El Pequeño Libro de Bitcoin

Por qué Bitcoin importa para tu libertad, tus finanzas y tu futuro

Timi Ajiboye
Luis Buenaventura
Alex Gladstein
Lily Liu
Alexander Lloyd
Alejandro Machado
Jimmy Song
Alena Vranova

Publicado por 21 Million Books
Redwood City, CA

Diseño e ilustración del libro por Luis Buenaventura.
“Ilustración “bloqueo venezolano” por Timi Ajiboye.

First Edition (Ed. 01-ES-201910181935)

ISBN 9781700678874

Contenidos

Prólogo

Somos activistas, educadores, emprendedores, ejecutivos, inversionistas e investigadores. Venimos de África, Asia, Europa, América del Norte y América del Sur. Discrepamos de muchas maneras, pero todos estamos fascinados por Bitcoin y el impacto que creemos que tendrá en nuestro mundo y en nuestras vidas.

En marzo de 2019, Jimmy habló con algunos de nosotros sobre la idea de hacer un sprint de libro, donde haríamos una reunión en un lugar aislado durante unos días para escribir un libro sobre Bitcoin y su importancia para la sociedad. Dos meses después, en el Oslo Freedom Forum, nos reunimos en una azotea en Noruega, rodeados por el emocionante zumbido de activistas de derechos humanos y periodistas de todos los continentes. La conversación inevitablemente condujo a Bitcoin y sus posibilidades de cambiar al mundo. Alex animó al grupo a escribir un libro explicando por qué Bitcoin importa sin usar el argot tecnológico que es tan común en los libros de este género. Queríamos ayudar a la persona curiosa a comprender el impacto humano de una de las innovaciones más profundas de nuestro tiempo. Unos meses después, los ocho nos reunimos en una casa en California para hacer realidad esta idea.

Lo que ahora tiene en sus manos es el resultado de ese esfuerzo de cuatro días. El objetivo de este libro es ayudarlo a comprender por qué hay problemas con el sistema monetario actual, por qué se inventó Bitcoin para proporcionar una alternativa, cómo cambiará la política y la sociedad, y lo que significa para el futuro.

Esperamos sinceramente que a medida que lea este libro, Bitcoin le sorprenda tanto como a nosotros.

8 de agosto de 2019
Redwood City, California

Sobre los Autores

Timi Ajiboye es un desarrollador de software y emprendedor que reside en Lagos, Nigeria. Es co-fundador y actualmente dirige BuyCoins (buycoins.africa), un portal de intercambio que permite a los africanos comprar y vender bitcoin fácilmente con su moneda local. Twitter: @timigod

Luis Buenaventura es co-fundador de BloomX (bloom.solutions), una startup en las Filipinas que está llevando el intercambio de criptomonedas al mundo emergente. Un autor y orador prolífico, también es el creador de Cryptopop.net, una iniciativa de arte que está volviendo las criptomonedas más accesibles al público en general. Twitter: @helloluis

Alex Gladstein es el Director de Estrategia de la Human Rights Foundation (hrf.org), una organización sin fines de lucro la cual promueve las libertades civiles y reta a los autoritarismos alrededor del mundo. También da conferencias sobre Bitcoin y gobernabilidad en la Singular University, y ha escrito sobre la intersección de la tecnología y la libertad en medios como TIME, CNN, y la Bitcoin Magazine. Twitter: @gladstein

Lily Liu es una empresaria y emprendedora. Recientemente fue co-fundadora y Directora de Finanzas de Earn.com, una plataforma que te permite ganar bitcoin en tu tiempo libre, la cual fue vendida a Coinbase en 2018. Anterior a esto, construyó un hospital en China, trabajó en KKR y McKinsey, y estudió en Stanford y Harvard. Twitter: @calilyliu

Alexander Lloyd ha estado invirtiendo en startups en fases iniciales desde 1998 y en 2008 fundó Accelerator Ventures. Su primer trabajo fue en Goldman Sachs en intercambio de divisas. En 2016, se unió a la junta de la Human Rights Foundation, donde se enfoca en Corea del Norte. Twitter: @alex01

Alejandro Machado es fundador de Open Money Initiative (openmoneyinitiative.org), una organización sin fines de lucro que investiga cómo la gente utiliza dinero en economías cerradas y sistemas monetarios colapsados. Está enfocado en mejorar el acceso al dinero digital para los venezolanos. Twitter: @alegw

Jimmy Song es un desarrollador de Bitcoin, educador y emprendedor. Es el autor de Programming Bitcoin (programmingbitcoin.com), publicado por O'Reilly. Está enfocado en llevar el dinero sólido al mundo. El color del sombrero de cowboy de Jimmy es un indicativo de si planea ser agradable o malo. Su clave pública PGP es C1D7 97BE 7D10 5291 228C D70C FAA6 17E3 2679 E455. Twitter: @jimmysong

Alena Vranova ha desarrollado negocios exitosos de servicios financieros desde 2003. Durante los últimos 7 años, ha estado ayudando a las personas y pequeños negocios a proteger sus bitcoins con productos y servicios sin custodio. En 2013, presentó Trezor, la primera billetera física de bitcoin, y actualmente es directora de estrategia de Casa (keys.casa), haciendo disponible para todo el mundo la seguridad personal de bitcoin, así como la soberanía financiera. Twitter: @AlenaSatoshi

Los autores en el Día 3 del sprint de libro.

Sobre los Traductor

Daniel Di Bartolomeo es abogado, especializado en derecho mercantil y traductor profesional certificado en la combinación inglés/español, Director de la agencia de traducción TuTraductorLegal.com. Es un apasionado de Bitcoin y se ofreció a realizar esta traducción a tasa preferencial y en un plazo muy corto, por lo cual los autores le estamos profundamente agradecidos.

CAPÍTULO UNO

¿Qué Hay de Malo con el Dinero Hoy en Día?

Es el año 1981.

En Manila, una joven mujer filipina trae al mundo a su primer hijo solo meses después de que se levante la ley marcial por primera vez en una década. El dictador Ferdinand Marcos habría de permanecer en el poder por unos años más, pero por ahora, los padres de Luis están preocupados únicamente por el bienestar de su joven familia. Tienen una pequeña cuenta de ahorros y han comenzado a guardar dinero seriamente por primera vez, preparándose para los años turbulentos por venir. La tasa de cambio es de siete pesos filipinos por un dólar americano.

Es el año 1993.

En Lagos, el General nigeriano Sani Abacha toma el poder y fija la tasa de un dólar americano a 22 nairas nigerianas. Es una movida agresiva que intenta estabilizar la economía evitando que la naira continúe su declive. La tasa fija da origen a una economía sumergida en la cual la naira se cotiza en un valor mucho más bajo. Al momento de la muerte de Abacha en 1998, los dólares cambian de manos en el mercado negro hasta por 88 nairas, cuatro veces la tasa oficial. Millones de personas sufren,

ya que no pueden costear los ascendentes precios de la comida con sus salarios estáticos fijados por el gobierno.

Es el año 2018.

A lo largo y ancho de la frontera vulnerable de Venezuela, los ciudadanos huyen de la inflación récord de 400.000% del país, cruzando a los países vecinos Colombia y Brasil. Más de 3 millones ya han escapado de la hambruna devastadora y la desintegración social.

Lorena, una panadera de 48 años, toma la difícil decisión de cruzar hacia Colombia. En la frontera, los guardias revisan sus pertenencias, buscando objetos valiosos que confiscar. No consiguen nada. No saben que Lorena tardó horas enrollando de forma cuidadosa los billetes de dólares americanos alrededor de ganchos de pelo y escondiéndolos en trenzas. Llega a un nuevo país, con la cabeza en alto.

En Manila, los padres de Luis ven que su suerte cambia para mal. La tasa de cambio actual es de 50 pesos filipinos por un dólar americano, y su ahorro paciente durante los años ha resultado en una pérdida generalizada del 80% de su riqueza. Con su retiro inminente, no tienen opción sino continuar trabajando y ahorrando para un futuro implacable e impredecible.

En Lagos, la naira está en un período de estabilidad relativa tras perder otro 50% frente al dólar. Los precios de los bienes locales han subido hasta las nubes de nuevo. Nadie confía en que el gobierno pueda evitar otra crisis económica, ni siquiera los funcionarios gubernamentales mismos.

Es el año 2019.

En Shanghai, una joven profesional llamada Annie envía un mensaje a uno de sus amigos en WeChat, la plataforma de red social utilizada diariamente por más de mil millones de chinos. Su amigo menciona que está en problemas por fumar mari-

huana, y en la mitad de la conversación, repentinamente él deja de responder.

Al día siguiente, un par de policías en ropa de civil visitan a Annie en su oficina y le piden que vaya con ellos. Sus compañeros de trabajo la ven irse y luego desaparece por varias semanas. Cuando vuelve a ponerse en línea, ha perdido algunas de las características de pago de WeChat. Ya no puede comprar billetes de avión o de tren. Su récord crediticio se desploma. Su vida está arruinada por una cadena de mensajes de texto.

En Oakland, Alex entra a una tienda de mascotas buscando comida para perros. Encuentra lo que está buscando, más un producto nuevo interesante, uno que le promete mejorar el aliento de su perro. Desliza su tarjeta Visa del Chase para pagar por la comida y sale. Unos minutos después, revisa Twitter, y le aparece una publicidad de golosinas para perros justo como la que acababa de comprar. Descubre que el Chase comparte información sobre sus pagos diarios con empresas externas.

Alex se da cuenta de que los detalles de su vida personal están siendo entregados a anunciantes con una sensación de intranquilidad muy similar a la de todos los de la generación de los teléfonos móviles inteligentes. Inclusive en los EE.UU, la privacidad financiera está desapareciendo.

Estas son historias de cómo el dinero está descompuesto.

Los padres de Luis y millones de personas de la clase media filipina y nigeriana vieron cómo sus ahorros se evaporaban en cámara lenta en una misma generación. Lorena necesitó de una forma de llevar sus escasos ahorros a un nuevo hogar en Colombia sin que fuesen confiscados, por lo que se volvió creativa con su estilo de peinado. Annie ahora se encuentra en la "cárcel financiera" porque uno de sus amigos fumó marihuana. Las compras de Alex son monitoreadas y revendidas a diversas corporaciones con cada deslizada de su tarjeta de crédito.

Estos casos no son únicos.

Desde el año 2000, casi todas las monedas han perdido un valor significativo frente al dólar americano. Varias, como el rand sudafricano, el peso argentino, la lira turca, y la corona checa han perdido casi el 50%. Algunas pocas desafortunadas como la grivna ucraniana o el peso dominicano han perdido hasta un 70%. Incluso el dólar americano y el Euro han perdido el 33% de su poder adquisitivo en ese período.

Alrededor del mundo, 250 millones de migrantes y refugiados luchan por enviar dinero a casa o llevárselo consigo a nuevas fronteras. Unos dos mil millones de personas no tienen acceso a cuentas bancarias o no tienen la identificación oficial necesaria para obtener una. En una economía cada vez más globalizada, el dinero sigue siendo tercamente local.

Mientras tanto, en las super ciudades como Shanghái o San Francisco, la sensación desconcertante de ser observado es palpable.

Por un lado, el Gran Hermano está mirando. Por el otro, el capitalismo vigilante registra cada compra y vende la data a docenas de compañías sin el permiso del comprador. La privacidad ahora es un lujo, el cual parece ser más caro con el pasar de los días.

¿Qué es el dinero?

En esencia, es un pacto social.

El dinero requiere que las personas confíen en que los billetes en sus carteras, los dígitos en sus cuentas bancarias y los saldos en sus tarjetas de regalo son canjeables en el futuro por las cosas que desean o necesitan. El vendedor debe aceptar que el dinero del comprador es valioso.

A lo largo de la historia, las sociedades han experimentado con diversas formas de llevar a cabo este acuerdo, utilizando de todo, desde conchas marinas, sal y oro, hasta los complejos sistemas de banca central que se utilizan actualmente. Algunos tipos de dinero son más sólidos que otros, lo que significa que mantienen mejor su valor con el tiempo.

Instintivamente, todos saben que el dinero importa y que quieren tener el dinero más sólido posible. Debido a que la mayoría de las personas intercambian su trabajo por dinero, viene a representar el tiempo y el esfuerzo de una persona. El dinero es el medio a través del cual el trabajo se convierte en bienes y servicios en el presente y el futuro. En este sentido, el acceso al dinero sólido es una de las formas más duraderas de poder personal.

El dinero también es muy importante para el gobierno. Debido a que las economías de hoy están organizadas por estados nacionales, los gobiernos tienen el poder de controlar el dinero. Sin embargo, el control del dinero puede ser algo tentador de lo que abusar. Los funcionarios a menudo manipulan este poder para satisfacer sus intereses. Solo los gobiernos más democráticos, que protegen los derechos individuales, la separación de poderes y el estado de derecho, pueden protegerse eficazmente contra el abuso monetario, como la inflación galopante, la confiscación arbitraria y la corrupción.

¿Cómo Funciona el Dinero Moderno?

Todas las monedas nacionales en circulación hoy se denominan monedas fiduciarias, que en latín significa “por decreto”. El valor de estas monedas se establece mediante el decreto de los Estados-nación que las emiten y aceptan. Dado que los gobiernos pueden crear más moneda fiduciaria a bajo costo,

es posible imprimir nuevas unidades de moneda ad infinitum cuando lo deseen.

Alan Greenspan, ex presidente de la Reserva Federal de los Estados Unidos, dijo que Estados Unidos puede "pagar cualquier deuda que tenga porque siempre podemos imprimir dinero para hacerlo". Esta práctica puede causar problemas, incluso en las economías más estables del mundo. La moneda nacional más antigua es la libra esterlina del Reino Unido, que ha perdido el 99.5% de su poder adquisitivo en los últimos 300 años. El dólar estadounidense ha perdido el 90% de su poder adquisitivo en el siglo pasado.

Un filete que costó $0.36 en 1925 costaba $3 en la década de 1990 y cuesta $12 hoy. Y estas son algunas de las monedas fiduciarias más estables que existen. La moneda fiduciaria promedio tiene una vida útil de solo 27 años.

La inflación baja y estable es el objetivo de los bancos centrales modernos, y ha habido diferentes períodos de éxito según el país. Sin embargo, la mayoría de las monedas sufren una alta inflación a largo plazo, lo que puede ser devastador para el ahorro. Esto es especialmente cierto para aquellos que no pueden pagar activos duros, como bienes raíces o acciones de primera línea, cuyos valores aumentan con la inflación. La alta inflación puede dificultar que todos, excepto los ricos, ahorren para el futuro.

Para miles de millones de personas que viven bajo regímenes autoritarios, el valor de sus ahorros disminuye debido a las decisiones de los funcionarios gubernamentales no elegidos. Solo la élite puede acceder a dólares, oro o bienes inmuebles para preservar el valor. Mientras tanto, los ciudadanos de las democracias ricas disfrutan de algunas protecciones importantes. Tienen fácil acceso a una moneda relativamente estable como el dólar o el euro. Sus economías tienden a tener un buen desempeño, por lo que es más probable que tengan un trabajo

que pague bien con el tiempo. También tienen acceso a una gama de productos de inversión para compensar o superar la inflación.

El efecto de que la élite se beneficie desproporcionadamente del dinero recién impreso es tan frecuente que hay un término para ello: el efecto Cantillon. Lleva el nombre de Richard Cantillon, un economista del siglo XVIII que notó este efecto mientras trabajaba como banquero en el Reino Unido. La inflación dramática o a gran escala puede ser una forma injusta de distribuir la riqueza, ya que inevitablemente beneficia a los que ya tienen a expensas de los que no tienen. Y aunque sus efectos pueden no ser evidentes para la persona promedio en los Estados Unidos o el Reino Unido, miles de millones de ciudadanos los sienten dolorosamente en países con economías menos estables.

Los sistemas monetarios fiduciarios también han sido facilitadores de las guerras prolongadas de la era moderna. Los gobiernos pueden imprimir más dinero para la guerra, distribuyendo el costo a las generaciones futuras a través de la inflación. Esto significa guerras más largas y más caras. La Primera Guerra Mundial es un ejemplo trágico, ya que los principales actores financiaron las etapas posteriores de las guerras con la inflación. Tanto Rusia como Alemania suspendieron el patrón oro, donde sus monedas fiduciarias eran convertibles a una cantidad fija de oro. En cambio, suspendieron la convertibilidad e imprimieron dinero sin respaldo para continuar luchando. Como resultado, la guerra terminó durando mucho más de lo que nadie creía posible. Cuando Alemania perdió, la única forma de pagar las enormes reparaciones fue imprimiendo aún más dinero. Para 1923, el marco alemán se depreció a una billonésima parte de su valor anterior a la guerra, preparando el escenario para la Segunda Guerra Mundial.

Un gasto despilfarrador similar también es evidente en los últimos tiempos. Independientemente de lo que se pueda

pensar sobre la participación militar de Estados Unidos en Afganistán e Irak, los costos de estas invasiones superan los $5,9 billones. Esto asciende a más de $46.000 por hogar si se le hubiera pedido al contribuyente estadounidense que financiara la guerra directamente.

Otra cuestión del sistema monetario moderno es que puede ser extremadamente difícil mover dinero entre diferentes naciones del mundo. Los gobiernos de países como China, Rusia, Argentina e Indonesia han restringido agresivamente la cantidad de dinero que sus ciudadanos pueden intercambiar, transferir o llevar al extranjero.

Esto se realiza principalmente mediante el control de la capacidad de cada individuo para cambiar su moneda local por moneda extranjera como el dólar estadounidense. Al ciudadano chino promedio, por ejemplo, solo se le permite convertir hasta $50.000 de su renminbi cada año.

En otras partes del mundo, incluso la capacidad de acceder localmente al propio dinero puede verse severamente limitada. Después de su crisis financiera de 2015, a los ciudadanos griegos se les restringió retirar más de 60 euros por día de sus cuentas bancarias, un claro recordatorio de que no controlaban su dinero.

Incluso cuando las personas pueden enviar dinero al extranjero, es engorroso y costoso. En 2018, los trabajadores migrantes y los refugiados enviaron casi $700 mil millones a través de las fronteras en remesas para apoyar a sus seres queridos. Los tipos de cambio y los aranceles se consumieron $45 mil millones de ese dinero, una cantidad enorme para aquellos que no tienen dinero de sobra.

Un Punto Único de Fallo Global

Todos los bancos centrales representan un punto único de fallo para sus economías nacionales. La Reserva Federal de los Estados Unidos actúa, en cierto modo, como un banco central para todos los bancos del mundo. Para los estadounidenses, este acuerdo parece funcionar muy bien. El dólar se acepta en todas partes, y para la mayoría de las personas es fácil abrir cuentas bancarias, obtener líneas de crédito y pagar bienes y servicios. La mayoría de los estadounidenses no sufren notablemente la inflación.

La economía dinámica de los Estados Unidos ayuda a apuntalar y alimentar el sistema económico global de hoy. En su corazón está el patrón del dólar, una hegemonía monetaria global que comenzó con un evento poco conocido en un hotel de New Hampshire en 1944 llamado el Acuerdo de Bretton Woods.

Las potencias mundiales organizaron una reunión en Bretton Woods para establecer un orden monetario unificador a medida que la Segunda Guerra Mundial llegaba a su fin. Durante tres semanas, más de 700 delegados de 44 países debatieron y negociaron la estructura del futuro sistema financiero. Algunos delegados sugirieron la creación de una nueva moneda de reserva internacional llamada bancor. Al final, los delegados acordaron que sus monedas estarían vinculadas al dólar estadounidense. Como resultado, el comercio internacional actual se liquida principalmente en dólares, y cada país trata de mantener una reserva de dólares.

La naturaleza central del dólar estadounidense para el sistema económico mundial se revela en la forma en que el dinero se mueve entre países. Tomemos, por ejemplo, el envío de dinero desde Corea del Sur a Filipinas. Por lo general, no es

posible que el won coreano se cambie directamente por pesos filipinos porque los dos países no tienen suficientes monedas del otro a la mano. En cambio, dependen del dólar y una serie de transacciones. Primero, el won coreano se vende por dólares en Seúl. Esos dólares se transfieren de un banco surcoreano a uno filipino a través de un banco estadounidense. Finalmente, el banco en Manila convierte los dólares a pesos filipinos. Esto toma al menos unos días e incurre en tasas de cambio y transacción que pueden variar desde un pequeño porcentaje para rutas populares hasta dígitos dobles bajos para las menos populares. El costo promedio global para este tipo de pagos transfronterizos se mantiene por encima del 7%, incluso para pequeñas remesas.

Si bien el mundo se ha beneficiado de muchas maneras de tener el patrón del dólar, también ha resultado en una fragilidad por la cual cada economía depende de alguna manera del dólar estadounidense y es vulnerable a su colapso. Esto da como resultado un sistema donde un puñado de quiebras bancarias en los EE. UU puede conducir a una catástrofe económica mundial.

El Fin de la Privacidad Financiera

La digitalización del dinero en las últimas dos décadas ha resultado en niveles cada vez menores de privacidad personal, con cada transacción ahora explotada para control político y potencial comercial. El dinero electrónico ha existido durante mucho tiempo, pero solo recientemente ha sido posible el análisis de big data necesario para llevar a cabo una vigilancia masiva de manera efectiva. Ni las compras en línea ni las físicas son seguras, ya que los gobiernos y los anunciantes aprovechan cada vez más los perfiles de las preferencias, decisiones y conexiones de cada individuo. Estos perfiles son como huellas de datos, exclusivos de cada persona, y se vuelven más refi-

nados y fácilmente identificables con cada nueva compra. Esto ha llevado a un mundo en el que una búsqueda en Google de un producto puede generar anuncios de Facebook e Instagram para ese mismo producto minutos después.

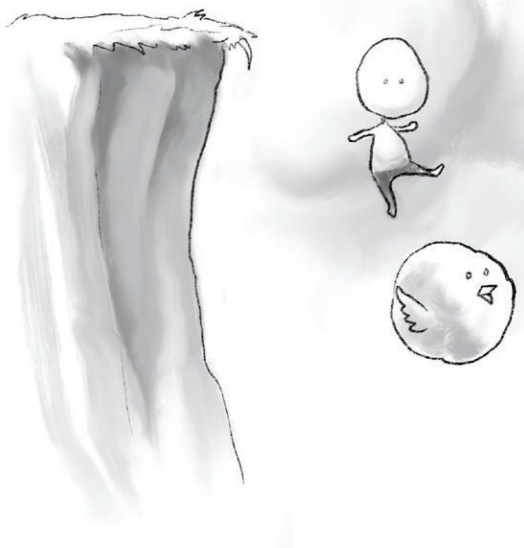
Dependiendo de la ubicación de la persona, las huellas digitales personales pueden tener repercusiones peligrosas. En el verano de 2019, los estudiantes en Hong Kong se unieron por decenas de miles para protestar contra un nuevo proyecto de ley que permitiría al gobierno chino extraditar a cualquiera a Pekín sin el debido proceso. Sabían que, si usaban sus tarjetas Octopus asociadas a la identificación de estudiante para navegar por el sistema de metro, sus ubicaciones serían reveladas, por lo que, en cambio, utilizaron dinero en efectivo para comprar billetes de un solo uso. Esta es una opción segura por ahora, pero el dinero de papel y metal está en camino de ser eliminado de la mayoría de las principales áreas urbanas durante la próxima década. En ese punto, no habrá forma de utilizar los sistemas de transporte público sin revelar la ubicación personal de uno a las autoridades y corporaciones. Las huellas digitales estarán en todas partes. La reacción pública al seguimiento corporativo y gubernamental de comportamiento de gasto de los ciudadanos oscila. Algunos simplemente lo consideran inquietante, otros lo denuncian como una violación importante de la privacidad, mientras que a la mayoría no parece importarle en absoluto. De cualquier manera, el hecho es que más allá de controlar el suministro de dinero y dónde se puede enviar el dinero, las autoridades ahora pueden aprender prácticamente todo sobre compradores y vendedores. Los sistemas de pago cada vez más digitales del mundo podrían llevar a la extinción de la privacidad personal.

¿Existe otra Forma?

Cuatro fenómenos globales - la devaluación de la riqueza personal, la restricción de la transferencia de valor, la centralización financiera y la pérdida de privacidad - representan riesgos importantes para la persona mientras navega por el sistema monetario del siglo XXI. Las personas de todo el mundo sienten la presión mientras los países luchan por mantener el status quo.

¿Qué pasaría si surgiera un nuevo sistema en el que los gobiernos no tuvieran la capacidad de devaluar arbitrariamente el dinero y las corporaciones sin rostro no pudieran congelar los fondos de los usuarios o negarse a procesar las transacciones? ¿Qué pasaría si el dinero fuera completamente digital, pudiendo ser utilizado por cualquier persona con acceso a Internet desde cualquier lugar del mundo, sin necesidad de pedir permiso a las autoridades?

A raíz de la crisis financiera de 2008, alguien decidió construir exactamente ese sistema, preparando el escenario para la próxima gran revolución financiera.



CAPÍTULO 2
¿Qué es Bitcoin?

El 15 de septiembre de 2008, el reconocido banco de inversión Lehman Brothers se declaró en lo que sería la quiebra más grande en la historia de los Estados Unidos. El colapso de Lehman Brothers, fundado en 1850, fue la culminación de un atracón de préstamos globales. La compañía había arriesgado mucho más que el valor total de la empresa en valores respaldados por hipotecas, incluidos muchos préstamos de alto riesgo. Cuando los propietarios dejaron de hacer los pagos de la hipoteca, la empresa se declaró insolvente y no pudo recuperarse.

De repente, la confianza que los bancos habían establecido en Lehman Brothers y en los demás se evaporó. En medio de esta crisis crediticia, a las empresas les resultó difícil obtener préstamos para financiar sus actividades. Sin fondos para comprar inventario, invertir en nuevos equipos o pagar a los empleados, parecía que las empresas en muchas industrias no podrían continuar operando. Una espiral viciosa hacia abajo parecía inminente.

El Tesoro de los Estados Unidos y la Reserva Federal actuaron rápidamente para evitar el desastre económico prestando dinero a los bancos para mantener a flote el sistema financiero. El 3 de octubre de 2008, el Congreso rescató a varios bancos en problemas con la Ley de Estabilización Económica de Emergencia de 2008. El gobierno gastó cientos de miles de millones de dólares para sacar a la superficie a un sector financiero colapsado.

Aparece Bitcoin

El 31 de octubre de 2008, unas pocas semanas después de que el gobierno de los EE. UU autorizase $700 mil millones para rescatar a los bancos, una persona desconocida o un grupo de personas que se hacía llamar Satoshi Nakamoto publicó un informe técnico o whitepaper que describía un nuevo sistema de pago electrónico llamado Bitcoin. Satoshi presentó el white-paper a una lista de correos electrónicos de investigadores de criptografía llamada cypherpunks, un grupo de activistas de la privacidad que crean herramientas para desafiar la vigilancia y el abuso del poder estatal.

El whitepaper tenía dos puntos importantes de intriga. Primero, el autor eligió usar un seudónimo. La identidad de Satoshi sigue siendo un misterio de interés popular hasta el día de hoy. En segundo lugar, el documento introdujo algo que nunca antes había existido: dinero digital que no dependía de una autoridad central. Pocos pensaron que un avance de este tipo fuera posible.

Unos meses más tarde, Satoshi lanzó la red Bitcoin y dejó una pista de por qué en una sola línea de texto, incrustada en la primera entrada del libro de contabilidad de Bitcoin:

The Times 03 / Ene / 2009 Ministro
a punto del segundo rescate para bancos

Esto se refería a un titular que apareció el 3 de enero de 2009 en The Times, un destacado periódico del Reino Unido. El mensaje de Satoshi al mundo fue que el sistema actual, donde los bancos fueron rescatados a expensas de la gente, se descompuso. La nueva tecnología financiera descentralizada de Bitcoin se creó para ser una salida.

Para comprender la innovación científica detrás de Bitcoin, primero es esencial comprender la escasez.

Dos Tipos de Escasez

En el ámbito físico, hay dos formas de escasez. La primera es hecha por el hombre y, en ese sentido, artificial: coleccionables como carteras Chanel de edición limitada, tarjetas de baloncesto Michael Jordan, cosechas raras de vino u obras de arte numeradas de un artista en particular. Esto también se llama escasez centralizada. Tenga en cuenta que estos artículos tienden a tener problemas de falsificación.

El segundo tipo de escasez es natural. Esta categoría incluye sal (el origen de la palabra salario), esferas de vidrio de Ghana, conchas marinas de la cultura nativa americana, plata de China y, por supuesto, oro en todo el mundo. Estos son ejemplos de escasez descentralizada y tienden a ser más difíciles de falsificar.

No es casualidad que los productos descentralizados y escasos como la sal y el oro se hayan utilizado como dinero. Primero, hay cierta justicia en utilizar un producto que ninguna persona o grupo controla. En segundo lugar, estos productos son mucho más difíciles de falsificar. Por último, la escasez ayuda a mantener las transacciones económicas fáciles de realizar, ya que no es necesario llevar cantidades irracionales para comprar algo.

Lo que diferencia las dos formas diferentes de escasez es el control. La escasez centralizada es creada por una empresa o persona, ya sea el Banco Popular de China, la Reserva Federal, un artista o una gran corporación multinacional. Esa entidad, o autoridad central, controla completamente la escasez de una mercancía mediante la creación, emisión, recompra y confiscación.

Los productos escasos descentralizados se crean por naturaleza, lo que significa que no existe una autoridad central que los produzca. No hay elaboración, más bien, el proceso es más parecido a recolectar o cosechar. Para extraer una mercancía

naturalmente escasa como el oro o el petróleo, un minero extrae lo que ya existe del suelo.

En el caso del oro, su acumulación históricamente no ha necesitado permiso de nadie que no sea el propietario de un sitio minero. En otras palabras, no hay un centro desde el cual todo el oro comience su vida y ninguna autoridad global facultada para restringir la minería o aumentar el suministro.

Esta es la distinción clave entre productos escasos centralizados y descentralizados, particularmente los que se utilizan como dinero.

Por Qué la Descentralización puede ser Algo Bueno para El Dinero

Como se mencionó anteriormente, una de las características ineludibles del dinero centralizado es que el creador puede inflar arbitrariamente la oferta, imprimiendo más por capricho. Si bien esto se hace con mucha más frecuencia y en mayor medida por los regímenes autoritarios que por las democracias, es algo que ocurre en todas las sociedades.

En la película Bugsy, el personaje principal vende acciones en papel del casino Pink Flamingo a los inversionistas una y otra vez. A cada persona le vende el 20% del casino por $10.000. Lo hace con más de una docena de inversionistas, tergiversando cuánto del casino han comprado. Cada inversionista supone que ahora posee el 20% del casino, pero en realidad posee mucho menos. Bugsy, sin embargo, se beneficia, ya que obtiene mucho más dinero.

Cada producto centralizado enfrenta el mismo problema de incentivos. La autoridad central puede crear más de la mercancía, diluyendo el valor para todos los demás propietarios. Los bancos centrales que imprimen más dinero generalmente lo hacen con objetivos positivos como construir infraestruc-

tura, apoyar programas de bienestar social o estabilizar una crisis económica. Sin embargo, recuerde el efecto Cantillon del Capítulo 1: incluso el uso razonable de este poder puede resultar en beneficios para los ricos y poderosos a expensas de los pobres e impotentes. La capacidad de imprimir dinero crea un riesgo moral.

Por supuesto, la dilución también puede suceder con el dinero descentralizado. La nueva tecnología puede hacer que la recolección de una mercancía rara que se produce naturalmente sea más barata y, como resultado, el mercado puede inundarse con una nueva oferta. Una vez que una mercancía pierde su escasez, se vuelve mucho más débil y menos sólida. Es por eso que la sal y las conchas marinas y las esferas de vidrio ya no se usan como dinero. Cada uno solía ser difícil de reunir a escala, pero su colección ahora es extremadamente fácil y barata debido a la innovación tecnológica.

El oro es una de las pocas excepciones y continúa manteniendo su valor notablemente bien incluso después de miles de años de minería. Si bien el oro tiene algunos usos industriales y decorativos, su dificultad minera histórica ha significado un dinero relativamente sólido cuyo poder adquisitivo estable lo ha convertido en una muy buena reserva de valor. Incluso hoy, la joyería de oro se usa en algunos países como una forma de protegerse contra las crisis económicas. La principal desventaja del oro es su aspecto físico y su peso, ya que el almacenamiento, la seguridad y la transferencia pueden ser un desafío.

Muchos defensores de Bitcoin creen que eventualmente puede reemplazar al oro como el depósito de valor preferido para los ahorros a largo plazo. Como lo mostrará este Capítulo, es descentralizado y más escaso que el oro, pero también es mucho más fácil de transportar y almacenar de forma segura.

Escasez Digital Descentralizada

Con el advenimiento del Internet, la información finalmente podría digitalizarse y distribuirse a gran escala. Copiar un archivo digital es mucho más fácil y económico que replicar algo en el mundo físico.

La digitalización del dinero fue una innovación necesaria para el comercio electrónico, eliminando la necesidad de transferencia física. Todo se puede enviar a la velocidad del correo electrónico o la carga de una página web, lo que reduce la fricción y permite que el comercio sea verdaderamente global. Los bancos crean versiones digitales del dinero fiduciario y luego las procesan las redes de tarjetas de crédito (Visa, MasterCard), las empresas minoristas (Alibaba, Amazon, Apple) e incluso los procesadores de pagos nativos de Internet (WeChat, PayPal, Square).

Como son los únicos árbitros de cómo se usa su dinero, todas estas empresas pueden censurar las transacciones. Pueden incautar dinero y cerrar cuentas, y muchas veces lo hacen sin el consentimiento del cliente. Además, dado que son estructuras centralizadas, estas empresas suelen ser objeto de presiones gubernamentales o incluso ataques de piratería que pueden provocar la pérdida de fondos o datos de los clientes. Antes de Bitcoin, esta era la compensación inevitable para el dinero digital: tenía que ser artificialmente escaso o estar controlado por las autoridades centrales. No parecía haber una forma de crear escasez en el ámbito digital.

Satoshi Nakamoto reveló un gran avance el 31 de octubre de 2008, al presentar Bitcoin como una nueva moneda digital cuya escasez se basa en el hecho de que hay elementos escasos en el ámbito digital: números escasos.

Algunos de los números más escasos son números primos. Un número primo, como 2, 3 o 5, solo se puede dividir por 1 y por sí mismo.

Los premios se vuelven cada vez más escasos a medida que aumentan los números. Por ejemplo, entre 1 y 100, hay 25 números primos. Entonces, usted esperaría que hubiesen 250 números primos entre 1 y 1-000, pero solo hay 168. Los números primos se vuelven increíblemente escasos después de 100 mil millones, tanto que sigue habiendo una búsqueda matemática global en curso para el número primo más grande.

En la red Bitcoin, la producción de nuevos bitcoins se produce a través de una competencia global en la que los participantes buscan números escasos, como los números primos. Esto permite la escasez descentralizada en el ámbito digital. Esto es lo que hace que la invención de Satoshi sea tan profunda. Todos los activos anteriores a Bitcoin estaban totalmente centralizados (oro de World of Warcraft), físicos (plata) o infinitamente abundantes (MP3). Un activo descentralizado, digital y escaso simplemente no existía antes de Bitcoin.

Minería de Bitcoin: Procesamiento de Pagos Descentralizado

La naturaleza descentralizada de Bitcoin se basa en el hecho de que es un bien natural escaso como el oro y es difícil de extraer. Al igual que la minería de oro, la minería de Bitcoin es la búsqueda de algo muy escaso en medio de lo mucho más común. Una vez que un minero de Bitcoin encuentra el número escaso correcto, otros pueden verificarlo de manera barata y fácil, al igual que el oro puede distinguirse con relativa facilidad del oro de los tontos.

En lugar de usar picos y máquinas de excavación para buscar oro, los mineros de bitcoin usan computadoras poderosas para

buscar números escasos particulares. Una vez encontrado, cada número escaso se llama prueba de trabajo porque le prueba a todos que se trabajó mucho para encontrarlo.

Al igual que con el oro, no se requiere permiso de una autoridad central para extraer: cualquiera puede descargar software de minería para comenzar a buscar números escasos que cumplan con los criterios.

Incluso mejor que la minería de oro, no se requiere un tipo especial de tierra, solo equipos informáticos y una fuente de energía asequible. Como resultado, los mineros de todo el mundo buscan de forma independiente en una competencia para encontrar pruebas de trabajo que cumplan con los criterios requeridos por la red Bitcoin.

Por lo tanto, Bitcoin se ejecuta sin un punto único de falla. Compare esto con los sistemas centralizados. Si la red Visa se cae, nadie puede pagar nada con sus tarjetas Visa. Lo mismo sucedería con Paypal o Amazon si sus respectivas redes dejaran de funcionar. A diferencia de estas compañías, Bitcoin no tiene autoridad central ni punto único de falla. Nadie puede elegir censurar una transacción en particular. La red imparable de mineros de Bitcoin proporciona un servicio crítico, procesando transacciones sin las vulnerabilidades de una autoridad central.

Cómo Funcionan las Transacciones de Bitcoin

¿Entonces cómo funcionan las transacciones de Bitcoin?

Para entender esto, considere algo que probablemente sea más familiar: el sistema de contabilidad de un banco. Después de que alguien emite un cheque para pagar un bien o servicio, el destinatario va a su banco a depositar el cheque. Suponiendo que ambos clientes tengan una cuenta en este banco, el banco solo tiene que debitar la cuenta del remitente y acreditar la

cuenta del receptor. Todo el proceso requiere agregar solo dos entradas en el libro de contabilidad del banco. Los funcionarios del banco no entran en una bóveda, sacan la cantidad exacta del alijo de monedas y billetes del remitente y luego lo colocan en el alijo de monedas y billetes del receptor. La contabilidad utilizando un libro mayor fue un invento histórico clave que hizo que la transferencia de dinero fuera mucho menos laboriosa. El equivalente de un cheque bancario en bitcoin es una transacción.

Bitcoin maneja un tipo especial de libro mayor llamado blockchain o cadena de bloques. Miles de personas que ejecutan el software de validación de Bitcoin verifican la cadena de bloques continuamente en lugar de una autoridad central. Cada persona que ejecuta el software guarda una copia de todo el libro mayor y verifica las nuevas entradas. Esto se llama ejecutar un nodo completo. Cada nodo completo verifica constantemente para hacer cumplir las mismas reglas de Bitcoin, y de esta manera, ninguna autoridad central puede editar arbitrariamente los registros para robar bitcoin o gastar bitcoin que no tienen. La cadena de bloques de Bitcoin se conoce como una cadena de bloques pública porque cualquiera puede ver el registro de las transacciones.

Los propietarios de Bitcoin realizan transacciones de la misma manera que podrían escribir un cheque. Especifican la cantidad y luego firman el cheque. Pero en lugar de garabatear sus nombres en un papel fácilmente falsificable, los propietarios de bitcoins firman sus transacciones con una firma digital mediante criptografía.

Esta firma digital se crea utilizando un secreto sólo conocido por el propietario de los bitcoins. Ese secreto se llama clave privada. Con la clave privada, el remitente puede hacer una firma digital que demuestre al receptor que el remitente posee los bitcoins.

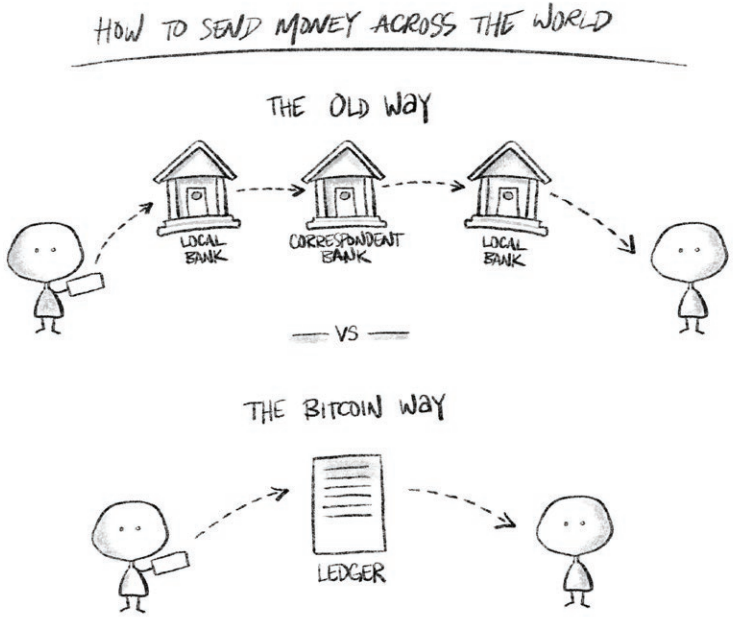
Los usuarios almacenan sus bitcoins en una billetera, que es un software que se ejecuta en una computadora, teléfono o hardware especializado. Cada segundo, las nuevas transacciones de Bitcoin se inician desde billeteras de todo el mundo, pero no hay un procesador central de pagos. En cambio, los mineros de todo el mundo compiten para registrar transacciones en el libro mayor. Ejecutan sus equipos informáticos y tratan de encontrar un número escaso en particular. Cada 10 minutos aproximadamente, un minero de Bitcoin en algún lugar del mundo encuentra una prueba de trabajo y la combina en un bloque con un grupo de transacciones que han estado esperando ser procesadas. El minero luego envía este bloque a la red Bitcoin para su validación.

Cada bloque es como una nueva página en el libro mayor global de Bitcoin, y los nodos completos en la red verifican que las transacciones contenidas en el mismo sean válidas. Cualquiera puede ejecutar un nodo completo, por lo que miles de usuarios verifican constantemente la validez de cada nuevo bloque. Si la red confirma que el bloque propuesto por un minero es válido, entonces el minero recibe una recompensa de 12.5 bitcoins nuevos, y el bloque y todas las transacciones que contiene se convierten en una parte permanente de la historia de Bitcoin. Al momento de escribir este artículo, una transacción típica de Bitcoin tarda menos de una hora en completarse en la cadena de bloques.

La cadena de bloques de Bitcoin recibe su nombre del hecho de que es la colección de todos los bloques, o todas las páginas, en el libro de contabilidad histórico. En otras palabras, blockchain es el libro de contabilidad completo e inmutable de todas las transacciones en la red de Bitcoin desde su creación en enero de 2009.

Hay miles de nodos completos que forman la red de Bitcoin. Cada nodo completo valida independientemente los

nuevos bloques propuestos por los mineros. Los requisitos bastante modesto sde hardware significan que la mayoría de las computadoras portátiles modernas pueden ejecutar un nodo completo de Bitcoin. Dado que ejecutar nodos completos sigue siendo relativamente barato y asequible, la red permanece descentralizada.



La Política Monetaria de Bitcoin

A diferencia del sistema actual de la banca central, que es opaco y cambia constantemente, la política monetaria de Bitcoin es transparente e inamovible.

¿Cómo se emiten los nuevos bitcoins? Como se mencionó, un minero que encuentra una prueba de trabajo válida y la combina con un grupo de transacciones válidas - haciendo

un nuevo bloque válido - tiene derecho a lo que se llama la recompensa del bloque. Al momento de escribir este artículo, la recompensa en bloque es de 12.5 bitcoins y se reduce a la mitad cada cuatro años, lo que significa que la recompensa será de 6.25 bitcoins en 2020, 3.125 bitcoins en 2024, y así sucesivamente.

Si un minero intenta hacer trampa y reclamar una recompensa por encima de la recompensa de bloque programada, ese bloque es rechazado por todos los nodos completos que verifican el bloque. Los nodos completos verifican todos los bloques propuestos y los que no siguen las reglas no se colocan en sus cadenas de bloques. Esto es similar a cuando un banco rechaza un cheque que sobregira la cuenta remitente. Como resultado, nadie puede falsificar bitcoins falsos. Cualquier transacción fraudulenta que intente gastar bitcoins que no existen y cualquier bloque que contenga dichas transacciones será rechazado por los nodos completos.

Un bloque inválido es costoso para los mineros, ya que es rechazado y se desperdicia la gran cantidad de electricidad que gastaron en el funcionamiento de su equipo informático para encontrar la prueba de trabajo. Esto hace que el fraude sea muy costoso y protege la red de Bitcoin. Aún así, si solo hubiera unos pocos nodos completos en la red de Bitcoin, un minero podría obtener un bloque fraudulento en la cadena de bloques sobornando a esos pocos nodos completos. Dado que hay varios miles de nodos completos en la red, y dado que están dispersos geográficamente y son desconocidos entre sí, es casi seguro que dicha estrategia fracasará.

Satoshi estableció el suministro total de todos los bitcoins desde el inicio en 21 millones. Hoy, más del 85% de todos los bitcoins ya se han extraído, lo que significa que más de 17 millones están ahora en circulación. El resto se lanzará como recompensa para los mineros en trozos cada vez más pequeños en un cronograma conocido públicamente.

Tecnología Blockchain: Aún a la Espera

Muchos han tratado de replicar el éxito de la invención de Satoshi. Una estrategia popular es tomar el sistema de contabilidad blockchain de Bitcoin y aplicarlo a otros casos prácticos. Desde 2014, muchas compañías conocidas han tratado de usar una cadena de bloques en varias industrias, invirtiendo muchos millones de dólares en el esfuerzo. Esto ha generado mucha publicidad y atención de los medios sobre la tecnología blockchain.

Desafortunadamente, la mayoría de estos intentos hasta ahora son comparables al uso de un montacargas para hacer las compras de supermercado. El vehículo funciona perfectamente bien dentro de su contexto original (almacenando el libro mayor para dinero digital descentralizado), pero parece ser demasiado lento, innecesariamente derrochador o no funcional para otras aplicaciones (es decir, atención médica en la cadena de bloques, seguimiento de frutas en la cadena de bloques, colocación de datos meteorológicos en blockchain, etc.).

Bitcoin es una combinación de cuatro componentes importantes, de los cuales blockchain es solo uno. El primero es que bitcoin es un activo digital escaso. El segundo es que Bitcoin es una red punto a punto de nodos completos que no pueden cerrarse ni censurarse. El tercero es que extraer Bitcoin requiere encontrar números de prueba de trabajo válidos, lo que hace que el fraude sea muy costoso. El cuarto es que Bitcoin tiene una cadena de bloques que es auditable total y públicamente. Estas cuatro tecnologías están estrechamente integradas, y cuando se elimina una parte, el resultado es algo mucho menos útil.

Para un activo puramente digital como Bitcoin, usar una cadena de bloques como registro público funciona. Tanto su creación como cada instancia de su transferencia están perfectamente registradas y son infalibles. Pero para los objetos del

mundo real como los granos de café o los datos de atención médica, no hay forma de garantizar que la información sea infalible, ya que siempre existe la posibilidad de que se cometan errores durante el ingreso de datos debido a negligencia o incluso fraude directamente. Por lo tanto, una autoridad central debe estar presente para garantizar toda la información, lo cual evita la necesidad de una cadena de bloques en primer lugar.

Sin embargo, se han invertido enormes sumas de dinero en la tecnología blockchain en busca de casos prácticos más allá del dinero descentralizado. Al escribir estas líneas, nadie ha podido crear un sistema de mantenimiento de registros a gran escala utilizando una cadena de bloques que mejore significativamente o incluso logre la paridad con enfoques más tradicionales.

¿Y Qué Hay de Otras Criptomonedas?

La gente no sólo ha intentado copiar la cadena de bloques de Bitcoin; también han intentado crear otras criptomonedas, llamadas así porque los remitentes de estos nuevos fondos digitales usan firmas digitales para firmar transacciones, al igual que Bitcoin. A menudo llamados altcoins o tokens, estos proyectos no están descentralizados, y muchos son directamente fraudes. Bitconnect es un famoso ejemplo de fraude de criptomonedas.

Un puñado de criptomonedas puede tener casos prácticos legítimos. Estos incluyen Monero (XMR) y Zcash (ZEC), que tienen como objetivo permitir a los usuarios realizar transacciones de una manera más privada que Bitcoin, o Ethereum (ETH), que se utiliza para tratar de construir plataformas de aplicaciones blockchain. Las principales empresas también están experimentando con criptomonedas. Facebook ha anunciado la criptomoneda Libra, que tiene el potencial de volverse muy popular debido a los miles de millones de personas que usan los servicios de Facebook. Sin embargo, Libra está central-

izado por naturaleza y no tendrá la resistencia a la censura y la escasez de Bitcoin.

Varios grupos han tratado de copiar el éxito de Satoshi de una manera especialmente descarada y han creado criptomonedas cuyos nombres contienen la palabra Bitcoin. Como tal, a menudo hay confusión sobre qué criptomoneda es realmente Bitcoin. Para distinguir, busque el símbolo bursátil BTC en portales de intercambio y billeteras. Las variantes de Bitcoin son como el oro de tontos; pueden parecer similares, pero están mucho más centralizados y tienen un precio mucho más bajo. Estos incluyen Bitcoin Cash (BCH), Bitcoin Gold (BTG) y Bitcoin Satoshi's Vision (BSV).

Resúmen

Bitcoin es un avance significativo de ingeniería que ofrece una nueva alternativa al sistema financiero existente.

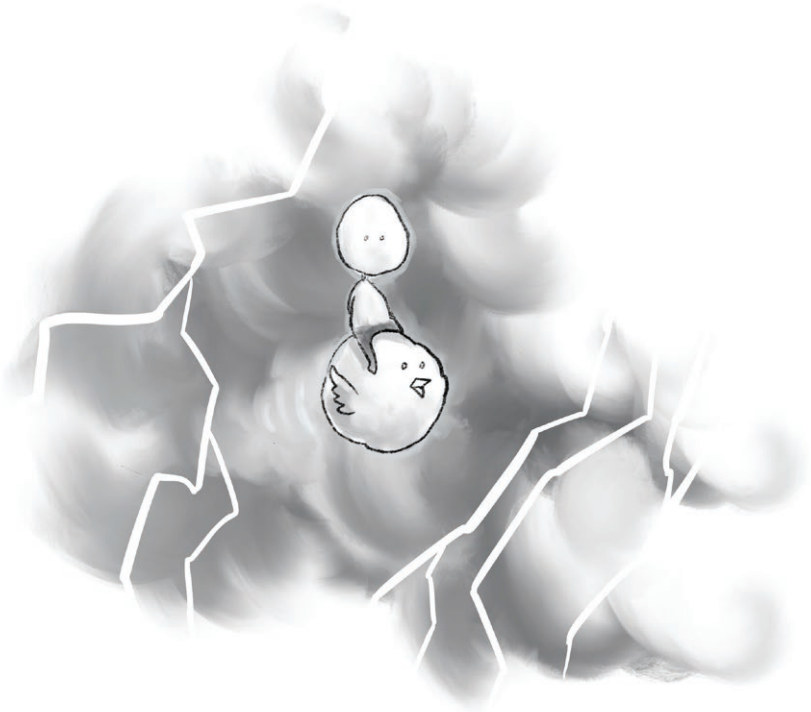
Bitcoin es dinero digital que es fácil de transar en todo el mundo dado que se liquida en minutos en lugar de días.

Bitcoin es un activo escaso, que protege contra la amenaza de inflación arbitraria.

Bitcoin está descentralizado, evitando que cualquiera censure los pagos.

Bitcoin es el único dinero descentralizado y digitalmente escaso del mundo.

Bitcoin tiene el potencial de volcar el orden monetario actual.



CAPÍTULO TRES

El Precio y la Volatilidad del Bitcoin

Descargo de responsabilidad: los autores de este libro no son profesionales de la inversión. Este capítulo propone posibles razones para el movimiento de precios de bitcoin y la volatilidad general, y no contiene consejos de inversión.

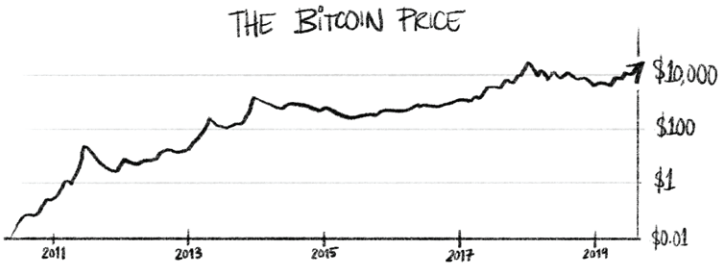
Todos quieren saber: ¿Por qué es valioso el bitcoin? ¿Por qué ha aumentado tanto el precio? ¿Por qué es tan volátil? ¿Por qué vale algo el bitcoin si, a diferencia del dólar estadounidense, el bitcoin no está respaldado por una economía, o más cínicamente, por amenazas de multas y cárcel?

El precio de un activo se mueve cuando hay un desequilibrio entre compradores y vendedores. En el caso de bitcoin, esos desequilibrios son impulsados por algunos factores que difieren en las perspectivas a largo plazo, mediano y corto plazo.

La Perspectiva de Largo Plazo

Durante la última década, el precio del bitcoin se ha incrementado desde una fracción de centavo hasta casi $20.000. El precio en agosto de 2019 era casi de $11.000.

El Precio del Bitcoin desde su Creación hasta la Actualidad (Escala Logarítmica)



Bitcoin es escaso. El suministro se establece en 21 millones de monedas como se explica en el Capítulo 2.

El suministro fijo de Bitcoin y el calendario de emisión transparente es atractivo para los compradores porque la alternativa - el dinero fiduciario - está universalmente sujeta a dilución y, por lo tanto, a inflación, lo que significa que la misma cantidad de dinero compra menos cada año. A largo plazo, es probable que más personas encuentren atractivo el bitcoin porque los gobiernos no pueden imprimir más de la misma o censurar las transacciones, y porque es difícil de confiscar.

El valor total de todos los bitcoins extraídos sigue siendo de solo $200 mil millones. Por el contrario, el valor de todo el oro extraído se estima en alrededor de $9 billones. Con solo el 2% del valor del oro, el mercado de bitcoin es pequeño y, por lo tanto, más sensible a las fluctuaciones de precios. El volumen diario negociado también es relativamente pequeño: aproximadamente $10 mil millones por día en comparación con $300 mil millones por día del oro. Debido a que hay menos liquidez, que es la cantidad que se compra o vende fácilmente en un período determinado, incluso los pequeños compra-

dores o vendedores pueden tener un gran impacto en el precio. A medida que aumenta la adopción de Bitcoin y Bitcoin crece como una clase de activo global, su volatilidad disminuirá. Esto podría llevar varias décadas.

La Perspectiva de Mediano Plazo

Mirando a Bitcoin en el plazo de meses y años, los principales impulsores del cambio de precios son los costos de minería, la demanda de grandes compradores institucionales y los eventos de reducción a la mitad o *halvings*.

La minería tiene costos: equipos, operaciones del centro de datos, electricidad. Estos costos deben pagarse con moneda fiduciaria. Por lo tanto, la mayoría de los mineros venderán regularmente parte o la totalidad del bitcoin que extraen para pagar los costos operativos, que equivalen aproximadamente a $250-300 millones por mes, o 40-50% del valor de bitcoin extraído mensualmente en el momento en que se escribe este artículo.

La demanda de bitcoin en esta escala generalmente proviene de compradores institucionales, personas adineradas, oficinas familiares y patrimonios que desean exponerse a la criptomoneda, y generalmente comienzan con bitcoin.

Otro factor importante que influye en el precio a mediano plazo es el halving. Como se describe en el Capítulo 2, la recompensa minera se reduce a la mitad una vez cada cuatro años. Bitcoin ha tenido dos reducciones a la mitad hasta ahora, en 2012 y 2016. Ambas reducciones a la mitad crearon un precipicio en la oferta que aumentó la volatilidad.

La escalada de los precios de bitcoin tiende a atraer a más especuladores, que van desde inversionistas minoristas que buscan comprar solo $100 en bitcoin hasta inversionistas insti-

tucionales que compran millones de dólares. Esto, a su vez, aumenta el precio de bitcoin a medida que la atención de los medios y el miedo a quedar fuera agrega combustible al fuego. Esta dinámica ha creado grandes burbujas de precios que terminan en caídas de precios del 80% o más. Es muy posible que estos ciclos de precios continúen en torno a futuros halvings.

La Perspectiva de Corto Plazo

No tener autoridad central tiene un efecto secundario importante: la volatilidad.

Donde se comercializa bitcoin ofrece un contexto crucial para las causas de la volatilidad a corto plazo. Hay muchos lugares para hacer esto, como los portales de intercambio de moneda fiduciaria a criptomoneda, que permiten el intercambio de moneda fiduciaria directamente a bitcoins, los portales de intercambio persona-a-persona, que requieren verse en persona, y los portales de intercambio cripto-a-cripto, que solo permiten intercambios entre criptomonedas. Debido a que los traders u operadores buscan ganancias de la volatilidad, hay intercambios apalancados, donde es posible operar hasta 100 veces el monto del depósito.

Los intercambios de criptomonedas existen principalmente en Internet. Por lo tanto, operan cada minuto del año y pueden servir directamente a los inversionistas minoristas. Por el contrario, los mercados tradicionales suelen estar anclados en un gran centro financiero como Londres, Nueva York o Hong Kong, están abiertos al comercio en vivo durante solo 7.5 horas de lunes a viernes, y son utilizados principalmente por corredores, no inversionistas minoristas.

Debido a que cualquiera puede enviar y recibir bitcoins con una computadora y una conexión a Internet, es relativa-

mente fácil para un empresario establecer un intercambio básico. Dado que bitcoin no se considera un valor o security, los portales de intercambio en los que se comercializa pueden estar sujetos a estándares regulatorios menos estrictos que los mercados tradicionales. Además, los portales de intercambio de cripto-a-cripto pueden ir en búsqueda de jurisdicciones anfitrionas amigables como Malta, Seychelles o Filipinas, ya que no necesitan cuentas bancarias fiduciarias, y los equipos pueden operar de forma remota. Depositar en un portal de intercambio significa confiar en que ese portal mantendrá los fondos seguros. Desafortunadamente, muchos portales de intercambio están mal administrados. Casos bien documentados de malversación o incompetencia que resultan en robo a gran escala incluyen Mt. Gox, Bitfinex y Quadriga, que juntos perdieron decenas de miles de bitcoins (con valor de miles de millones de dólares).

Advertencia para los lectores: varios portales de intercambio han sido hackeados o han perdido los bitcoins de sus clientes. Los lectores deben tener precaución al usar un portal de intercambio y solo deben arriesgar cantidades de bitcoin que se sienten cómodos perdiendo.

La idoneidad de Bitcoin para el comercio minorista en línea contribuye a su volatilidad a corto plazo. Mientras que los bancos centrales generalmente buscan minimizar la volatilidad, los operadores prefieren la volatilidad porque es rentable.

Dentro de los plazos de un mes hasta un minuto, la volatilidad de los precios de bitcoin puede ser extrema. El 1 de enero de 2019, un bitcoin costó $3.500. En agosto de 2019, costaba casi $11.000. Las fluctuaciones diarias de hasta el 20% no son anormales. Esto es aterrador para los inversionistas, pero es un paraíso para los especuladores que buscan beneficiarse del movimiento de los precios.

A diferencia de los mercados tradicionales de acciones o de deuda, bitcoin no tiene fundamentos comerciales que determinen el consenso de precios. Bitcoin no tiene empleados, ni

rendimiento del producto, ni flujos de efectivo. La falta de tales indicadores de rendimiento a corto plazo significa un énfasis en los elementos técnicos de la negociación, que a menudo es de suma cero. Para tales especuladores, el comercio de criptomonedas es otra forma de póker en línea, que requiere ventajas menores durante largos períodos de tiempo, se juega en la comodidad de sus salas de estar y a su conveniencia.

Al igual que con los mercados tradicionales, el precio de bitcoin responde a noticias importantes, pero no siempre sube con buenas noticias o baja con malas noticias. Por ejemplo, en 2013, los piratas informáticos atacaron un portal de intercambio llamado Mt.Gox, el portal de intercambio más grande en ese momento, y siguió una disminución significativa de los precios. Sin embargo, en 2018, Binance, el mayor portal de intercambio de hoy, fue hackeado por alrededor de $40 millones y el precio de bitcoin en realidad aumentó.

A medida que Bitcoin se vuelve más valioso y más líquido, la volatilidad probablemente disminuirá. Esto es similar a las fluctuaciones de precios en acciones famosas versus acciones menos conocidas. Por ejemplo, es mucho más difícil para un comerciante individual mover el precio de Apple que el precio de una acción de centavo.

Bitcoin es un vehículo único y muy arriesgado para los comerciantes. El atractivo de bitcoin para los comerciantes, combinado con su falta de liquidez y la disponibilidad de operaciones apalancadas agrega una volatilidad significativa a corto plazo a su precio.

Resúmen

Desde su creación, el precio de bitcoin se ha movido hacia arriba y hacia la derecha en función de su oferta fija y la creci-

ente demanda. En el corto plazo, el precio está sujeto a especulación, manipulación del mercado y volatilidad masiva.

En última instancia, el suministro fijo y la naturaleza descentralizada de Bitcoin son lo que le dan tanto su valor como su volatilidad.

Si bitcoin evoluciona más allá de una reserva de valor y llega a representar el tamaño de la economía digital (como lo hace la moneda fiduciaria para las economías físicas hoy), bitcoin se convertirá en un método de pago y una unidad de cuenta. En ese punto, la volatilidad puede disminuir a medida que Bitcoin está anclado en el intercambio de valor en lugar de la actividad especulativa. Mientras tanto, permanecerá al antojo de las fuerzas del mercado descritas en las secciones de Mediano Plazo y Corto Plazo en este capítulo y continuará fluctuando dramáticamente.

CAPÍTULO CUATRO

¿Por qué es importante Bitcoin para los Derechos Humanos?

Con la invención de Bitcoin, las personas ahora pueden consolidar el resultado de su arduo trabajo y almacenar su riqueza como información digital. Esto evita que regímenes y corporaciones controlen de forma arbitraria la manera en que sus ciudadanos ahorran o transfieren su dinero. Las ramificaciones de los derechos humanos de esta revolución financiera ya se están sintiendo y continuarán intensificándose alrededor del mundo, especialmente en dictadura, pero también en democracias liberales.

El Capítulo 1 presentó historias de personas desde Nigeria hasta Venezuela que han luchado contra altas inflaciones, vigilancia financiera, banca inaccesible e infraestructuras económicas descompuestas.

Éstas no son historias aisladas. De acuerdo con la data de Human Rights Foundation, aproximadamente la mitad de la población mundial vive bajo un autoritarismo. Eso es aproximadamente 4 mil millones de personas desde Cuba hasta Bielorrusia hasta Arabia Saudita hasta Vietnam, quienes son oprimidos de forma severa por sus gobiernos. Muchos de ellos son refugiados económicos o presos políticos. Estos individuos no gozan del Estado de Derecho ni de la posibilidad de lograr que se apruebe pacíficamente alguna reforma. Incluso el gobi-

erno americano y los europeos oprimen de forma financiera a sus ciudadanos ocasionalmente a través de su ascendente vigilancia e inflación. Rescates a banqueros, intervenciones militares externas, seguridad fronteriza mejorada, y ayuda social subsidiada son algunas de las actividades cuestionables que son posibles mediante la impresión de más dinero.

Cuando los ciudadanos son forzados a utilizar plataformas de pagos centralizadas como el WeChat de China, la cual realiza micro-rastreo a millones de personas, cuando un dictador congela la cuenta bancaria de un grupo de derechos humanos, o cuando las sanciones a un país castigan a las personas por crímenes que han cometido sus jerarcas no electos, Bitcoin puede ser una salida. La invención de Satoshi puede ayudar en gran medida a los cientos de millones de personas sin cuenta bancaria o documentos de identidad formales para que puedan tener y hacer uso de dinero. Tan solo con un teléfono y conexión a internet, los individuos más vulnerables del planeta pueden recibir bitcoin de cualquier persona rápidamente y de forma económica sin posibilidad de censura o incautación.

Como resultado, Bitcoin está cambiando el juego de los pagos transfronterizos y las remesas, y tiene el potencial de mejorar muchos otros aspectos de la sociedad. Bitcoin crea un mercado realmente global para bienes y servicios y prepara el camino para una igualdad de condiciones.

Ser tu propio banco

En lugares como Bahréin, Rusia y Zimbabwe, los gobiernos ejercen control dictatorial sobre el sistema bancario, resultando en altos niveles de apropiación indebida y corrupción. Bitcoin sienta las bases para un mundo en el cual los regímenes y corporaciones tienen menos control y en el cual las personas tienen más libertad y elección individual.

Bitcoin es un instrumento al portador, lo que quiere decir que las personas pueden estar en total control sobre los bitcoins que poseen. Adicionalmente, cuando se envía el Bitcoin, no existe intermediario que pueda censurar la transacción o filtrar la información personal del remitente. Esto provee protección frente a ladrones, empresas maliciosas y gobiernos espías. Ninguna otra moneda o empresa de pagos puede tener este tipo de seguridad.

Esconder el dinero en efectivo bajo un colchón ha sido por mucho tiempo la forma en que aquellos que viven en economías deshechas almacenan su dinero. La parte negativa evidente es que el dinero en efectivo es difícil de proteger y su transmisión no es conveniente. Si las autoridades se presentan en sus puertas, pueden incautarle el dinero en efectivo que consigan. Por otro lado, el bitcoin es fácil de almacenar y proteger, puesto que las claves privadas o contraseñas secretas pueden ser almacenadas en papel, en una computadora, en un dispositivo USB, o incluso memorizadas. La negación creíble de la propiedad de bitcoin es posible y las autoridades no tienen una manera fácil de incautar de forma física los bitcoins.

Escapando a la alta inflación

Los ciudadanos desde Irán a Somalilandia viven bajo regímenes que imprimen moneda de forma imprudente, diluyendo los ahorros ganados con esfuerzo de sus economías.

Por supuesto, la inflación es algo que todos los bancos centrales llevan a cabo. Generalmente consideran como deseable la inyección de pequeñas cantidades de dinero en efectivo, puesto a que esto mantiene a los mercados en movimiento. Puede que las democracias muestren algún tipo de moderación, pero como hemos visto, la inflación puede salirse de las manos rápidamente.

De acuerdo a los índices de precios al consumidor, de 2018 a 2019 los precios se incrementaron en 1.7% en Alemania y 1.9% en los Estados Unidos. En muchos países, los precios de bienes de consumo subieron mucho más: 3.75% en Brasil, 5% en India, 11% en Nigeria, 20% en Turquía, y un enorme 47% en Argentina. La gente en países con incrementos de precio superiores al 10% notan una depreciación abrupta de sus ganancias y ahorros.

Un caso extremo es Venezuela. Debido a la impresión incesante de dinero, la corrupción sistemática y la mala gerencia económica, los precios se incrementaron un 2.300.000% en 2018 – una hiperinflación tan severa que hace que ahorrar sea imposible. El dinero se comienza a evaporar horas después de llegar a las cuentas bancarias. Esto obliga a los venezolanos a vivir el día a día, gastando el dinero en los productos básicos literalmente tan pronto como lo obtienen. Los venezolanos viven bajo un régimen autoritario, y no tienen posibilidad de participar en elecciones libres y justas en las cuales pudiesen hacer que su gobierno rindiese cuentas. En los últimos años, más de 4 millones de ciudadanos, que son más del 10% de la población del país, han huido a países vecinos tales como Brasil y Colombia, en lo que ha sido una de las crisis de refugiados más graves del mundo.

Además de desmembrar la economía nacional, el régimen venezolano ha impuesto controles de capital severos por más de dos décadas. Enviar dinero hacia o desde el país es extremadamente difícil. La principal forma de enviar dinero es a través de intermediarios que tengan una cuenta en Venezuela, quien transfiere la cantidad equivalente de bolívares venezolanos a su destino final. Inclusive este método alternativo está siendo detenido por los bancos, bajo presión gubernamental, quienes están identificando a las personas que utilizan sus cuentas venezolanas desde el exterior. Volvamos al Capítulo 1: el régimen no quiere que su población acceda a dinero que sea mejor y más sólido que el bolívar.

Otra opción es tener amigos o familiares que vivan en los Estados Unidos y envíen USD a una oficina de Western Union en una ciudad fronteriza en Colombia. El receptor debe escapar de Venezuela, viajar a dicha ciudad con un enorme riesgo, retirar los USD en Western Union e ingresar sigilosamente a Venezuela con dinero en efectivo escondido entre sus ropas. Esto, evidentemente, requiere de tiempo y es peligroso puesto que las fronteras terrestres y los aeropuertos están inundados de oficiales corruptos queriendo confiscar el dinero en efectivo.

La solución: utilizar bitcoin para transferir valor más allá de las fronteras. Los venezolanos pueden solicitarle bitcoin a amigos o familiares en el exterior por medio de mensajes de texto y recibirlo momentos después por una pequeña tasa. Esta transacción es imposible de censurar y no es fácil de rastrear. Para las personas que viven en economías estables, el bitcoin pudiese lucir volátil, pero para los venezolanos, incluso una variación abrupta de 20% en el precio del bitcoin es leve comparada con la depreciación reciente de 2.300.000% del bolívar.

Una vez que han recibido los bitcoins en su teléfono o computadora, pueden fácilmente convertirlo en moneda local a través de LocalBitcoins.com, un sitio web al estilo eBay que conecta a comerciantes en más de 100 países. Ellos pueden publicar a la venta el Bitcoin recibido recientemente, y recibir ofertas de compra casi de forma inmediata. En menos de 15 minutos pueden vender los bitcoins y recibir bolívares en sus cuentas bancarias. Este sistema suele mover millones de dólares hacia y desde Venezuela cada día. Desde mediados del 2019, el Bitcoin ya se ha convertido en una economía paralela de último recurso para las personas en sistemas económicos descompuestos como el de Venezuela.

El acceso universal al dinero

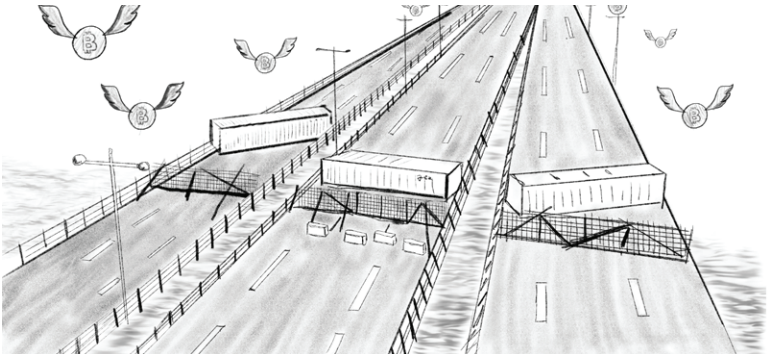
Es fácil para un ciudadano estudiado de una democracia estable abrir una cuenta bancaria. Pero ese no es el caso para miles de millones de personas alrededor del mundo. Algunos ejemplos son sorprendentes. En Afganistán y Arabia Saudita, las mujeres tienen prohibido por sus familiares masculinos abrir sus propias cuentas bancarias. Se les despoja de forma efectiva de su libertad financiera.

Para ellas, bitcoin puede ser un salvavidas. En el 2014, una emprendedora afgana llamada Roya Mahboob se enfrentó a un gran reto: no podía pagarle a sus empleadas. Si les daba dinero en efectivo, sus familias se lo quitarían. Los familiares masculinos no las dejaban abrir cuentas bancarias. Los softwares tales como PayPal no estaban disponibles en su país. Una amiga le mencionó la posibilidad de utilizar bitcoin y ella lo utilizó para pagarle a sus empleadas. Les dio soberanía financiera individual.

Una de estas jóvenes mujeres tuvo que huir de Afganistán puesto que había una amenaza contra su vida. Pero ella se llevó sus bitcoins consigo, almacenados en su teléfono. Viajó a través de Irán y Turquía y eventualmente llegó a Alemania. Allí, ella intercambió sus bitcoins – los cuales, afortunadamente, se habían apreciado de forma dramática durante su travesía – por Euros, para comenzar una nueva vida. Bitcoin puede ayudar a los oprimidos y no bancarizados cuando no hay otras opciones.

En la medida en que la infraestructura y los intercambios locales persona-a-persona de Bitcoin crezcan en los años venideros, tendrá un gran impacto en la ayuda extranjera y la asistencia humanitaria. Quizás la imagen más vívida de lo que sucede en el área de la ayuda es la foto que se tomó en la frontera venezolana en febrero de 2019, cuando el régimen de Maduro evitó que ayuda extranjera ingresara al país colocando barricadas en el puente fronterizo con semi-remolques. Lo que

no se vio en la foto fueron los millones de dólares en bitcoin entrando y saliendo por encima del control gubernamental.



El sistema actual de ayuda extranjera tiene vulnerabilidades evidentes. Bien sea en el caso de un gobierno que envía ayuda a otro, una organización filantrópica que hace un regalo a una ONG, o una persona que envía dinero a su familia en una emergencia médica, el dinero solo llega a su destino tras viajar a través de terceros. Incluso en la situación más básica, hay por lo menos tres intermediarios: el banco del remitente, un banco central y el banco del receptor. Frecuentemente hay más intermediarios, algunas veces hasta siete. Cada uno puede ralentizar el proceso, congelar la transacción o incluso robarse el dinero. El ex Secretario General Ban Ki-moon declaró en un discurso del 2012 que durante el año anterior la corrupción había "impedido que el 30% de toda la asistencia al desarrollo llegase a su destino final".

De acuerdo a investigaciones realizadas por organizaciones tales como GiveDirectly y el Banco Mundial, las transferencias directas de dinero en efectivo son la manera más efectiva de llevar ayuda. Bitcoin facilita transferencias sin necesidad de permisos para cualquier persona en el planeta en minutos. El receptor no necesita tener ni siquiera una cuenta bancaria o identificación oficial, solo acceso al internet.

Un estudio reciente realizado por Pew determinó que el 45% de las personas en economías emergentes ya tienen un teléfono móvil inteligente, un número que continúa incrementándose. Para entender el impacto potencial del Bitcoin en esta área, tenga en cuenta que, en un país como Filipinas, solo el 20% de los adultos tienen una cuenta bancaria.

Para ser utilizado como un canal de pago, el receptor debe poder intercambiarlo por moneda local. Bitcoin no es útil actualmente como ayuda a no ser que pueda ser intercambiado por bienes y servicios. Pero según un análisis detallado de información de mercado de bitcoin realizado por Matt Ahlborg, se está volviendo más fácil para las personas en las economías emergentes desde Asia del Este hasta el oeste de África intercambiar bitcoin por monedas locales.

Además, cuando los bancos tradicionales cierran, la red Bitcoin sigue operando. En la medida en que su infraestructura mundial provea liquidez y acceso para las personas alrededor del mundo, la posibilidad de Bitcoin de actuar como salvavidas para aquellos que reciben ayuda se incrementará de forma dramática.

Ya existen redes de malla, sistemas satélites, y técnicas basadas en radio que permiten que la gente envíe y reciba bitcoin sin acceso a internet. Hay ingenieros trabajando en innovaciones para dificultar cada vez más a los gobiernos el prohibir el acceso al bitcoin, una moneda que no pueden inflar o confiscar de forma fácil.

La Sociedad sin Dinero en Efectivo

La idea de una sociedad sin dinero en efectivo generalmente se presenta como algo muy conveniente. Pero desde la perspectiva de los derechos humanos, introduce nuevos peligros, dándole a los gobiernos y a los bancos un poder sin prece-

dentes. El dinero en efectivo es una de las mejores maneras de proteger la privacidad de una persona. Cuando se paga por algo con un billete, solo el comprador y el vendedor tienen conocimiento de la transacción, y se vuelve difícil para los gobiernos rastrear el comportamiento de compra. Los pagos anónimos son posibles con el dinero en efectivo tal como cuando se introducen billetes en una caja de donaciones de caridad.

Desafortunadamente, el dinero en efectivo está desapareciendo en el mundo. En sociedades hiperinflacionarias tales como Venezuela o Somalilandia, los billetes tienen tan poco valor que deben ser pesadas en montones por kilos. Mientras tanto, en áreas urbanas avanzadas como Estocolmo y Shanghái, los residentes hacen uso de pagos digitales de forma casi exclusiva. Se estima que solo el 8% de las transacciones globales son llevadas a cabo aun en monedas o billetes. Para el 2030, la cantidad de personas que puedan utilizar el dinero en efectivo en sus vidas diarias será cercana a cero. Como se vio en el Capítulo 1, esto puede ser un panorama aterrador para manifestantes que dependen del dinero en efectivo en lugares como Hong Kong para comprar billetes de transporte público o líneas móviles SIM descartables para proteger la privacidad y la vigilancia de los vuelos. Sin algo de dinero en efectivo, o algún equivalente digital, coordinar protestas políticas mientras se protege la seguridad personal será casi imposible.

En Estonia, el gobierno está proveyendo de forma gratuita el transporte público. Suena fantástico, pero viene con un truco: los pasajeros solo pueden obtener viajes gratuitos haciendo uso de sus identificaciones personales, permitiendo así que el gobierno pueda rastrear sus movimientos. A pesar de que posiblemente los estonios no tengan de qué preocuparse, los ciudadanos de gobiernos autoritarios cercanos tales como Rusia o Bielorrusia sí tienen serios motivos para estar preocupados.

Mientras tanto, el Partido Comunista Chino tiene control sobre sistemas con más de mil millones de usuarios tales como Alipay o WeChat. Las autoridades no solo ejercen vigilancia y control sobre el dinero de las personas, también regulan las acciones y opiniones de sus ciudadanos a través de sistemas sociales de crédito. En los sistemas sociales de crédito, tal como el que se está implementando en toda la China, los ciudadanos son valorados no solo con respecto a su salud financiera, sino también con respecto a sus opiniones políticas, identidad y círculos sociales. El gobierno incentiva el comportamiento de ciudadanos leales y castiga a los creadores de problemas evitando que viajen al exterior, obtengan internet más rápido, envíen a sus hijos a buenos colegios u obtengan buenas tasas en los préstamos. Estos sistemas sociales de crédito aún están emergiendo, pero están en camino a dar un control sin precedentes al gobierno chino y constituye el proyecto de ingeniería social más grande en la historia de la humanidad.

Tendencias menos perturbadoras, pero similares, están comenzando a surgir en democracias occidentales, con las compañías de tarjetas de crédito vendiéndole la actividad de las transacciones a los anunciantes a cambio de una ganancia.

Bitcoin vs. El Gran Hermano

Lo que la gente compra revela más que lo que la gente dice. Las transacciones divulgan una cantidad enorme sobre lo que la gente es y lo que hace, a dónde va y cuándo, o lo que le gusta o disgusta. Mientras se rastrea de forma más extensiva el gasto, lo más probable que las personas se enfrenten a un resultado orwelliano.

En las sociedades democráticas, está emergiendo un debate con respecto al papel de las corporaciones tales como Facebook como emisores de sus propias monedas. Facebook está proponiendo introducir Libra a cientos de millones de personas a

través de las ya existentes cuentas de redes sociales en Whatsapp, Instagram o Messenger. A pesar de que un proyecto como Libra podría perfectamente dar acceso a una cantidad de personas que actualmente no están bancarizadas, muchos temen que Facebook registrará la actividad de pagos de los usuarios, influenciará elecciones, o dará de baja de la plataforma a individuos y congelará su posibilidad de realizar pagos por expresar opiniones políticas particulares.

Para detener al Gran Hermano, todos deben reducir sus crecientes huellas de datos. Mientras menos se disemine y se comparta la información asociada a la identidad entre empresas y gobiernos, más difícil se volverá vigilar, manipular y controlar a las personas.

Una sociedad sin dinero en efectivo es una sociedad vigilada. Bien sea con el modelo WeChat controlado por el gobierno o el modelo Libra controlado por una corporación, las empresas pueden rastrear la actividad financiera para obtener ganancias, oprimir, o algo peor.

¿Y qué tal si el futuro pudiese ser diferente? ¿Qué tal si pudiese existir el dinero en efectivo de forma digital? A pesar de que las transacciones de bitcoin actualmente son solamente pseudo-anónimas, hay mucho trabajo por hacer en la comunidad de desarrolladores para traer más privacidad a la red de Bitcoin y a sus usuarios. En el futuro próximo, cuando se compre algo en línea, comprar un billete de autobús o de metro, o suscribirse a revistas políticas o podcasts, las personas no tendrán que revelar su identidad al efectuar pagos.

Hacer al Bitcoin Privado con la Red Lightning

Los consumidores están perdiendo cada vez más la privacidad financiera. Puede que exista una solución con Lightning, una red de pagos que se está construyendo actualmente sobre el Bitcoin.

El sistema de pagos existente crea todo tipo de honeypots o señuelos, puesto que todo intermediario financiero es un potencial agujero de seguridad. Bitcoin es distinto, puesto que no hay intermediarios, por lo que, por lo menos en principio, esta vulnerabilidad puede ser eliminada. Desafortunadamente, los detalles clave de las transacciones de bitcoin se registran en la cadena de bloques, pudiendo ser vistos por cualquier persona. Los investigadores han explorado si existe la posibilidad de esconder u oscurecer los detalles específicos de una transacción y aún pagar con bitcoin, y esto es posible con Lightning.

La Red Lightning no registra los detalles de cada transacción a la cadena de bloques Bitcoin de forma directa. El objetivo de Lightning es incrementar la velocidad y el volumen de las transacciones que Bitcoin puede manejar. La privacidad viene siendo un efecto secundario en la obtención de este objetivo.

Este avance técnico se parece bastante al Bitcoin en el sentido de que es de código abierto, sin necesidad de permisos, y disponible para todo el mundo, independientemente de su ubicación, edad, ingresos, género o nacionalidad. Bitcoin en Lightning pudiese ayudar a evitar un futuro distópico en el cual la privacidad sea costosa y solo obtenible por parte de personas adineradas.

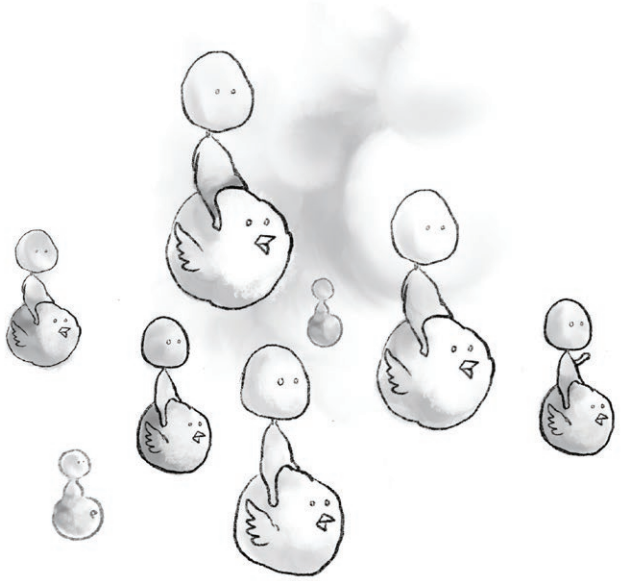
Incluso en una sociedad sin dinero efectivo, pronto debería ser posible usar una aplicación Lightning en un teléfono para comprar billetes de transporte de forma anónima para asistir a una manifestación o comprar libros políticos en línea. La

máquina de billetes de metro o Amazon no sabrán nada sobre los compradores, y no podrán filtrar sus datos o compartir su información con los gobiernos.

Dicho esto, Lightning no es una panacea de privacidad. Anonimizar la información de pago es solo un paso para garantizar la privacidad total, ya que las brechas de privacidad como las puertas traseras en los teléfonos, el seguimiento de geolocalización y las cámaras de vigilancia también deben ser abolidas.

El autor de Black Swan, Nassim Taleb, escribió que Bitcoin es "una póliza de seguro contra un futuro orwelliano". A medida que continúan las tendencias mundiales de vigilancia creciente y desaparición de efectivo, ese futuro parece estar presionándonos.

La tecnología no siempre mejora la libertad en todo el mundo. Por el contrario, la inteligencia artificial y el análisis de big data están despojando sistemáticamente a las personas de sus libertades, especialmente en lugares como China. El historiador y autor de Sapiens, Yuval Noah Harari, advirtió que la tecnología de la información moderna tiende a favorecer la tiranía, pero la tecnología también puede favorecer la libertad cuando se diseña y despliega deliberadamente con este propósito. Bitcoin, especialmente cuando está potenciado con nuevos desarrollos como la Red Lightning, puede ser una herramienta importante en la lucha global por los derechos humanos.That said, Lightning is not a privacy panacea. Anonymizing payment information is only one step towards securing full privacy, as privacy gaps like backdoors on phones, geolocation tracking, and surveillance cameras also need to be abolished.



CAPÍTULO CINCO
Historia de Dos Futuros

Es el año 2039.

Los últimos 20 años han visto un aumento significativo en la guerra global. Los países luchan para desbancar al dólar estadounidense y al renminbi chino de sus posiciones dominantes. Algunas veces esta turbulencia económica estalla en un conflicto violento. Los países ricos sufren un declive político y una recesión económica insoluble, mientras que los países pobres se ciernen cerca del colapso total a medida que las sucesivas crisis económicas consolidan la riqueza y el poder de los poderes centrales estatales y corporativos.

Las compañías tecnológicas dominantes como Alibaba, Tencent, Facebook, Google y Amazon controlan el mercado global, y después de varias rondas de presión gubernamental, demandas antimonopolio y acuerdos, han acordado entregar los datos de los usuarios a cambio de protección del mercado. Las empresas comparten información completa de los usuarios con los gobiernos de todo el mundo sobre lo que todos compran, lo que todos escuchan, sobre lo que todos publican y dónde están todos. Las empresas se han convertido en satélites del estado. La privacidad personal es inexistente.

Esto le da a los gobiernos un control sin precedentes sobre sus ciudadanos. La brecha entre los ricos y los pobres continúa ensanchándose, a medida que el efecto Cantillon aumenta y aquellos con conexiones con el régimen prosperan de manera desproporcionada. La vigilancia digital es la norma, mien-

tras que las críticas a los gobiernos autoritarios se evaporan. El control del dinero por parte del gobierno y las empresas significa que pueden censurar el discurso, ya que a los creadores disidentes no se les puede pagar ni apoyar para hacer su trabajo.

La diversidad de pensamiento es ahora disidente. Los estados policiales de todo el mundo usan el Internet de cosas, datos de implantes médicos, rastreo de teléfonos, historial de transacciones y consultas de búsqueda para localizar y castigar a los disidentes. La oposición es esencialmente imposible, ya que el efectivo ha desaparecido y todas las compras (incluso para artículos como billetes de metro, periódicos y máscaras que podrían ocultar la identidad de uno) son digitales y monitoreados. El estado y las corporaciones multinacionales son más poderosas que nunca.

Es el año 2039.

Una economía global vibrante continúa floreciendo. Cada vez más personas en todo el mundo están ahorrando, acumulando riqueza, son capaces de pagar casas y tienen nuevos negocios. Los emprendedores de lo que solían llamarse países del tercer mundo están impulsando la innovación en la economía global. Cambiarse de jurisdicción es más fácil que nunca. Los gobiernos compiten puesto que los ciudadanos eligen dónde quieren vivir, trabajar y pagar impuestos. Los impuestos sobre la renta disminuyen, mientras que la calidad de la infraestructura, los servicios y las escuelas aumentan como resultado de la competencia global.

La proliferación de tantos nuevos bienes y servicios proporcionados por muchas más pequeñas empresas ha traído más innovación de la que se creía posible. Muchas empresas multinacionales que solían dominar el mercado han sido superadas por los numerosos jugadores más pequeños de todos los rincones del mundo. Cualquiera puede pagar cualquier cosa mediante pagos privados y sin permiso.

Muchos regímenes autoritarios han sido derrocados o debilitados a medida que los ciudadanos se vuelven más expertos en eludir los controles draconianos del capital y preservar la riqueza para ellos mismos en el lugar de cederla a las élites.

Los gobiernos se han visto obligados a pasar del control a la competencia; los individuos son más libres que nunca.

¿Cómo luce un mundo más basado en Bitcoin?

Predecir el futuro es siempre una propuesta arriesgada. Estas son dos visiones alternativas dada la trayectoria actual del mundo. Es probable que ninguno de los extremos se materialice, pero los individuos tienen control sobre qué dirección tomará su sociedad.

El sistema monetario se encuentra en medio de la encrucijada. Bitcoin tiene el potencial de separar dinero y estado. Vale la pena preguntarse, ¿cómo podría la adopción global de Bitcoin cambiar la sociedad?

Emerge la Economía Sin Fronteras

Desde el siglo XX, las economías han sido controladas en gran medida por los estados nacionales. La transición al dinero digital inicialmente permitió a los gobiernos controlar las economías de una manera sin precedentes al aumentar fácilmente la oferta de dinero para pagar las iniciativas.

Pero a medida que avanzaba la era digital, las economías comenzaron a trascender los estados. A principios del siglo XXI, esto era obvio ya que los consumidores compraban bienes producidos en la mitad del mundo. Las empresas contrataron trabajadores independientes de Filipinas a Nigeria como desarrolladores de software, asistentes virtuales o incluso radiólogos

remotos. Los socios comerciales podrían estar separados por miles de kilómetros. Toda la comunicación fue digital, instantánea y sin interrupciones. Sin embargo, realizar pagos transfronterizos todavía era lento y costoso. El pago de los bienes en línea todavía dependía de los canales tradicionales, y la liquidación en USD entre las instituciones financieras aún tomaba varios días. El sistema monetario aún no se había adaptado para alcanzar al mundo cada vez más conectado.

El surgimiento de Bitcoin es la chispa que permitirá la próxima ola de evolución financiera.

Los productos digitalmente nativos, como el contenido de las redes sociales y los artículos de videojuegos, consumirán una mayor parte de la economía mundial. Bitcoin se utilizará cada vez más como método de pago en transacciones transfronterizas porque el dinero fiduciario seguirá siendo engorroso. Las microtransacciones de Bitcoin, la rápida liquidación y la creciente base de usuarios obligarán a los comerciantes a denominar precios en bitcoin.

Estas economías son pequeñas hoy en día - como las comunidades que chateaban en AOL en la década de 1990 - pero a medida que crezcan, erosionarán aún más el control económico de los estados. A medida que se obtenga más riqueza de las redes sin fronteras y se denomine en una moneda sin fronteras propiedad de las personas, la riqueza será más fácil de mover y se liberará de la economía física de cualquier estado nacional.

Los Gobiernos se Enfrentan al Verdadero Precio de la Guerra

Cuando bitcoin se vuelva omnipresente, la capacidad del estado de simplemente imprimir más dinero para financiar la guerra será mucho más limitada. Las guerras ya no se finan-

ciarán tan fácilmente como lo han hecho en los últimos cien años. Si las guerras suceden, serán más limitadas y breves.

Los conflictos prolongados como la intervención rusa de Siria y Ucrania o la ocupación estadounidense de Irak y Afganistán pueden convertirse en cosa del pasado, ya que tales operaciones serán cada vez más difíciles de financiar. La guerra entre estados nacionales se convierte en una última opción desesperada de lo que es hoy, ya que los gobiernos están mucho más incentivados para encontrar formas menos costosas de resolver los desacuerdos.

El Autoritarismo se Torna muy Costoso

Los estados autoritarios tendrán dificultades para competir en un entorno global que es más difícil para ellos de controlar. Con personas en todo el mundo controlando su transferencia de valor personal, los ciudadanos más productivos de cualquier país simplemente se irán con su riqueza a una jurisdicción competitiva si las condiciones no son deseables. Para mantener a esos ciudadanos productivos, los gobiernos tendrán que imponer controles fronterizos severos o darles voz a dichos ciudadanos en su propio gobierno.

Las dictaduras no van a desaparecer en silencio, pero se verán obligadas a elegir: enfrentar la fuga de capitales en masa o permitir más libertad. Gracias a las redes de información, las obras liberales de literatura y cine ahora se abren camino rutinariamente en hogares que viven incluso bajo los regímenes más tiránicos como Eritrea y Corea del Norte. Este fenómeno se acelerará con dinero tan transferible y asegurable como la información.

Los Activos se Tasan Correctamente

Bitcoin ofrece una reserva de valor para todos, independientemente de su estado, origen étnico o ubicación geográfica. Como reacción a la inflación del dinero fiduciario, la mayoría de las personas actualmente eligen almacenar parte de su riqueza en bienes raíces, acciones y metales preciosos, todos los cuales están más centralizados y, por lo tanto, son más difíciles de acceder que Bitcoin. En un mundo donde el almacenamiento de riqueza en Bitcoin es la norma, las burbujas especulativas en estos activos ya no serán tan frecuentes.

Por ejemplo, habrá menos casos de burbujas de vivienda inducidas por la inflación, ya que menos extranjeros comprarán grandes porciones de las viviendas disponibles de una ciudad sin planes de vivir allí. Con Bitcoin como una alternativa superior, comprar activos estables en el extranjero no será atractivo. Los precios no se dispararán y más personas podrán pagar casas en sus propias ciudades.

Llegan las Finanzas Descentralizadas

La dominación estadounidense, europea y china se desvanecerá a medida que los países puedan liquidar las transacciones en bitcoin, una verdadera moneda de reserva global, en lugar de los USD, EUR o CNY regionales. Las fuerzas laborales serán libres de moverse por el mundo y habrá más competencia por la mano de obra, dando a los trabajadores más del valor que producen.

Los bancos estadounidenses, europeos y chinos perderán su influencia opresiva, ya que cada persona puede ser su propio banco, lo que permite un verdadero ahorro con el tiempo. La riqueza se acumulará en los países que exportan mano de obra, lo que permitirá el surgimiento de empresas nacionales y la construcción de infraestructura y servicios.

El Poder de los Grandes Bancos se Contrae

Los bancos, que han crecido enormemente debido a su relación especial con los gobiernos y su control sobre el dinero de las personas, irán a la bancarrota o se volverán mucho más pequeños. "Too big to fail" o "Demasiado grande para fracasar" ya no será la norma, y los bancos y las grandes corporaciones ya no podrán depender de los rescates del gobierno cada vez que cometan errores, como en la crisis financiera de 2008.

Sin estas ventajas, los bancos y las corporaciones multinacionales necesitarán enfocarse en proporcionar servicios a sus clientes, en lugar de complacer a los gobiernos para obtener dádivas. Las compañías y bancos más pequeños, gracias a la naturaleza sin fronteras de bitcoin, podrán servir a clientes en todo el mundo y desplazarán a los gigantes arcaicos del pasado.

El Declive del Gran Hermano y el Capitalismo Vigilante

Actualmente, la información de pago digital es explotada por las empresas con fines de lucro y utilizada para la vigilancia del gobierno. Debido a que el Internet evolucionó como un mercado abierto predeterminado, los estándares de privacidad han tardado en proteger la información cada vez más personal e importante que está en línea. Como resultado, los datos personales se vuelven a empaquetar, analizar y usar constantemente sin conocimiento o permiso explícito.

Con el advenimiento y la adopción de los pagos Lightning además de Bitcoin, la mayoría de las compras diarias pequeñas se desconectarán de la identidad.

Al comprar algo en línea, suscribirse a una revista política, donar a una organización de la sociedad civil o pagar un trata-

miento médico, nadie más que el consumidor conocerá todos los detalles de la transacción. No habrá procesador de pagos para filtrar información desde una posición intermediaria, ya que las transacciones son de persona a persona y el comerciante solo ve el pago. Sin información de identificación en este entorno, será mucho más difícil para los sistemas de vigilancia rastrear el comportamiento de los consumidores y predecir sus acciones.

El Inicio de la Soberanía Individual

Bitcoin es un fenómeno de impacto potencial similar a la democracia y el Internet: tecnologías que derrocaron respectivamente la tiranía del poder político y el control corporativo del conocimiento. A través de la democracia, los ciudadanos mantienen colectivamente bajo control el poder del gobierno y de los dictadores, y a través de Internet, los ciudadanos promedio obtienen una voz más fuerte y un acceso más libre al conocimiento.

En el mismo tenor, Bitcoin destrozará el monopolio monetario del que gozan los estados y las corporaciones. Dentro de un siglo, las personas mirarán hacia atrás en 2019 y recordarán como obsoleta una época en la que unos pocos privilegiados controlaban la economía, al igual que hoy alguien recuerda la idea del sistema feudal monárquico o la propaganda estatal como obsoleta. Esta evolución tendrá lugar en tres fases a medida que Bitcoin evoluciona hacia la moneda del mundo.

Fase 1: Reserva de valor

El primer paso para la adopción de Bitcoin será como una reserva de valor. Esta es la etapa en la que los ahorradores de todo el mundo se protegen contra la inflación de sus gobiernos locales. Esto está sucediendo hoy no solo en economías hiper-

inflacionarias como las de Venezuela y Zimbabwe, sino también en lugares como Estados Unidos y Europa, donde el bitcoin ha superado a la moneda fiduciaria local durante tramos de varios años. Al final de la fase de almacenamiento de valor, los fondos de pensiones y las instituciones financieras convencionales comenzarán a agregar bitcoins a sus carteras, y aún más tarde, los gobiernos comenzarán a agregar bitcoins a sus reservas.

La adopción durante esta fase crecerá lenta y orgánicamente a medida que las personas se den cuenta de sus beneficios.

Fase 2: Método de Pago

Cuando suficientes comerciantes se den cuenta de que el dinero que no es bitcoin es, de hecho, una reserva de valor inferior, querrán que se les pague en bitcoin. Esto es similar a los comerciantes del mercado negro en Venezuela que rechazan bolívares y demandan dólares estadounidenses. A medida que más comerciantes, empresarios y empleados prefieran bitcoin, la demanda de bitcoin aumentará de la misma manera que la demanda de dólares estadounidenses se disparó tras la introducción del sistema de convertibilidad de oro de Bretton Woods.

Esto no sucederá inicialmente en economías avanzadas como la de los Estados Unidos, sino en economías descompuestas con inflación salvaje y corrupción intratable. Es probable que estas sociedades estén regidas por regímenes opresivos que disminuyan la utilidad de reservas de valor fácilmente confiscables, como los billetes en dólares y el oro. Las personas en esos lugares usarán bitcoin para evadir la incautación de su riqueza y, si es necesario, para escapar por completo.

En esta fase, el software bien diseñado, las tecnologías de liquidación más rápidas, la infraestructura mejorada y las innovaciones de privacidad saldrán a la vanguardia. Los usuarios de

Bitcoin podrán llevar a cabo transacciones de forma instantánea y privada, lo que hará que la vigilancia sea mucho más difícil.

Fase 3: Unidad de Cuenta

A medida que más personas posean y ganen bitcoins en lugar de su moneda local, los bienes y servicios comenzarán a cotizarse en su precio absoluto de bitcoins en lugar de la moneda local o el USD. En este punto, habrá oportunidades de arbitraje lucrativas, por lo que sacar préstamos en monedas que se deprecian rápidamente y convertirlas en bitcoins será rentable.

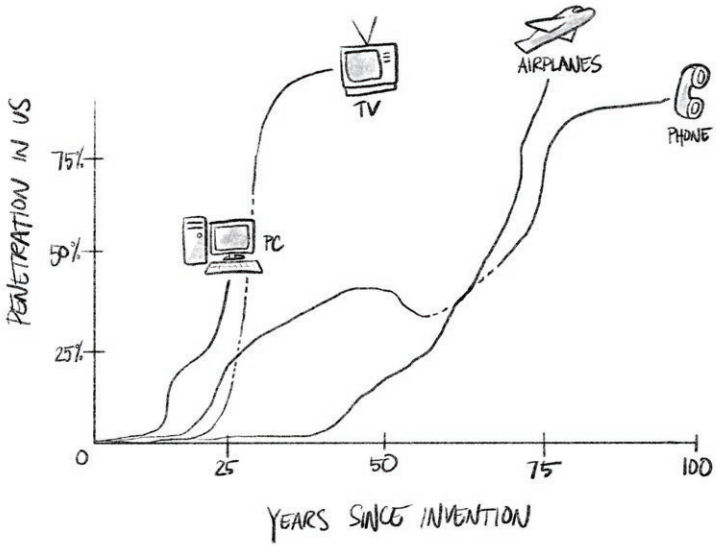
Este será el comienzo de la hiperbitcoinización, donde el USD y el CNY perderán sus posiciones privilegiadas y Bitcoin se convertirá en la moneda de liquidación mundial. Esto, a su vez, causará hiperinflación por parte de la mayoría de las otras monedas, ya que los préstamos serán muy caros para evitar el arbitraje. Como Bitcoin será el lugar más deseable para almacenar valor, el ciclo de retroalimentación positiva hará que muchas otras monedas se deprecien sustancialmente.

Aún es Pronto

La mayoría de las tecnologías que cambian el mundo son descartadas por la multitud al principio. Pongamos como ejemplo la electricidad, que se consideraba muy peligrosa; el teléfono, que nadie quería comprar; el automóvil, que seguramente no podría funcionar en carreteras empedradas; el avión, que posiblemente no podría estar a salvo; el microondas, que supuestamente eliminó todo valor nutricional de los alimentos; el teléfono móvil, que presuntamente causó cáncer; o internet, que estaba destinado al fracaso. Recuerde las palabras del columnista del New York Times Paul Krugman, quien escribió

en 1998 que "para 2005, quedará claro que el impacto de Internet en la economía no ha sido mayor que la máquina de fax".

Cualquier tecnología fundamental, desde el refrigerador hasta la tarjeta de crédito, sigue una curva de adopción, y siempre hay muchos escépticos al principio. Eventualmente, la curva se eleva exponencialmente, formando una S, y la tecnología se extiende. Es difícil imaginar una idea más justa o democrática que el hecho de que cualquiera - independientemente de su ubicación, género, idioma, edad, nivel de educación o riqueza, pueda involucrarse significativamente con Bitcoin - una tecnología exponencial que todavía está en la parte inferior de la curva de adopción en forma de S.



Actualmente, Bitcoin está lejos de donde debe estar en términos de usabilidad, capacidad, conciencia pública e interés comercial. No hay suficientes compañías construyendo sobre Bitcoin; no hay suficientes estudiantes enfocados en ello; no hay suficientes maestros asignándolo; no hay suficientes

comerciantes que lo acepten; no hay suficientes fundaciones filantrópicas que respalden su desarrollo; y no hay suficientes líderes públicos que tomen en serio su capacidad de ayudar a lograr la privacidad financiera. Se necesita más interés, compromiso y pensamiento crítico en esta área.

Menos del 1% de la población mundial ha tenido bitcoins. Si se invierte el tiempo y los recursos adecuados en el desarrollo de billeteras, intercambios y materiales educativos fáciles de usar, Bitcoin tiene el potencial de marcar una diferencia real para miles de millones en todo el mundo. Bitcoin puede ayudar a cualquiera a lograr más libertad financiera, pero es probable que primero ayude a quienes más lo necesitan.

Las personas en Nigeria, Turquía, Filipinas, Venezuela, Irán, China, Rusia o Palestina no tienen las mismas libertades, derechos humanos y confianza en su sistema financiero que las de Occidente. Para ellos, Bitcoin es una forma de escapar.

La exclusión, el silencio y la salida son las nuevas formas de protesta. Para promulgar el cambio, una persona no necesita coordinarse con miles de personas de ideas afines para inundar las calles durante un día o una semana a la vez. Dichas personas pueden exportar su riqueza tan fácilmente como pueden enviar un correo electrónico. Las protestas ahora pueden ocurrir una persona a la vez. Al principio, la adopción será un goteo, luego un arroyo y, finalmente, una inundación.

El Futuro Está en Sus Manos

Bitcoin es una invención significativa que proporciona nuevas alternativas a muchos problemas del sistema monetario y económico actual. La desigualdad, las corporaciones multinacionales monopólicas y el autoritarismo son, en parte, alimentados por el control estatal del dinero. A medida que el mundo aprenda sobre Bitcoin y cómo permite la soberanía

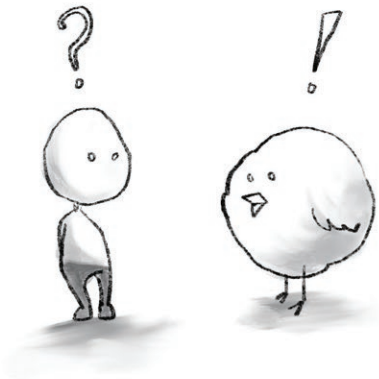
individual, el poder se descentralizará de manera significativa en todo el mundo. En lugar de regímenes autoritarios, más gobierno respetarán la dignidad humana, el valor y el talento. En lugar de corporaciones multinacionales desconectadas, habrá compañías más pequeñas que trabajarán para atender a sus clientes. Si bien la igualdad de resultados no es posible, Bitcoin nivelará el campo de juego al permitir que los humanos capturen y conserven el valor que crean.

¿Qué podría ser más justo que la idea de que todo lo que se necesita para participar en la próxima revolución financiera sea el acceso a un teléfono inteligente de bajo costo e Internet? Ningún banco, ningún regulador gubernamental, no se requiere permiso para ser parte de este futuro.

Al recuperar el control de la riqueza de los caprichos de quienes tienen el control, todos pueden ser más libres para crear su propio destino.

Bitcoin permite la libertad humana de una manera que nunca se pensó posible a principios del siglo XXI.

Pase este libro y ayude a correr la voz.



Q&A de Bitcoin

En los últimos años, los novatos y los escépticos han formulado muchas preguntas sobre Bitcoin. Esta sección intenta responder a las importantes y frecuentes, abordando algunos de los mitos, desafíos, desventajas y confusiones comunes en torno a Bitcoin. Esta sección tiene como objetivo proporcionar suficiente información fundamental para que una mente curiosa tenga un buen comienzo, pero de ninguna manera es exhaustiva.

¿Quién es Satoshi Nakamoto?

Satoshi Nakamoto es el creador anónimo de Bitcoin.

En los primeros dos años de la historia de Bitcoin, Satoshi Nakamoto fue un miembro activo de la comunidad. Satoshi publicaba en línea con frecuencia ideas sobre la tecnología de Bitcoin y su impacto social, al mismo tiempo que contribuía al desarrollo de software. A finales de 2010, Satoshi desapareció.

Satoshi probablemente posee cientos de millones de dólares en bitcoins, que cualquiera puede ver en la cadena de bloques. Estas monedas nunca se han movido, lo que sugiere que la desaparición podría ser permanente. Al escribir estas líneas, la identidad de Satoshi no se ha revelado, lo que lo convierte en uno de los mayores misterios del siglo XXI.

¿Quién Controla Bitcoin?

No hay una autoridad central a cargo de Bitcoin. No hay CEO, ni junta directiva, ni compañía controladora. Uno de los atributos más fuertes de Bitcoin es que su creador ya no está involucrado.

Hay miles de validadores en todo el mundo que verifican la cadena de bloques de Bitcoin y almacenan el historial completo de las transacciones de bitcoin. Estos validadores se denominan nodos completos.

Como se discutió en el Capítulo 2, los mineros de todo el mundo compiten para producir bloques. Esos bloques son validados por los nodos completos. El software utilizado para ejecutar esos nodos completos está escrito por desarrolladores de Bitcoin. Y, por supuesto, las transacciones dentro de esos bloques son iniciadas por los usuarios desde sus intercambios, billeteras o procesadores de pagos. Todos estos participantes son esenciales para que Bitcoin funcione, pero ninguno de ellos controla Bitcoin.

Si un desarrollador decide crear un software de nodo completo que es radicalmente diferente, pocos ejecutarán ese software. Si un minero intenta colarse en un nuevo bloque de transacciones que no cumple con los requisitos de validación, los nodos completos rechazarán ese bloque. Si los mineros intentan un golpe de estado para imponer nuevas funciones en la red, fracasarán ya que no pueden obligar a los usuarios a ejecutar software que no quieren ejecutar.

Por lo tanto, cualquier cambio en Bitcoin requiere consenso. En este sentido, el modelo de gobierno de Bitcoin es similar a una democracia con controles y equilibrios. Los mineros son como la rama ejecutiva del gobierno, manejan operaciones y hacen cumplir las reglas; los desarrolladores son como el poder legislativo, desarrollando y aprobando nuevas leyes; los

usuarios son la rama judicial, asegurándose de que las otras dos ramas no cometan nada inconstitucional.

¿No es Bitcoin muy volátil?

Bitcoin ha experimentado una tremenda volatilidad desde su creación en 2009. Visto en un período de tiempo más largo, Bitcoin se ha apreciado significativamente desde el inicio, de menos de $.001 a más de $ 11.000 al momento de escribir este artículo. Como se explicó en el Capítulo 3, varios factores han impulsado su precio a largo plazo y probablemente continuarán haciéndolo.

Satoshi Nakamoto estableció la política monetaria de Bitcoin al inicio. Ninguna persona o grupo puede decidir crear más bitcoins o cambiar su programa de suministro, ya que los nodos completos rechazarán dicho cambio.

Como resultado, Bitcoin será más vulnerable a la manipulación del mercado ya que no tiene un mecanismo de corrección de la banca central. Un banco central puede imprimir dinero nuevo o comprar más de su propio dinero para mantener la estabilidad de precios. Como moneda descentralizada, sin reguladores correctivos, continuará experimentando volatilidad a medida que se adopte en todo el mundo.

La realidad económica es esta: las monedas tienen que elegir entre la estabilidad de precios a corto plazo a través de la centralización o el potencial para una apreciación de los precios a largo plazo a través de la descentralización. Satoshi Nakamoto eligió la descentralización.

Lo más importante es que la volatilidad de bitcoin no ha impedido que tenga un enorme valor en el mundo real como herramienta financiera para las personas atrapadas en sistemas financieros deshechos. Los casos prácticos de Bitcoin incluyen

escapar de sanciones, hiperinflación, controles de capital y vigilancia. Por ahora, la volatilidad del día a día es una compensación que los propietarios han estado dispuestos a pagar.

¿Qué realmente respalda el valor del Bitcoin?

Esta respuesta breve es que la gente respalda Bitcoin. Suficientes inversionistas lo compran, por lo que tiene valor. Consulte el Capítulo 3 para obtener una explicación detallada de lo que le da a Bitcoin su precio históricamente ascendente. Existe una demanda global de bitcoin como un activo que es escaso, tiene utilidad y hace las cosas como una tecnología que ninguna otra herramienta financiera puede hacer.

¿Cómo se puede confiar en Bitcoin?

El mundo moderno está lleno de sistemas o dispositivos complejos que no se entienden completamente, pero no son confiables. La atención médica se brinda a personas que no son médicos. Los pronósticos del tiempo se publican para no meteorólogos. Las computadoras portátiles son utilizadas por personas que no son ingenieros eléctricos. Los viajeros no tienen que entender la aerodinámica para viajar en aviones.

Los estándares para confiar en los nuevos sistemas monetarios deberían ser más estrictos, ya que hay abusos frecuentes de esa confianza, muchos de los cuales se han documentado a lo largo de este libro. Pero en última instancia, la experiencia en el tema no será necesaria para usar y confiar en Bitcoin. Eventualmente, enviar y recibir bitcoins será tan fácil como enviar y recibir un correo electrónico. Por ahora, los interesados en Bitcoin definitivamente deberían hacer su propia investigación. En la sección Recursos Adicionales de este libro se incluyen muchas buenas fuentes de información, incluido el código fuente de Bitcoin Core, otros libros, sitios web y podcasts.

¿Qué tan confiable es Bitcoin?

Cuando se usa correctamente, Bitcoin es mucho más seguro, más robusto y más privado que cualquier procesador de pagos centralizado. Mastercard y Visa, por ejemplo, tienen interrupciones ocasionalmente. Bitcoin ha estado en pleno funcionamiento durante el 99,98% de su historia desde su lanzamiento en enero de 2009. Las compañías de tarjetas de crédito también venden regularmente información de clientes y son hackeadas. Bitcoin no puede vender ninguna información sobre sus usuarios porque nadie tiene el control. A diferencia de los procesadores de pago y muchos bancos, Bitcoin no ha sido hackeado significativamente desde que el precio subió por encima de $0.10 en 2010. Nunca se han robado las monedas de nadie a nivel de red. Este es un historial admirable.

¿Por qué han sido hackeados tantos portales de intercambio de Bitcoin?

Los portales de intercambio de criptomonedas son muy populares, tanto como un lugar para que los inversionistas compren bitcoin por primera vez como un lugar para que los especuladores intercambien bitcoin por moneda fiduciaria u otras criptomonedas. Como resultado, los portales de intercambio contienen grandes cantidades de bitcoin y moneda fiduciaria en nombre de sus clientes, lo que los convierte en objetivos atractivos para hackers y ladrones. Los servicios de custodia también almacenan copias de identificaciones personales, pasaportes y domicilios de sus clientes como parte de sus procedimientos KYC ("Conozca a su cliente").

Los ataques pueden ocurrir tanto interna como externamente. Los ataques internos pueden provenir de empleados que tienen acceso privilegiado al sistema del portal de intercambio y lo utilizan para robar fondos de los clientes. Los

ataques externos son llevados a cabo por hackers que utilizan vulnerabilidades de software, seguridad operativa débil e ingeniería social para robar bitcoins.

Muchos portales de intercambio han sido atacados tanto interna como externamente. Solo algunos ejemplos incluyen Mt.Gox en Japón, Bitfinex en Hong Kong, Bitstamp en la UE y más recientemente Quadriga en Canadá. Cada uno resultó en millones de dólares en bitcoins perdidos. Estos hackeos son una fuerte advertencia para los usuarios que permiten que otra persona tome la custodia de sus bitcoins. Los clientes que operan en intercambios pueden retirar sus bitcoins periódicamente en billeteras personales para evitar posibles pérdidas por hackeos.

¿Utilizan los criminales bitcoin para lavado de dinero?

Sí. Los delincuentes han utilizado bitcoin para el lavado de dinero y actividades ilegales, y continuarán haciéndolo. El caso más famoso es la Ruta de la Seda o Silk Road, un mercado de redes oscuras donde se usaba bitcoin para comprar y vender drogas consideradas ilegales en los Estados Unidos.

Debido a que Bitcoin es una tecnología que no requiere permisos, cualquiera puede usarla, como el teléfono móvil o el Internet. Pocos cuestionan la legitimidad de estas tecnologías ubicuas hoy en día o piden su prohibición porque los malos actores las usan. Muchas personas dirigen el escepticismo hostil a las tecnologías cuando están surgiendo por primera vez.

En cualquier caso, la mayoría absoluta de los delitos financieros en el mundo de hoy se lleva a cabo utilizando el sistema financiero existente a través de bancos regulados y transmisores de dinero. La mayoría del fraude es cometido por gobiernos y corporaciones multinacionales, no por individuos deshonestos.

Los gobiernos democráticos han establecido reglas contra el lavado de dinero (AML) para presionar a los bancos a detener ciertas transacciones, sin embargo, cada año se lava más de $1 billón a través del sistema bancario. Para dar un ejemplo, los informes revelaron recientemente que una sola oficina del Danske Bank en Dinamarca había lavado la asombrosa cantidad de $230 mil millones, que es más que el valor de mercado de todos los bitcoins en circulación al momento de escribir este artículo.

Entonces, aunque los delincuentes han utilizado bitcoin, los delincuentes prefieren el sistema de dinero fiduciario.

¿Es Bitcoin un Esquema Ponzi?

Un esquema Ponzi promete a los inversionistas grandes ganancias con muy poco riesgo. Los esquemas de Ponzi logran estos retornos para sus primeros inversionistas al pagarles con el dinero recaudado de los inversionistas posteriores. No existe un mecanismo real para obtener ganancias, aparte de tratar de obtener la mayor cantidad posible de nuevos inversionistas para pagar los que vinieron antes. Estos esquemas colapsan cuando no se encuentran nuevos inversionistas.

Bitcoin no es un esquema Ponzi. No hay un grupo de personas detrás de Bitcoin que intente atraer a nuevos compradores para que paguen y liberen a los compradores antiguos. Sin embargo, las personas que organizan los esquemas de Ponzi pueden aceptar bitcoins de sus inversionistas de la misma manera que lo hacen con todas las demás formas de dinero.

¿Es Bitcoin una Burbuja?

Una burbuja ocurre cuando los inversionistas especulativos compran un activo financiero en masa a un precio muy supe-

rior al que justifica su valor fundamental. Las burbujas siempre aparecen tan pronto como se pierde la fe en el activo, y ningún otro inversionista está dispuesto a comprar al precio de venta. Los ejemplos históricos incluyen tulipanes holandeses en el siglo XVI, South Sea Company en el siglo XVII y acciones de Puntocom a principios del 2000.

El Capítulo 3 describía algunos de los principales impulsores de la volatilidad de los precios de Bitcoin. Debido a la volatilidad natural de un activo con una política monetaria rígida, choques de oferta regulares, la inestabilidad y el colapso de otras criptomonedas, la manipulación del mercado y la naturaleza apalancada del comercio de bitcoin, han habido varios aumentos de precios que han sido seguidos por importantes caídas. Esta es una tendencia que probablemente continuará.

Al considerar el valor a largo plazo, los determinadores de precios y la naturaleza descentralizada de Bitcoin, su valor debería aumentar naturalmente a medida que más personas lo usen. A diferencia de los tulipanes o las acciones Puntocom, el valor de Bitcoin se ha recuperado y tendido al alza repetidamente después de cada caída importante del mercado a medida que más y más personas en todo el mundo adquieren bitcoins.

¿Qué es Tether y cómo afecta al Bitcoin?

Tether, o USDT, es una moneda que se supone que está vinculada al dólar estadounidense. Para lograr esto, la compañía detrás de Tether tenía la intención de respaldar cada token de Tether en circulación con un dólar estadounidense en la cuenta bancaria de la compañía. Esto hizo que fuese más fácil especular sobre la criptomoneda, ya que la mayoría de las personas todavía piensan en moneda fiduciaria, por lo que tener el USDT como proxy de los dólares estadounidenses ha hecho posible que cualquiera de los muchos portales de intercambio cripto-a-

cripto pueda comerciar activamente contra el dólar estadounidense.

Sin embargo, en abril de 2019, el abogado general de Tether reveló que solo tenían dólares estadounidenses para respaldar el 74% de Tether en circulación. Si se rompe la vinculación del dólar de Tether, su colapso de precios puede causar volatilidad de bitcoin a corto plazo - pero hay una serie de competidores de Tether que están bien preparados para cumplir su función.

¿Pueden los gobiernos prohibir o apagar a Bitcoin?

Debido a que no hay una compañía, ni un conjunto de servidores coordinados centralmente, ni un solo equipo que ejecute Bitcoin, no hay una forma práctica de cerrar la red.

Bitcoin es un software de código abierto, lo que significa que el código fuente está abiertamente disponible en Internet. Corromper o cambiar ese software es muy difícil porque la gente está mirando. Cualquiera puede descargar, usar, copiar y ejecutar el software de Bitcoin y validar el libro mayor. Esto se llama ejecutar un nodo completo. Cuantos más nodos completos estén en la red, más resistente será Bitcoin.

Los gobiernos pueden hacer que Bitcoin sea más difícil de usar, pero luego se convierte en un juego de whack-a-mole. Considere la experiencia de intercambiar moneda fiduciaria por Bitcoin en un país como China. Como se mencionó en el Capítulo 1, las personas chinas tienen limitado convertir hasta $50.000 cada año de su CNY, pero continúan usando bitcoin para mover dinero al extranjero.

Incluso un estado grande, rico y policial no puede evitar que su ciudadanía use Bitcoin. Debido a que la red no tiene

un punto único de falla, los gobiernos no pueden apagar la red Bitcoin.

Bitcoin es similar a Internet de esta manera. Un gobierno puede evitar que los ciudadanos accedan a partes de Internet, por ejemplo, el Gran Firewall chino, pero los ciudadanos censurados utilizarán herramientas como VPN e ingenio para sortear estas restricciones. Ningún gobierno puede bloquear el acceso a la red Bitcoin sin eliminar el acceso a Internet, un costo en el que pocos gobiernos más allá de Corea del Norte parecen estar dispuestos a incurrir.

Los gobiernos autoritarios podrían prohibir la posesión de bitcoin, pero la aplicación sería extremadamente difícil. Debido a su naturaleza digital, ocultar bitcoin es relativamente fácil. Almacenar bitcoins en un teléfono, en un dispositivo USB o incluso en la mente de una persona son todas las opciones que son muy difíciles de descubrir y penalizar. En contraste, el oro, los bienes raíces, las acciones y las cuentas bancarias fiduciarias son relativamente fáciles de localizar y confiscar para los gobiernos.

¿Es legal el Bitcoin?

Mayormente sí. A partir de agosto de 2019, su posesión está permitida en todos los países, excepto Namibia, Argelia, Bolivia, Irak, Marruecos, Nepal, Pakistán, Emiratos Árabes Unidos y Vietnam. Desde un punto de vista regulatorio, Bitcoin ha recorrido un largo camino: en los últimos 10 años, Bitcoin ha progresado desde ser visto como el dinero de los delincuentes en línea hasta ser reconocido por el FMI, los miembros del Congreso de los Estados Unidos y Wall Street.

En China, el gobierno ha vigilado los portales de intercambio de criptomonedas y la creación de nuevos tokens, pero bitcoin

está legalmente reconocido como propiedad digital. Incluso en Irán, la minería de bitcoins es ahora una industria legalizada.

En el continente africano, los gobiernos de la mayoría de los países no tienen una postura pública. En lugares como Nigeria y Kenia, los funcionarios públicos advierten contra su uso, pero no hay regulaciones concretas. Sudáfrica es actualmente el único país africano donde Bitcoin es oficialmente aceptado y regulado.

En Canadá, los EE. UU. Y la UE, la posesión y el uso de bitcoin es legal.

Algunos países han creado un marco de licencia específico para empresas que desean operar portales de intercambio de criptomonedas. Estos incluyen Japón, Malta, Filipinas y Tailandia.

Las implicaciones fiscales son más complicadas y están determinadas por la forma en que cada gobierno clasifica bitcoin. Si una autoridad tributaria considera la propiedad de bitcoin, entonces los individuos serán gravados de acuerdo con su adquisición, liquidación, apreciación y depreciación, similar a una propiedad inmobiliaria.

Mirando hacia el futuro, si los gobiernos quisieran conspirar para prohibir Bitcoin, es poco probable que puedan llegar a un acuerdo. Incluso si algunos países lograran establecer una prohibición, otros países intervendrían y darían la bienvenida a los mineros, empresarios y comerciantes de bitcoins. Habría una migración de talento y riqueza a esas jurisdicciones más amigables, haciendo que los gobiernos restrictivos reconsideren sus políticas.

¿Es la minería de bitcoin un desperdicio de energía o mala para el medioambiente?

A partir de junio de 2019, la red de Bitcoin consume alrededor de 73 teravatios-hora al año de electricidad. Esto es un poco más de consumo que el país de Austria (69 teravatios-hora al año), pero mucho menos que China (6.100 teravatios-hora al año) y los Estados Unidos (3.900 teravatios-hora al año), los dos mayores consumidores de energía.

Los críticos señalan rápidamente que se trata de una enorme cantidad de poder. Si bien eso es técnicamente cierto, no aborda si Bitcoin desperdicia energía o es perjudicial para el medio ambiente. Las fuentes de energía que los mineros de Bitcoin usan típicamente y el valor que proporciona Bitcoin pueden proporcionar algún contexto.

Evitar el Desperdicio de Energía con la Minería de Bitcoin

La minería de Bitcoin puede ayudar al exceso de capacidad a encontrar un buen uso. La minería es un negocio tanto móvil como de bajo margen. Por lo tanto, las compañías mineras tienen un incentivo especialmente grande y la capacidad de buscar físicamente la electricidad más barata posible. Con frecuencia, las fuentes de energía más baratas se encuentran en lugares remotos o inaccesibles donde hay capacidad no utilizada.

La mayoría de la minería de Bitcoin se lleva a cabo en China, donde las plantas de energía producen colectivamente un excedente de 200 teravatios-hora en un momento dado. Dado que no es posible almacenar tanta energía (la granja de baterías más grande del mundo solo puede contener alrededor del 0,5% de esa cantidad) - y dado que no es posible transmitir eficazmente la energía a regiones remotas - la electricidad normalmente no

se aprovecha. En lugar de desperdiciar ese potencial, las plantas de energía pueden comprar equipos de minería de bitcoin y convertir el exceso de energía en nuevos bitcoins. Esto es cierto en cualquier lugar donde una fuente de energía genera demasiado para uso inmediato.

La Dependencia de la Minería de Bitcoin de Energía Renovable

La mayoría de la minería de bitcoins hoy en día se realiza con energía renovable que tiene un costo mínimo para el medio ambiente. Según las últimas estimaciones, alrededor del 75% de toda la minería de bitcoins se realiza actualmente con fuentes de energía hidroeléctrica, solar, eólica y geotérmica. Alrededor del 50% de la minería bitcoin de energía renovable se realiza en un área de China, impulsada por represas hidroeléctricas.

Las centrales hidroeléctricas tienen una capacidad de producción de energía masiva, pero a menudo están subutilizadas. La minería de Bitcoin pone el exceso de capacidad en uso, ya que la operación de minería se puede colocar al lado de la planta hidroeléctrica, eliminando los costos de transmisión. Los ingresos generados hacen que la producción y la investigación de la energía hidroeléctrica sean más rentables, fomentando su uso. De esta manera, la minería de Bitcoin subsidia la energía hidroeléctrica.

La minería también puede incentivar una mayor producción de energía solar, eólica y geotérmica.

La Minería de Bitcoin Permite Tener Dinero Seguro y Accesible

Los mineros de Bitcoin proporcionan seguridad para la red. Como se discutió en el capítulo 2, la electricidad requerida por los mineros para buscar números de prueba de trabajo escasos para proponer bloques válidos hace que el fraude sea muy costoso. Cuanta más minería de bitcoins haya, más difícil será atacar la red. La energía utilizada para asegurar el libro mayor se puede comparar con el costo de crear y mantener una bóveda de alta seguridad que protege $200 mil millones en activos.

Bitcoin podría ser solo una de las muchas opciones financieras para quienes viven en el primer mundo, pero en otras partes del mundo, los servicios de pago como Venmo o ApplePay no están disponibles. Descartar la minería de Bitcoin como un desperdicio de energía es descontar la utilidad que Bitcoin le da a la subclase tecnológica. Parte de esta energía se destina al procesamiento de transacciones para personas que no tienen cuentas bancarias o identificaciones, o que no desean que su actividad fiscal sea estrictamente vigilada por los gobiernos. Los bancos y las tarjetas de crédito pueden superar la utilidad de Bitcoin en un lugar como los Estados Unidos, pero no hacen nada por un trabajador migratorio no bancarizado en Dubai o un iraní que vive bajo las sanciones de la ONU.

Uso de Energía e Innovación Tecnológica

Bitcoin es una innovación técnica importante, que permite muchas cosas descritas en este libro que el sistema monetario actual no puede hacer. Históricamente, la nueva tecnología usa más energía que los sistemas antiguos que desplazan. Por ejemplo, considere la interrupción del caballo por el automóvil; la tienda de campaña junto al hospital moderno; lavandería manual por una lavadora; un depósito de hielo junto al refrigerador; y lámparas de aceite por lámparas eléctricas. El costo

de la electricidad de la innovación técnica se compensa con la mejor calidad de vida que facilita. A medida que avanza la civilización, se gasta más energía por individuo. La innovación mejora la sociedad, y ninguna innovación se adopta sin algunas concesiones. Las concesiones en Bitcoin son el uso de electricidad a cambio de un sistema monetario justo, conveniente y seguro. Bitcoin utiliza mucha energía, pero está impulsando la innovación para las energías renovables. Bitcoin proporciona un valor tremendo, especialmente para los pobres y los oprimidos, y reemplaza un sistema antiguo y defectuoso que usa aún más energía.

¿Qué sucede si una persona con una supercomputadora o computadora cuántica hackea la red de Bitcoin?

En teoría, la red de Bitcoin puede verse comprometida por un atacante con suficiente potencia informática. En la práctica, eso es muy difícil de hacer.

Con el hardware actual, un atacante debe financiar, construir y operar una instalación minera a un costo de más de mil millones de dólares, y luego encontrar un proveedor de energía con una producción equivalente a 8 Presas Hoover. Los mismos recursos, cuando se dedican a la minería de forma honesta serían una empresa extremadamente rentable. Tal ataque es, por lo tanto, económicamente irracional.

Al escribir estas líneas, estas cosas son ciertas sobre la computación cuántica:

1. Las computadoras cuánticas son extremadamente lentas en comparación con las computadoras convencionales en muchos órdenes de magnitud.

2. Las computadoras cuánticas son extremadamente caras de construir y seguirán siendo prohibitivas debido a su costo durante bastante tiempo.

3. Los algoritmos cuánticos más conocidos son un avance significativo, pero aún requerirían varios miles de millones de computadoras que se ejecuten durante miles de millones de años para descifrar la criptografía utilizada en Bitcoin.

Incluso si los científicos descubrieran nuevos algoritmos cuánticos que pudiesen romper la criptografía moderna, la criptografía cuántica segura se incorporaría entonces a Bitcoin.

En otras palabras, los usuarios de Bitcoin y la comunidad de desarrolladores podrían estar un paso por delante de cualquier atacante cuántico. Si bien la comunidad de Bitcoin debe estar atenta a las posibilidades de ataques a gran escala, el usuario promedio de bitcoin no necesita preocuparse.

¿Cómo puede Bitcoin permanecer descentralizado?

Una de las propiedades más importantes de Bitcoin es que cualquier persona en el mundo puede descargar una copia completa del libro mayor de Bitcoin - cada transacción realizada en la red - y verificar por sí mismos que el registro histórico es correcto.

Como se cubre en el Capítulo 2, esta práctica se llama ejecutar un nodo completo. La facilidad de operar un nodo completo es fundamental para la resistencia general a la censura de la red Bitcoin. Si la red de Bitcoin dependiera de un puñado de compañías o un pequeño grupo de personas ricas para ejecutar nodos completos, podrían coludir y editar los registros, o robar monedas. Cada usuario puede, al ejecutar un

nodo completo, verificar todo y no tener que confiar en nadie más. Si se requiriese un equipo costoso de servidor o conexiones rápidas a Internet para ejecutar un nodo completo, esto obligaría a las personas más pobres a confiar en los demás. La red se centralizaría naturalmente en ubicaciones del primer mundo y negocios de alta tecnología.

Afortunadamente, como los requisitos para ejecutar un nodo completo son muy bajos, muchos miles de usuarios en diferentes continentes, completamente desconocidos entre sí, verifican la cadena de bloques de Bitcoin de forma continua. Además, con los nodos completos de hardware intuitivos cada vez más disponibles en el mercado, la operación de un nodo completo en el hogar es accesible para usuarios no técnicos. Actualmente, varios científicos de instituciones como MIT y Stanford están ayudando a idear formas para que cualquiera pueda ejecutar un nodo completo en su teléfono móvil en el futuro, lo que mejoraría aún más la descentralización de la red de Bitcoin.

¿Protege Bitcoin la Privacidad?

Un concepto popular erróneo es que Bitcoin es anónimo. Bitcoin es seudónimo y, con suficiente trabajo detectivesco y análisis forense, se pueden conectar las transacciones y la identidad de un usuario. Con la seguridad operativa adecuada, un usuario inteligente de bitcoin puede disfrazar las transacciones hasta el punto de dificultar la vigilancia. Sin embargo, con suficiente tiempo o recursos, un estado nacional o una corporación motivada aún puede rastrear a un individuo.

Dicho esto, bitcoin proporciona una privacidad mucho mejor para las transacciones que los sistemas de pago existentes. Las compras en línea se pueden hacer con bitcoin sin revelar datos privados como el nombre, la cuenta bancaria o la dirección de alguien. Esa es una mejora con respecto al

sistema bancario existente donde los gobiernos, corporaciones y comerciantes solicitan y luego comparten, venden o filtran datos privados a diario.

Las mejoras continuas y programadas de Bitcoin, como la Red Lightning, Taproot, Graftroot y Firmas Schnorr, colectivamente harán que las transacciones privadas de bitcoin sean más baratas y fáciles. Bitcoin tiene el potencial de ser una excelente tecnología de privacidad, lo que hace que la vigilancia financiera masiva sea extremadamente difícil.

El Internet fue alguna vez completamente abierto y público. A medida que los usuarios y las empresas requerían más transacciones privadas, los ingenieros agregaron capas de privacidad además del Internet original. La comunicación privada ahora es posible utilizando aplicaciones que envían mensajes cifrados automáticamente. Bitcoin está siguiendo un camino similar.

¿Cómo Puede Bitcoin Suplir las Necesidades de 7 Mil Millones de Personas?

En 1989, cuando los científicos inventaron la World Wide Web para funcionar sobre Internet, la idea de que los usuarios algún día podrían estar intercambiando fotos, y mucho menos videos, parecía técnicamente imposible. A medida que la tecnología mejoró y evolucionó, el Internet se ha ampliado para dar lugar a aplicaciones que antes eran impensables y que requerían muchos recursos, como compartir videos y conferencias. Cada minuto se suben 300 horas de video a YouTube y se ven 5 mil millones de videos todos los días. Al igual que Internet, hay muchas formas de escalar Bitcoin.

Como se discutió en el Capítulo 4, las capacidades de Bitcoin se están incrementando actualmente a través de la Red Lightning. Además de mejorar la privacidad de las transacciones, Lightning también escala la red de Bitcoin.

Lightning puede manejar millones de transacciones de bitcoin por segundo. Bitcoin está en camino de escalar exponencialmente, mientras que las redes de pago tradicionales como Visa escalan linealmente al agregar más y más servidores. Bitcoin podría revolucionar el dinero y habilitar productos completamente nuevos utilizando micropagos tan granulares como una milésima (1/1000) de satoshi a la vez.

Mediante una combinación de transacciones ocasionales, en cadena, cautelosas, lentas, ultra seguras y resistentes a la censura, y transacciones por lotes, instantáneas y económicas en Lightning, Bitcoin puede convertirse en un sistema de pago global con todas las funciones. Esta es una visión que vale la pena perseguir, ya que quitaría aún más el poder sobre las finanzas de los gobiernos y las corporaciones y lo volvería a poner en manos de la gente.

Aunque es difícil de imaginar hoy, que Bitcoin satisfaga las necesidades de miles de millones de personas no es un concepto menos extravagante que transmitir video a miles de millones de espectadores una vez lo fue en el Internet.

¿Existe Desigualdad de Riqueza Extrema en Bitcoin?

Las personas que estuvieron involucradas con Bitcoin en una etapa temprana tuvieron la oportunidad de acumular una gran cantidad de Bitcoin. La cadena de bloques, sin embargo, muestra que muchos de los primeros usuarios de 2009 a 2012 también vendieron sus Bitcoin en el mismo período de tiempo. Muchos compradores a $1 en 2011 vendieron por $4 varios meses después o $30 un par de meses después.

Muchos de los primeros usuarios no tuvieron el estómago para enfrentar la extrema volatilidad e incertidumbre de los primeros días, o perdieron sus claves privadas, lo que hizo que

sus bitcoins se perdieran permanentemente. Los que se mantuvieron, apoyaron el ecosistema desde su infancia y realmente creen en el potencial de Bitcoin para cambiar el mundo. Hoy en día, hay unos pocos miles de direcciones que almacenan la mayoría de Bitcoin. Algunos son personas que ahora son extremadamente ricos. La mayoría son compañías que usan tales direcciones para almacenar la riqueza de decenas de miles de sus clientes (por ejemplo, Coinbase, Binance). Como no existe una correlación uno a uno entre las direcciones y los usuarios, es difícil saber exactamente cuál podría ser la distribución de la riqueza.

Bitcoin no va a resolver la desigualdad económica. Cualquiera que diga eso está mintiendo. Sin embargo, como una reserva de valor universalmente accesible que los gobiernos no pueden devaluar, Bitcoin ofrece a los ahorradores una oportunidad justa de mantener lo que ganan a medida que envejecen, a diferencia del sistema monetario actual.

¿Si solo hay 21 millones de bitcoins, cómo puede el mundo hacer uso de ellos?

Las unidades de moneda fiduciaria tradicionales generalmente se dividen en 100 subunidades llamadas centavos o céntimos. USD y EUR se pueden dividir en 100 centavos, CNY en 10 jiaos o 100 fens, y CZK (corona checa) en 100 halers.

Los bitcoins, por otro lado, se pueden dividir en 100.000.000 (cien millones) de unidades más pequeñas. La unidad atómica de bitcoin se llama satoshi (o sat, para abreviar) nombrada así en honor al inventor de Bitcoin.

Por lo tanto, el suministro total de bitcoin es 2.100.000.000.000.000 satoshis. Para obtener contexto, esto es más divisible que el USD, cuya oferta monetaria M2 es de 1.500.000.000.000.000 centavos al momento de escribir estas

líneas. La divisibilidad de bitcoin está a la par o mejor que el USD.

Como ejercicio de pensamiento, dividir todos los satoshis existentes entre 7 mil millones de personas produce 300.000 sats por persona. Eso parece suficiente divisibilidad para satisfacer las actividades económicas de cada individuo en caso de que Bitcoin se convierta en el dinero dominante del mundo.

¿Cómo Puedo Costear un Bitcoin? ¡El precio es tan alto!

Bitcoin es divisible, por lo que es posible comprar una pequeña fracción de un bitcoin - $5 o $25 en bitcoin actualmente equivalen a 0.00044 bitcoins y 0.00222 bitcoins, respectivamente.

¿Cómo adquiero bitcoins?

Las principales formas de obtener bitcoin incluyen:

1. Minería
2. Compra
3. Ganancia

Minería

En este punto de la historia de Bitcoin, la minería de Bitcoin es un negocio de muy bajo margen. Al igual que la extracción de oro, el equipo, los contactos de la industria y el conocimiento especializado para extraer de manera rentable requieren años de experiencia y millones de dólares en capital. Como tal, la minería se ha convertido en el dominio de las empresas y organizaciones con importantes recursos y conocimientos, y no es factible que las personas sin experiencia minen de manera

rentable. Para los nuevos usuarios, Bitcoin será más barato de adquirir comprando o ganando que la minería.

Compra

Hay varias formas de comprar bitcoin, algunas más privadas que otras. Los cajeros automáticos de Bitcoin y el comercio entre personas son rápidos y relativamente privados.

Los inversionistas pueden suscribirse a portales de intercambio en línea, muchos de los cuales se nombran en Recursos Adicionales. Se requiere que los nuevos clientes envíen su información personal, y el proceso de aprobación lleva de unos minutos a unos pocos días. Estas compañías actúan como bancos y mantienen los bitcoins y la moneda fiduciaria de sus clientes bajo custodia. Por lo tanto, usarlos implica renunciar a cierta privacidad, pero los clientes pueden garantizar la propiedad de sus bitcoins realizando retiros de estos servicios a sus billeteras personales.

Ganancia

Usando una billetera Bitcoin o una Lightning, cualquiera puede recibir directamente bitcoin como pago por bienes o servicios. Los empleados pueden usar los servicios de nómina de Bitcoin para recibir una parte de sus salarios en bitcoin en lugar de moneda fiduciaria.

¿Cómo hago uso de una billetera de bitcoin?

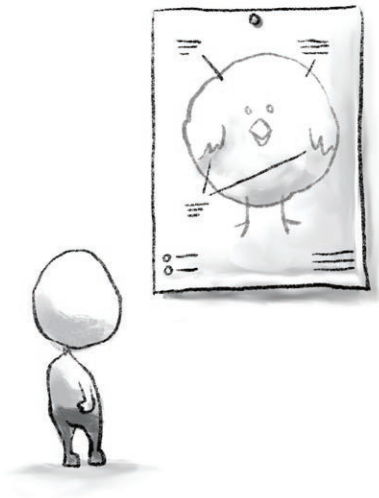
Hay muchos tipos diferentes de billeteras bitcoin, incluidas las billeteras de hardware, de escritorio, móviles y billeteras en línea. Cada uno tiene diferentes compromisos de seguridad, conveniencia y privacidad que los usuarios querrán estudiar.

Una forma razonablemente segura de almacenar bitcoin es a través de una billetera sin custodia, que se menciona en Carteras de Hardware en Recursos Adicionales. Mientras tanto, la forma más conveniente de comenzar es descargar una billetera móvil gratuita, algunas de las cuales se mencionan en Carteras Móviles en Recursos Adicionales.

Después de descargar, el primer paso para configurar una billetera Bitcoin es crear una copia de seguridad. Esta copia de seguridad se conoce como una frase semilla y se usa para recrear la billetera en caso de que se pierda. La frase semilla es una lista de palabras que generalmente se escribe en una hoja de papel. Debido a que se puede usar una frase semilla para recrear la billetera, debe almacenarse con cuidado. Piense en esta frase semilla de la misma manera que una barra de oro o un diamante. La frase semilla tiene un valor significativo y por consiguiente debe protegerse. A medida que el ecosistema crece, las nuevas billeteras se han centrado en disminuir la complejidad y mejorar la usabilidad, la seguridad y la privacidad.

Una vez que se configura una billetera, puede generar direcciones únicas para cada pago nuevo. Esto es diferente de la forma en que funcionan los pagos bancarios habituales, donde a un cliente generalmente se le ofrece un solo número de cuenta. Bitcoin brinda una mejor privacidad financiera al emitir direcciones únicas, todas las cuales pertenecen a la misma billetera de bitcoin.

Como se menciona en la sección *¿Por Qué Han Sido Hackeados Tantos Portales de Intercambio?*, los inversionistas que utilizan servicios de custodia están sujetos al riesgo de hackeo. Retirar fondos hacia billeteras personales después de la compra mitigará ese riesgo.



Recursos Adicionales

El Informe Técnico o Whitepaper de Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System (*Bitcoin: Un Sistema de Dinero Efectivo Electrónico Persona-a-Persona*) de Satoshi Nakamoto es la obra maestra original que colocó a la innovación financiera de los últimos diez años en movimiento.

Código Fuente

Bitcoin Core es el código fuente para el software de nodo completo de referencia de Bitcoin. Creado originalmente por Satoshi Nakamoto, Bitcoin Core tiene contribuciones de más de 500 desarrolladores alrededor del mundo.

Libros

The Internet of Money (Vol 1 & 2) de Andreas M. Antonopoulos es una inmersión profunda hacia el "por qué" de Bitcoin en una serie de ensayos y charlas

Programming Bitcoin de Jimmy Song es una guía técnica práctica de uno de los maestros líderes en programación de Bitcoin para desarrolladores interesados en construir y contribuir con la tecnología.

The Bitcoin Standard de Saifedean Ammous provee una historia económica del dinero y una explicación de cómo Bitcoin provee una alternativa a la banca central.

Inventing Bitcoin de Yan Pritzker es una guía paso a paso de cómo funciona Bitcoin, sin necesidad de algo más que un nivel de matemática de bachillerato.

Grokking Bitcoin de Kalle Rosenbaum es una guía ilustrada de cómo funciona Bitcoin.

Bitcoin Money: A Tale of Bitville Discovering Good Money de The Bitcoin Rabbi es un libro infantil con letras coloridas para ayudar a los niños a aprender sobre Bitcoin.

Mastering Bitcoin: Programming the Open Blockchain de Andreas M. Antonopoulos es una guía integral para programar para y con Bitcoin.

Sitios Web & Publicaciones

Bitcoin.org contiene información útil sobre cómo comenzar, junto con documentación y enlaces a otros recursos. No se recomienda el uso de Bitcoin.com, ya que el sitio web combina intencionalmente otras criptomonedas con BTC en un intento de hacer que los clientes las compren.

Bitcoin.page es un verdadero tesoro de recursos educativos e información sobre Bitcoin cuidadosamente seleccionados por Jameson Lopp.

Bitcoin Wiki es un recurso público para la comunidad de usuarios de Bitcoin, desarrolladores, empresas y cualquier persona interesada en Bitcoin.

Coin Center es una organización sin fines de lucro con sede en EE. UU. centrada en los problemas de política que enfrentan Bitcoin y otras criptomonedas. Publican constantemente explicaciones perspicaces en lenguaje sencillo sobre diversos temas.

Bitcoinmining.com tiene recursos sobre minería de Bitcoin; cómo funciona, cómo comenzar y una lista de comparaciones de hardware.

Global Coin Research se centra en las tendencias de criptomonedas entre los Estados Unidos y Asia.

Podcasts

Tales from the Crypt es un podcast presentado por Marty Bent quien se sienta a discutir sobre Bitcoin con personas interesantes.

What Bitcoin Did es un programa dos veces por semana en el que Peter McCormack entrevista a líderes e influences de la comunidad Bitcoin.

The Stephan Livera Podcast es un podcast enfocado en entrevistas educativas y discusiones sobre la economía y la tecnología de Bitcoin.

Noded es un podcast presentado por Michael Goldstein y Pierre Rochard enfocado en nuevos desarrollos técnicos sobre Bitcoin.

Off the Chain es un podcast de Anthony Pompliano que explora cómo los inversionistas del nuevo y antiguo sistema financiero están pensando en activos digitales como Bitcoin.

Unchained y Unconfirmed son podcasts semanales en los que la presentadora Laura Shin entrevista nombres importantes en criptomonedas.

Let's Talk Bitcoin presenta las ideas y las personas involucradas con la criptomoneda a través de una serie de entrevistas y conversaciones con un grupo de anfitriones habituales.

The Bitcoin Knowledge Podcast es un programa en el que Trace Mayer entrevista a contribuyentes destacados dentro de la industria de Bitcoin para ayudar a los oyentes a comprender mejor la tecnología.

Online Exchanges

Descargo de responsabilidad: aunque esta sección menciona sitios, aplicaciones o servicios específicos dentro del ecosistema de Bitcoin, esto no debe interpretarse como avales o consejos de inversión. Al igual que con otras partes de este libro, se alienta al lector a hacer su propia investigación.

Moneda Fiduciaria a Criptomoneda

Bitfinex - Portal con sede en Hong Kong inaugurado en 2014
CashApp - App de Square para iOS y Androide para comprar bitcoin usando la tarjeta de débito.
Kraken - Portal de los EE.UU y la UE inaugurado en 2014.

Criptomoneda a Criptomoneda

Binance - Portal con sede en Malta inaugurado en 2017.
BitMex - Portal basado en las Seychelles inaugurado en 2014.
Bittrex - Portal basado en los EE.UU inaugurado en 2016.

Mercados Persona-a-Persona

LocalBitcoins - Mercado finlandés de Bitcoin inaugurado en 2012
Paxful - Mercado de Bitcoin de los EE.UU inaugurado en 2015.
Bisq - Un mercado basado en privacidad inaugurado en 2014.

Billeteras

Con Custodia (los clientes no controlan sus claves privadas)

Blockchain.info
CashApp
Coinbase

Sin Custodia (los clientes controlan sus claves privadas)

BreadWallet - Billetera iOS
Bitcoin Core - Billetera de Escritorio
Casa Keymaster - App multi firma de Androide y iOS con soporte de billetera física
Samourai - Billetera de Androide.
Wasabi - Billetera de Escritorio.

Billetera Física (los clientes controlan sus claves privadas)

ColdCard
Ledger
Trezor

Soluciones de Nodo Completo

Casa Node - Nodo completo Plug&Play de Lightning y Bitcoin.
Nodl - Nodo completo de Bitcoin y Lightning.

Glosario

autoridad central - una agencia u organización que toma decisiones para un sistema dado.

bancor - la unidad para una moneda global propuesta en Bretton Woods en 1944.

billetera - una aplicación o dispositivo hardware el cual permite que los usuarios envíen y reciban bitcoins.

Bitcoin - un sistema de dinero descentralizado, digital y escaso creado por Satoshi Nakamoto.

bitcoin - la unidad de valor en la red Bitcoin. Cada bitcoin es 100,000,000 satoshis.

blockchain - un sistema de contabilidad descentralizado pionero de Bitcoin. En Bitcoin, la cadena de bloques rastrea la cantidad de bitcoin que hay en cada dirección. Los componentes de una cadena de bloques son bloques.

blockchain pública - una blockchain que puede ser descargada, accesada y navegada por cualquiera.

bloque - un grupo de transacciones de bitcoin combinadas con un número escaso de prueba de trabajo. Un bloque es equivalente a una página en el libro de contabilidad de Bitcoin. Se crea un nuevo bloque aproximadamente cada 10 minutos.

centralizado - un sistema con un punto único de fallo. Esto puede ser, por ejemplo, un sistema administrado por una persona, fundación, empresa o gobierno.

claves privadas - similar a una clave de una cuenta bancaria, una clave privada desbloquea la posibilidad de transferir bitcoins desde una determinada billetera. La propiedad de las claves privadas es pues, lo mismo que la propiedad de los bitcoins.

descentralizado - un sistema sin un punto único de fallo.

dirección - Similar a un número de cuenta bancaria, una dirección de bitcoin es donde se recibe bitcoin. Cada dirección tiene una clave privada correspondiente que le permite al propietario gastar el bitcoin creando una firma digital.

el patrón del dólar - el sistema de dominación monetaria por USD en el comercio global. Comenzó en 1944 después de Bretton Woods y continuó en 1971 a través del petrodólar.

el patrón oro - un sistema monetario mundial dominante en el cual el valor de una moneda fiduciaria de una nación se encontraba respaldado por la cantidad de oro que dicho gobierno mantenía en reservas.

firma digital - prueba de que el usuario o firmante conoce la clave privada de una dirección determinada. Esto es conceptualmente similar a firmar un cheque bancario para confirmar que una persona determinada es el titular de la cuenta, pero tiene la ventaja adicional de no tener que revelar la escritura a mano de la persona. Al enviar bitcoins, el remitente firma la transacción, demostrando la propiedad del bitcoin, sin revelar la clave privada.

FOMO - "Fear Of Missing Out," o "Miedo a Quedarse Fuera" es un término utilizado frecuentemente para describir la mentalidad de rebaño y las decisiones irracionales de compra.

halving - un evento en la red de Bitcoin en el cual cada 4 años, la recompensa de minería en un bloque se reduce a la mitad.

KYC - "Know Your Customer," o "Conoce a Tu Cliente" es una práctica llevada a cabo por gobiernos mediante la cual los bancos deben recabar bastante información confidencial sobre una persona para poder proveerle un servicio financiero. Esta información es luego transmitida a los gobiernos a través de las leyes tales como La Ley de Secreto Bancario de los Estados Unidos.

liquidez - la cantidad de un activo que se compra o vende con facilidad en un período determinado.

minero - una persona o grupo (llamadas "piscinas de minería") que utilizan computadoras para encontrar números escasos de prueba de trabajo para crear nuevos bloques.

moneda fiduciaria - una moneda que puede ser emitida por un banco central.

nodo completo - software utilizado para validar las transacciones y la integridad del blockchain.

portales de intercambio apalancados - un portal de intercambio que permite intercambiar hasta 100 veces el importe depositado.

portales de intercambio cripto-a-cripto - un portal de intercambio que permite el intercambio únicamente entre criptomonedas.

Portales de intercambio de moneda fiduciaria a cripto - un portal de intercambio que permite el intercambio de moneda fiduciaria directamente a criptomonedas.

portales de intercambio persona-a-persona - un portal de intercambio que requiere encontrarse en persona para ejecutar un intercambio.

Prueba de trabajo - el proceso mediante el cual los mineros prueban que han gastado energía para proponer un nuevo bloque válido que pudieses ser añadido a la blockchain.

recompensa del minero / tarifa del minero - los bitcoins que recibe un minero por procesar transacciones y asegurar la red Bitcoin.

Red Lightning - un sistema desarrollado para escalar la capacidad de Bitcoin a millones de transacciones por segundo. Esta innovación también añade privacidad significativa a las transacciones de Bitcoin.

sat / satoshi - la unidad más pequeña de bitcoin. 100.000.000 satoshis son 1 bitcoin.

Satoshi Nakamoto - el creador de Bitcoin.

Símbolo/Teletipo BTC - utilizado para representar bitcoin en portales de intercambio, comercios y billeteras. XBT es también un símbolo popular.

tarjeta Octopus - una tarjeta de pago electrónico en Hong Kong.

tecnología blockchain - sistemas creados para utilizar la innovación blockchain de Bitcoin de alguna manera. No ha habido ninguno que haya visto una adopción generalizada además de Bitcoin y un puñado de otras criptomonedas.

transacción en la cadena - una transacción que es procesada y registrada directamente en la blockchain de Bitcoin.

transacción fuera de la cadena - una transacción que no es registrada en la blockchain de Bitcoin, como es el caso de las transacciones en la red Lightning.

Whitepaper / informe técnico - un informe de autoridad, frecuentemente académico, con la intención de informar plenamente al lector sobre un tema en particular. El documento original que describe Bitcoin y sus detalles técnicos fue presentado en este formato en octubre de 2008 por Satoshi Nakamoto.

Reconocimientos

Los autores desean agradecer a las siguientes personas por prestar su tiempo y experiencia a lo que de otro modo habría sido una tarea mucho más desafiante:

Leigh Cuen
Sam Corcos
Nick Foley
Irl Nathan
Jane Song Lee
June Park
Rodrigo Linares
Jan Čapek
Nick Neuman
Tomiwa Lasebikan

También nos gustaría agradecer a las siguientes personas por apoyarnos durante nuestro sprint del libro:

Bill Barhydt
Daniel Buchner
Cryptograffiti
Jill Carlson
Juan Gutiérrez
Han Hua
Ben Richman
Bill Tai
Mike Youssefmir
Sebastien Lhuilieri

Las siguientes personas nos han informado e inspirado a lo largo de los años:

Nick Szabo
Andreas Antonopoulos
Jameson Lopp
Elizabeth Stark
Marek Palatinus
Pavol Rusnak
Michelle Lai

Las siguientes organizaciones nos animaron a escribir este libro:

Blockchain Capital
BloomX
BuyCoins Africa
Casa
Human Rights Foundation
Open Money Initiative
University of Texas

Y, por supuesto, estamos muy agradecidos con Tim Chang por permitirnos usar su maravilloso hogar, y lo más importante, nuestras familias y seres queridos por animarnos.