston es un miembro directivo principal: David Johnston, entrevistado por Michael J. Casey, 25 de enero de 2014.

A mediados de 2013, el periodista Vitalik Buterin también obtuvo: Vitalik Buterin, entrevistado por Michael J. Casey, 26 de enero de 2014.

Buterin expuso por primera vez su visión en un libro blanco: Vitalik Buterin, "White Paper Ethereum", enero de 2014, https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf.

El equipo también planeó un evento para recaudar fondos: Michael J. Casey, "BitBeat: Ethereum Presale tiene un precio de $ 12.7 millones Tally", Wall Street Journal, blog de MoneyBeat, http://blogs.wsj.com/moneybeat/2014/08/05/ bitbeat-ethereum-preventa-hits-12-7-million-tally /.

Aquí, una vez más a la vanguardia: "The Ripple Protocol: Executive Summary for Financial Institutions", Ripple.com, https://ripple.com/files/ripple-FIs.pdf.

David Andolfatto, economista jefe de: David Andolfatto, "Bitcoin y más allá: las posibilidades y las trampas de las monedas virtuales", Banco de la Reserva Federal de St. Louis, 31 de marzo de 2014, http://www.stlouisfed.org/dialogue -with-the-fed / bitcoin-and-beyond.cfm.

El tema de los motivos de lucro de Ripple: Jed McCaleb, "Selling My XRP", XRPtalk, 22 de mayo de 2014, https://xrptalk.org/topic/2629-selling-my-xrp/.

Pero luego las cosas se pusieron feas cuando: Jesse Powell, "miembro de la Junta de Ripple dimite", Reddit, 24 de mayo de 2014, http://www.reddit.com/r/Ripple/comments/26ccz3/ripple_board_member_resigns/.

Las cercas se repararon tres meses después: Monica Long, "Solución del XRP de Jed", Ripple Forum, https://ripple.com/forum/viewtopic.php?f=1&t=7641.

Larsen no minimiza que Ripple Labs: Chris Larsen, entrevistado por Michael J. Casey, 5 de mayo de 2014.

Jed McCaleb usaría algo completamente nuevo: Michael J. Casey y Paul Vigna, "Mt Gox, Ripple Founder presenta Stellar, un nuevo proyecto de moneda digital", Wall Street Journal, blog de MoneyBeat, 31 de julio de 2014, http: // blogs. wsj.com/moneybeat/2014/07/31/mt-gox-ripple-founder-unveils-stellar-a-new-digital-currency-project/.

MaidSafe se basa en la noción de que muchas personas: "Descripción general de la plataforma distribuida", MaidSafe, http://maidsafe.net/overview.

pretende evitar el "desastre ecológico" que se avecina: David Irvine, entrevistado por Michael J. Casey y Paul Vigna, 8 de abril de 2014.

Para una moneda interna que MaidSafe: Michael J. Casey y Paul Vigna, "BitBeat: La oferta maníaca de MaidSafe destaca a Hot Bitcoin 2.0", Wall Street Journal, blog de MoneyBeat, 24 de abril de 2014, http://blogs.wsj.com/moneybeat / 2014/04/24 / bitbeat-maidsafes-manic-offer-highlights-hot-bitcoin-2-0 /.

la Comisión de Bolsa y Valores impuso: "La SEC acusa al empresario Bitcoin de ofrecer valores no registrados", Comisión de Bolsa y Valores de EE. UU., 3 de junio de 2014, http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370541972520#. VA2lhBBdWsA.

"Crees que es difícil saber qué bitcoin": Jacob Farber, hablando en la conferencia Inside Bitcoins, Nueva York, 7 de abril de 2014.

Realcoin, fundada por el prolífico inversor de bitcoin Brock Pierce: Michael J. Casey, "La moneda digital respaldada por el dólar tiene como objetivo arreglar el dilema de volatilidad de Bitcoin", Wall Street Journal, blog de MoneyBeat, 8 de junio de 2014, http://blogs.wsj.com / moneybeat / 2014/07/08 / dollar-backed-digital-currency-aims-to-fix-bitcoins-volatility-dilemma /.

Una versión aún más centralizada de un concepto similar es Bitreserve: Paul Vigna y Michael J. Casey, "BitBeat: BitReserve promete costos parecidos a Bitcoin, sin riesgo similar a Bitcoin", Wall Street Journal, blog MoneyBeat, 15 de mayo de 2014, http : //blogs.wsj.com/moneybeat/2014/05/15/bitbeat-bitreserve-vows-bitcoin-like-costs-no-bitcoin-like-risk/.

"Es como si fuéramos Henry Ford y estamos trabajando con esto": Nicholas Cary, entrevistado por Michael J. Casey y Paul Vigna, 6 de junio de 2014.

"Este no es el sueño de Satoshi": Chris Odom, hablando en la Conferencia Norteamericana de Bitcoin, Miami Beach, 25 de enero de 2014.

10. Cosas Que No Encajan

Gavin Andresen abrió la puerta: detalles de los eventos relacionados con el ataque de maleabilidad de la transacción Mt Gox tomados de las entrevistas que Michael J. Casey tuvo con Gavin Andresen el 11 y 14 de febrero de 2014 y con Jeff Garzik el 14 de febrero de 2014.

"Contrariamente a la declaración de Mt Gox, Bitcoin no tiene la culpa": Gavin Andresen, "Al contrario de la Declaración de Mt Gox, Bitcoin no está en peligro", Fundación Bitcoin, entrada de blog, https://bitcoinfoundation.org/2014/02/contrary -to-mt-goxs-statement-bitcoin-is-not-at-fault /.

El precio de bitcoin, en $ 703: Fuente: índice de precios de Bitcoin, CoinDesk, http://www.coindesk.com/price.

En el peor momento: detalles del precio del índice de precios de Bitcoin, CoinDesk, http://www.coindesk.com/price/; información de capitalización de mercado de http://www.coinmarketcap.com.

"Probablemente diez mil de los mejores desarrolladores": Chris Dixon, entrevista telefónica con Michael J. Casey, 25 de junio de 2014.

En su libro de 2006: Ori Brafman y Rod Beckstrom, The Starfish and the Spider: El poder imparable de las organizaciones sin líderes (Portfolio, 2006).

según un esquema de la estructura de la red: Paul Baran, "On Distributed Communication", The Rand Corporation, agosto de 1964, http://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf.

En junio de 2013, la División de Instituciones Financieras de California: Jon Matonis, "La Fundación Bitcoin recibe orden de cese y desistimiento de California", Forbes, 23 de junio de 2013, http://www.forbes.com/sites/jonmatonis/2013/06 / 23 / bitcoin-foundation-receives-cese-and-desist-order-from-california /.

En febrero de 2014, el senador demócrata de West Virginia: el senador Joe Manchin, "Manchin exige a los reguladores federales Ban Bitcoin", una carta dirigida al secretario del Tesoro Jacob Lew, la presidenta de la Reserva Federal Janet Yellen, y otros, http: //www.manchin.senate. gov / public / index.cfm / 2014/2 / manchin-demands-federal-regulators-ban-bitcoin.

Como Gareth Murphy, director de mercados: Amir Mizroch, "Banquero central irlandés establece la ley en la reunión de Bitcoin", Wall Street Journal, blog Digits, 3 de julio de 2014, http://blogs.wsj.com/digits/2014 / 07/03 / irish-central-banker-lays-down-the-law-at-bitcoin-gathering /.

Esto preparó el escenario para una audiencia en el Senado muy anticipada: Jennifer Shasky Calvery, "Declaración de Jennifer Shasky Calvery, Directora de la Red de Delitos Financieros del Departamento del Tesoro de los Estados Unidos", Comité Senatorial de Banca, Vivienda y Asuntos Urbanos, noviembre 19, 2013, http://www.fincen.gov/news_room/testimony/html/20131119.html.

Algunos estados, como Texas, adoptaron una postura deliberadamente complaciente: el comisionado bancario de Texas, George T. Cooper, argumentó que las monedas virtuales no cumplían con la definición de dinero y, por lo tanto, no podían caer bajo las reglas de transmisión de dinero del estado. Ver la declaración del 3 de abril de 2014 en http://www.dob.texas.gov/public/uploads/files/Laws-Regulations/New-Actions/sm1037.pdf.

Eso llevó a un montón de escaparates en lugares texanos tecnológicos como Austin: Dave Byknish y Paul Shelton, "Austin obtiene el segundo cajero automático Bitcoin; Está en una tienda de armas ", kxan.com, 2 de marzo de 2014, http://kxan.com/2014/03/02/austin-gets-2nd-bitcoin-atm-its-at-a-gun-store/ .

Superintendente ambicioso del Departamento de Servicios Financieros de Nueva York: Benjamin M. Lawsky, "Aviso de intención de celebrar audiencia sobre monedas virtuales, incluida la posible emisión del NYDFS de una 'BitLicense'", 14 de noviembre de 2013, http: //www.dfs. ny.gov/about/press2013/virtual-currency-131114.pdf.

En febrero del año siguiente: Declaraciones de testigos, sitio web del Departamento de Servicios Financieros de Nueva York, http://www.dfs.ny.gov/.

Después de las audiencias, Lawsky llevó a Reddit: Benjamin M. Lawsky, "Según lo solicitado, soy Ben Lawsky, superintendente del Departamento de Servicios Financieros de Nueva York, aquí para una AMA sobre Bitcoin / Moneda Virtual", Reddit.com, 20 de febrero. , 2014, publicado como BenLawsky,
http://www.reddit.com/r/IAmA/comments/1ygcil/as_requested_im_ben_lawsky_superintendent_of_the.

La presidenta de la Fed Janet Yellen señaló: Steven Russolillo, "Yellen en Bitcoin: la Fed no tiene autoridad para regularlo de ninguna manera", Wall Street Journal, blog de MoneyBeat, 27 de febrero de 2014.

Abogado con sede en Miami Andrew Ittleman: Entrevista realizada por Michael J. Casey, 29 de mayo de 2014.

Finalmente, un fallo formal cayó en abril de 2014: Paul Vigna, "Los precios de Bitcoin cayeron un 10% después de que los bancos chinos cortaran los intercambios locales", Wall Street Journal, blog de MoneyBeat, 10 de abril de 2014, http://blogs.wsj.com / moneybeat / 2014/04/10 / bitcoin-prices-down-10-after-chinese-banks-cut-off-local-exchanges /.

Después de eso, la Autoridad Bancaria Europea: Viktorai Dendrinou, "La UE advierte a los bancos sobre las monedas virtuales", Wall Street Journal, 4 de julio de 2014.

El principal oficial de enlace con el gobierno de la Fundación Bitcoin: Jim Harper, "¿Europa escuchará a 'Europa'?", Blog de la Fundación Bitcoin, 4 de julio de 2014, https://bitcoinfoundation.org/2014/07/will-europe-listen-a Europa/.

De regreso en los Estados Unidos, el 25 de marzo: John D. McKinnon y Ryan Tracy, "IRS dice que Bitcoin es propiedad, no moneda", Wall Street Journal, 25 de marzo de 2014.

Unos meses más tarde, en julio: Paul Vigna, "NY Financial Regulator lanza un borrador de 'Bitlicense' para las empresas de Bitcoin", Wall Street Journal, blog de MoneyBeat, 17 de julio de 2014, http://blogs.wsj.com/moneybeat/ 2014/07/17 / ny-financial-regulator-releases-draft-of-bitlicense-for-bitcoin-businesses /.

Mientras tanto, Perianne Boring: Perianne Boring, "Comentarios de BitLicense de la Cámara de Comercio Digital", 18 de agosto de 2014, http://www.digitalchamber.org/assets/chamber-bitlicense-comments-final.pdf.

Una petición circuló rápidamente: cartas y firmantes disponibles en el sitio web de la Cámara de Comercio Digital, http://www.digitalchamber.org/ny- bitlicense.html.

Algunos sugirieron acciones más drásticas y comenzaron a cabildear: la Asociación de Desarrolladores Financieros de Código Abierto, "Detenga BitLicense de Harming Small Businesses and Tech Innovation in NY", solicite al Gobernador Andrew Cuomo a través de change.org, http://www.change.org/ p / governor-andrew-m-cuomo-and-the-new-york-state-legislature-stop-bitlicense-from-harming-small-business-and-tech-innovation-in-ny.

Más dramáticamente, el CEO de Circle Jeremy Allaire: Jeremy Allaire, "Reflexiones sobre la Propuesta de Nueva York BitLicense", 13 de agosto de 2014, blog de Circle Internet Financial, https://www.circle.com/2014/08/13/thoughts-new -york-bitlicense-propuesta.

Reconociendo que el NYDFS no tenía "el monopolio de la verdad": Paul Vigna, "BitBeat: BitLicense obtiene extensión; Lawsky: 'No tenemos el monopolio de la verdad' ", Wall Street Journal, blog de MoneyBeat, 21 de agosto de 2014, http://blogs.wsj.com/moneybeat/2014/08/21/bitbeat-bitlicense- gets-extension-lawsky-we-dont-have-a-monopoly-on-the-truth /.

Como señala Harper of the Bitcoin Foundation: Jim Harper, entrevistado por Michael J. Casey, 8 de agosto de 2014.

en algún lugar entre $ 5 billones y $ 32 billones: estimación de $ 5 billones en 2007 de la Organización para la Cooperación y el Desarrollo Económico en "Places in the Sun", Economista, 22 de febrero de 2007; $ 32 trillones se encuentran entre los $ 21 trillones más valorados en $ 32 trillones estimados por Tax Justice Network en su informe "The Price of Offshore Revisited", publicado el 22 de julio de 2012, http://www.taxjustice.net/cms/upload/pdf /The_Price_of_Offshore_Revisited_Presser_120722.pdf.

Bulgaria, cuya agencia tributaria: Ali Najjar, "NRA búlgara ofrece directrices fiscales de Bitcoin", CoinReport, 2 de abril de 2014, https://coinreport.net/bulgaria-bitcoin-tax-guidelines/.

La Autoridad Supervisora del Mercado Financiero Suizo anunció: Emily Spaven, "Informe del Gobierno suizo: Bitcoin Demasiado 'insignificante' para la legislación," 25 de junio de 2014, CoinDesk, http://www.coindesk.com/switzerland-government-report-bitcoin- insignificante-legislación /.

Este enfoque de no intervención ha cambiado: Michael J. Casey, "BitBeat: Crypto Innovators Find Fertile Ground en Soft-Touch Switzerland", Wall Street Journal, blog de MoneyBeat, 4 de agosto de 2014, http://blogs.wsj.com/ moneybeat / 2014/08/04 / bitbeat-crypto-innovators-find-fertile-ground-in-soft-touch-switzerland /.

En agosto de 2014, la Canciller del Tesoro: Anna Irrera, "U.K. para examinar la regulación de moneda virtual, "Wall Street Journal, Digits blog, 6 de agosto de 2014, http://blogs.wsj.com/digits/2014/08/06/uk-to-examine-virtual-currency-regulation/.

El primer fondo de inversión de bitcoin completamente regulado: Nermin Hajdarbegovic, "primer fondo de inversión de Bitcoin regulado para lanzar en la isla de Jersey", 10 de julio de 2014, CoinDesk, http://www.coindesk.com/first-regulated-bitcoin-investment- fund-launch-island-jersey /.

La Isla de Man anunció: Robert Paul Davis, "Isla de Man da la bienvenida a los intercambios de divisas digitales 'No se requiere licencia'", CoinDesk, 28 de marzo de 2014, http://www.coindesk.com/isle-man-welcomes-digital- currency-exchanges-license-required /.

El gobierno canadiense rompió su silencio: Samuel Rubenfeld, "Canadá promulga regulaciones de Bitcoin", blog de The Wall Street Journal, Risk & Compliance, 23 de junio de 2014, http://blogs.wsj.com/riskandcompliance/2014/06/23/canada -enacts-bitcoin-regulations /.

En cuanto a México, en julio: Tanaya Macheel, "El caso para fusionar el peso de México con la tecnología de la cadena de bloques", CoinDesk, 26 de julio de 2014, http://www.coindesk.com/case-merging-mexicos-peso-block- cadena de tecnología /.

"Todos los bancos están asustados": Aurélien Menant, entrevistado por Michael J. Casey, 20 de julio de 2014.

CEO estadounidense de veintiocho años, Autumn Radtke: Newley Purnell, "Singapur investiga muerte del CEO de American Startup", Wall Street Journal, blog Digits, 7 de marzo de 2014, http://blogs.wsj.com/digits/ 2014/03/07 / singapore-investiga-death-of-american-startup-ceo /.

La Autoridad monetaria de Singapur dijo en marzo: Sanat Vallikappen, "Singapur regulará a los operadores de Bitcoin para el riesgo de lavado", 13 de marzo de 2014, Bloomberg,

http://www.bloomberg.com/news/2014-03-13/singapore-to -regulate-bitcoin-operators-for-money-laundering.html.

Según un informe, el gigantesco conglomerado estatal Temasek: Jon Southurst, "Experimentos de la firma de inversión del gobierno de Singapur con Bitcoin", CoinDesk, 27 de junio de 2014, http://www.coindesk.com/singapore-government -owned-investment-firm-experiments-bitcoin /.

Reuters informó que solo Karpelès conocía las contraseñas: Sophie Knight, "En Mt Gox Bitcoin Hub, 'Geek' CEO Sought Both Control y Escape", Reuters, 21 de abril de 2014, http://www.reuters.com/article/2014 / 04/21 / us-bitcoin-mtgox-karpeles-insight-idUSBREA3K01D20140421.

Roger Ver y su amigo de la escuela secundaria Jesse Powell: Detalles de la experiencia de Powell y Ver en Mt Gox en junio de 2011 tomados de la entrevista a Jesse Powell por Paul Vigna, 3 de marzo de 2014.

Interactuando en foros de bitcoin con otros bitcoiners: Adam B. Levine, "El fantasma en la máquina en MtGox", 27 de febrero de 2014, Hablemos de Bitcoin, http://letstalkbitcoin.com/the-ghost-in-the-machine- at-mtgox /.

Muchas teorías se desarrollarían más tarde: muchas de las teorías fueron descritas en una publicación de blog por Cameron Winklevoss en el sitio web de Winklevoss Capital el 14 de marzo de 2014, https://winklevosscapital.com/what-may-have-happened-at-mt- gox /.

Esto parece ser un juego de un meme popular: Douglas Adams, Life, the Universe y Everything (Harmony Books, 1982).

Adam Levine, presentador de un programa de entrevistas de bitcoin: Adam B. Levine, entrevistado por Michael J. Casey, 28 de febrero de 2014.

La billetera multi-sig altamente segura de BitGo salió en este momento: Michael J. Casey, "Bitcoin entra en la era Multi-Sig", en "BitBeat: Rep. Stockman quiere que el IRS reconsidere la decisión de Bitcoin", Wall Street Journal, blog MoneyBeat , 8 de abril de 2014, http://blogs.wsj.com/moneybeat/2014/04/08/bitbeat-rep-stockman-wants-irs-to-reconsider-bitcoin-decision/.

Mientras tanto, los gemelos Winklevoss progresaron con una solicitud: Michael J. Casey, "Abogado de Bitcoins ETF de Winklevoss Twins dice que la revisión de la SEC avanza sin problemas", Wall Street Journal, blog de MoneyBeat, 17 de enero de 2014, http: //blogs.wsj. com / moneybeat / 2014/01/17 / lawyer-for-winkelvoss-twins-bitcoin-etf-says-sec-review-going-smoothly /.

Más tarde, Atlas ATS lanzó una red: Michael J. Casey, "Perseus, Atlas lanza la plataforma global de comercio de Bitcoin", Wall Street Journal, 12 de marzo de 2014.

El entusiasta de Bitcoin, Barry Silbert, lanzó su propio fondo de bitcoin: Michael J. Casey y Paul Vigna, "SecondMarket busca abrir un fondo de Bitcoin para inversores ordinarios", Wall Street Journal, 19 de marzo de 2014.

Silbert también comenzó a construir su propio intercambio: Michael J. Casey y Robin Sidel, "Firms Bank on a Bitcoin Bounceback", Wall Street Journal, 26 de febrero de 2014.

Su solución más radical: Danny Yadron, "Tech Renegade: desde las pistolas de impresión en el hogar a la moneda imposible de rastrear", Wall Street Journal, 31 de diciembre de 2013.

"Están llegando muchas nuevas empresas": Cody Wilson, entrevistado por Michael J. Casey, 20 de marzo de 2014.

En otra parte, Wilson fue citado describiéndola: Andy Greenberg, "Dark Wallet está a punto de hacer que el blanqueo de dinero con Bitcoin sea más fácil que nunca", 29 de abril de 2014, http://www.wired.com/2014/04/dark-wallet /.

el científico en jefe de la Fundación Bitcoin, lo llamó "fantástico": Kadhim Shubber, "Gavin Andresen: el aumento de las tarifas de transacción podría sacar a los pobres de Bitcoin", CoinDesk, 16 de mayo de 2014, http://www.coindesk.com/gavin-andresen -rising-transaction-fees-price-poor-bitcoin /.

Sin embargo, el periodista independiente: Ryan Selkis, "Carteras oscuras son una pesadilla reglamentaria para Bitcoin", blog TwoBitIdiot, 1 de mayo de 2014, http://two-bit-idiot.tumblr.com/post/84454892629/dark-wallets- are-a-regulatory-nightmare-for-bitcoin.

11. Una nueva economía

en muchas medidas, solo se ha vuelto más intenso desde esa crisis: Luke Johnson, "Elizabeth Warren: 'Demasiado grande para fallar es peor que antes de la crisis financiera", Huffington Post, 12 de noviembre de 2013, http://www.huffingtonpost.com/ 2013/11/12 / elizabeth-warren-too-big-to-fail_n_4260871.html.

la brecha de riqueza más amplia desde la Gran Depresión: Scott Neuman, "Estudio dice que la brecha de ingresos de Estados Unidos es la más grande desde la Gran Depresión", NPR, 10 de septiembre de 2013, http://www.npr.org/blogs/thetwo-way/2013/09 / 10/221124533 / study-says-americas-income-gap-widest-since-great-depression.

Como dijo el ex vicepresidente de los Estados Unidos Al Gore: Al Gore, "El punto de inflexión: Nueva esperanza para el clima", Rolling Stone, 18 de junio de 2014, http://www.rollingstone.com/politics/news/the-turning -point-new-hope-for-the-climate-20140618.

La gente ha descubierto que si tienen activos inactivos: "El aumento de la economía compartida", Economist, 9 de marzo de 2013, http://www.economist.com/news/leaders/21573104-internet-everything-hire-rise -sharing-economy.

Una frase de David Johnston de Mastercoin: David Johnston, "Ley de Johnston", http://www.johnstonslaw.org/.

entre una gran cantidad de publicidades del Super Bowl XXXIV: Dashiell Bennett, "8 Dot-Coms que gastaron millones en anuncios del Super Bowl y ya no existen", Business Insider, 2 de febrero de 2011, http://www.businessinsider.com/8 -dot-com-super-bowl-publicisers-that-no-longer-exist-2011-2? op = 1.

para lo cual Eastman Kodak ofrece una historia de advertencia: Mike Spector y Dana Mattiolo, "Kodak Teeters on the Brink", Wall Street Journal, 5 de enero de 2012.

Pero los cabilderos de Wall Street lucharon: David Enrich, "Los bancos regresan con una meta: retrocediendo", Wall Street Journal, 26 de enero de 2011.

U-Haul, la venerable empresa de alquiler de camiones: la información sobre el programa de préstamos de U-Haul se puede encontrar en http://www.uhaulinvestorsclub.com/AboutUs.

"El mundo no está corto de monedas": Francesco Guerrera, "La crisis de Bitcoin es un punto de inflexión para la moneda", Wall Street Journal, blog de MoneyBeat, 17 de febrero de 2014, http://blogs.wsj.com/moneybeat/2014/02 / 17 / bitcoins-crisis-es-turning-point-for-currency /.

La empresa de cabildeo de DC Peck Madigan Jones para presionar al Congreso: Olga Kharif y Elizabeth Dexheimer, "Lobbyist de MasterCard agrega Bitcoin a la lista de temas", Bloomberg, 30 de abril de 2014, http://www.bloomberg.com/news/2014-04- 30 / mastercard-lobbyist-adds-bitcoin-to-list-of-topics.html.

Jason Oxman, el CEO: Jason Oxman, entrevistado por Michael J. Casey, 24 de junio de 2014.

admite pagos en puntos de venta a través de códigos QR: Donna Tam, "PayPal ofrece compras de tiendas de códigos QR", CNET, 8 de octubre de 2013, http://www.cnet.com/news/paypal-offers-qr-codes- para-tiendas-tienda-compras /.

Se cree ampliamente que Facebook está funcionando: Samuel Gibbs, "Facebook se prepara para lanzar el servicio de transferencia electrónica de dinero en Europa", Guardian, 14 de abril de 2014, http://www.theguardian.com/technology/2014/apr/14/ facebook-e-money-transfer-service-europe.

ahora solo viene a los Estados Unidos: John Ginovsky, "EMV, un trabajo en progreso en los EE. UU.", ABA Banking Journal, 24 de agosto de 2014, http://www.ababj.com/blogs-3/making-sense-of- it-all / item / 4859-emv-a-work-in-progress-in-us /.

Square, que registró una pérdida de $ 100 millones en 2013: Alistair Barr, Douglas MacMillan y Evelyn M. Rusli, "Cuadrilla de inicio de pagos móviles habla de posible venta", Wall Street Journal, 21 de abril de 2014.

"Ahora la multitud tiene su propio modelo de negocio": Jeremiah Owyang, entrevistado por Paul Vigna, 11 de julio de 2014.

Un exhaustivo estudio de 2011 de la sociedad estadounidense realizado por Pew Research Center: "Millennials in adulthood", Pew Research Social & Demographic Trends, 7 de marzo de 2014, http://www.pewsocialtrends.org/2014/03/07/millennials-in -edad adulta/.

Datos separados de Pew del mismo estudio: Ibid.

Gil Luria, analista de Wedbush Securities: Michael J. Casey, "Los analistas de WedBush Securities Gil Luria y Aaron Turner hacen algunos grandes reclamos", en "BitBeat: Bitcoin sigue creciendo con cautela" en China ", Wall Street Journal, blog de MoneyBeat , 28 de mayo de 2014.

Glorivee Caban sabe una cosa o dos: Glorivee Caban, entrevistado por Michael J. Casey, 7 de agosto de 2014.

Visa, MasterCard y Western Union: recuentos de empleados tomados de los informes anuales de 2013 para Visa Inc., MasterCard Inc. y Western Union Holding Inc.

Capitalista de riesgo de Andreessen Horowitz: Chris Dixon, entrevista telefónica con Michael J. Casey, 25 de junio de 2014.

Se le pidió que describiera el mercado de trabajo: Daniel Larimer, entrevistado por Michael J. Casey, 8 de abril de 2014.

Como Tyler Cowen señaló en su libro: Tyler Cowan, El promedio ha terminado: impulsando a Estados Unidos más allá de la era del gran estancamiento (Dutton, 2013).

Robert Shiller de Yale: Joe Weisenthal, "Robert Shiller: Bitcoin es un ejemplo asombroso de una burbuja", Business Insider, 24 de enero de 2014, http://www.businessinsider.com/robert-shiller-bitcoin-2014-1#ixzz3Cmp0YFyx .

Nouriel Roubini de la Universidad de Nueva York: Erik Holm, "Nouriel Roubini: Bitcoin es un 'Juego de Ponzi'", 10 de marzo de 2014, Wall Street Journal, blog de MoneyBeat, http://blogs.wsj.com/moneybeat/2014/03/ 10 / nouriel-roubini-bitcoin-es-un-juego-ponzi /.

Ex secretario del Tesoro de EE. UU .: Lawrence Summers, entrevista telefónica de Michael J. Casey, 30 de abril de 2014.

En 2014, la Comisión Electoral Federal de EE. UU .: Michael J. Casey, "Las donaciones de la campaña Bitcoin obtienen luz verde de FEC", Wall Street Journal, blog MoneyBeat, 8 de mayo de 2014, http://blogs.wsj.com/moneybeat/2014 / 05/08 / bitcoin-campaign-donations-get-green-light-from-fec /.

De acuerdo con Make Your Laws: https://makeyourlaws.org/fec/bitcoin/pacs.

Conclusión: Pase lo que pase

para fijarlo en un número bajo, alrededor del 1 por ciento: Ben Popper, "Conoce al hombre que construye el Fort Knox de Bitcoin", Verge, 29 de agosto de 2014, http://www.theverge.com/2014/8/29/ 6082195 / the-fort-knox-de-bitcoin-xapo-wences-casares; también, Rob Wile, "CEO de Overstock: ahora estamos promediando $ 15,000 por día en ventas de Bitcoin", Business Insider, 13 de agosto de 2014, http://www.businessinsider.com/overstock-patrick-byrne-talks-bitcoin- ventas-2014-8.

solo alrededor de la mitad de los ciudadanos estadounidenses sabían: Paul Vigna y Michael J. Casey, "BitBeat: más gente sabe sobre Bitcoin, pero pocos dispuestos a usarlo", Wall Street Journal, blog de MoneyBeat, 27 de agosto de 2014, http: // blogs.wsj.com/moneybeat/2014/08/27/bitbeat-more-people-know-about-bitcoin-but-few-willing-to-use-it/.

Economistas como el de Boston University: Mark T. Williams, "Profesor de finanzas: Bitcoin podría convertirse en una amenaza existencial digna de una película de ciencia ficción", Business Insider, 13 de febrero de 2014, http://www.businessinsider.com/bitcoin- sovereign-attack-2014-2? op = 1; Paul Krugman, "Golden Cyberfetters", blog de The New York Times, Conscience of a Liberal, 7 de septiembre de 2011, http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfetters/.

Ya sabemos que Canadá: David George-Cosh, "Canadá cierra el plan MintChip, podría vender el programa de moneda digital", blog de Wall Street Journal, Canadá en tiempo real, 4 de abril de 2014, http://blogs.wsj.com/ canadarealtime / 2014/04/04 / canada-puts-halt-to-mintchip-plans-could-sell-digital-currency-program /.

Ecuador tiene previsto presentar: Daniel A. Media, "Introducción a la primera moneda digital nacional del mundo", Quartz, 4 de septiembre de 2014, http://qz.com/258989/introducing-the-worlds-first-national-digital- moneda/.

creación del navegador web Netscape: Eric Niiler, "Aniversario de IPO de Netscape y el boom de Internet", NPR, 9 de agosto de 2005, http://www.npr.org/templates/story/story.php?storyId=4792365.

por qué la grabadora de video Betamax fue técnicamente: Bill Hammack, "Cómo Betamax de Sony perdió ante la grabadora de video VHS de JVC", EngineerGuy.com, 17 de junio de 2014, https://www.youtube.com/watch?v=ddYZITaxlTQ.

el dolor de cabeza del seguimiento del impuesto a las ganancias de capital: Aviso 2014-21, Internal Revenue Service, 25 de marzo de 2014, http://www.irs.gov/pub/irs-drop/n-14-21.pdf.

Algunos de los estados más amigables con las criptomonedas: el sitio web BitLegal ofrece informes completos sobre el estado legal de Bitcoin en todo el mundo, http://www.bitlegal.net/index.php.

Wences Casares, CEO de bitcoin wallet: Entrevista realizada por Michael J. Casey, 12 de septiembre de 2014.

Gerente de inversiones y alta tecnología con sede en Zurich: Richard Olsen, entrevistado por Michael J. Casey, el 11 de diciembre de 2013 y el 13 de junio de 2014.

cuando el dólar se vuelve digital, "las fronteras nacionales son": Eswar Prasad, entrevistado por Michael J. Casey, 7 de febrero de 2014.

como el sistema de Bretton Woods de vinculación: MJ Stephey, "Sistema de Bretton Woods", Hora, 21 de octubre de 2008, http://content.time.com/time/business/article/0,8599,1852254,00.html.

"Si de repente todo el mundo comienza": Roger Ver, hablando en la Conferencia Norteamericana de Bitcoin, Miami Beach, 26 de enero de 2014.