
BRIAN KELLY
The
Bitcoin
Big Bang
Como las Monedas Alternativas estan por
Cambiar al Mundo
WILEY

Prefacio

De vez en cuando me encuentro con el deseo insaciable de saltar desde un acantilado y pensar en las consecuencias más adelante. Algunos pueden llamarlo curiosidad, mientras que otros piensan que estoy loco. Normalmente disfruto el escepticismo, ya que he descubierto que las mejores oportunidades surgen cuando todos los demás piensan que estoy un poco loco. El Big Bang de Bitcoin fue uno de estos tiempos; en realidad, a decir verdad, esta vez yo fui el escéptico. A pesar de mi miedo, incertidumbre y duda, salté de todos modos.

Cuando comencé a escribir El Bitcoin Big Bang, fue por razones egoístas: había comprado Bitcoin cerca del pico y ahora estaba perdiendo y necesitaba saber todo sobre esta "inversión". Pensé que podría convertir mi investigación en un libro. y aprende algunas cosas en el proceso. No sabía que había tropezado con uno de los avances tecnológicos más fascinantes y prometedores desde Internet. Cuando escuché por primera vez sobre Bitcoin, fue a través de los mercados de divisas, y ahí es donde comenzó mi viaje hacia la Iluminación de Bitcoin.

Supuse erróneamente que Bitcoin era una nueva moneda interesante que había sido poco prometedora. Después de todo, ¿realmente el gobierno de EE. UU. Iba a permitir una moneda no regulada basada en el código de computadora para reemplazar el dólar? Lo que ahora me doy cuenta es que la moneda no es la innovación; la tecnología blockchain es el cambio de juego. La moneda-bitcoin-es una moneda alternativa fascinante que tiene el potencial de perturbar las redes de pago globales. Sin embargo, es la tecnología blockchain la que es revolucionaria.

El concepto de blockchain permite la transferencia de información segura a través de una red no segura. Esto puede sonar como un pequeño paso, pero es la primera vez en la historia humana que esto ha sido posible. El blockchain resuelve un problema de varias décadas en las redes informáticas, y puede aplicarse a algo más que a las monedas. Tiene el potencial de terminar con el robo de identidad, crear una Internet segura sin necesidad de contraseñas y revolucionar la forma en que las empresas hacen negocios.

Cuando Jeff Bezos dejó un trabajo lucrativo como banquero de inversiones para comenzar una librería de Internet llamada Amazon, todos pensaron que estaba loco. En ese momento, las tiendas de videos como Blockbuster estaban en su mejor momento y los teléfonos inteligentes eran fijos con un contestador automático adjunto. Hoy, esa misma compañía (Amazon) es líder en la transmisión de contenido de video a una computadora de mano llamada teléfono inteligente.

No sé cómo serán las monedas alternativas ni lo lograré en los próximos 20 años, pero sí sé que cuando nace una tecnología revolucionaria, el mundo cambia.

Mi objetivo con el libro fue responder cuatro preguntas:

1. ¿Qué es Bitcoin y por qué es revolucionario?
2. ¿Cómo funciona?
3. ¿Por qué las monedas digitales son un nuevo tipo de inversión?
4. ¿Cómo cambiarán las monedas alternativas el mundo?

Con este fin, el libro fue escrito con dos secciones en mente. La primera mitad del libro describe qué es Bitcoin y cómo funciona, mientras que la segunda mitad ilustra los múltiples usos de la tecnología blockchain y explora las ramificaciones para inversiones, negocios y gobierno.

Una tecnología innovadora fue creada por un programador anónimo, que la ha regalado de forma gratuita. Esta creación ha estimulado una explosión tecnológica similar a la computadora personal e Internet, y, al igual que sus predecesores, las monedas alternativas son sobre el cambio en el mundo.

Reconcomiento

Cuando comencé a escribir este libro, pensé que sería un esfuerzo solitario: incontables horas escribiendo solo para producir un manuscrito que alguien podría decidir leer. Chico, estaba equivocado! Este libro no existiría sin las contribuciones de amigos y colegas.

Permítanme comenzar agradeciendo a Jeffery Krames, quien me contactó hace cuatro años y me convenció de que debería escribir un libro. Tomó un tiempo, pero este libro es un testimonio de su persistencia, paciencia y convicción. Siempre supo que tenía un libro en mí.

Al equipo de producción de CNBC Fast Money: gracias por apoyar este proyecto y por ser una parte integral del lanzamiento de Nautiluscoin. Lisa Villalobos, la multifabricada productora ejecutiva de Fast Money, usted fue capaz de tomar mis diapositivas de funciones de hash criptográficas y teoría económica y convertirlas en un segmento de televisión digerible. Lo haces parecer fácil. Michael Newberg, a quien se le encomendó la tarea de producir un segmento sobre un tema que todavía estaba luchando por comprender: usted tomó hábilmente un concepto esotérico y lo convirtió en un segmento de televisión que todos podían entender.

Melissa Lee, fuiste una de las primeras en comprender la naturaleza revolucionaria de las monedas digitales. Tu visión y curiosidad intelectual son una gran razón por la que Nautiluscoin existe. Es notable su capacidad para hacer malabarismos hábilmente con los eventos que mueven el mercado y gestionar cuatro operadores con opiniones firmes.

Lo que me lleva a mis amigos de Fast Money: Guy Adami, Karen Finerman, Steven Grasso, Jon y Pete Najarian, Dan Nathan y Tim Seymour; todos ustedes han sido una inspiración y estoy constantemente asombrado de lo afortunado que soy de poder trabajar contigo. Todos ustedes fueron parte de mi viaje hacia la Iluminación de Bitcoin. Fuiste testigo de mi escepticismo, luego de mi descubrimiento, y en el camino, puedo haber convencido a algunos de ustedes de que hay algo en esta locura por las divisas digitales.

Para mis padres, que siempre me animaron a sentir curiosidad y aceptar el descubrimiento, te aseguraste de que siempre tuviera la oportunidad de absorber, incluso en la escuela secundaria, cuando pensaba que nunca necesitaría aprender a escribir.

Estoy eternamente agradecido con el grupo de Austin Global Exchange: Justin Northcutt y Ryan Crow; tuvieron la oportunidad de obtener una nueva moneda y fueron verdaderos profesionales durante todo el proyecto.

Nautiluscoin, tal como está hoy, no existiría sin las talentosas habilidades de codificación de Jared Tate de DigiByte. Me considero afortunado de haberlo conocido antes de que el mundo descubra su talento.

Para el equipo editorial de Wiley, especialmente Lia Ottaviano, gracias por guiar a este autor novel y responder a una cantidad incalculable de preguntas tontas. Para Evan Burton, gracias por creer en este proyecto y ser su campeón.

Por último, pero ciertamente no menos importante, para mi esposa Dawn, alias Mrs. BK, este proyecto completo no habría ocurrido sin su apoyo. Además de escuchar innumerables horas de mi zumbido acerca de cuán asombrosas son las monedas digitales, usted era una caja de resonancia muy necesaria. Siempre desafiaste mis puntos de vista, este libro y yo soy mejor para eso.

Sobre el Autor

Brian Kelly es el fundador de Brian Kelly Capital LLC, un administrador global de macro inversiones con un enfoque en las monedas. Tiene una experiencia de inversión de 20 años en el comercio de valores estadounidenses e internacionales, divisas, opciones, futuros, metales y productos básicos. A lo largo de su carrera, Brian se ha especializado en el comercio de múltiples clases de activos, inversiones transfronterizas y arbitraje de riesgos.

Brian es colaborador de CNBC y se puede ver en Fast Money (host:

Melissa Lee), Informe de medio tiempo (anfitrión: Scott Wapner) y The Kudlow Report (anfitrión: Larry Kudlow).

Brian se graduó en la Universidad de Vermont, donde recibió una licenciatura en finanzas. También posee un MBA de Babson Graduate School of Business, con una concentración en finanzas y econometría.

La pasión por las inversiones y el espíritu empresarial ha llevado a Brian a iniciar varios negocios de inversión exitosos. Su empresa más reciente (Brian Kelly Capital) es una firma global de gestión de inversiones que se especializa en inversiones macro y monetarias globales.

Capítulo 1

Cuando veo una burbuja, compro esa burbuja, porque así es como gano dinero.

-George Soros

1.1- Bitcoin es una burbuja

Fad, scheme, scam, tulipmania, and bubble son todos términos que he usado para describir a Bitcoin. La mayor parte de mi carrera profesional en administración de dinero se gastó en los mercados de divisas, y como un experto me convencí de que Bitcoin no era más que una burbuja especulativa. Parecía imposible que una serie de números respaldados por nada y sin un ejército pudieran cumplir la definición aceptada de una moneda como un medio plausible de intercambio, depósito de valor o unidad de cuenta. Más de una vez, afirmé con confianza que Bitcoin no era más que "Tulipmania 2.0", una referencia a la burbuja tulipán holandesa del siglo XVII. Por supuesto, lo único que sabía sobre Bitcoin era que la gente lo llamaba moneda digital, un término que era nuevo para mí. Desafortunadamente, ni siquiera la ignorancia me impedía gritar en la televisión nacional que Bitcoin no duraría.

Había leído por primera vez sobre Bitcoin en 2011 mientras navegaba por mis sitios web habituales de divisas en busca de ideas de inversión. A fines de la primavera de 2011, el precio del bitcoin había alcanzado la paridad con el dólar estadounidense, y en julio, un bitcoin valía $ 31. Cualquier inversión que tenga un aumento del valor de 3.000 por ciento atraerá mucha atención, pero dos décadas trabajando en Wall Street me han enseñado no solo a ser escéptico sino a descartar automáticamente estas inversiones como burbujas insostenibles.

Bitcoin parecía ser un pequeño proyecto peculiar alucinado por un críptico programador de computadoras que estaba desilusionado con el mundo de la crisis post-financiera. Fue interesante, pero no pensé que hubiera dinero, así que rápidamente me olvidé de esta diversión y continué felizmente inconsciente de que una revolución estaba en marcha. No fue sino hasta el otoño de 2013 que Bitcoin reaparecería en mi radar.

En octubre de 2013, la Reserva Federal de EE. UU. Me consumió con la investigación sobre el final de la flexibilización cuantitativa. La llamada puesta a punto había sacudido a los mercados financieros, y necesitaba una plantilla para guiar mis decisiones de inversión. Dado que muchos creían que Bitcoin era una respuesta directa a la flexibilización cuantitativa, los dos conceptos se habían hermanado, especialmente en Internet. A través de mi investigación, comencé a notar que el precio del bitcoin estaba una vez más en alza. Después de estancarse por debajo de $ 31, el precio de bitcoin había pasado el año pasado subiendo a $ 150.

A medida que el precio subió, la atención de los medios creció, particularmente en el canal comercial CNBC, en el que aparecí. Si hay algo que aprendí de la televisión, es "si sangra, conduce", y Bitcoin estuvo tan cerca como las noticias de negocios llegan a un titular sangrante. No solo el precio subió rápidamente, sino que el creador clandestino hizo que la historia fuera fascinante. Lo más importante, las personas estaban interesadas. Tal vez todos sentimos que algo extraordinario estaba sucediendo y todos ansiamos el conocimiento. La información se convierte en un bien valioso en tiempos de incertidumbre.

A pesar de mi profundo escepticismo, me obsesionó una cita del famoso inversor George Soros. Soros estaba hablando del oro como la burbuja definitiva cuando The Australian lo citó diciendo:

"Cuando veo una burbuja, compro esa burbuja, porque así es como gano". Bueno, esta era mi burbuja y tenía estado sin saberlo acechándome por dos años. Ya no podía ignorar la euforia palpable. Yo quería entrar, no, lo necesitaba.

1.2- La búsqueda de comprar Bitcoin

En mi trabajo cotidiano, estoy acostumbrado a correr riesgos, pero cuando contemplé comprar el bombo de Bitcoin, el miedo corría por mis venas. Este era un tipo diferente de riesgo; Bitcoin tenía una mala reputación. El notorio sitio web Silk Road acaba de ser clausurado y su tesoro de bitcoins es confiscado por el FBI. Los personajes con apodos como Dread Pirate Roberts gobernaron este reino, mientras que los piratas informáticos constantemente lanzaban ataques. Si tuviera que adentrarme en esta tierra mostrando mis credenciales de Wall Street, sería un objetivo fácil. La precaución y el anonimato serían mis amigos en esta búsqueda.

Al hacer clic en el modo de sigilo, escribí "cómo comprar Bitcoin" y el algoritmo de Google produjo 166,000 resultados. La primera página de resultados no tenía sentido para este neófito, a excepción de uno: Mt Gox. Desde el monte. Gox era el intercambio más grande del mundo, estaba vagamente familiarizado con el nombre. Fue reconfortante que el Monte. Gox fue el mayor intercambio de bitcoins en el mundo, y decidí inmediatamente ascender al monte. Gox para hacer mi compra. Sorprendentemente, no me molestó que hace poco tiempo el monte. Gox significaba Magic: The Gathering Online Exchange y era un lugar para intercambiar tarjetas de juego mágicas. Bitcoin era vanguardista, era el Salvaje Oeste; Necesitaba tomar un riesgo. En un arrebato de éxtasis, me convencí de que desde el Monte. Gox se encontraba en Japón y el inventor de Bitcoin se llamaba Satoshi Nakamoto, entonces Japón debe ser el epicentro de Bitcoin.

Haciendo mi mejor impresión de James Bond, creé una cuenta ficticia de Gmail para seguir siendo tan anónima como todos los demás que repartieron estas "monedas". Mi pulso se aceleró cuando me registré bajo mi alias: no estaba seguro si estaba infringiendo la ley o tropezando sobre una fortuna escondida. Inspeccioné mis nuevos alrededores, y decidí hacer una compra; este fue mi primer paso hacia riquezas incalculables. Pero todo se detuvo cuando me di cuenta de que pasaba por alto un pequeño detalle: necesitaba una cuenta bancaria real con dinero real para comprar las monedas.

Estaba decidido a sacar provecho de mi burbuja y rápidamente formulé un plan.

Cuando inicié sesión en Mt Gox, un mensaje informó que había una lista de espera de personas que intentaban comprar bitcoins. El intercambio estuvo tan ocupado que no pudieron procesar todas las solicitudes, y el mensaje indicó que pasarían cinco días antes de que mi documentación pudiera procesarse. Estuve encantada de tener cinco días adicionales para abrir una cuenta bancaria de los EE. UU. Para una "persona" con solo una dirección de Gmail falsa. Todavía no estaba claro para mí que mi juicio había sido comprometido por las visiones de aviones, autos y joyas. Finalmente, volví a la realidad y comencé a tramar un plan mejor.

Aunque Bitcoin era anónimo, rápidamente reconocí que mis sueños de billones de bitcoins requerían mi información personal. Inmediatamente comencé a buscar una capa de seguridad. Otra búsqueda en Internet me llevó a eBay, donde abundaban los vendedores de bitcoins. Parecía que podía usar PayPal, lo que significaba que no necesitaba una cuenta bancaria y mi información estaría protegida. Por desgracia, una vez más había pasado por alto un detalle pequeño, pero importante. Si comprara bitcoins en eBay, sería el sueño de un falsificador. Esta es una moneda que vive en Internet. Si bien estaba acostumbrado a negociar en moneda extranjera, comprar JPY de JPMorgan dista mucho de haber comprado una moneda digital a un extraño en EBay. No sabía

si debería esperar un archivo zip de código de computadora o una moneda de metal real. Obviamente, necesitaba el Plan C.

Después de una aparición en Fast Money, donde revelé partes de mi aventura de compra de Bitcoin, un seguidor de Twitter mencionó a Coinbase como una alternativa al monte. Gox. No había oído hablar de Coinbase, así que volví al modo sigilo de Google. Como resultado, Coinbase es una de las billeteras digitales más grandes, y es un broker bitcoin que podría manejar mi compra sin problemas. Me sentí aún más cómodo cuando supe que Coinbase tenía su sede en los Estados Unidos y estaba respaldado por una de las firmas de capital de riesgo más grandes de Silicon Valley.

Ahora que estaba en el camino de la riqueza, necesitaba registrarme, verificar una cuenta bancaria y transferir fondos. Todo el proceso tomaría más de una semana: tres días para verificar la cuenta bancaria, un día para comprar los bitcoins y otros cinco días antes de que aparecieran las monedas en mi cuenta. Esto era inaceptable: estaba a punto de hacer una fortuna y cada segundo contaba. Lamentablemente, no tenía opciones. Como era técnicamente inepto y no tenía ni idea de cómo funcionaba Bitcoin, me encontraba en una grave desventaja. Solo tuve que esperar, lo cual fue una tarea monumental para este comerciante desafiado por la atención. Durante una semana revisé mi cuenta como un niño la noche antes de Navidad: ¿estaban allí todavía? ¿Que tal ahora? ¿Ahora? ¿Ahora? ¿Ahora?

Mi expectativa fue excedida solo por mi emoción cuando finalmente llegaron las monedas. Todo lo que quedaba era relajación, planificación de mi compra en un jet privado y esperar a que el mundo se pusiera al día y comprara bitcoins. Estaba esperando un tonto más grande que yo, y no pasó mucho tiempo antes de que llegara un montón de tontos. El precio de bitcoin se disparó desde mi compra a $ 795 a $ 1,200 en cuestión de días. Calculé rápidamente el rendimiento anual: $ 400 en 4 días significaba $ 100 por día; multiplicado por 365 días significaba que acababa de convertir $ 795 en $ 36,500, una ganancia del 4591 por ciento. Este iba a ser el mejor intercambio que jamás haya hecho: soltar el micrófono y salir del escenario.

No tan rápido, héroe.

En cuestión de días, el gobierno chino prohibió a los bancos negociar con bitcoins, cerrando efectivamente el mercado más grande. El precio se desplomó a $ 500 casi de la noche a la mañana. Hay un dicho en Wall Street sobre la pérdida de posiciones: comienzan como un intercambio y terminan como inversiones-racionalización en su máxima expresión. Mi comercio "no se puede perder, seguro" se acaba de convertir en una inversión. Yo estaba en el largo plazo.

Ahora que era un "inversor", pensé que sería mejor que descubriera lo que realmente poseía. Por lo general, confío en un conocimiento profundo de los mercados que comercializo antes de poner el dinero en riesgo. En el caso de Bitcoin, había sucumbido a la poderosa emoción de la codicia. Irónicamente, me gano la vida buscando la codicia y el miedo, actuando solo cuando las emociones de otras personas han alcanzado su cenit. En el caso de Bitcoin, era un novato y había pagado el precio de la inexperiencia.

Con el fin de suplantar mi ignorancia con conocimiento, comencé a investigar Bitcoin como una moneda. Si Bitcoin era un nuevo tipo de moneda, entonces el lugar lógico para comenzar mi viaje era desde un punto de vista familiar. Dado que Bitcoin fue diseñado para tener un suministro de dinero finito -sólo 21 millones de monedas existirán alguna vez-, parecía ser similar al oro digital. El proceso de minería encajaba con esta analogía, y el hecho de que los mineros recibieran monedas gratis era intrigante. Sin embargo, a diferencia del oro, se usaban bitcoins para comprar

todo, desde pizza hasta automóviles Tesla. Como medio de intercambio, los bitcoins cumplían al menos una de las tres funciones del dinero.

Al igual que muchos otros exploradores de Bitcoin, tuve mi momento "aha" cuando me di cuenta de que si la gente podía comprar una pizza con bitcoins tan fácilmente como una tarjeta de crédito, entonces Bitcoin también era un sistema de pago. Esta tecnología disruptiva era un sistema de pago gratuito, sin tasas de tarjeta de crédito para aquellos que se permitían la pizza o la pizzería. Esta tecnología no solo era perjudicial sino que estaba sucediendo en mi industria. Me enganché; Necesitaba saber todo. No importaba que ahora pudiera vender mis bitcoins por una pequeña ganancia; Estaba demasiado hundido para regresar.

1.3- Iluminación de Bitcoin

Mi camino a Bitcoin Enlightenment se desarrolló entre funciones de hash criptográficas y el balance simple que es el corazón de Bitcoin. La búsqueda del misterioso creador, Satoshi Nakamoto, fue una lectura interesante, pero no fue hasta que vi Bitcoin como dinero inteligente y una red social que realmente entendí la revolución.

Eliminar al intermediario tiene una larga historia de interrupciones en los negocios: la computadora personal colocó la capacidad de cómputo del ordenador central en el escritorio, mientras que Internet permitió la comunicación entre pares. La colisión de computadoras personales e Internet generó compañías como Apple, Netflix, Twitter y Facebook.

Bitcoin Big Bang es una historia de evolución. Es la evolución de las monedas, los sistemas de pago, cómo se usa el dinero, los servicios financieros e incluso la forma en que se organiza el negocio. Es ese momento en el que te das cuenta de que el mundo ha cambiado, de forma permanente y para siempre. La evolución es una rutina laboriosa, hasta que BANG, todo cambia a la vez.

Aunque sabía que Bitcoin estaba cambiando el juego, todavía estaba en su infancia. Si me convertí en evangelizador de la tecnología, corría el riesgo de parecer un loco que creía haber visto un unicornio. Tal vez fue duda propia o un anhelo innato de ser parte de una multitud, pero estaría inquieto sin validación. Luego, aparentemente de la nada, tropecé con una serie de citas de capitalistas de riesgo que estaban comprometiendo grandes sumas de dinero con Bitcoin. Mi cordura fue restaurada.

> Con el tiempo, los principales productos, empresas e industrias emergen para comercializarlo; sus efectos se vuelven profundos; y más tarde, muchas personas se preguntan por qué su poderosa promesa no fue más obvia desde el principio. ¿De qué tecnología estoy hablando? Computadoras personales en 1975, Internet en 1993 y, creo, Bitcoin en 2014.
>
> -Marc Andreessen, inventor del navegador web y cofundador de Netscape

Marc Andreessen no es solo el inventor del navegador web; también es socio fundador de la firma de capital de riesgo Andreessen Horowitz, que ha invertido $ 50 millones en empresas relacionadas con Bitcoin, incluido mi servicio de billetera, Coinbase.

En 2010, BusinessWeek nombró a Chris Dixon como el mejor inversionista ángel en la industria de la tecnología. En 2012, el Sr. Dixon se unió a Andreessen Horowitz, y en 2013, escribió estas palabras:

> Al igual que mucha gente, inicialmente rechacé a Bitcoin como una burbuja especulativa ("bulbos de tulipán de Internet") o un lugar para esconder dinero para personas preocupadas por la inflación ("oro de Internet"). En algún momento, tuve un momento de "¡ajá!" Y me di cuenta de que Bitcoin se entendía mejor como un nuevo protocolo de software mediante el cual se podía reconstruir la industria de pagos de maneras que son mejores y más baratas.

Y Peter Thiel, el fundador multimillonario de otro "pequeño" sistema de pago llamado PayPal, dijo lo siguiente sobre Bitcoin:

> Vale la pena pensar en el dinero como la burbuja que nunca termina. Existe este tipo de potencial que bitcoin podría convertirse en este nuevo fenómeno ...

El Sr. Thiel ha pasado a invertir millones en compañías de Bitcoin como BitPay. Si no recuerda a Peter Thiel de PayPal, puede recordar a su socio comercial, Elon Musk, el fundador de Tesla. Si eso no es suficiente credibilidad callejera, también puede recordar de la película The Social Network que Peter Thiel fue uno de los primeros inversionistas externos en una prometedora puesta en marcha llamada The Facebook.

Twitter, Tumblr, Foursquare, Zynga y Kickstarter son todas compañías en las que Fred Wilson, cofundador de Union Square Ventures, fue uno de los primeros inversores. ¿Qué piensa él de Bitcoin?

> Creemos que el bitcoin representa algo fundamental y poderoso, un protocolo abierto y distribuido de igual a igual para transferir el poder adquisitivo. Nos recuerda a SMTP, HTTP, RSS y BitTorrent en su arquitectura y apertura.

Estos capitalistas de riesgo han hecho exitosas carreras para resolver problemas. Si una idea no resuelve un problema, es poco probable que la empresa sea rentable. Si bien sabía que Bitcoin era importante, no pude entender el problema que estaba resolviendo. Quizás fue porque yo también tenía un problema: mi viaje hacia la Iluminación de Bitcoin accidentalmente me convirtió en el experto residente de CNBC, pero estaba luchando por definir Bitcoin. Tenía la sensación de que algo grande estaba sucediendo, pero no podía entenderlo. Tal vez fueron los instintos perfeccionados por los bordes de los mercados financieros o tal vez fue una ilusión, pero podía sentir el cambio. No hay nada como convertirse en un experto en televisión para motivar su educación. Como uno de los primeros "turistas" de Bitcoin, sabía más que la mayoría, pero finalmente eso no fue suficiente. Cuanto más subía la escalera del "experto", más me encontraba buscando una definición.

Bitcoin es más que un medio de intercambio; es más que una moneda emergente, y esta tecnología tiene el poder revolucionario de la computadora personal e Internet. Retrocedía cada vez que leía un artículo desdeñoso; no entendieron lo que yo había visto ... otra vez, yo tampoco. Durante este proceso agonizante, tropecé con docenas de usos y un puñado de ideas comerciales interesantes, pero encontré una definición simple elusiva. Luego, durante un insoportable período de 48 horas, no solo logré molestar a mi esposa, sino también destilar Bitcoin a sus cuatro elementos principales. Bitcoin era el terreno fértil de una nueva moneda; estaba respirando nueva vida en nuestros anticuados sistemas de pago; como dinero inteligente, estaba creando nuevos tipos de flujos de dinero; y ardió con la intensidad de una red social.

Los economistas de la corriente principal han dudado en definir Bitcoin como una moneda porque su precio es demasiado volátil para ser considerado como una reserva de valor y no se puede pagar sus impuestos con bitcoins. No hay duda de que la volatilidad es un gran obstáculo; sin

embargo, los cambios de precios se han vuelto menos pronunciados a medida que la moneda ha ganado aceptación. En cuanto a los impuestos, tampoco se puede pagar el Tesoro de los EE. UU. En yenes o euros japoneses, pero se consideran monedas. En el corazón del argumento del pago de impuestos está una suposición implícita de que el gobierno de EE. UU. Es el ejecutor principal de los pagarés o dinero. En los capítulos posteriores, nos sumergiremos en la implementación de IOU incorporada de Bitcoin, sin intermediarios ni gobiernos necesarios.

1.4- Las monedas son una cuestión de confianza

La pregunta que constantemente recibo es por qué alguien aceptaría un bitcoin en primer lugar. Mi respuesta es que, al igual que cualquier otra moneda, es una cuestión de confianza. Uno debe creer que aceptar esta forma de pago significa que pueden usarla en otra parte para comprar algo que quieren o necesitan. Siempre que tenga una expectativa razonable de que podrá convertir una moneda en un bien o servicio, entonces "realmente" la moneda no importa. En los sistemas económicos primitivos que utilizaban el trueque, la moneda no existía, pero la gente confiaba en que si aceptaban un pelaje de piel, podría usarse para obtener alimentos y agua.

De hecho, ha habido cosas más locas que las usadas por Bitcoin como moneda. Una concha marina, específicamente wampum, fue una vez la moneda de la tierra, los nativos americanos confiaban en que wampum podría obtener bienes y servicios. Wampum era difícil de obtener, ya que vivía en alta mar en las partes más profundas de la costa. Sin embargo, la razón más importante por la cual wampum se convirtió en una moneda fue la confianza. Cuando los comerciantes europeos llegaron a América del Norte, inmediatamente reconocieron la importancia del wampum para los nativos americanos, y comenzaron a comerciar con la moneda. De hecho, Wampum era de curso legal en Nueva Inglaterra desde 1637 hasta 1661.

Wampum funcionó bien como moneda siempre y cuando estuvieras comercializando bienes y servicios dentro de Native America. Sin embargo, fuera de América del Norte, wampum no gozaba de la misma confianza y, por lo tanto, no se podían comprar bienes con los proyectiles. Eventualmente, la libra británica desplazó a las conchas marinas, ya que los comerciantes ambulantes necesitaban la libra para obtener bienes y servicios fuera del ecosistema wampum. Aquellos que llevaban a cabo negocios dentro del ecosistema se vieron obligados a convertir su wampum en libras, dando a luz al término bombardeo.

Otra forma de pensar en este asunto de la confianza es a través de millas de viajero frecuente de la aerolínea. Algunos de nosotros usamos estas millas para comprar boletos de recompensa mientras que otros los usan para actualizarse a clases de negocios; en cualquier caso, estas millas son moneda. Estoy dispuesto a mantener un saldo de millas en mi cuenta porque confío en que podré usarlos para comprar un servicio, un boleto de avión. Sin embargo, no puedo gastar mis millas de United Airlines fuera del ecosistema para comprar un boleto de American Airlines. De esta manera, wampum y millas de viajero frecuente son similares; funcionan como una moneda solo dentro de un ecosistema.

Al igual que Wampum y las millas de viajero frecuente, en los primeros días, Bitcoin era un ecosistema cerrado. Cuando los comerciantes comenzaron a aceptar el bitcoin, adoptaron las características de una moneda y más comerciantes significaron un precio más alto para el bitcoin. El valor de bitcoin se unió a su creciente base de usuarios. De hecho, muchas monedas emergentes muestran tendencias similares: a menos que se acepte, no tiene valor. La primera moneda digital que creé se llamaba BKoin; duerme en mi computadora y no es aceptado en ninguna parte. Traté de enviarle algo a mi esposa, pero ella apenas sonrió, es una moneda muerta.

Pensando en Bitcoin como un sistema de pago es donde la mayoría de los evangelistas de Bitcoin tienen sus mejores momentos. A diferencia de una tarjeta de crédito, donde se nos cobra el privilegio de uso y aceptación, realizar un pago con bitcoins es gratis y rápido. Bitcoin no requiere información personal, lo que debería ser una buena noticia para aquellos que compraron en Target durante la temporada de fiestas de 2013. El sistema de pago de Bitcoin no tiene fronteras nacionales y no requiere una cuenta bancaria, lo que la convierte en la tecnología ideal para las transferencias internacionales de dinero y para los que no tienen acceso a servicios bancarios.

Bitcoin nació de la Gran Recesión y la crisis financiera de 2008. Fue una reacción a la revolución financiera que se había producido en los últimos 20 años. Ganó fuerza a medida que los bancos centrales globales comenzaron a imprimir dinero para combatir la Gran Recesión. Los primeros usuarios consideraron que la flexibilización cuantitativa era una amenaza para su sustento. Pero al igual que las cooperativas alimentarias llevaron a la formación de clubes mayoristas, Bitcoin llevará a una adopción empresarial más convencional.

Me costó varios intentos entender que la innovación de Bitcoin era la eliminación del intermediario de servicios financieros. Los mayores obstáculos fueron los acrónimos. En cualquier industria, la taquigrafía tiende a confundir al principiante y ayudar al experto. Mi inexperiencia con la criptografía, las redes P2P y los protocolos de código abierto significaba que tenía una tarea formidable por delante. Recordando mi sueño de un jet privado, avancé penosamente a través de la barrera del idioma hacia mi fortuna, sin saber que algún día compartiría este conocimiento.

1.5- ¿Qué es Bitcoin?

Una de las primeras cosas que aprendí fue que Bitcoin era conocida como una red peerto-peer, que es un sofisticado lenguaje de computadora para ningún intermediario. El concepto detrás de la tecnología es tan antiguo como el comercio en sí: reduce el costo de un intermediario y puede ofrecer un producto más económico. Los imperios comerciales se han construido sobre este concepto, por ejemplo, las cooperativas de alimentos de los años setenta en los Estados Unidos fueron la primera generación de Costco, BJ's Wholesale y Sam's Club.

Las redes punto a punto tienen una historia de industrias revolucionarias. La creación de Sean Parker, Napster, es un gran ejemplo de una red peer-to-peer que cambió la música. Con Napster, los archivos de música se podían compartir entre amigos (pares) sin tener que ir a Tower Records y comprar el álbum. Una vez que el álbum fue comprado, su compañero podría hacerle una copia y llevarlo a su casa. Este engorroso intercambio no solo involucró a varios intermediarios; también implicó que te levantaras del sofá. Napster eliminó a los intermediarios y le permitió compartir su canción favorita desde la comodidad de su hogar.

Por supuesto, los intermediarios no estaban muy contentos con el Sr. Parker, y lanzaron una andanada de demandas para reclamar su territorio. Eventualmente, los costos legales causaron que Napster cerrara, pero no antes de que cambiara la industria de la música de forma permanente. Muchos consideran que el servicio de intercambio de archivos de una canción es predecesor de iTunes de Apple. La industria discográfica estaba acostumbrada a vender álbumes completos repletos de canciones que pocos querían escuchar. Lo que Napster hizo fue ilustrar que el consumidor prefería las compras de música a la carta, y Apple respondió a esta demanda. "Napster puede haber cambiado la forma en que las personas compartían música, pero Apple cambió la forma en que la compraron. Aún más, iTunes ha cambiado la forma en que se graba y se lanza la música. Muchos pueden lamentar la muerte del álbum, pero Napster e iTunes se han asegurado de que no haya vuelta atrás.

Cuando se lo considera un servicio de intercambio de archivos, Bitcoin no es muy diferente de Napster. Los archivos que se comparten son unidades de valor en lugar de música. Si pudieras encontrar una tienda de comestibles que aceptara música como pago por comida, entonces Napster podría convertirse en una moneda como Bitcoin. Una vez más, se trata de si el archivo que recibe (música o bitcoin) se puede utilizar para comprar otra cosa. Tan pronto como el archivo se puede cambiar por otra cosa, se convierte en una moneda, y si por algún milagro el resto del mundo decide aceptar música como pago, entonces el valor de esa "moneda" probablemente aumentará. Una vez que algo se convierte en moneda, se necesita un nuevo nivel de seguridad.

La seguridad de la tecnología de Bitcoin es lo que lo hace más adecuado que Napster como moneda. En el corazón de Bitcoin hay un libro de contabilidad global, o balance general, llamado blockchain. Este libro de contabilidad global registra cada transacción que tiene lugar con bitcoin. Desde el momento en que se acuña un bitcoin, se registran todos sus movimientos, y es este registro el que asegura que los bitcoins no se pueden falsificar. Para crear la cadena de bloques, aproximadamente cada 10 minutos, el software Bitcoin compila todas las transacciones que se han producido en un archivo llamado bloque. Este bloque contiene una referencia al archivo anterior y es un registro de cada transacción que ha ocurrido. Cuando todos los bloques están vinculados entre sí, forma una cadena de bloques, por lo tanto, la cadena de bloques.

La seguridad de Bitcoin depende del proceso de vincular todas las transacciones. Imagine si se siguiera un billete de un dólar cada vez que se usara, desde su impresión hasta su posible retiro. Cada paquete de chicle, soda, flor o juguete que alguna vez se haya comprado con ese dólar se registraría. Si un falsificador hiciera una copia de este billete de dólar, contendría un registro del propietario legítimo, y cuando intentara gastarlo, la seguridad incorporada no permitiría la transacción. Un falsificador tendría que retroceder y convencer a cada comerciante de que la transacción nunca tuvo lugar. En esencia, un falsificador tendría que cambiar cada transacción antes de hacer la copia.

La solución de Bitcoin al problema de la falsificación es la combinación de la cadena de bloques y los mineros. A medida que se agregan más transacciones, el blockchain hace que sea prácticamente imposible cambiar las transacciones anteriores. Los mineros están acusados de confirmar que el bitcoin que se transfiere no es falso. El acto de extraer bitcoins implica el uso de computadoras potentes para resolver una ecuación matemática compleja. La respuesta a la ecuación contiene una clave que verifica todas las transacciones anteriores. Si esta clave no coincide con las transacciones anteriores, los mineros saben que el bitcoin es falso.

En términos muy simples, así es como funciona una transacción de bitcoins: si Keith quiere enviar un bitcoin a Alan, debe transmitir ese mensaje a la red de Bitcoin. Los mineros escuchan este mensaje y luego usan computadoras sobrealimentadas para asegurarse de que Keith sea el propietario legítimo. Una vez que verifican la propiedad de Keith, permiten que ocurra la transacción y la registran en la cadena de bloques. Por su trabajo, los mineros son recompensados con monedas gratis llamadas coinbases, actualmente, para cada grupo de transacciones (bloque) que un minero verifica, el minero recibe 25 bitcoins.

A medida que continuemos nuestro viaje hacia la Iluminación de Bitcoin, lucharemos con varios términos más que pueden desafiar a algunos y cautivar a otros. Por ahora, los términos más importantes para recordar son la red peer-to-peer, bloques, blockchain y mineros. La red de igual a igual de Bitcoin permite a los usuarios transferir el valor; estas transacciones se almacenan en archivos llamados bloques; estos bloques están unidos para formar una cadena de bloques; y los mineros resuelven una ecuación matemática que prueba la propiedad de un bitcoin.

1.6- ¿Es una moneda?

Como comerciante de divisas y nerd economista autoproclamado, pensé que definir Bitcoin como moneda sería bastante simple. Para que algo se llame moneda, tradicionalmente ha necesitado ser un medio de intercambio, una tienda de valores y una unidad de cuenta. Como medio de intercambio, Bitcoin pasó con gran éxito; cuando se compró la primera pizza con bitcoin, satisfizo esta condición. Como una reserva de valor, se quedó un poco corto: las oscilaciones de los precios han hecho que sea difícil para Bitcoin convertirse en una tienda de valores de confianza. Finalmente, en cuanto a una unidad de cuenta, el jurado todavía está fuera. Actualmente, no hay productos o productos que tengan su valor expresado en unidades de Bitcoin, pero esto está cambiando rápidamente.

Tal vez estamos demasiado atados a la definición convencional de una moneda como un medio de intercambio, una tienda de valores y una unidad de cuenta. En última instancia, tanto el papel moneda como el bitcoin solo son valiosos como moneda si la aceptación es generalizada o necesaria. Es la condición "requerida" que conlleva todo el peso. Si no paga sus impuestos, el gobierno tiene derecho a confiscar su propiedad. Le hemos otorgado al gobierno el derecho a emitir moneda y el derecho a hacer cumplir su uso; esto no es una declaración política, es solo la ley de la tierra. El argumento en contra de Bitcoin como moneda es que no puedes usarlo para pagar impuestos, y no está respaldado por una autoridad de aplicación como un ejército. Ambos son ciertos, pero el argumento pierde una oportunidad más grande.

¿Qué pasa si Bitcoin no tiene que estar a la altura de la definición de libro de texto de una moneda? ¿Qué pasaría si fuera un híbrido? Tal vez es un producto básico o tal vez es un sistema de pago, o tal vez es algo intermedio. Pero el bitcoin se está utilizando como medio de intercambio, e independientemente de su definición formal, la tecnología es revolucionaria. Como muchos otros, llegó mi momento de aha cuando comencé a pensar en Bitcoin como un sistema de pago. Ver Bitcoin como más que una moneda me permitió ver que tiene todas las características de una tecnología revolucionaria: es fuerte, rápido y eficiente.

La fuerza de Bitcoin es la falta de un único punto de falla. Cuando los hackers atacaron a Target, lo tuvieron fácil. Todo lo que tenían que hacer era encontrar una puerta abierta a la base de datos única que contenía toda la información personal de los clientes. Bitcoin no requiere información personal, y la base de datos se distribuye en un número infinito de computadoras. Si bien los hackers han podido encontrar la forma de acceder a algunas computadoras, ninguno de los ataques obstaculizó a toda la organización. Incluso el fracaso de Mt Gox, anteriormente el mayor intercambio de bitcoins, apenas causó un contratiempo. Imagínese si una importante bolsa de valores cerrara sin previo aviso: nuestro sistema financiero estaría en ruinas.

Bitcoin es rápido porque reinventa al intermediario. Piense en lo que se necesita para transferir dinero de una persona a otra. En primer lugar, ambos tenemos que abrir una cuenta bancaria, que se acompaña de una montaña de documentos para verificar las identidades. Luego, debo indicarle a mi banco que retire dinero de mi cuenta escribiendo un cheque, enviando un cable o usando un débito electrónico. Una vez que llega, el pago debe verificarse, compensarse y entregarse. A lo largo del camino, existen numerosos puntos de fricción, y en todo el camino, esta fricción nos cuesta una tarifa.

Bitcoin es eficiente porque el intermediario es compensado por la tecnología. El software de Bitcoin paga al intermediario, también conocido como mineros, una cantidad predeterminada de dinero. Pagar a los mineros bitcoins es también el canal por el cual se desarrolla constantemente

el suministro de dinero. Los mineros compiten para ser los primeros en resolver una ecuación matemática, que procesa la transacción y garantiza que los bitcoins no sean falsificados. El primero en resolver el problema recibe bitcoins recién acuñadas. Es esta innovación lo que hace que sea poco práctico despojar a la moneda de la tecnología. La moneda es una parte integral, similar a cómo sin el signo "@", el correo electrónico no funcionaría.

Discutir si se trata de una moneda pasa por alto el objetivo de la tecnología. Bitcoin es una herramienta que verifica, borra y transmite transacciones financieras de forma segura. En resumen, redefine el rol del intermediario en la industria de servicios financieros. El correo electrónico nos permitió enviar un mensaje mejor, más rápido y más eficiente. Bitcoin hace lo mismo por dinero.

Echemos un vistazo más profundo sobre cómo Bitcoin actúa como una herramienta para verificar, borrar y transmitir transacciones financieras. La revolución es la combinación de la cadena de bloques y los mineros; en conjunto, estos componentes se convierten en el intermediario financiero reinventado. El blockchain registra cada transacción, mientras que los mineros verifican y transmiten la transacción.

Comenzando con el primer bitcoin creado, el software de Bitcoin comenzó a registrar todos sus movimientos. Siempre me resulta más fácil humanizar nuevos conceptos, así que vamos a llamar al primer bitcoin una comunidad llamada Genesis. Donde sea que vaya Génesis, la cadena de bloques registra sus movimientos. En esencia, está tomando fotos de cada uno de sus movimientos y grabándolos para la posteridad. Cada 10 minutos, estas imágenes se juntan en un archivo llamado bloque. Dentro de este archivo hay una imagen no solo de Génesis, sino de todos sus amigos; donde quiera que fueron en los últimos 10 minutos se registra en el archivo. También se incluye en este nuevo archivo una imagen del bloque anterior. Esta imagen del pasado vincula todos los bloques, formando una cadena llamada blockchain. ¿Alguna vez te has tomado una foto en un espejo doble? El mismo efecto ocurre con Bitcoin: parece que puedes ver para siempre.

El blockchain es el paparazzi del mundo de Bitcoin. Donde sea que vaya Génesis, los fotógrafos la siguen: si ella compra un paquete de chicles, los paparazzi están allí; si ella sale a un club, los paparazzi están allí; incluso si ella se sienta en su sofá en casa, los paparazzi están grabando todo. Ahora cuando Genesis se gasta en el club por una botella de Crystal, los mineros se involucran.

Los mineros resuelven un rompecabezas matemático que les permite ver todas las imágenes que los paparazzi tomaron de Génesis. Los mineros regresan y rastrean cada uno de sus movimientos para asegurarse de que el Génesis en el club sea el verdadero Génesis y no un impostor. El primer minero que resuelve el acertijo y mira todas las imágenes se paga en bitcoins.

Lo que hace que Bitcoin sea fuerte es que cualquiera puede ser un paparazzo y cualquiera puede ser un minero. Cualquiera que descargue el software de Bitcoin también descarga toda la cadena de bloques, lo que significa que todas las imágenes no se almacenan en un solo lugar. Las imágenes se distribuyen por todo el mundo en infinitas computadoras. Si una computadora falla, la red Bitcoin sigue zumbando. Si derramo café en mi computadora o me piratean, la red de Bitcoin solo usa las otras computadoras.

Piensa en lo que sucedió con el Monte. Gox. Este fue el mayor intercambio de bitcoins en el mundo. Fue la Bolsa de Nueva York (NYSE) y el Nasdaq combinados, y falló. Sin embargo, su fracaso no paralizó a Bitcoin. Hubo una disminución en el precio de los bitcoins, pero la red siguió funcionando, las transacciones aún se procesaron y los paparazzi siguieron el seguimiento de Genesis. Imagínese si tanto el NYSE como el Nasdaq se apagaran sin previo aviso. El sistema financiero se aprovecharía, y probablemente tendríamos que declarar un feriado bancario para

calmar el pánico. Sin embargo, después del fracaso de Mt. Gox, la cantidad de comerciantes que aceptan bitcoin se está expandiendo y el ecosistema está creciendo.

La razón Mt. Gox apenas causó un tropiezo es que el sistema es autosuficiente. Desde Islandia hasta Oregón, los mineros compiten para ser los primeros en resolver la ecuación matemática, y si ganan, la recompensa es de 25 bitcoins o alrededor de $ 11,250. Once grandes cada 10 minutos no es un mal día de pago. ¡De hecho, hay una operación minera en el estado de Washington que gana $ 8 millones por mes!

Obviamente, el incentivo financiero ha atraído a una gran cantidad de mineros, al igual que el oro en 1849. Y al igual que el oro, a medida que el precio del bitcoin aumenta, los mineros ganan más dinero. Para darte una idea de cuánto poder de cómputo persigue ese 25 bitcoins, a partir de hoy los mineros calculan aproximadamente 50 cuatrillones de ecuaciones matemáticas por segundo. Sí, ¡50 cuatrillones!

Lo increíble es que todo este poder de computación y el crecimiento en las transacciones han sucedido orgánicamente. La red Bitcoin no solo está viva, ¡está prosperando! Y todo se debe al mecanismo autosostenido en el corazón del sistema. La interacción minero-blockchain es sostenida por el sistema mismo. Es autorreforzante. El proceso autosuficiente y autorreforzante en el núcleo de Bitcoin asegura su supervivencia.

Entonces, ¿quién vendió las primeras monedas y de dónde vinieron? Muchas de las monedas vendidas provienen de los mineros, son las monedas que se reciben como recompensa por resolver la ecuación. Así es como los mineros convierten sus bitcoins en moneda fiduciaria.

Ahora, ¿qué pasa si estas monedas fueron pre minado y utilizadas para reunir capital para cualquier cantidad de proyectos? ¿Cómo funcionaría esto? El creador de la moneda mina las monedas antes de que sean lanzadas. Recuerda, los paparazzi o blockchain siempre registran la acción, incluso si la moneda no hace nada. Una vez que el creador de la moneda tiene un tesoro de monedas, ella puede venderlas al público en general. Los ingresos podrían ser utilizados para donaciones de caridad, o podrían ser utilizados para comenzar un nuevo negocio.

Otra parte interesante de la tecnología de Bitcoin es que puedo programar un dividendo en cualquier transacción. Por ejemplo, supongamos que te vendo el 10 por ciento de mi empresa por 100 bitcoins. Puedo programar en esa transacción que por cada dólar que reciba vendiendo mi producto, obtendrá automáticamente $0.10. De esta forma, Bitcoin podría usarse como financiamiento de riesgo.

También hay otra forma de usar Bitcoin para resolver problemas cotidianos de manera eficiente. La próxima generación de Bitcoin implica Smart Contracts, que le permite designar un bitcoin para un uso específico. Por ejemplo, si acepto pagarle una cierta suma en el cierre de una casa, entonces, en lugar de depositar el dinero en una cuenta de custodia, puede usar Mastercoin para designar una cierta cantidad de bitcoins que se pagarán a una hora específica. Esta es una de las formas en que Bitcoin elimina al intermediario de las transacciones en custodia.

Por supuesto, con cualquier acuerdo necesitará un contrato, pero sin una autoridad central, se vuelve imposible de hacer cumplir, a menos que sea un Contrato inteligente, es decir, un contrato adjunto a una transacción de bitcoin y almacenado en la cadena de bloques. Los contratos se pueden escribir directamente en una transacción bitcoin que especifica el uso, el momento y las partes en la transacción. Toda esta información es "fotografiada" por los paparazzi (la cadena de bloques) y se aplica a través del proceso de verificación de la minería. Los mineros no opinan

sobre el contrato; solo verifican que ambas partes acordaron y procesaron la transacción. El blockchain se convierte en el ejecutor descentralizado e infiel del contrato.

1.7- Es Revolucionario

Al pensar en la evolución de Bitcoin, se hizo evidente que es más que una forma de comprar algo de forma barata y anónima. Dentro del software de Bitcoin hay marcas de tiempo que le permiten programar pagos. Usando esta característica, las condiciones de pago en contratos y facturas pueden ser programadas en el dinero, haciéndolo "inteligente". Las características de dinero inteligente de Bitcoin pueden usarse incluso para eliminar los bancos fiduciarios al transferir riqueza generacional.

Si pensabas que definir Bitcoin como moneda era controvertido, entonces llamarlo una red social probablemente sea la gota que derrumbe el camello, pero quédate conmigo. Twitter y Facebook son simplemente sistemas de mensajería: cuando twitteo una foto de vacaciones y se retweetea, se le da valor a esa imagen; más re-tweets o "me gusta" implican un valor más alto.

En esencia, estoy enviando mi foto a una red para su verificación. Si la red acepta que este mensaje tiene valor, entonces se "permite" que se transfiera. El mismo concepto ocurre con Bitcoin, en su esencia es un sistema de mensajería, pero dado que se trata de dinero, se necesita un mayor nivel de seguridad. La red de Bitcoin no solo verifica que poseo la foto de vacaciones (no hay cuentas pirateadas aquí), sino que también puedo adjuntar un valor a mi imagen. Si a uno de mis seguidores le gusta la foto, implica que está de acuerdo con el valor que he puesto en mi foto. La red social de Bitcoin luego registra este acuerdo sobre el valor y me permite usarlo en otro lugar.

En las siguientes páginas, viajaremos juntos para explorar cómo funciona la tecnología y quién la inventó. Este viaje nos llevará a las minas de Bitcoin y al ecosistema. Aprenderemos por qué los bancos tienen tanto miedo y los minoristas se regocijan. Incluso crearemos nuestra propia moneda para responder a algunas de las críticas de Bitcoin. Finalmente, terminaremos en la tierra de las Organizaciones Autónomas Descentralizadas y descubriremos por qué estas creaciones algún día competirán con las compañías Fortune 500.

Únete a mí, si quieres, en el camino hacia la Iluminación de Bitcoin. Si elige este camino, no puedo prometer una fogata y una ronda de "Kumbaya" al final, pero puedo prometer que tendrá un asiento de primera fila de lo que podría ser la tecnología más perjudicial desde que Internet y la computadora personal.

Capitulo 2

Tienes que aprender las reglas del juego. Y luego debes jugar mejor que nadie.

-Albert Einstein

2.1- Entendiendo la fiebre del oro digital

En enero de 1848, James Marshall, un capataz que trabajaba en el aserradero de madera de John Sutter, encontró una pieza de metal brillante en el ramal de carga. La roca brillante fue pinchada, pinchada y pinchada hasta que pudieron determinar eso, ¡y he aquí, era oro! Con este descubrimiento comenzó la fiebre del oro en California. En tres años, San Francisco pasó de una avanzada de 200 residentes a una ciudad en auge de 36,000. Pocos lo sabían en ese momento, pero los iconos estadounidenses nacían; Levi Strauss y Wells Fargo son los más reconocibles, pero no se olvide Studebaker e incluso el nombre moderno del equipo de fútbol de la ciudad.

El descubrimiento de oro resultó en una prisa para extraer porque el oro era la base metálica del dólar de EE. UU. No siempre ha sido suficiente para respaldar el dólar de EE. UU. Con toda la fe y el crédito del gobierno de EE. UU. En 1848, los Estados Unidos estaban en la infancia de su crecimiento a la superpotencia; no estaba claro si la fe y el crédito estarían presentes en el futuro. Por supuesto, Estados Unidos no fue el primer país en adoptar el estándar de oro. El metal brillante tiene una historia de 5.000 años como medio de intercambio. ¿Pero por qué? Después de todo, el oro no es más que una roca, pero es una roca especial.

El oro tiene una cualidad única que lo hace popular como moneda: densidad. El oro es uno de los elementos naturales más densos y, de hecho, es más denso que el hierro. Su densidad hace que el oro sea un medio de intercambio ideal. Una onza de oro se puede transportar fácilmente y agrega un gran valor en un paquete pequeño. Supongamos que estás haciendo el largo viaje por el campo. Llevar un baúl lleno de dinero en efectivo no era práctico, especialmente si hacía el viaje a pie. Sin embargo, llevar una onza de oro no solo era más ligero sino también mucho más seguro, ya que podía ocultarse en la ropa. Un baúl lleno de efectivo es mucho más difícil de ocultar debajo de la camisa.

A medida que el sistema financiero creció, el oro continuó desempeñando un papel central en el sistema monetario. De hecho, no fue hasta 1973 que Estados Unidos abandonó por completo el patrón oro. La era electrónica de las finanzas hizo que la propiedad que hacía que el oro fuera irrelevante en las transacciones financieras modernas. Hoy, el dinero se mueve alrededor del mundo con solo deslizar un dedo y hacer clic con el mouse. No se deje engañar: el hecho de que la tecnología moderna haya permitido la transferencia fluida de dinero no significa que no tenga fricción. En todo momento, el dinero debe pasar por los bancos, las compañías de tarjetas de crédito, los gobiernos y los bancos centrales. Cada uno de estos jugadores en el sistema financiero representa un punto de fricción, y en finanzas, la fricción es sinónimo de honorarios. Mientras que el dinero se mueve por el mundo, no lo hace sin el intermediario.

Esta dinámica de un sistema financiero basado en comisiones que consiste en una red de intermediarios está siendo cuestionada por la invención de Satoshi Nakamoto. A pesar de que todavía no estamos seguros de si Satoshi es un individuo o un grupo, la invención está interrumpiendo rápidamente las finanzas. Bitcoin está encontrando rápidamente una forma de desintermediar la industria de servicios financieros; es decir, Satoshi Nakamoto tenía la intención de eliminar a los grandes intermediarios en el sistema financiero centralizado.

Hay más en la historia de Satoshi Nakamoto y un sistema financiero descentralizado, pero antes de que podamos saltar por ese agujero de conejo, necesitamos saber lo básico. Hasta 2013, cuando el precio de un bitcoin se disparó de $ 10 a más de $ 1,000, la criptomoneda vivió en el reino de los entusiastas de la codificación y los criminales. La tecnología estaba contaminada por los usos del mercado negro y la falta de aceptación de la corriente principal. Además de la reputación nefasta, la actividad especulativa le valió a Bitcoin la etiqueta de esquema Ponzi y Tulipmania 2.0. Lo que se perdió en la cacofonía fue la tecnología que subyace en el núcleo: la capacidad de transferir riqueza a cualquier persona, en cualquier lugar, de forma instantánea, segura y sin un intermediario de confianza.

A medida que Bitcoin ganó la atención de la corriente principal, la prisa por sacar provecho de la tecnología comenzó en serio. Los intercambios de divisas de Bitcoin surgieron para facilitar la compra de bitcoins, mientras que las empresas de billeteras digitales ofrecieron almacenar de forma segura las monedas recién compradas. Estos intercambios y carteras son el comienzo del ecosistema financiero de Bitcoin y son la vanguardia de un sistema financiero descentralizado. Esta evolución no es diferente de cuando los fundadores de American Express, Henry Wells y William Fargo, crearon Wells Fargo & Company para proporcionar servicios bancarios a California en 1852. Al igual que Wells y Fargo, los empresarios de divisas digitales de hoy en día están satisfaciendo una necesidad. Sin embargo, mientras que Wells y Fargo intentaron ser el intermediario, los Bitcoiners están tratando de eliminar al intermediario.

En el corazón de Bitcoin hay un proceso de autorrefuerzo que verifica y transfiere valor. Este proceso se llama minería, y es el nuevo banquero del sistema financiero. Los banqueros tradicionales se destacan en el centro del sistema financiero y aseguran que el dinero pase de un propietario legítimo a otro. Los mineros de Bitcoin hacen lo mismo, pero sin la necesidad de emplear miles o construir rascacielos.

La popularidad y rentabilidad de la minería para bitcoins creció a medida que el precio de la moneda digital comenzó a subir. Los mineros desbloquean bitcoins recién acuñadas resolviendo problemas matemáticos complejos y verificando que se haya realizado una transacción. En los primeros días, todo el camino de regreso en 2010, la minería se podía hacer en computadoras caseras simples, pero a medida que se volvió más rentable, los mineros se trasladaron a computadoras sobrealimentadas. Por supuesto, hay muchas compañías que están muy felices de suministrar este pico digital.

El pico digital ha evolucionado de una simple computadora en un dormitorio extra a lo que se conoce como minero ASIC. ASIC significa circuito integrado específico de la aplicación y está diseñado específicamente para ser el primero en resolver la ecuación matemática en el núcleo de la red de Bitcoin. Empresas como KNC Miner, BitFurry y Butterfly Labs se están beneficiando de la fiebre del oro digital. De hecho, la demanda de los productos ha sido tan sólida que algunos han tenido problemas para completar los pedidos. Los mineros indignados que esperan la última máquina han criticado las demoras, pero la verdadera preocupación es seguir el avance tecnológico más reciente. Dado que la minería Bitcoin es tanto una competencia como un juego de azar, el minero con la computadora más rápida tiene las mejores probabilidades de ser el primero en adivinar la solución correcta.

Quizás estos nuevos negocios se convertirán en el próximo Levi Strauss, que en 1850 utilizó su conocimiento de la fabricación de lonas de lona para crear pantalones resistentes que se usaron durante 16 horas de martilleo de rocas. Es probable que en alguna parte del ecosistema de Bitcoin haya un John Studebaker moderno que, antes de construir su compañía automovilística homónima, fabricó carretillas para los buscadores de oro.

Durante la fiebre del oro de California, los mercaderes hicieron más fortunas que los mineros. Levi Strauss, John Studebaker y Henry Wells y William Fargo se enteraron de la industria de la extracción de oro y luego proporcionaron productos muy necesarios. La característica distintiva de estos constructores de imperios es que se adaptaron a una industria emergente. Estudiaron el paisaje y aplicaron su conjunto de habilidades; en el proceso, construyeron íconos estadounidenses. Si uno de nosotros se va a convertir en el próximo multimillonario de Bitcoin, entonces tenemos que aprender algunas definiciones y el lenguaje de Bitcoin.

2.2- El lenguaje de Bitcoin

En primer lugar, puede haber notado que a veces Bitcoin se escribe con mayúscula "B" y es singular, mientras que otras veces es minúscula y plural, como en bitcoins. Debido a que Bitcoin es a la vez una moneda y una tecnología, es una práctica aceptada utilizar una "B" mayúscula cuando se refiere a la tecnología y minúscula al referirse a la porción de la moneda-bitcoins. Parafraseando y blasfemando a los satélites de Georgia, si tienes algún cambio en tu bolsillo vayan ching-a-ling-a-ling ... son bitcoins.

Una vez que tiene sus bitcoins, necesita saber cómo la red de Bitcoin procesa una transacción. Los tres pilares sobre los que descansa Bitcoin son la cadena de bloques, las claves privadas y la minería. El blockchain es el registro de todas las transacciones, las claves privadas son el sistema de seguridad y la minería es el proceso de verificación de las transacciones.

El Blockchain

Los registros bancarios más antiguos conocidos datan de 9000 a. C., cuando los agricultores intercambiaban granos por ganado. Las transacciones fueron literalmente escritas en piedra, y estas tabletas se convirtieron en los primeros libros públicos. En el corazón de Bitcoin también se encuentra un libro de contabilidad público que almacena cada transacción que se haya producido alguna vez. Cuando las personas se refieren a las transacciones de bitcoin como transparentes, esto es de lo que están hablando.

Por ejemplo, esos zapatos que compraste con bitcoins para que tu cónyuge no pudiera ver la carga, sí, esa transacción se registró en la cadena de bloques. No se desespere, mientras todos podemos ver que alguien compró los zapatos, ninguno de nosotros puede determinar quién era, gracias a las llaves privadas. Tu secreto sigue siendo seguro.

La razón por la que los primeros banqueros escribieron transacciones en piedra fue para evitar el doble gasto. Los libros contables registraron quién era dueño del grano y quién era el dueño del ganado. De esta forma, impidieron que un agricultor inescrupuloso vendiera granos que él no poseía legítimamente. Esto funcionó bien si todas las transacciones pasaron por un solo banquero, pero a medida que el comercio se expandió hubo una necesidad de otra capa de seguridad. Un agricultor que compró grano en el pueblo A necesitaba probar que era el dueño antes de venderlo en el pueblo B. Lamentablemente, la forma más temprana de seguridad era la violencia: si le robabas el grano que vendías al banquero en el pueblo A, lo harías probablemente sea visitado por hombres de cuello grueso que buscan infligir daño físico. Afortunadamente, hoy tenemos una rama de las matemáticas llamada criptografía, que nos permite crear pruebas matemáticas que brindan seguridad. Para algunos, resolver ecuaciones matemáticas complejas puede ser equivalente a un daño físico, pero no temas, no se necesitan matemáticas para usar bitcoins.

Si Alice envía bitcoins a Bob, el software de Bitcoin ajusta esa transacción en una función de hash criptográfica, es decir, un complejo problema matemático. Esta función hash criptográfica convierte el mensaje "Alicia envía un bitcoin a Bob" en una cadena ilegible de letras y números que pueden ser decodificados solo por una computadora adivinando la combinación precisa de letras y números. La cadena alfanumérica es única solo para la transacción Alice y Bob; cada otra transacción de bitcoin obtiene una encriptación completamente diferente. Una vez que se descifra el código, el minero puede verificar que Alice es la propietaria legítima a través de su clave privada.

Claves públicas y privadas

Al igual que algunos de nosotros, los bitcoins tienen una imagen pública y una persona privada. La persona pública se conoce como una dirección, mientras que la persona privada se llama la clave privada. La dirección le dice a las personas dónde vive en la red de Bitcoin para que sepan dónde transferir el valor. Cuando Alice envía a Bob un bitcoin, Bob debe proporcionar la dirección en la que desea recibir el pago. Además, Alice adjunta una dirección al bitcoin que desea enviar y luego transmite a los mineros este mensaje: "Alice posee un bitcoin que vive en esta dirección (inserte la dirección de bitcoin).

Alice desea enviar este bitcoin a Bob en esta dirección (dirección BTC) ".

Mientras Alice anuncia públicamente su intención, también debe enviarle a Bob la clave que le permita a Bob desbloquear la transacción y demostrar que ahora es el propietario legítimo. Al igual que nuestros hogares reales, existe una clave privada para cada bitcoin que demuestra que el titular de la clave es el propietario legítimo. En la red de Bitcoin, una clave privada es una pieza secreta de datos que está protegida por una firma criptográfica que demuestra su derecho a gastar bitcoins.

La combinación de su dirección de Bitcoin y su clave privada se denomina par de claves pública / privada. Si bien la red de Bitcoin siempre puede ver su dirección, nunca puede ver su clave privada. El problema de software que combina su dirección con su clave privada se conoce como billetera, y la mejor manera de pensar sobre esto es con una chequera. En sus cheques hay un número de cuenta, un número de ruta y un número de cheque. Usted completa cuánto dinero se retirará de su cuenta bancaria y designará quién está autorizado a retirar. Además, firma el cheque para que sea válido. Bitcoin funciona exactamente de la misma manera.

Su billetera constituye tanto su cuenta bancaria como sus cheques; se combinan en un sistema de almacenamiento electrónico eficiente similar a la banca en línea. Cuando "escribe un cheque" en la red de Bitcoin, toma bitcoins de su billetera y escribe el monto del "cheque". Su dirección de Bitcoin que se transmite públicamente contiene su número de cuenta y su número de ruta. El software de Bitcoin firma digitalmente su "verificación" con su clave privada y envía la transacción a la red para su verificación y transferencia.

Una vez transmitido, el blockchain registra el hecho de que los bitcoins fueron transferidos de la billetera de Alice a la billetera de Bob. El código de Bitcoin luego compila las transacciones más recientes en un archivo llamado bloque. Cada bloque contiene una referencia al bloque de transacciones anterior, formando así una "cadena" de transacción, y voila: hemos creado el blockchain.

El papel de los mineros

Ahora que tenemos un bloque de transacciones, debemos asegurarnos de que ninguno de estos bitcoins se haya gastado antes, y aquí es donde los mineros entran en juego. El código de software de Bitcoin reúne todas las transacciones (bloques) y transmite las transacciones a cualquier computadora que esté escuchando la red de Bitcoin. Las computadoras que están escuchando la red se conocen como mineros.

Como me gusta el helado, usemos un ejemplo de helado. Supongamos que un maestro trata de descubrir quién le dio secretamente una manzana (la transacción), y supongamos también que hay una ecuación matemática que le dirá exactamente quién era el dueño de la manzana antes de que se le transfiriera. El maestro llama a su clase desde el recreo y transmite a la red (a los niños) el hecho de que alguien ha transferido una manzana. Escribe la ecuación matemática en la pizarra y le pide a sus alumnos que resuelvan el problema. Como llamó a los niños desde el recreo, tiene que darles un incentivo para resolver la ecuación. Si los niños resuelven la ecuación matemática, recibirán una bola de helado con trocitos de chocolate. Como la respuesta a la ecuación contiene la clave privada, una vez que se resuelve la ecuación, el profesor sabrá quién le dio la manzana. Finalmente, para asegurarse de que la solución es correcta, el maestro estipula que seis niños deben llegar a la misma respuesta y deben mostrar su trabajo.

Los niños, desesperados por su recompensa, comienzan a trabajar con furia en la solución, quemando mucha energía en el proceso. Eventualmente, uno de los niños resuelve el problema y se le permite compartir la solución con el resto de la clase. Ahora el resto de la clase puede usar la respuesta para retroceder y demostrar que la ecuación original produciría esta respuesta. El primer niño que verifica la respuesta obtiene helado. La red Bitcoin funciona de la misma manera. Se transmite una transacción (manzana) a la red (clase de niños, también conocidos como mineros), y los mineros trabajan para resolver la ecuación y verificar que el dueño anterior de la manzana (bitcoin) tenía derecho a dársela al maestro. Una vez que seis mineros verifican la transacción, obtienen bitcoins (helado).

Justo ahora probablemente estés pensando: "¡Qué pequeño sistema de incentivos tan ingenioso! ¿Por qué no pensé en eso?" Bueno, en muchas formas, ya lo tenemos. La técnica de la zanahoria y el palo ha existido por milenios; es solo que Satoshi Nakamoto descubrió una forma de usar de forma segura la técnica de la zanahoria y el palo a través de Internet. Puede parecer extraño que un científico informático desconocido haya desarrollado un programa en el que todos "confiemos" para transferir valor. El sistema fue diseñado para ser inseguro y, como tal, el creador se ha vuelto inmaterial. El hecho de que no "conozcamos" al creador no significa que no podamos usar la tecnología; después de todo, ninguno de nosotros conoce a Thomas Edison, pero todos usamos electricidad. La chispa que creó Bitcoin fue el libro blanco de Satoshi, y, como el descubrimiento de Edison, la "cuadrícula" se ha expandido exponencialmente. El ecosistema de Bitcoin ahora incluye procesadores de pagos, mineros, fabricantes de equipos, intercambios y servicios financieros.

2.3- ¿Cómo compro Bitcoin?

Afortunadamente, ahora estás empezando a ver cómo está hecho Kool-Aid, te das cuenta de que no es veneno y estás pensando en tomar un sorbo. Está listo para salir corriendo, comprar su primer bitcoin y sacar provecho de la fiebre del oro digital. Bueno, frenar, vaquero. Para saciar tu sed insaciable de bitcoins, vas a tener que completar unos pocos pasos. Antes que nada, necesitas un lugar para guardar tus monedas. En el mundo de Bitcoin, donde almacena monedas, se lo conoce con el nombre increíblemente técnico ... billetera.

Ahora, no vaya a desempolvar el monedero de plástico que recibió cuando abrió su primera cuenta bancaria. Recuerde, un bitcoin es simplemente una cadena de números que identifica una unidad de moneda única. El tipo de billetera que necesitará para este viaje es una billetera electrónica, y estas billeteras electrónicas vienen en dos formas: billetera de software y billetera web. También hay algo llamado billetera de papel, pero aprenderemos sobre eso cuando hablamos de almacenamiento en frío y en caliente. Por ahora, no dejemos el carro delante del caballo.

La principal diferencia entre los dos tipos de billeteras es donde se almacenan sus monedas. En una billetera de software, sus bitcoins se almacenan en su disco duro. Esto significa que cualquier computadora en la que descargue la billetera de software se convertirá en su bóveda de bitcoins. Si la computadora se cuelga, perderá todas sus monedas, a menos que, por supuesto, haya respaldado la billetera en otro lugar. Si no desea tener una bóveda en su computadora portátil, puede optar por una billetera web, que utiliza la nube y proporciona acceso a sus monedas en cualquier lugar donde pueda conectarse a Internet. Similar a la banca en línea, con una billetera web puede ver su saldo en cualquier momento que se conecte a Internet. Al igual que un banco tradicional, el proveedor de la billetera web ahora se encarga de mantener la bóveda a salvo de los ladrones. Sin embargo, a diferencia de un banco, estos billeteros web no están asegurados por el gobierno. Si su empresa de billetera web es hackeada, tendrá pocos recursos.

Su elección de billetera dependerá de dos factores muy importantes: seguridad y facilidad de uso. Las carteras de software tienden a ser un poco torpes para el principiante, pero puede encriptar y hacer una copia de seguridad de su billetera en una memoria USB para mantenerse alejado de los intrusos. La desventaja de usar una billetera de software en su escritorio es que requiere que descargue toda la cadena de bloques. Descargar todo el blockchain significa descargar cada transacción que haya tenido lugar con bitcoins. Esto no solo puede ocupar mucha memoria, sino que también puede tomar algunos días.

El monedero original del software de Bitcoin se conoce como Bitcoin-QT. En realidad, es más que una billetera: es el software de Bitcoin, la billetera es simplemente una característica necesaria. Cuando descargue Bitcoin-QT, también estará descargando toda la cadena de bloques, y tendrá acceso a cada transacción que haya tenido lugar con bitcoins. Pero espera hay mas. También tendrás la capacidad de extraer monedas. Desafortunadamente, los días de usar el simple minero incorporado ya pasaron. Minería en estos días significa computadoras especialmente construidas con suficientes ventiladores para enfriar un elefante en la sabana.

Dos de las carteras web más conocidas son Coinbase y Blockchain.info, estas empresas juntas tienen más de tres millones de descargas de sus billeteras. Estas carteras son increíblemente fáciles de usar y no requieren descargar toda la información sobre la cadena de bloques de Bitcoin. Aún más, compañías como Coinbase también comprarán bitcoins en su nombre. No cabe duda de que la seguridad siempre es una preocupación, pero incluso antes del colapso de Mt Gox, estos servicios de billetera web estaban atrayendo grandes inversiones de capital de riesgo, lo que les permitió agregar muchas capas de seguridad.

Independientemente de la billetera que elijas, será necesario completarla. Recuerde, el banco no llenó su monedero de plástico; esperaban que hicieras el trabajo pesado. Así que ahora necesita una forma de llenar su billetera con bitcoins, y al igual que en la vida real, puede elegir hacer o comprar. Es decir, puedes extraer bitcoins, y si eres el primero en resolver la ecuación matemática, serás recompensado con bitcoins recién acuñadas. En un capítulo posterior, exploraremos la minería de bitcoin en profundidad, por ahora, solo sé que si eliges esta ruta, tu factura de electricidad casi seguramente se duplicará y tu pareja podría obligarte a mudarte. Ambas declaraciones son impresionantes pero verdaderas. Le sucedió a Emmanuel Abiodun, ¡su esposa lo obligó a mudarse a Islandia!

Suponiendo que valora su residencia actual y otra muy importante más que bitcoins, es probable que desee comprar sus monedas a través de un intercambio o corredor. Para intercambiar moneda fiduciaria (dólares, euros, yen, etc.) por bitcoin, necesitará una puerta de enlace a la red bitcoin. Alguien en la red debe estar dispuesto a desprenderse de sus bitcoins a cambio de dinero en efectivo. Puede realizar esta tarea usted mismo llamando a todos los contactos de la agenda y con la esperanza de que no solo encuentre a alguien que tenga bitcoins, sino que también quiera venderlos. Alternativamente, puede hacer lo que hacen las personas más cuerdas e ir a un intercambio o contratar a un agente.

Exchange versus Broker

Cuando compré bitcoins por primera vez, utilicé Coinbase. Fue relativamente sin dolor, excepto por la anticipación. Si desea comprar bitcoins con moneda fiduciaria, debe vincular una cuenta bancaria a Coinbase y transferir dinero, lo que generalmente demora unos días en completarse. Una vez que la moneda fiduciaria esté en su cuenta, Coinbase se pondrá en contacto con un intercambio y comprará bitcoins en su nombre. Para evitar fraudes, Coinbase le exige que espere sus bitcoins durante varios días hábiles para asegurarse de que la transacción se haya completado. Si quiere sus monedas antes, puede vincular una tarjeta de crédito a su cuenta como pago de respaldo. Muchos de los intercambios de Bitcoin actúan de manera similar; transfieres moneda fiduciaria al intercambio, y luego puedes comprar bitcoins de la gran cantidad de vendedores.

Hay una muy buena razón para que estos corredores e intercambios te hagan esperar por tus bitcoins. A diferencia de una transacción de tarjeta de crédito, las transacciones de bitcoin son irreversibles; una vez que se envía el bitcoin, se ha ido de su billetera para siempre. Con las transacciones con tarjeta de crédito, si no recibe el producto que solicitó, siempre puede llamar a Visa o American Express y solicitar que se revierte el cargo. Esto no sucede con bitcoins. El problema de permitir compras con tarjeta de crédito de bitcoins es que una persona inescrupulosa puede comprar bitcoins con una tarjeta de crédito y luego reclamar que nunca los recibió. La compañía de tarjeta de crédito no tiene manera de probar que los recibió o no y podría revertir el cargo, dejando al vendedor fuera de bitcoins y moneda fiduciaria.

Bitcoin está en las primeras etapas de desarrollo; de hecho, muchos de los desarrolladores principales consideran Bitcoin como un experimento. Al igual que con cualquier tecnología nueva, el panorama está cambiando rápidamente, y tanto los actores buenos como los malos pueden aparecer de la noche a la mañana. A medida que el ecosistema evoluciona, la crema se elevará a la cima, pero en esta etapa, la diligencia debida es tu mejor amigo. Antes de transferir dinero a cualquier bolsa, broker o vendedor individual de bitcoins, compruébelo. La comunidad de Bitcoin tiene un fuerte sentido de autocontrol, y muchos de los malos actores son llamados a Internet mucho antes de que ocurra algún problema. Si no le daría $ 10,000 a un extraño en un país extranjero para que lo retuviera, entonces tampoco se lo telegrafíe para comprar bitcoins. De acuerdo, volcamos la seguridad.

Ahora estamos equipados con los conocimientos básicos que mejorarán nuestro viaje hacia Bitcoin Big Shot. Nuestro siguiente paso es comprender lo que las empresas establecidas están haciendo con Bitcoin. En esta fiebre del oro digital, algunas empresas están adoptando la tecnología, otras temen y otras intentan adaptarse. Levi Strauss tenía planes de abrir una tienda de lona en el centro de San Francisco, hasta que miró a su alrededor y se dio cuenta de que los pantalones resistentes tenían una gran demanda. Puede estar seguro de que hay muchos Levi Strauss buscando en el ecosistema de Bitcoin e intentando adaptar sus habilidades.

2.4- ¿Quién lo "consigue"?

Los líderes del pensamiento, las corporaciones y los capitalistas de riesgo entienden la naturaleza transformadora de las monedas digitales como un sistema de pago. Además, la tecnología blockchain representa una revolución en la informática que se utiliza para transformar industrias. La explosión de las empresas y aplicaciones de Bitcoin ha llamado la atención de los minoristas, como Overstock, que se regocijan por la transferencia de valor sin fricciones y gratuita. Sin embargo, los intermediarios como Wells Fargo tienen razón al tener curiosidad sobre una tecnología que amenaza a su franquicia. Como primer paso, el 14 de enero de 2014, Wells Fargo se reunió con expertos en monedas virtuales para "aprender más" sobre esta tecnología. Cuando se le preguntó acerca de la reunión, Mary Eshet, vocera de Wells Fargo, dijo: "Es una moneda nueva, en evolución ... y como tenemos tanto interés e invertimos en sistemas de pago, queremos comprender todo lo que es relevante al respecto".

Ciertamente, las compañías de tarjetas de crédito tienen más que perder por la interrupción de Bitcoin, pero algunas están comenzando a adoptar la tecnología. En junio de 2014, MasterCard presentó una patente de EE. UU. Que le permitiría integrar bitcoins en su carrito de compras global. El impacto inicial y tal vez el temor se están reduciendo, y las compañías de tarjetas de crédito se están dando cuenta de que su fortaleza es el tamaño de su red, no el intercambio de medios subyacente. No obstante, la capacidad de transferir dinero con pocas tarifas afectará casi con certeza los márgenes de ganancia de compañías como Visa, MasterCard y American Express. Bitcoin tiene la capacidad de reemplazar tarjetas de crédito; si lo hará o no aún no se ha determinado.

En el otro extremo de la red centralizada se encuentran empresas como Overstock.com, que comenzó a aceptar bitcoins el 10 de enero de 2014. Patrick Byrne, CEO de Overstock, llevó a Twitter y anunció los resultados:

> # El primer día completo de Bitcoin en @ overstock.com fue un gran éxito: 840 pedidos, $ 130,000 en ventas. Casi todos los nuevos clientes. #aturdido
>
> -Patrick Byrne, @OverstockCEO

Lo que el Sr. Byrne no menciona es que el proceso de aceptar bitcoins está comenzando a simplificarse. Overstock, como cualquier otra empresa, necesita convertir los bitcoins recibidos en moneda fiduciaria (dólares estadounidenses, euros, libras, etc.) para pagar a sus proveedores y proveedores. Estas empresas confían en los procesadores de pago para completar esta tarea. Antes de los procesadores de pago, las empresas que aceptaban bitcoins tendrían que cambiarlos por moneda fiduciaria en una de las bolsas y luego transferir el dinero a la cuenta bancaria corporativa. Esto cambió cuando pioneros como BitPay ingresaron al mercado y ofrecieron el servicio de convertir bitcoins instantáneamente en fiat. BitPay no solo convierte bitcoins; también proporciona una solución de software sencilla para aceptar bitcoins que también se integra con el sistema de contabilidad de una empresa.

En 2012, BitPay llegó a los titulares al suscribir a más de 1,000 comerciantes para aceptar bitcoins, y a partir de mediados de 2014, ese número ha crecido a 30,000 empresas y organizaciones. BitPay, al igual que otros procesadores de pago, permite a los comerciantes en línea aceptar bitcoins con la misma facilidad que las tarjetas de crédito. La ventaja que ofrece esta empresa ilustra el poder disruptivo de Bitcoin como sistema de pago. En el sitio web de la compañía hay una práctica calculadora que determina la cantidad de dinero que un comerciante puede ahorrar al usar Bitcoin. Un comerciante típico que procesa $ 100,000 de pagos cada mes podría pagar $ 3,255 en tarifas de procesamiento de tarjetas de crédito. El mismo comerciante que acepta

bitcoins paga a Bitpay solo $ 300 para que actúe como su agente de procesamiento bitcoin, lo que resulta en un ahorro de casi $ 3,000 por mes. Dicho de otra manera, este comerciante podría aumentar su margen de ganancia en un 3 por ciento aceptando bitcoins, o podría usar los ahorros para bajar el precio de la mercancía, creando así una ventaja competitiva.

2.5- La fiebre del oro recién comienza

Los pioneros del Bitcoin Big Bang son solo la vanguardia. Hay una infraestructura económica completa para ser construida. En la década de 1850, en California, una vez que se obtenía el oro de fácil acceso, la fiebre del oro comenzó a desvanecerse. Sin embargo, su legado siempre está presente: California todavía se conoce como Golden State y San Francisco es un centro de descubrimiento empresarial. Incluso las señales de tráfico para las rutas estatales de California tienen la forma de una espada de minero. Del mismo modo, la fiebre del oro digital está comenzando a influir en su entorno. San Francisco es un hervidero de nuevas empresas de Bitcoin, y tanto Nueva York como California están compitiendo por ser las capitales de divisas digitales. A diferencia de la fiebre del oro de California de corta duración, el Big Bang de Bitcoin tiene el potencial de ser tan generalizado que esta fiebre del oro debería durar décadas. Sin duda, algunos de los primeros mineros de Bitcoin recolectaron el "oro" de fácil acceso, pero esta tecnología ofrece mucho más que el oro digital.

Las aplicaciones se están desarrollando utilizando la tecnología Blockchain de Bitcoin para interrumpir el profesional legal, los mercados financieros, la banca e incluso el voto. Bitcoin como moneda, o medio de intercambio, es solo el comienzo. Es el helado de vainilla dentro del helado de chocolate caliente. En la parte superior de la tecnología estarán las aplicaciones que permitirán que los préstamos peerto-peer aumenten, los documentos legales se conviertan en contratos inteligentes digitalizados y la votación se realice desde su teléfono móvil.

Al igual que Internet, los usos potenciales de Bitcoin son infinitos, lo que significa que esta fiebre del oro digital apenas está comenzando. Todavía hay tiempo para convertirse en el próximo Levi Strauss o Wells y Fargo. Para cumplir con nuestro destino, necesitamos saber más sobre el genio detrás de la tecnología y cómo resolvió un problema que ha dejado perplejos a las mentes más brillantes durante más de 30 años. Finalmente, necesitamos saber por qué el creador, Satoshi Nakamoto, decidió permanecer en el anonimato y seguir siendo un misterio.

Capítulo 3

> Toda persona informada necesita saber sobre Bitcoin porque podría ser uno de los desarrollos más importantes del mundo.
>
> -Leon Louw, nominado al Premio Nobel de la Paz

3.1- Bitcoin es más que oro digital

Cuando descubrí por primera vez Bitcoin, estaba firmemente en el campamento de "Tulipmania". ¿Cómo podría una cadena de números, respaldada por nada, y sin un ejército para hacer cumplir su uso, constituir una moneda? Bueno, espero que comiences a ver lo que finalmente vi: Bitcoin es más que una moneda, y es mucho más que oro digital. Es una tecnología disruptiva que destruye el crowdsourcing, la criptografía y la economía para producir la capacidad de transferir de manera rápida, segura y sin fricciones prácticamente cualquier cosa. Es un salto cuántico en el fenómeno de la red punto a punto. Bitcoin valora transferir lo que Napster era a la música.

Hay más en Bitcoin que solo la transferencia de valor, pero en los primeros días las redes de pago centralizadas son la fruta más fácil de conseguir para los Bitcoiners. La mayoría de la gente viene a Bitcoin como yo, primero escéptica, luego estudiante y finalmente creyente. La creación de Satoshi Nakamoto trasciende el oro digital y resuelve un problema que ha obstaculizado a los científicos informáticos durante más de 30 años. El problema de los generales bizantinos ha sido el principal obstáculo para la transmisión segura de valor a través de Internet no segura. Satoshi Nakamoto brindó una solución a este problema y luego se deslizó silenciosamente.

El enigma que es Satoshi Nakamoto ha llevado a muchos a recopilar evidencia circunstancial y declarar un descubrimiento. Por desgracia, ninguno de los buscadores de Satoshi ha podido encontrar la figura elusiva, e incluso los desarrolladores originales de Bitcoin que se correspondían con Satoshi han perdido el contacto. El tesoro inicial de bitcoins Satoshi minado vale millones y se piensa que no se gasta. ¿Quién es este genio clandestino y por qué el secreto?

3.2- Buscando a Satoshi

El 14 de marzo de 2008 comenzó como cualquier otro día de negociación; Revisé las noticias de la mañana y formulé mi plan de ataque. El S & P 500 había caído más del 15 por ciento desde octubre de 2013, y la economía de EE. UU. Había entrado en recesión, pero pocos podrían haber predicho lo que estaba a punto de ocurrir. La noche anterior, la empresa de corretaje Bear Stearns fue golpeada por una crisis de liquidez. Los clientes y acreedores del banco de inversión exigieron que se les devolviera el dinero, lo que dejó a la compañía insolvente. Esta era una carrera pasada de moda en el banco, y fiel a su función como prestamista de último recurso, la Reserva Federal necesitaba actuar. Los inversionistas se regocijaron cuando se hizo el anuncio de que JPMorgan, con la ayuda de la Fed, le prestaría dinero a Bear Stearns por 28 días.

A medida que la euforia disminuía, los inversores comenzaron a digerir las noticias y compraron acciones de Bear Stearns. Yo era escéptico del anuncio. Algo me estaba molestando: no podía entender cómo los inversionistas podían justificar la compra de acciones de una compañía insolvente. Los mercados rara vez viven en el ámbito de lo racional; la exuberancia irracional y el miedo son los estados donde los mercados pasan la mayor parte del tiempo. Comencé a comprar opciones de venta de acciones de Bear Stearns, que serían rentables una vez que se hubiera cumplido el extremo irracional y el precio de las acciones comenzara a caer. Al principio mi

apuesta fue un perdedor; los inversionistas continuaron creyendo que 28 días era todo lo que Bear Stearns necesitaba para salir de la peor crisis crediticia desde la Gran Depresión. En mi opinión, no estaba haciendo la apuesta de que Bear Stearns fracasaría, solo que los inversores estaban demasiado entusiasmados con el rescate. Al final del día, el precio de las acciones había caído a $ 30 por acción y mi apuesta estaba en el dinero. Decidí mantener mi apuesta abierta durante el fin de semana, creyendo que el pesimismo irracional aún no se había alcanzado. No tenía idea de lo que traerían las próximas 48 horas.

Luego de un tumultuoso fin de semana de negociaciones, se anunció que Bear Stearns había fallado, y JPMorgan compró los activos restantes a un precio de $ 2 por acción. Inadvertidamente había hecho uno de los mejores oficios de mi carrera, pero la victoria fue hueca. El colapso de Bear Stearns le había costado a la gente no solo sus trabajos sino también una gran parte de los ahorros de su vida. La razón dada por la Reserva Federal para permitir el colapso fue que Bear Stearns fue insolvente y lo mejor era dejar que un jugador fuerte como JPMorgan ayudara a limpiar el desastre. La Reserva Federal pensó que estaba actuando bajo su mandato para garantizar la estabilidad financiera; sin embargo, dentro de seis meses, Lehman Brothers había fallado y el sistema financiero mundial estaba al borde de la extinción.

Lo que ocurrió fue el fracaso en el centro del sistema financiero. Por su propia admisión, los banqueros centrales globales tardaron en comprender la gravedad de la crisis crediticia que se estaba desarrollando. El fracaso de Lehman Brothers y el posterior rescate de AIG pusieron de relieve este hecho. Ben Bernanke, el presidente de la Reserva Federal, era un académico especialista en la Gran Depresión, y estaba decidido a no repetir los errores de sus predecesores. Junto con el Secretario del Tesoro, Hank Paulson, presentó un plan para recapitalizar el sistema bancario; se llamaba Programa de Alivio de Activos en Problemas o TARP.

Solo quince días después de que el Tesoro de EE. UU. Anunciara que usaría TARP para comprar participaciones en los bancos más grandes, se publicó un documento a través de la Lista de distribución de criptografía que describe un sistema de transacción sin efectivo de punto a punto. En medio de una crisis financiera, el papel oscuro solo hizo una onda dentro de la comunidad criptológica. Al igual que mi operación con Bear Stearns, pocos tenían idea de cuán grande sería. El documento fue escrito por Satoshi Nakamoto. La función "Bitcoin P2P E-Cash Paper" presenta la publicación original.

Papel Bitcoin P2P E-Cash

Satoshi Nakamoto, sáb, 01 de noviembre de 2008 16:16:33 -0700

He estado trabajando en un nuevo sistema electrónico de efectivo que es totalmente par a par, sin terceros confiables.

El documento está disponible en: http://www.bitcoin.org/bitcoin.pdf

Las propiedades principales:

El doble gasto se previene con una red de igual a igual.

Sin menta u otras partes de confianza.

Los participantes pueden ser anónimos.

Las nuevas monedas están hechas de prueba de trabajo de estilo Hashcash.

La prueba de trabajo para la nueva generación de monedas también impulsa a la red para evitar el doble gasto.

Bitcoin: un sistema de efectivo electrónico punto a punto

Abstracto. Una versión puramente de igual a igual del efectivo electrónico permitiría que los pagos en línea se envíen directamente de una parte a otra sin la carga de pasar por una institución financiera.

Las firmas digitales brindan parte de la solución, pero los beneficios principales se pierden si aún se requiere una parte confiable para evitar el doble gasto. Proponemos una solución para el problema del gasto en dobles usando una red de igual a igual. La red marca las transacciones al tiempo que las mezcla en una cadena continua de prueba de trabajo basada en hash, formando un registro que no se puede cambiar sin rehacer la prueba de trabajo. La cadena más larga no solo sirve como prueba de la secuencia de eventos atestiguada, sino como prueba de que proviene del mayor conjunto de potencia de la CPU.

Siempre que los nodos honestos controlen la mayor potencia de CPU en la red, pueden generar la cadena más larga y superar a los atacantes. La red en sí misma requiere una estructura mínima. Los mensajes se emiten sobre la base del mejor esfuerzo, y los nodos pueden salir y unirse a la red a voluntad, aceptando la cadena de prueba de trabajo más larga como prueba de lo que sucedió mientras ellos no estaban.

Documento completo en: www.bitcoin.org/bitcoin.pdf Satoshi Nakamoto

Antes de publicar este artículo sobre una cosa llamada Bitcoin, Satoshi era relativamente desconocido. De hecho, no estaba claro si Satoshi era una sola persona o un grupo. Satoshi tenía un perfil en el sitio web de la Fundación P2P que lo describió como un hombre japonés de 37 años, pero un análisis exhaustivo de la codificación y los mensajes de Satoshi Nakamoto llevó a muchos a creer que no eran en absoluto japoneses. Los primeros codificadores que trabajaron en Bitcoin e interactuaron con Satoshi a través del correo electrónico describieron que Satoshi hablaba inglés con fluidez y comúnmente usaba la ortografía inglesa.

Después de publicar el documento, Satoshi trabajó en el proyecto Bitcoin hasta abril de 2011 y luego se escabulló silenciosamente.

3.3- La búsqueda

La búsqueda de la identidad de Satoshi comenzó con algunos de los usuarios del foro de Bitcoin revisando las publicaciones en busca de cualquier cosa que revelara el verdadero genio. Cuando el examen inicial de las publicaciones arrojó pocas pistas, un codificador activo del foro de Bitcoin llamado Stefan Thomas grabó las más de 500 publicaciones del foro de Satoshi. Thomas descubrió que casi no había mensajes entre las 5 a.m. y a las 11 a.m. Meridiano de Greenwich. La implicación fue que Satoshi estaba durmiendo durante estas horas. Yendo más lejos, muchos supusieron que Satoshi era un durmiente convencional y esto significaba que Satoshi Nakamoto residía en las zonas horarias central o del este de América del Norte o en el Caribe.

El problema, por supuesto, era que todos suponían que Satoshi Nakamoto era convencional. Si Satoshi es / fue una sola persona, no solo necesitaría ser un hábil programador de computadoras, sino también estar familiarizado con la criptografía y tener una comprensión íntima de la economía. La palabra criptografía tiene sus raíces en las palabras griegas para "oculto" y "secreto". La criptografía moderna depende en gran medida de la teoría matemática y de los algoritmos para encriptar las comunicaciones. La excelencia en cualquiera de estos campos calificaría al individuo como extraordinario. La excelencia en los tres campos sería asombrosa por cualquier medida.

A pesar de las formidables probabilidades de encontrar un criptógrafo experto (especialmente uno que no quisiera ser encontrado), la búsqueda continuó. Aquellos en persecución recurrieron a la lingüística para desentrañar la identidad de Satoshi. Términos como sangrientos en publicaciones hicieron creer a muchos que se originaron o vivieron en Gran Bretaña. Aún más fascinante es que dentro del código de Bitcoin hay una etiqueta relacionada con un informe del Times of London publicado en enero de 2009 sobre el rescate de los bancos británicos. Estas pistas fueron descubiertas por Joshua Davis y publicadas en un artículo para The New Yorker.

Armado con evidencia circunstancial bien razonada, Joshua Davis elaboró una breve lista de posibles Satoshis. Después de todo, solo había unas pocas personas en el mundo con el conocimiento para crear Bitcoin. La codificación requerida y las habilidades criptográficas descartaban la mayoría en la profesión de economía, por lo que Davis se volvió hacia el mundo clandestino de la criptografía.

A pesar de que todavía era estudiante en el Trinity College de Dublín, Michael Clear era una estrella de 23 años en el mundo de la criptografía cuando Joshua Davis lo confrontó en la conferencia Crypto 2011 en Santa Bárbara. Se ajustaba perfectamente a la descripción de "Satoshi"; según todos los informes, era un brillante codificador y criptólogo, había trabajado en finanzas y había sido coautor de un documento sobre tecnología entre pares. Su ciudadanía británica le agregó profundidad a la imagen, pero cuando Davis le preguntó a Michael Clear si era Satoshi, simplemente respondió: "No soy Satoshi, pero incluso si lo fuera, no te lo diría". Como puedes imaginar, este La respuesta hizo poco para calmar la especulación, si acaso, aumentó el misterio. Finalmente, después de una vorágine mediática, Michael Clear le dijo al IrishCentral: "Siempre lo he negado con vehemencia (siendo Satoshi). Nunca me permitiría ser reconocido ni remotamente por la creatividad y el arduo trabajo de otra persona. "Esto pareció ser el truco, y la investigación avanzó.

Joshua Davis no fue el único que buscó a Satoshi. Aproximadamente al mismo tiempo, Adam Penenberg estaba recopilando su propia evidencia circunstancial. Presentó su investigación ciertamente acientífica pero convincente en un artículo para la revista Fast Company. Su primer trabajo de detective fue encontrar una línea oscura de texto del documento original de Bitcoin escrito por Satoshi Nakamoto. Se decidió por la frase "impracticable desde el punto de vista computacional para revertir".

Penenberg conectó expectantemente la frase en la búsqueda de Google y se descubrió una solicitud de patente con la misma frase. La patente fue fechada el 15 de agosto de 2008, y fue por un método para encriptar secretos entre computadoras. Concluyó que transferir valor de una computadora a otra no era más que un secreto compartido. Una investigación adicional lo llevó a buscar cuando se registró el nombre de dominio BITCOIN.ORG, y descubrió que se registró apenas 72 horas después de que se presentó la solicitud de patente.

Quizás este feliz accidente no fue en absoluto un accidente. Penenberg se propuso encontrar a los tres hombres enumerados en la solicitud. Neal King, Vladimir Oksman y Charles Bry están listados en la patente # 20100042841. Cada uno de estos hombres tenía amplios antecedentes en

codificación de computadoras y criptología. Y cada uno de estos hombres negó que juntos o por separado sean Satoshi Nakamoto.

La búsqueda había llegado a otro callejón sin salida. Ya fuera intencional o no, Satoshi había dejado suficientes migas de pan para satisfacer a los curiosos, pero no lo suficiente como para saciar a los hambrientos. Tal vez estos callejones sin salida eran parte del plan de Satoshi para permanecer en el anonimato, o tal vez las pistas correctas aún no se habían descubierto.

El siguiente nombre en la lista puede ser el más fascinante a la luz de la implosión del intercambio de Mt Gox. Jed McCaleb abandonó UC Berkeley y fundó el intercambio Mt Gox. McCaleb ciertamente tiene la formación técnica para ser el famoso Satoshi; de hecho, no solo fundó la red de intercambio de archivos punto a punto eDonkey en 2000, sino que también es uno de los fundadores de Ripple, una criptomoneda alternativa. Cuando Jed vendió el intercambio de Mt Gox, fue citado diciendo que el intercambio era "genial y necesitaba existir", pero que ya no lo encontraba "técnicamente interesante". La similitud de esta respuesta a una cita del último correo electrónico de Satoshi tenía muchos creían que McCaleb y Satoshi eran uno y el mismo. Sin embargo, al igual que sus predecesores, Jed McCaleb también ha negado ser Satoshi.

Las adiciones más recientes a la lista de sospechosos son Shinichi Mochizuki y Nick Szabo. Mochizuki es descrito como un genio excéntrico que resolvió la Conjetura ABC, una de las ecuaciones matemáticas más complejas del mundo. Se especula que Mochizuki creó Bitcoin en su tiempo libre, como si resolver problemas matemáticos complicados no fuera lo suficientemente complicado. Publicó su solución a la Conjetura ABC en Internet en lugar de las revistas académicas más tradicionales, y luego ... se alejó. Se ha negado a explicar su solución a los matemáticos y ha negado que sea Satoshi. Excéntrico, sí. Satoshi? Nunca sabremos.

Nick Szabo no solo es un ex profesor de la Facultad de Derecho de la Universidad George Washington, sino que también es un científico informático conocido por acuñar el término contratos inteligentes. Aprenderemos mucho más sobre contratos inteligentes en capítulos posteriores. Por ahora, lo que necesita saber sobre Nick Szabo es que inventó una moneda digital descentralizada llamada "bit gold" y que ha negado ser Satoshi Nakamoto.

A medida que la búsqueda de un creador basado en el carbono se quedó corta, muchos comenzaron a especular que tal vez una corporación o agencia gubernamental estaba detrás de la criptomoneda. Tal vez había un equipo secreto encerrado en Google, codificando subrepticiamente el código y guiando el movimiento. Otros sugirieron que las primeras letras de cuatro grandes compañías tecnológicas podrían usarse para deletrear Satoshi Nakamoto: SAmsung, TOSHIba, NAKAmichi y MOTOrola. Para no quedarse atrás, la multitud de la teoría de la conspiración comenzó a pensar que la NSA o la CIA habían creado la moneda para rastrear los hábitos de gasto.

El 23 de abril de 2011, la cuenta asociada con Satoshi envió su correo electrónico final, que decía: "Pasé a otras cosas. Está en buenas manos con Gavin y con todos ". Con esas simples palabras crípticas, el creador de la invención más fascinante desde la computadora personal e Internet desapareció en el mismo éter del que surgió.

Por cierto, "Gavin" es Gavin Andresen, el científico jefe de la Fundación Bitcoin; él también ha sido nombrado posible sospechoso en la búsqueda de Satoshi. Por desgracia, como los demás en la cadena, ha negado que sea el creador enigmático.

Fue Leah McGrath Goodman quien causó el mayor revuelo con su exposición de Dorian S. Nakamoto para el relanzamiento de la revista Newsweek. Cuando Goodman siguió a Dorian S.

Nakamoto a su modesta casa en Temple City, California, apostaba que la "S" representaba a Satoshi. Estaba convencida de que el creador de Bitcoin se estaba escondiendo a plena vista. Mientras que Leah McGrath Goodman se había comunicado con Dorian por correo electrónico, cuando preguntó por Bitcoin, las comunicaciones cesaron. Decidida a seguir este ejemplo, apareció sin previo aviso en la casa de Dorian Nakamoto, pero su inesperada llegada hizo que Dorian llamara a la policía local. Con la protección de la policía de Temple City, Dorian Nakamoto se encontró con la Sra. Goodman al final de su entrada. Cuando se le preguntó acerca de Bitcoin, Dorian S. Nakamoto habría dicho que "ya no estoy involucrado en eso y no puedo discutirlo". Ha sido entregado a otras personas. Ellos están a cargo de eso ahora. Ya no tengo ninguna conexión".

Los oficiales de policía que fueron llamados al hogar confirman las palabras de Dorian. Sin embargo, la comunidad Bitcoin está en negación. La Fundación Bitcoin emitió una declaración escrita por Jeff Garzik en su blog oficial (vea la función "We Are All Bitcoin").

> Todos somos Bitcoin
>
> Jeff Garzik, Bitcoin Core Dev Team, Guest Blogger,
>
> 6 de marzo de 2014
>
> Nunca hay un momento aburrido en Bitcoin. Hoy hemos visto una mayor especulación de los medios sobre la identidad de Satoshi Nakamoto. Al escribir estas líneas, no hemos visto evidencia concluyente de que la persona identificada sea la diseñadora de Bitcoin. Aquellos que están más cerca del proyecto de Bitcoin, el equipo informal de desarrolladores centrales, siempre han ignorado la verdadera identidad de Nakamoto, ya que Nakamoto se comunicó puramente a través de medios electrónicos.
>
> Aún así, es una oportunidad útil para revisar la identidad de Nakamoto y su relación con el proyecto actual. El diseño de Bitcoin está intencionalmente descentralizado de muchas maneras, sin duda, la operación de cadena de bloques y la red P2P, pero es más que eso. Los datos de blockchain de Bitcoin son cero confianza. Cada nodo completo en la red P2P valida el 100 por ciento del historial de transacciones, sin confiar en ninguna autoridad central. Más allá de los datos, el software Bitcoin en sí mismo es de código abierto y está disponible para su revisión por cualquier persona. Cualquiera puede bifurcar el software, crear una mejor versión y ganar usuarios.
>
> Todos los que están involucrados en Bitcoin entienden la fuerza del diseño. El diseñador, que opera bajo un presunto seudónimo, reforzó esto. No había necesidad de conocer y confiar en Satoshi Nakamoto. El diseño se mantuvo en pie, abierto a la inspección por todos. Satoshi Nakamoto finalmente creó un "lenguaje" de clases con el protocolo bitcoin. Un protocolo de red, como Bitcoin, no es más que una lingua franca común que permite que varias partes se comuniquen de forma útil entre sí. Al igual que otros idiomas hablados en todo el mundo, el protocolo bitcoin crece y cambia a medida que los usuarios cambian, en última instancia, controlados por nadie.
>
> El proyecto de Bitcoin está descentralizado. No tiene un líder por diseño. Cada miembro de la comunidad contribuye y colabora con otros en función de sus propias necesidades, elecciones y libre albedrío. La implementación de

> referencia de Bitcoin tiene un científico en jefe, pero en última instancia el liderazgo siempre descansa en las manos de cada usuario de bitcoins. La Fundación Bitcoin está abriendo capítulos de afiliados en todo el mundo, y otros están organizando sus propios grupos de Bitcoin de forma descentralizada. La Fundación Bitcoin es un líder de Bitcoin, pero ciertamente no es el líder de Bitcoin.
>
> La identidad de Satoshi puede o no revelarse a tiempo. Según la investigación actual de Sergio Lerner, Satoshi no parece haberse movido ni gastado ningún bitcoins. Es poco probable que Satoshi esté sentado en una playa en Tahití, al lado de una mansión multimillonaria. Es poco probable que Satoshi esté preparado para ladrones decididos y potencialmente violentos y buscadores de curiosidad. La curiosidad en la identidad de Satoshi es comprensible, pero por favor considere la revelación responsable y el peligro que tal revelación puede generar.
>
> El protocolo de Bitcoin no existiría sin Satoshi, que sin dudas es un diseñador brillante. Sin embargo, Bitcoin perdurará mucho después de Satoshi, ya que Bitcoin es todo el mundo que lo usa, no solo una persona.

Dorian Nakamoto es un entusiasta de los trenes de modelo y, según informes, trabajó en varios proyectos clasificados para corporaciones y el gobierno de EE. UU., Pero su situación financiera no gritaba sobre una persona con un valor de más de $ 500 millones. Vive en una casa modesta con un Toyota Corolla estacionado en el camino de entrada. El tesoro original de bitcoins que se cree que pertenece a Satoshi Nakamoto sigue sin gastarse, y muchos especulan que Dorian Nakamoto puede haber perdido las llaves privadas. Si Dorian Nakamoto es el creador de Bitcoin, podría haber una explicación simple para su apariencia financiera externa: él es un experto en criptografía. Tal vez parezca ser un mendigo es simplemente una función, o función de hash criptográfico si se quiere. En la película Goodfellas, Jimmy Conway le dice a sus co-conspiradores que permanezcan discretos después del famoso robo de Lufthansa; quizás Dorian Nakamoto está siguiendo ese consejo.

O tal vez él no es el verdadero Satoshi. Apenas unos días después de que se publicara la historia de Newsweek, la cuenta de Satoshi en la página Ning de la Fundación P2P cobró vida. El mensaje simple era "No soy Dorian Nakamoto". El creador y el operador de la página confirmaron que la cuenta utilizada para publicar este mensaje era la misma cuenta asociada con la publicación original del documento de Bitcoin. Sin embargo, no hay forma de saber si el creador de la cuenta es el "verdadero" Satoshi o simplemente otra barba.

Dado que recopilar evidencia circunstancial está de moda en la búsqueda de Satoshi, agregaré una pieza más al rompecabezas. Una compañía de juegos basada en el Reino Unido llamada Mind Candy ha creado Perplex City, una ciudad en línea donde los residentes resuelven rompecabezas y cifrados complejos. En 2007, la compañía de juegos lanzó un desafío a los residentes de Perplex City: encontrar a un individuo con solo su primer nombre e imagen. Publicaron este desafío en el sitio web www.billion2one.org. La imagen parece ser una selfie de un hombre asiático parado en Alsacia, Francia. La única pista dada a los jugadores es el primer nombre del caballero: Satoshi. Sería un genio puro para el creador de Bitcoin usurpar el nombre del hombre en este juego y usarlo para ofuscar su verdadera identidad. Por supuesto, como cualquier otro buscador de Satoshi, no tengo absolutamente ninguna evidencia de que esto haya ocurrido, pero seguro que se sumaría al misterio.

3.4- ¿Por qué Satoshi es un genio?

Aquellos que interactuaron con Satoshi coinciden en que lo único que el creador no quería era que Bitcoin se asociara con cualquier individuo. Como sistema descentralizado, debía permanecer sobre el software, no sobre el creador. Si efectivamente el blockchain se convirtiera en el nuevo tercero de confianza, un único punto de falla no podría estar presente. Bitcoin necesitaba ser una comunidad, un grupo de personas que se unieran para resolver una tarea. Lo que Satoshi Nakamoto había hecho era resolver el problema de los Generales bizantinos, y su elegante solución requería consenso.

El problema de los generales bizantinos fue propuesto primero por los informáticos Leslie Lamport, Robert Shostak y Marshall Pease en 1982. En esencia, el problema de los generales bizantinos es el problema de establecer la confianza entre partes no relacionadas a través de una red de comunicación en la que no se puede confiar.

Internet le ha dado acceso a la información a cualquiera que se conecte a la red. Esto en sí mismo no tiene precedentes en la historia humana y ha desencadenado numerosas revoluciones democráticas. Nunca antes la población masiva tuvo acceso a la misma información que los líderes. Sin embargo, como sabemos muy bien, dado que cualquiera puede publicar información en Internet, no siempre se puede confiar en esa información. Antes de Bitcoin, la información confiable se centralizaba en terceros, como medios de comunicación respetados y agencias gubernamentales. Por supuesto, estos terceros representan un único punto de falla y se ha encontrado que no siempre realizan sus funciones. De hecho, algunos de estos terceros han utilizado su posición de poder para manipular la información para su propio beneficio.

El problema de los generales bizantinos ha confundido a los científicos informáticos durante más de tres décadas, y hasta Bitcoin, muchos pensaron que el problema no tenía solución. La solución de Satoshi Nakamoto, llamada protocolo Bitcoin, no solo le brinda a cada usuario de Internet una forma segura de transferir información, sino que también garantiza que la información sea legítima. Este es un avance en la ciencia de la computación y la historia humana que no se puede exagerar. Con Bitcoin, el viejo dicho de que "no se puede confiar en todo lo que se lee en Internet" es solo eso ... un viejo dicho.

Bitcoin fue diseñado para ser infiel. Es decir, el sistema no requiere que los usuarios confíen entre sí. Todo lo que necesitan los usuarios es el acceso a las "imágenes" tomadas por los paparazzi para verificar dónde ha estado cada bitcoin. Un sistema sin confianza no puede tener una figura central; socavaría todo el proyecto. Bitcoin nació de la crisis financiera de 2008, un momento en el que la confianza era un bien escaso.

En el núcleo de nuestro sistema financiero está la confianza de que la moneda que estamos intercambiando será aceptada en otra parte. Esta confianza es un resultado directo de terceros confiables que avalan su valor. Ya sea que esta moneda sea el dólar estadounidense, el yen japonés o incluso una garantía respaldada por hipotecas, si la creencia en terceros se deteriora, todo el sistema falla. Bitcoin fue la solución correcta en el momento adecuado. Ofrecía una manera de confiar en el valor sin la necesidad de un tercero. Bitcoin intervino donde los bancos de inversión habían fallado.

El desastre de Bear Stearns y el colapso de Lehman Brothers mostraron que los puntos únicos de falla pueden conducir a una falla completa del sistema. La Reserva Federal salvó el sistema al actuar como el prestamista centralizado de último recurso, pero la Fed pagó por estas acciones

con una pérdida de credibilidad. Incluso el venerado ex presidente de la Reserva Federal Paul Volcker dijo en un discurso que la Fed había tomado "acciones que se extienden hasta el límite de sus poderes legales e implícitos". Bitcoin puede ser una respuesta a esta pérdida de credibilidad y quien lo creó fue a grandes longitudes para eliminar cualquier tercero centralizado.

Tal vez Satoshi sabía demasiado bien que un sistema centralizado es tan fuerte como la creencia en la autoridad central para hacer lo correcto. Si el creador de Bitcoin intentaba provocar una revolución, no podría construirse en un solo punto. Es por esta razón que nunca podremos conocer al verdadero Satoshi. Un criptógrafo experto que no quiere ser encontrado tiene la ventaja última, y Satoshi hasta ahora ha demostrado que el anonimato es primordial.

3.5- Más grande que Satoshi

Puede que nunca encontremos a Satoshi, y si no lo hacemos, el ecosistema de Bitcoin puede prosperar; esa es la belleza de la naturaleza descentralizada de la tecnología. Afortunadamente, la solución elegante y autosuficiente para el problema de los Generales bizantinos se está volviendo clara para usted. Tal vez su mente está explotando con ideas sobre cómo aplicar esta solución a una gran cantidad de industrias. No estas solo.

Como veremos en capítulos posteriores, los individuos están construyendo bolsas descentralizadas basadas en la tecnología blockchain; mientras que otros tomaron la moneda original de Satoshi y mejoraron el código para crear nuevas monedas. Estas monedas denominadas alternativas se utilizan para llevar agua a quienes la necesitan y para reducir los costos que los comerciantes y consumidores pagan para intercambiar bienes y servicios.

No hay una persona viva hoy que "conozca" a Thomas Edison, pero eso no nos impide usar su invención para impulsar ciudades y manejar nuestra economía. Buscar, encontrar y conocer a Satoshi Nakamoto es noticia en los titulares que venden revistas, pero es irrelevante para el uso y la función de la creación. Al igual que la electricidad, Bitcoin se ha vuelto más grande que el individuo.

La búsqueda de Satoshi comenzó como una búsqueda para encontrar un hombre, mujer o grupo, pero en un sentido más amplio es una búsqueda para reconstruir el fracturado sistema financiero. La confianza fue destruida por la crisis financiera de 2008 y Satoshi encontró una manera de reconstruir. El sistema descentralizado y sin confianza llamado Bitcoin es una tecnología sobre la que se puede construir el nuevo sistema financiero. En particular, el concepto de blockchain o "paparazzi" que registra todas las transacciones podría tener un efecto transformador sobre cómo funciona el sistema financiero.

Hace más de 300 años, se establecieron los primeros bancos centrales modernos en Suecia e Inglaterra, y durante los últimos tres siglos el sistema financiero se construyó sobre una autoridad monetaria centralizada. La idea de un sistema financiero descentralizado es algo que puede amenazar a quienes están en el medio del sistema actual, pero debe considerarse como una oportunidad. Si de hecho surge un nuevo sistema descentralizado, entonces se debe construir una nueva infraestructura.

Habrá oportunidades para que surjan nuevos JPMorgans. En algún lugar de Silicon Valley podría haber otro Henry Wells o William Fargo trabajando en el próximo banco American Express y Wells Fargo. Se ha dicho que salir de la crisis trae oportunidades, y ningún lugar es más evidente que el mundo de las monedas alternativas. La búsqueda de Satoshi debería tratarse más de encontrar estas oportunidades que de encontrar al creador. Incluso si Satoshi se desenmascara, no debería

tener ningún impacto en Bitcoin o en el nuevo sistema financiero que se está formando a su alrededor. La búsqueda de Satoshi es una búsqueda de un sistema financiero mejor y más fuerte. Encontrar a Satoshi debería significar que hemos aprendido de los errores del pasado y adoptado nuevas ideas. Debería significar que estamos en el camino de la reconstrucción.

El 14 de marzo de 2008, tuvimos la suerte de tener un liderazgo de acción rápida. Las acciones de la Reserva Federal y del Tesoro probablemente evitaron un colapso financiero total. Lamentablemente, aún no está claro qué precio, si es que hay alguno, tendremos que pagar. ¿La inflación finalmente volverá a su horrible cabeza, o la brecha de la desigualdad conducirá a la agitación social? O tal vez, solo tal vez, estos valientes líderes encontraron una solución a un problema que ha plagado a los bancos centrales durante 300 años. Si lo han hecho, significa que han encontrado la cura para las recesiones y los pánicos financieros. Por desgracia, mi fe en el comportamiento humano me lleva a creer que los extremos de miedo y avaricia son más grandes que un banco central. Un banco central puede actuar como un bache de velocidad para frenar el pánico o sofocar la euforia, pero la cura sigue siendo esquiva.

La creación de Satoshi puede ser un elixir para nuestro sistema financiero. Si hemos aprendido algo de la crisis financiera de 2008, es que un único punto de falla tiene el potencial de destruir todo el sistema. El legado de Satoshi será una solución a este problema. Bitcoin y el concepto de blockchain es una forma elegante de reducir los puntos únicos de falla y descentralizar el sistema financiero. Para estar seguros, todas las creaciones humanas son defectuosas y en el camino descubriremos las limitaciones de Bitcoin. Sin embargo, la descentralización es un paso en la dirección correcta. En palabras de Victor Hugo, "Nada puede detener una idea cuyo momento ha llegado".

Capítulo 4

El que sabe cuándo puede luchar y cuándo no puede, será victorioso.

-Sun Tzu

4.1- Problema generales de los bizantinos

Los empresarios exitosos están constantemente examinando el paisaje en busca de problemas para resolver. Ser el primero en resolver un gran problema social no solo puede conducir a una acumulación sustancial de riqueza, sino que puede hacer que el emprendedor sea más popular de lo que nunca imaginó. No necesitamos mirar mucho más allá de Mark Zuckerberg y Facebook para un buen ejemplo; estaba frustrado con la incapacidad de comunicarse con sus compañeros y se vio obstaculizado por una cultura excluyente. Su solución fue crear una plataforma de comunicación abierta a todos, abierta a todos los que tenían la capacidad de asistir a Harvard. Su solución se hizo conocida como la red social; se hizo multimillonario y realizó una importante película sobre el desarrollo de Facebook.

Es una apuesta segura que Hollywood finalmente hará una película sobre Satoshi Nakamoto, incluso si tienen que inventarse. El creador de Bitcoin ha hecho todo lo posible para ocultar su identidad, lo que hace que la historia sea aún más fascinante. Sin embargo, la atención que tanto el creador como la subida de precios han acumulado enmascara la verdadera razón por la cual Bitcoin cambia las reglas del juego. El problema que resolvió Bitcoin ha eludido a todos los científicos informáticos desde su concepción; se llama el problema de los generales bizantinos.

El problema de los generales bizantinos fue propuesto por primera vez por los informáticos Leslie Lamport, Robert Shostak y Marshall Pease en 1982. El problema original se planteó de esta manera:

Imaginamos que varias divisiones del ejército bizantino están acampadas fuera de una ciudad enemiga, cada división comandada por su propio general. Los generales pueden comunicarse entre sí solo por mensajero. Después de observar al enemigo, deben decidir sobre un plan de acción común. Sin embargo, algunos de los generales pueden ser traidores, tratando de evitar que los generales leales lleguen a un acuerdo.

Los generales deben tener un algoritmo para garantizar que A. Todos los generales leales deciden el mismo plan de acción.

Los generales leales harán lo que el algoritmo diga que deben hacer, pero los traidores pueden hacer lo que quieran. El algoritmo debe garantizar la condición A independientemente de lo que hagan los traidores.

Los generales leales no solo deben llegar a un acuerdo, sino que deben acordar un plan razonable. Por lo tanto, también queremos asegurar que B. Un pequeño número de traidores no puede hacer que los generales leales adopten un mal plan.

Sin embargo, esta descripción es realmente solo una extensión del Problema de los Dos Generales primero propuesto por. A. Akkoyunlu, K. Ekanadham y R. V. Huber en 1975 en "Algunas limitaciones y concesiones en el diseño de las comunicaciones de red".

El problema de los dos generales comienza con dos ejércitos que quieren atacar una ciudad y saquear las riquezas que se encuentran dentro. La ciudad fortificada se encuentra en un valle entre las dos colinas y solo se puede conquistar si ambos ejércitos atacan al mismo tiempo. Los generales deciden comunicar el momento del ataque una vez que han tenido la oportunidad de inspeccionar la ciudad y ubican a sus tropas en colinas opuestas. Una vez que los generales llegan a sus respectivas colinas, la única forma de comunicarse es enviar un mensajero a través del valle, lo que puede provocar la captura o enviar un mensaje falso. El problema de los dos generales es que necesitan comunicar el momento de un ataque sincronizado enviando un mensajero a través del valle inseguro.

La metáfora ayuda a comprender el problema que puede experimentar una red de computadoras si se pasa información valiosa entre los nodos. Cada computadora en la red se llama nodo y es sinónimo de general. La única forma de que las computadoras se comuniquen es mediante una telaraña insegura de líneas telefónicas, cables de fibra óptica e incluso satélites, es decir, Internet. Internet en el problema de los dos generales es el valle por el que debe pasar el mensaje. Cada nodo de la red necesita una forma de determinar si el mensaje que recibe es legítimo. Como lo ilustró la Agencia de Seguridad Nacional de los Estados Unidos, los mensajes enviados a través de Internet pueden ser interceptados, y eso es problemático cuando se trata de enviar algo de valor.

El problema que debe resolverse es cómo comunicar el mensaje de "ataquemos a las nueve en punto" para que ambos generales puedan acordar lanzar la ofensiva en un momento sincronizado. Esto puede parecer simple, pero su complejidad radica en su sutileza. Una vez que el primer general envía al mensajero, no tiene manera de saber si el mensajero atravesó el valle. Además, el general receptor no puede estar seguro de que el mensajero que llega a su campamento es el mensajero oficial. Recuerde que atravesar el valle significa captura potencial y manipulación traidora.

A primera vista, uno podría concluir que la solución es enviar múltiples mensajeros, ya que es poco probable que todos los mensajeros sean capturados, y por lo tanto algunos mensajes legítimos lo harán. Sin embargo, uno se da cuenta rápidamente de que independientemente de cuántos mensajeros se envíen, todavía no hay seguridad de que el mensajero que llega lleve el mensaje correcto. De nuevo, puede pensar que, en la medida en que la mayoría de los mensajes recibidos diga "ataquemos a las nueve en punto", se podría llegar a un consenso. Sin embargo, ninguno de los generales puede estar seguro de que su mensaje se transmitió o que la mayoría de los mensajeros que llegan no son traidores.

Por supuesto, cada general podría enviar una confirmación de que el mensaje fue recibido. Desafortunadamente, puedes ver cómo surge el mismo enigma. Ninguno de los generales puede estar seguro de que la confirmación es válida, incluso si permitimos una cantidad infinita de mensajes. Si cualquiera de los generales duda debido a la incertidumbre, entonces el ataque fallará. Este ha sido el problema al que se han enfrentado los informáticos desde 1975; los autores de la conjetura original concluyeron que el problema de los dos generales era imposible de resolver. El campo de la ciencia de la computación aceptó esta conclusión como un hecho, hasta que Satoshi Nakamoto lo criticó.

Cuando Leslie Lamport, Robert Shostak y Marshall Pease propusieron el problema de los generales bizantinos (BGP) fue una extensión del problema de los dos generales. Al agregar más generales, el problema se vuelve aún más complejo. La computación en red, y más específicamente

Internet, se convirtió en un laboratorio del mundo real donde el BGP planteaba un problema del mundo real. Internet es una red insegura de computadoras; es el valle a través del cual todos los mensajes deben ser enviados. Cuando Alice envía un correo electrónico a Bob, debe pasar por un valle traicionero y no hay garantía de que el mensaje recibido sea el que se envió. La solución simple para proteger un correo electrónico era encriptar el mensaje, pero eso aún no ofrecía la seguridad necesaria para transferir algo de valor. Es demasiado fácil para un mal actor enviar un mensaje falso que está encriptado; El hecho de que el mensaje esté envuelto en Kevlar no significa que su contenido sea genuino.

Si Alice y Bob solo se ocupan de programar una reunión a la que probablemente ninguno de los dos quiere asistir, salvaguardar la transmisión válida es menos importante. Si la hora de una reunión programada fue manipulada durante la transmisión, haciendo que Bob tarde, entonces Alice simplemente podría llamar a Bob y decirle que se apresure a la sala de conferencias. Sin embargo, ¿qué pasa si ese correo electrónico contiene propiedad intelectual patentada? ¿Confía en enviarlo en un correo electrónico? ¿O qué pasa si el mensaje enviado contiene todas las transacciones completadas con tarjeta de crédito en un minorista importante como Target? Como hemos visto, en el mundo real, el BGP puede tener efectos devastadores cuando algo de valor se transfiere a través de una red insegura.

4.2- ¿Cómo resuelve Bitcoin el BGP?

Una solución al BGP requería varias partes móviles trabajando en concierto. La solución requería un método para proteger el contenido del mensaje, una forma de reducir el número de mensajes enviados, una forma de detectar un mensaje falso y alguna forma de pagar por ello. Bitcoin resuelve el BGP encriptando el mensaje, imponiendo un costo para decodificar el mensaje, proporcionando una forma de verificar que el mensaje fue decodificado legítimamente, y proporcionando un incentivo a los generales honestos.

Cuando se genera un mensaje, el código de Bitcoin usa criptografía para transformar un mensaje de cualquier tamaño en 64 bits, esto se conoce como el algoritmo SHA-256 para Secure Hash Algorithm. Usando este algoritmo, un mensaje que tiene dos párrafos se reducirá a 64 caracteres alfanuméricos aleatorios; un mensaje de dos oraciones también se transformará en una cadena de letras y números de 64 bits. Una vez que el mensaje se transforma, se vuelve irreconocible y solo se puede decodificar resolviendo una ecuación matemática compleja.

La ecuación real que necesita ser resuelta es menos relevante que lo difícil que es resolver el problema. El esfuerzo realizado para resolver el problema es una prueba de que trabajó en la solución. La ecuación debe ser lo suficientemente dura para que las mentes o máquinas más rápidas y nítidas tomen el mismo tiempo para dar una respuesta. Se requiere una cantidad de tiempo estandarizada para garantizar que la dificultad del problema no sea demasiado difícil o demasiado fácil. Un problema excesivamente difícil paralizará la red ya que las computadoras tardan mucho tiempo en resolverlo, mientras que un problema fácil corre el riesgo de la seguridad de la red.

El código de Bitcoin especifica que la ecuación debe tomar 10 minutos para resolver la computadora más rápida, y cada dos semanas ajusta la dificultad para que el tiempo promedio para resolver sea de 10 minutos. La potencia de cálculo y la energía necesaria para resolver el problema de matemáticas sirve como un costo para enviar un mensaje falso. Usando el protocolo de Bitcoin, si un general traicionero quería enviar un mensaje falso, tendría que pagar por una computadora rápida y la electricidad requerida para operarla. Si un general quería transmitir un mensaje falso sin hacer el trabajo para resolver la ecuación, los otros generales simplemente

podrían ver cuánto poder de computación gastó el general traicionero. Si se usaba poca o ninguna potencia de cálculo, los generales podían asumir inmediatamente que el mensaje era falso.

Para que los generales verifiquen que un mensaje fue decodificado legítimamente, cada general debe demostrar que le tomó 10 minutos resolver el problema. Los generales lo hacen al observar la cantidad total de poder de cómputo en la red. Si la red total tarda 10 minutos en resolver el problema matemático, los generales pueden suponer que los mensajes que se están transmitiendo se han descodificado legítimamente.

Además, Bitcoin requiere que seis generales confirmen que recibieron el mismo mensaje. Al requerir confirmación y prueba de que se trabajó para resolver la ecuación, todos los generales pueden estar seguros de que la transmisión del mensaje es válida.

Finalmente, el protocolo Bitcoin proporciona un incentivo a los generales honestos por ser los primeros en decodificar el mensaje legítimamente. El primer general que resuelve el problema y transmite el mensaje válido a la red recibe una compensación en forma de moneda. A medida que crezca el valor de la moneda, también crecerá el incentivo para ser un general honesto. De esta manera, Bitcoin proporciona un mecanismo de autorrefuerzo para recompensar la honestidad.

La moneda de esta solución se llama bitcoin (minúscula b) y representa una pieza conocida de información legítima. Se sabe que esta información es verdadera porque el protocolo de Bitcoin rastrea su origen para verificar su legitimidad. Cada pieza de información (bitcoins) en la red se registra desde su inicio. No es demasiado diferente a tener a los paparazzi grabando cada movimiento de la vida de una celebridad comenzando con su nacimiento. Estas "imágenes" se almacenan en un libro mayor para que todos las vean, pero el protocolo de Bitcoin asegura que cambiar las imágenes sería estadísticamente imposible y prohibitivamente costoso.

Bitcoin usa la ciencia de la criptología y un esquema de prueba de trabajo para resolver el BGP. Los generales bizantinos no pueden confiar en que el mensaje que escucharon fue el mensaje legítimo; en términos simples, el mensaje podría ser "ataque" o "retroceso". El protocolo de Bitcoin envuelve el mensaje en una ecuación matemática increíblemente difícil y la solución al problema es el mensaje válido de "ataque" o "retroceso". Una capa adicional de seguridad se logra mediante la ecuación criptográfica en sí misma. Si bien la solución se puede descubrir, no se puede modificar por ingeniería inversa. Un traidor o un pirata informático no puede comenzar con "ataque" y descubrir la ecuación matemática envuelta alrededor del mensaje. El mensaje transformado sin descifrar es un misterio hasta que se resuelva el hash criptográfico.

Para resolver el BGP, Bitcoin envía el mensaje a todos los generales al mismo tiempo. Cuando todos los generales reciben el mensaje, comienzan a trabajar para resolver el problema matemático. El primero en resolver el problema transmite la respuesta a los otros generales. Una vez que los otros generales resuelven el problema, pueden verificar que recibieron la misma solución al compararla con la respuesta de cada otro general. El poder computacional utilizado para resolver el problema es una prueba de que los generales efectivamente hicieron el trabajo para resolver el problema, también conocido como prueba de trabajo.

Los generales traicioneros pueden transmitir un mensaje falso, pero cuando los otros generales resuelven el problema, no obtendrán la misma respuesta que el traidor transmitió. Cuando el 51 por ciento de los generales verifica la misma respuesta, el mensaje se considera verdadero. Es similar a cómo se presentan los avances científicos a la comunidad para ser verificados. Por ejemplo, si un experimento en un laboratorio produce un método para la fusión en frío, se invita a otros científicos a replicar el experimento. Si la mayoría de los científicos pueden reproducir los resultados del experimento original, entonces se declara un nuevo avance.

Cada vez que el experimento se replica con éxito, se vuelve más difícil para un pirata informático o un científico desleal regresar y cambiar los resultados de cada experimento. Así es como Bitcoin se vuelve más fuerte y más seguro a medida que crece. Además, los generales leales son recompensados con dinero para transmitir legítimamente el mensaje correcto; esto alinea los incentivos del individuo con los incentivos del grupo.

4.3- 51 por ciento de ataque

Ahora bien, esta elegante solución tiene un defecto importante: el protocolo de Bitcoin supone que los nefastos generales nunca podrían obtener más del 51 por ciento de la potencia de cómputo en la red. Bitcoin impone un costo al envío de mensajes falsos, pero también proporciona un incentivo para resolver la ecuación matemática. Dado que Bitcoin depende del consenso de la mayoría del poder de cómputo, es vulnerable a que el 51 por ciento de la red caiga bajo el control de una parte nefasta.

Para comprender el ataque del 51 por ciento, supongamos que tenemos un grupo de 10 generales que usan el protocolo Bitcoin para descifrar un mensaje de "ataque" o "retroceso". En este caso, 6 de los 10 generales necesitarían confirmar que el mensaje fue legítimo al comparar el mensaje que recibieron con otros 5 mensajes. Mientras que un total de 6 mensajes coincidan, entonces todo el grupo de generales acepta seguir ese mensaje. El error es que asume que todos los generales están trabajando independientemente.

Si el grupo de 10 incluye 6 generales traidores, entonces es concebible que 6 mensajes traidores puedan ser enviados y acordados.

Sin embargo, la probabilidad de que esto ocurra aleatoriamente es bastante pequeña, pero no despreciable, especialmente cuando se trata de la transferencia de algo valioso.

Supongamos que 6 de los generales decidieron por adelantado enviar un mensaje falso: si esto ocurriera, el sistema fallaría. Pero, ¿por qué querrían hacer esto? Usando el BGP, volveremos a la razón original para atacar a la ciudad: si los generales tienen éxito, recibirán una compensación monetaria. Se supone que la ciudad atacada está llena de riquezas incalculables que se dividirán entre los conquistadores. Bitcoin asegura que el mensaje correcto se envía y recibe proporcionando bitcoins al primer general honesto para resolver la ecuación matemática.

Sin embargo, este sistema se rompe si el incentivo para resolver la ecuación se vuelve más valioso que la riqueza que un general recibiría después de un ataque exitoso. Además, si el incentivo (bitcoins) es significativamente más valioso que la potencia de la computadora necesaria para resolver el problema, entonces la estructura cambia.

Por ejemplo, establezcamos las condiciones iniciales de modo que cueste a cada uno de los generales $ 1,000 comprar una computadora para resolver la ecuación. Además, supongamos que el costo eléctrico para ejecutar la computadora es de $ 100, para una inversión total de $ 1,100. Si el general recibe $ 500 por resolver el problema y $ 700 por atacar la ciudad, entonces obtiene una ganancia de $ 100 y tiene un incentivo monetario para seguir siendo honesto. Sin embargo, si el dinero recibido al resolver el problema y atacar la ciudad cae por debajo de los $ 1.100, es poco probable que el general participe. Recuerde que todos los generales deben participar para que el ataque tenga éxito.

Pero, ¿qué pasaría si el valor del incentivo para resolver la ecuación aumentara significativamente, por ejemplo, a $ 20,000? En este caso, el general recibiría más para resolver la ecuación que para atacar. Esta es la razón por la cual el algoritmo de Bitcoin requiere acción al resolver el problema. Los dos actos no pueden separarse. Pero hay otro problema: el incentivo es lo suficientemente alto como para fomentar un comportamiento nefasto.

Cualquier general podría comprar seis computadoras y ejecutarlas por un costo total de $ 6,600. Como este general sería el único capaz de confirmar 6 mensajes, podría controlar la red. Además, también controlaría la mayor potencia informática de la red y estaría en posición de ser continuamente el primer general en resolver el problema. En este caso, el general recibiría $ 20,000 para resolver el problema, mientras que gastaría solo $ 6,600 para el poder computacional. La ganancia de $ 13,400 sería un poderoso incentivo para ser deshonesto. En el lenguaje Bitcoin, esto se llama un ataque del 51 por ciento.

Es posible que un individuo o grupo deshonesto compre suficiente potencia informática para controlar toda la red. La solución de Bitcoin al BGP se rompe si el incentivo recibido excede el costo de la potencia de cálculo. Esto no es solo un problema teórico; está ocurriendo mientras estas palabras están siendo escritas. El poder de las computadoras utilizadas para resolver la ecuación matemática ha ido aumentando a un ritmo exponencial. Esto ha resultado en que algunos grupos, conocidos como grupos de minería, tengan suficiente poder de cómputo para controlar toda la red de Bitcoin.

4.4- Una solución elegante

En términos simples, la solución de Bitcoin al BGP es reemplazar la comunicación con el cálculo. Dado que el envío de mensajes es prácticamente gratuito, Bitcoin impone un costo para enviar esos mensajes. Este costo reduce la cantidad de mensajes enviados y, combinado con el incentivo para resolver la ecuación, garantiza que los generales honestos envíen y reciban el mensaje válido. Es una solución elegante, pero, como hemos visto, no sin defectos.

El BGP en su forma más pura aún permanece sin resolver. Satoshi Nakamoto impuso restricciones brillantes al problema y desarrolló una solución que funcionaba dentro de estas limitaciones. El hecho de que el BGP puro permanezca sin resolver no disminuye la aplicación en el mundo real de esta solución. Siempre que las restricciones estén presentes, la solución funciona. En el mundo real, podemos aplicar esta solución a un número ilimitado de situaciones. La solución de Bitcoin se puede aplicar en cualquier lugar donde se necesite enviar información segura a través de una línea de comunicación no segura. Este logro no puede ser subestimado; es simplemente revolucionario.

Si bien las aplicaciones potenciales son ilimitadas, la industria más obvia para que Bitcoin interrumpa es los servicios financieros. Debido a que Bitcoin proporciona una forma segura de transferir valor, tiene la capacidad de eliminar una amplia franja de intermediarios de servicios financieros. El sistema financiero actual se basa en instituciones centralizadas que actúan como agentes de tráfico y cobran una tarifa por este servicio. La solución de Bitcoin para BGP tiene el potencial de revolucionar la industria de servicios financieros. Tiene el potencial de descentralizar el sistema.

Un sistema financiero descentralizado es algo que no ha estado presente en la historia moderna. Las semillas de un sistema descentralizado son el crowdsourcing y las redes de microcrédito peer-to-peer, pero sin seguridad ha sido imposible ampliar estas redes. Las personas pueden estar dispuestas a prestar una pequeña cantidad de dinero para poner en marcha un proyecto creativo,

pero el crowdsourcing para construir una nueva fábrica hasta ahora ha sido inimaginable. La solución de Bitcoin al BGP hace posible la financiación a gran escala de fuentes múltiples.

Antes de Bitcoin, el financiamiento masivo a gran escala era el territorio del sistema bancario. En esencia, un banco es simplemente un intermediario que reúne fondos de un gran grupo de personas y transfiere de forma segura esos fondos a quienes los necesitan. La tarifa que se cobra por este servicio se justifica por la función de terceros de confianza que desempeña el banco. Cualquiera puede solicitar fondos, pero solo aquellos que el banco considere confiables reciben fondos. Resolver el BGP significa que la decisión sobre la asignación de fondos se elimina del banco y se vuelve a poner en manos de los titulares de los fondos.

Un sistema financiero descentralizado es una desviación radical de nuestra estructura actual, pero no es necesario temer el cambio. Un sistema financiero descentralizado es más democrático y tiene el potencial de financiar proyectos que de otro modo podrían haberse pasado por alto. La desintermediación a menudo libera una industria y le permite florecer.

Capítulo 5

> El cambio es la ley de la vida. Y aquellos que solo miran al pasado o al presente seguramente perderán el futuro.
>
> -John F. Kennedy

5.1- Un sistema financiero descentralizado

La pregunta que hace la mayoría de la gente es por qué Bitcoin se ha vuelto tan popular. Surgió de las cenizas de la crisis financiera de 2008 para convertirse en un jugador legítimo en el sistema financiero global. Pero, ¿de qué se trata toda la emoción y por qué la gente abrazó las monedas digitales en general? La euforia se deriva de la constatación de que Bitcoin podría ser el vehículo que transforma el sistema financiero de centralizado a descentralizado. Nuestro moderno sistema de transferencia de dinero puede basarse ostensiblemente en bits y bytes, pero en su núcleo se encuentra una red centralizada de intermediarios anticuada.

La banca, tal como la conocemos, tiene sus raíces en los préstamos agrícolas entre comerciantes de granos y comerciantes que transportaban bienes a través de Asiria y Babilonia alrededor del año 2000 a. Los registros de transacciones y préstamos se hicieron en templos y palacios. De hecho, uno de los primeros escritos conocidos, El Código de Hammurabi, se refiere a las leyes que rigen una forma de banca. El legado de este sistema financiero puede ser difícil de descifrar en el mundo financiero moderno de hoy en día, pero sigue habiendo un elemento clave. Entonces y ahora, el sistema financiero gira en torno a un punto central. En Babilonia fueron los templos, mientras que hoy son los bancos centrales globales.

Los bancos que se asemejan a nuestro sistema financiero moderno se desarrollaron durante el período del Renacimiento en Italia. En 1397, Giovanni Medici estableció Medici Bank para servir a los ricos mercaderes y comerciantes de Europa. La familia Medici creció su imperio y se convirtió en una de las familias más ricas de Europa mejorando el sistema de contabilidad general. A los Médicis se les acredita el desarrollo del sistema de contabilidad de doble entrada que cualquiera que haya tomado una clase en contabilidad reconocería y, si usted es como yo, detestaría.

El sistema de teneduría de libros de doble entrada puede haber parecido un salto cuántico, pero una vez más estas instituciones financieras se basaron en un punto central de control. Los comerciantes, los comerciantes y los consumidores estaban sujetos a las reglas, regulaciones y, en ocasiones, a los caprichos de quienes manejan los bolsillos. A medida que las familias bancarias se enriquecieron, se hizo aún más difícil para el hombre de la calle abrir y operar un banco. Las economías de escala y el poder político sirvieron como barreras efectivas para la entrada. Los bancos comerciales modernos deben su posición en el centro del sistema financiero al legado establecido por los Médicis y otros.

Durante la dinastía Qing (1644-1911), China utilizó un sistema monetario bimetálico de monedas de cobre y lingotes de plata. Las monedas de cobre cuadradas tenían un agujero en el medio para que pudieran medirse en cuerdas. Si una persona con 100 monedas sueltas deseaba transferirlas a otro, necesitaban estar en una cuerda. Esta persona podría ir a un cambiador de dinero e intercambiar las monedas por una cadena de 100; sin embargo, para sus problemas, el cambiador de dinero mantendría una moneda, devolviendo una cadena de 99. Este sistema de tasas se asemeja a los cargos bancarios que experimentamos cuando conectamos dinero entre dos partes.

En el otro lado del mundo, el Banco de Inglaterra fue creado en 1694. El Banco de Inglaterra era una solución a un problema financiero al que se enfrentaba el Rey de Inglaterra. Después de ser derrotado en la guerra por Francia, el rey Guillermo III quería construir una armada fuerte, pero sus finanzas estaban en una condición tan grave que no pudo obtener un préstamo. La solución fue el Banco de Inglaterra, un intermediario recién creado.

El Banco de Inglaterra suscribió un préstamo a King William, y los suscriptores del préstamo recibieron acciones en el Banco de Inglaterra. De esta forma, los acreedores tenían capital en el Banco de Inglaterra si el rey incumplía sus pagos. Para que el capital del Banco de Inglaterra tenga valor, se le otorgó el poder exclusivo de emitir billetes. Hoy, el Banco de Inglaterra sirve como modelo para prácticamente todos los bancos centrales modernos.

Salta 200 años antes de 1871, cuando Western Union completó la primera transferencia de dinero por cable. Estos "giros postales" fueron la primera red peer-peer (P2P). Por primera vez, una persona en Nueva York podría transferir dinero instantáneamente a alguien en San Francisco. En ese momento, esto fue revolucionario. Wells Fargo había construido un verdadero imperio a partir de la transferencia física de la riqueza a través de sus diligencias, pero ahora con el toque de un telégrafo, las diligencias se convirtieron en pintorescas reliquias. Sin embargo, las transferencias fueron posibles solo a causa de una red centralizada de bancos y líneas de telégrafos. Estos representaban fricción, costo y un único punto de falla.

Western Union no podría haber existido si las líneas telegráficas no se extendieran a través de los Estados Unidos. Además, una vez que el giro postal llegó a su destino, la oficina de Western Union tendría que retirar efectivo de su banco, sin la sucursal bancaria local de Wells Fargo, esto no se pudo lograr. Del mismo modo, Bitcoin no podría existir sin Internet o la evolución de la informática P2P. Al igual que el giro bancario de Western Union, Bitcoin utiliza la tecnología existente de una forma nueva y novedosa para proporcionar un servicio que hace que la transferencia de valor sea más fácil y económica.

Nuestro sistema financiero moderno puede parecer avanzado, pero en esencia es una estructura centralizada ineficiente. Cualquiera que desee transferir dinero o riqueza a otra persona debe pasar por una serie de intermediarios, todos más que dispuestos a cobrar una tarifa. Los bancos le cobran por mantener su dinero, mientras que las compañías de tarjetas de crédito le cobran por gastar su dinero. Enviar un cable a nivel nacional no solo tiene un costo monetario, sino también el costo del tiempo perdido. Conducir hasta el banco, completar un formulario de transferencia bancaria y esperar horas para la confirmación son todos costos de envío de dinero.

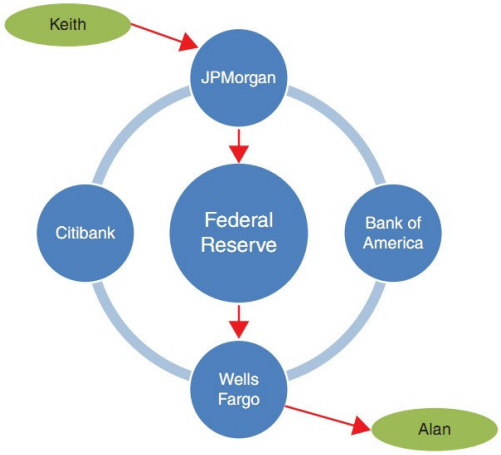

Figura 5.1: Una transacción simple en un sistema financiero centralizado

Una simple transferencia de dinero puede parecerse a esto: supongamos que Alan ha realizado trabajos de jardinería para Keith y ahora solicita un pago. Alan envía una factura a Keith, quien luego debe enviar el pago a través de su cuenta bancaria. En los términos más simples, si Keith quiere transferir dinero a Alan, debe contactar a su intermediario (JPMorgan) para usar el sistema de la Reserva Federal para enviar dinero al intermediario de Alan (Wells Fargo), que lo envía a la cuenta de Alan. En el camino, los bancos crean fricción en forma de tarifas. Ver figura 5.1.

Este sistema no es muy diferente de los antiguos comerciantes de granos que caminaban hasta el templo más cercano para registrar una transferencia de bienes. Aquellos que deseen financiar un negocio durante el Renacimiento probablemente necesiten ponerse en contacto con Medicis, quienes encontrarían un prestamista dispuesto o harían el préstamo ellos mismos. La clave, por supuesto, era el sistema hub-and-spoke que todavía tenemos hoy. Los que están en el medio tienen una ventaja, su posición les da poder. Bitcoin cambia todo esto.

La concentración de poder fue un resultado directo de la incapacidad de resolver el problema de los Generales bizantinos. Si bien este problema fue formalmente nombrado y examinado en 1982, realmente ha existido por milenios. Los banqueros tradicionalmente han desempeñado el papel del tercero de confianza, pasando de actores no relacionados y asegurando que el mensaje transmitido sea legítimo. Antes de Bitcoin, la única manera de confiar en que el mensaje era real era enlistar a un tercero neutral. Cuando el mensaje fue un transporte de valor (también conocido como dinero), los banqueros surgieron como intermediarios.

¿Qué pasa si el poder no se concentra en el medio? ¿Qué pasa si cada jugador en el sistema financiero ya no necesita un tercero de confianza? ¿Cómo se vería este sistema financiero?

5.2- Estación Gran Central

Un sistema financiero desprovisto de intermediarios de confianza sería una desviación radical del sistema que ha estado en marcha la mayor parte de la historia humana. Sin embargo, eso no significa que otros sistemas no hayan existido; simplemente no eran prácticos de implementar. El sistema de trueque era una forma primitiva de comercio que tenía un defecto importante. Los economistas llaman a la falla en el sistema de trueque la coincidencia de los deseos. En un sistema de trueque, si eras agricultor de maíz y querías una vaca, necesitarías encontrar un dueño de una vaca que quisiera maíz. En una comunidad pequeña con economía cerrada, este sistema era suficiente, pero a medida que el comercio florecía y los sistemas económicos se abrían, se necesitaba una nueva forma de intercambiar bienes. El dinero fue creado para resolver el problema de la coincidencia de los deseos.

Con la llegada del dinero, el sistema de trueque desapareció, pero surgió un nuevo problema. ¿Cómo podría un comerciante confiar en que la moneda ofrecida por un comprador desconocido era legítima? Los comerciantes recurrieron a terceros de confianza recién inventados llamados banqueros. Estos banqueros se paran en medio de la transacción y verifican su legitimidad. Los banqueros, como Medicis, desarrollaron un sistema de contabilidad diseñado para evitar el doble gasto y las monedas falsas. El intermediario, o banquero, había sido la única forma de resolver el problema de los generales bizantinos hasta que Satoshi Nakamoto creó Bitcoin.

Bitcoin es lo que se conoce como una red descentralizada distribuida punto a punto. Este tipo de red permite a las personas transferir algo de valor sin el gasto de un intermediario. Antes del telégrafo de Western Union, Pony Express era la única forma de transferir información a través de los Estados Unidos. De manera similar, antes del correo electrónico e Internet, el Servicio Postal de los Estados Unidos tenía un monopolio virtual sobre la transferencia de información. Bitcoin

está por hacer con la industria de servicios financieros lo que el telégrafo le hizo al Pony Express y el correo electrónico al servicio postal de los Estados Unidos.

Antes de sumergirnos en los ganadores y perdedores de esta interrupción, será útil examinar los tres tipos de sistemas que existen. Los informáticos están bien versados en los diferentes tipos de sistemas que existen, pero dado que los servicios financieros han operado de una sola manera, no hubo necesidad de examinar otras formas de realizar transacciones.

Al describir los tipos de sistema, utilizaremos los términos de informática y los relacionaremos con el sistema financiero. Estos sistemas describen cómo funciona un proceso, es decir, un proceso puede tener un solo intermediario, grupos de intermediarios o operar directamente entre pares. Ver figura 5.2.

Los tres tipos más comunes de sistemas son:

1. Centralizado
2. Descentralizado
3. Distribuido

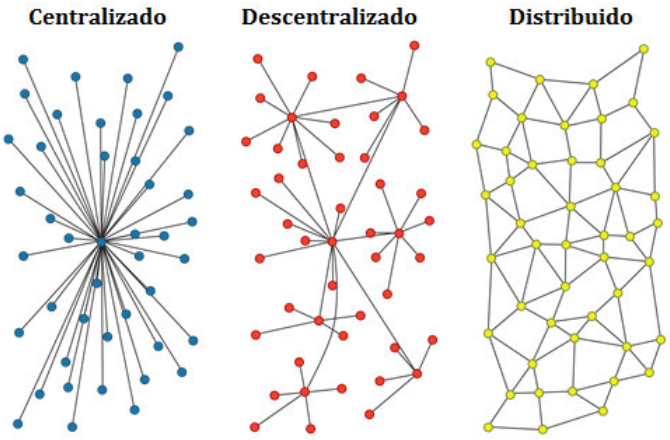

Figura 5.2: Tipos de sistemas

FUENTE: p2pfoundation.net

Un sistema centralizado se puede considerar mejor como una estructura de centro neurálgico, donde el jugador clave se encuentra en el medio y dirige todo el tráfico. Esta no es solo la estructura del sistema financiero moderno; también ha sido utilizado por aerolíneas comerciales y planificadores urbanos. La ciudad de Boston recibe el sobrenombre de "The Hub" porque la ciudad se encuentra en el centro de un sistema de radios que conforma los suburbios. En la hora punta, si ocurre un accidente en el centro de "The Hub", puede afectar a los viajeros en toda el área de Greater Boston. Además, cualquier persona que haya volado a través de Atlanta o Chicago durante el mal tiempo también puede informarle sobre la falla en el sistema centralizado. Una tormenta en Atlanta puede causar retrasos en Los Angeles. En otras palabras, si el concentrador falla, los rayos también fallan.

Si bien un viaje diario complicado o un vuelo retrasado puede ser extremadamente frustrante, generalmente se resuelven con poco efecto sobre la función futura del sistema. Mañana, el tráfico se despejará y el vuelo a Los Ángeles puede llegar temprano utilizando el mismo sistema centralizado. Sin embargo, la crisis financiera de 2008 arrojó una luz dura sobre los límites y los peligros de un único punto de falla en un sistema financiero. Una falla en el centro puede significar que el sistema no funciona mañana. Por su propia admisión, la Junta de Gobernadores de la

Reserva Federal y su presidente, Ben Bernanke, no reconocieron la gravedad de la crisis financiera que se estaba desarrollando. El presidente Bernanke dijo que la crisis subprime estaba contenida y no amenazaría al resto de la economía. Estaba equivocado y el sistema financiero se detuvo. Para su crédito, cuando el presidente Bernanke reconoció su error, actuó con valentía y rapidez para evitar un colapso financiero total.

Si Ben Bernanke, Hank Paulson y Tim Geithner no hubieran podido resucitar el sistema financiero centralizado, es muy posible que la economía mundial se hubiera sumido en una depresión peor que la Gran Depresión de los años treinta. La Gran Depresión es otro ejemplo de los peligros de utilizar un sistema financiero centralizado. La Reserva Federal no solo no reconoció la gravedad de la desaceleración económica; pueden haberlo exacerbado por inacción. Además, las ramas ejecutiva y legislativa del gobierno tampoco lograron evitar que la crisis se extendiera.

En un documento de los años 90, "El patrón oro, la deflación y la crisis financiera en la Gran Depresión: una comparación internacional", Ben Bernanke argumentó que el estándar de oro en el centro del sistema financiero era culpable de crear un malestar económico más profundo. Bernanke identificó tres fallas en el estándar de oro que contribuyeron a que la depresión se convirtiera en Grande:

1. La asimetría entre los países con superávit y déficit en la respuesta monetaria requerida a los flujos de oro.
2. La piramidación de las reservas.
3. Poderes insuficientes de los bancos centrales.

Analizar si Bernanke estaba en lo correcto está más allá del alcance de este libro, pero lo relevante es cómo un sistema centralizado como el estándar de oro puede sufrir fallas en el centro. Cuando Bernanke escribe sobre la "asimetría entre países con superávit y déficit", utiliza el ejemplo de la negativa de Francia a jugar según las "reglas del juego". Para que el sistema estándar internacional funcione correctamente, los países que experimentaron entradas de oro deberían han permitido que sus economías se inflen. Si bien Francia recibió el oro, no permitió que se inflara la oferta monetaria, y Bernanke sugiere que esto llevó a una exacerbación de la desaceleración global. Si pensamos en el patrón oro como un sistema centralizado, podemos ver que la falla en el centro causó la falla de todo el sistema.

La piramidación de las reservas se produjo cuando los bancos centrales abandonarían las monedas extranjeras que estaban siendo activamente devaluadas. Esta reducción en las reservas puede haber llevado a una reducción en la oferta monetaria global. Bernanke también sugiere que los principales bancos europeos no tenían los poderes suficientes para llevar a cabo operaciones monetarias de mercado abierto. Se ha escrito sobre la validez de estos reclamos, pero queda un hecho: la institución del centro no actuó de manera que beneficiara a todo el sistema. Era este defecto el que más probablemente culpara por el prolongado período de depresión económica.

Un sistema descentralizado busca corregir el defecto creando múltiples centros y radios. En un sistema descentralizado, hay muchos nodos (o concentradores), cada uno de los cuales se encarga de garantizar el flujo fluido del tráfico, ya sea que el tráfico sea información, mensajes de texto o transacciones financieras. El Sistema Federal de Reserva Federal de EE. UU. Es un buen ejemplo de un sistema descentralizado. Cada uno de los bancos regionales de la Reserva Federal debe asegurarse de que la plomería financiera en su región funcione. Sin embargo, los bancos regionales de la Reserva Federal deben informar y cumplir con la Reserva Federal en Washington, D.C. Esta estructura crea un único punto de falla, es decir, la Junta de la Reserva Federal. Si la Junta de Gobernadores de la Reserva Federal falla al llevar a cabo la política, entonces todo el sistema falla.

Un sistema descentralizado es superior al sistema centralizado cuando es esencial evitar una falla en el centro. Sigue existiendo el riesgo de que varios centros fallen al mismo tiempo, pero es un paso adelante en la evolución de los sistemas. También es particularmente útil cuando cada centro puede actuar de forma autónoma.

La próxima evolución es un sistema distribuido, donde cada jugador actúa como un centro. Cada individuo, empresa, computadora o gobierno tiene la misma responsabilidad: garantizar el buen funcionamiento del sistema. En un sistema distribuido, si un nodo (o concentrador) falla, los otros nodos simplemente recogen la holgura y se aseguran de que el tráfico fluya sin problemas. Un sistema distribuido funciona mejor cuando el proceso de toma de decisiones puede automatizarse o codificarse en una serie de preguntas de sí / no. Si cada nodo es responsable del mismo resultado, entonces el proceso de toma de decisiones debe ser idéntico. Utilizando el ejemplo de las "reglas del juego" de la mención del estándar de oro internacional de Ben Bernanke, Francia no podría evitar que la oferta de dinero se infle. Francia simplemente actuaría como un nodo en el sistema financiero; si decidía no inflarse, los otros nodos tomarían el control e inflarían el suministro de dinero de Francia. Inmediatamente, uno puede ver por qué este tipo de sistema aún no se ha integrado en las economías soberanas. Renunciar al control de la oferta de dinero equivale a renunciar a la soberanía nacional.

Examinando el sistema monetario de Hong Kong, podemos ver dónde puede surgir un conflicto si un sistema distribuido no está diseñado adecuadamente. Desde 1983, Hong Kong ha vinculado la tasa de cambio del dólar de Hong Kong con el precio del dólar de EE. UU. En la práctica, lo que esto significa es que si el dólar de EE. UU. Se devalúa, entonces el dólar de Hong Kong también disminuirá de valor y viceversa. Esencialmente, Hong Kong ha subcontratado su política monetaria a la Reserva Federal de los Estados Unidos. Esto funcionó bien cuando la Reserva Federal de EE. UU. No buscaba activamente devaluar el dólar.

La economía de Hong Kong ahora está más ligada a la economía china que en 1983. El resultado es que Estados Unidos puede estar devaluando su moneda para estimular la economía interna de Estados Unidos, mientras que la economía de Hong Kong está expuesta a la creciente economía china. . Al externalizar su política monetaria, Hong Kong corre el riesgo de estimular su economía en el momento exacto en que debería tomar medidas para desacelerar el crecimiento. El resultado podría ser una inflación desenfrenada o una ruptura del tipo de cambio del dólar de EE. UU. Para nuestros propósitos, este es un ejemplo de falla en un sistema distribuido; más exactamente, el sistema debe estar diseñado para manejar correctamente estas situaciones.

Dado que la economía de Bitcoin sigue creciendo, y lo está haciendo en un momento de integración económica global masiva, tiene una oportunidad sin precedentes de ser la solución flexible para sincronizar la política monetaria. Si se lo deja solo, la economía de Bitcoin tiene la capacidad de ajustarse rápidamente a los desequilibrios sin depender de una autoridad central para tomar la decisión correcta. Como sistema distribuido, cada nodo de la red Bitcoin se encarga de garantizar que las transacciones financieras sean genuinas. Bitcoin realiza esta tarea con 31,000 líneas de código diseñadas para rastrear cada transacción hasta su origen para confirmar la legitimidad. Debido a que Bitcoin es un sistema financiero, usa criptología para encriptar las transacciones y mantenerlas a salvo de posibles piratas informáticos.

Recordemos la transacción entre Keith y Alan, donde necesitaban usar la torpe red centralizada de intermediarios para transferir el valor. Utilizando la red Bitcoin sin igual ni punto a punto, Keith puede transferir valor de forma instantánea a Alan de forma gratuita. La Figura 5.3 muestra cómo se ve esa red usando Bitcoin.

No permita que la simplicidad del gráfico lo engañe haciéndole creer que la red de Bitcoin no es sofisticada. Bitcoin ha hecho lo que ningún otro programa de computadora ha hecho en la historia de los sistemas financieros: ha automatizado el papel del intermediario. Además, los desarrolladores de Bitcoin lo han regalado de forma gratuita. La familia Medici ganó poder y riqueza haciendo una simple mejora al sistema existente. Imagine si hubieran inventado un nuevo sistema por completo.

El logro revolucionario de Satoshi Nakamoto fue reducir la complicada maraña de intermediarios financieros globales en un elegante paquete de software que se puede descargar en un teléfono inteligente. Esta hazaña no es solo asombrosa, no tiene precedentes.

Figura 5.3: Una transacción usando la red descentralizada de Bitcoin

La historia de los negocios está repleta de ejemplos de industrias que se han transformado más allá del reconocimiento por la desintermediación. ¿Cuándo fue la última vez que entraste en la oficina de un agente de viajes? ¿O le preguntaste a un agente de bienes raíces por un folleto? ¿O miró en la guía telefónica? Debido a la necesidad de confianza y seguridad, hay una industria que ha desaparecido de la lista: servicios financieros. Ahora, el protocolo de Bitcoin puede afectar al tercero de confianza de los servicios financieros, permitiendo que florezcan los préstamos entre pares, la banca y las transacciones.

5.3- ¿Qué cosa está en juego?

La amenaza de Bitcoin es una interrupción completa del status quo. En su forma más pura, ya no se necesitan los bancos centrales ni los bancos comerciales. Además, los proveedores de servicios como Visa, MasterCard y American Express tienen toda su franquicia en juego. Si la Revolución Industrial fue el catalizador de las economías modernas para pasar de una sociedad agraria a una industrial, entonces el Bitcoin es el vehículo que transportará el sistema financiero de centralizado a descentralizado.

Antes de la Revolución Industrial, un tercio de los estadounidenses trabajaba en la agricultura; hoy, ese número se ha reducido a solo 1.1 por ciento. Sin embargo, los avances tecnológicos han permitido que los trabajadores agrícolas sean mucho más productivos y cultiven más alimentos. La industria agrícola es un excelente ejemplo de cómo la tecnología puede cambiar la dinámica dentro de la industria sin reducir la producción. Desafortunadamente, durante la transición, muchos trabajadores son desplazados. A medida que el sistema financiero avanza hacia la descentralización, es probable que las filas de los empleados en esta industria disminuyan. Al mismo tiempo, quienes abrazan la descentralización florecerán.

En 1919, Frank Little y Alva Kinney ensamblaron cuatro molinos de grano para formar una compañía llamada Nebraska Consolidated Mills. Esta empresa adoptó la tecnología de la Revolución Industrial y la utilizó para expandir un negocio de molinería en uno de los procesadores de alimentos más grandes del mundo. En 1971, Nebraska Consolidated Mills cambió su nombre a ConAgra y es el orgulloso propietario de marcas como Reddi-Wip, Slim Jim, Chef Boyardee, PAM y Orville Redenbacher, por nombrar solo algunas. Es lógico pensar que en algún lugar hay otro Frank Little y Alva Kinney acumulando cuatro compañías de servicios financieros y preparándose para construir un gigante descentralizado.

Según el Departamento de Comercio de EE. UU., En 2012, 5,87 millones de personas trabajaban en la industria de servicios financieros, lo que representaba aproximadamente el 6 por ciento de la fuerza de trabajo. Estos 5,87 millones de personas produjeron $ 1,24 billones de servicios o el 7,9 por ciento del producto interno bruto de EE. UU. (Sin incluir los bienes inmuebles). Bitcoin proporciona la herramienta para reducir la cantidad de mano de obra que trabaja en servicios financieros, mientras que al mismo tiempo mantiene o incluso aumenta la producción. Este es un proceso multidecade, por lo que los que están en servicios financieros tienen tiempo para adaptarse, pero no se equivoquen: se avecina un cambio.

Durante siglos, el transporte involucró lo que parecía ser un uso eficiente de caballos y carruajes. Los cocheros usarían un látigo con caña para estimular a los caballos a un ritmo más rápido, y luego llegaron los caballos de acero (ferrocarriles) y el carruaje sin caballos (automóviles). Estas tecnologías disruptivas no solo hicieron el caballo y el carro pintorescos; hizo que el látigo caído fuera obsoleto. Los látigos de hoy en día son tarjetas de crédito.

La razón de ser de las compañías de tarjetas de crédito es / era transferir fácilmente el valor de una parte a otra. Las tarjetas de crédito no solo ofrecen comodidad sino también seguridad. El efectivo es un instrumento al portador que significa que quien lo tiene es dueño de él. Las tarjetas de créditos requieren firmas y segundas formas de identificación; esto se conoce en el mundo de las monedas alternativas como cifrado dual. Para este servicio, MasterCard, Visa y American Express no solo cobran a sus clientes por el privilegio de usar la tarjeta, sino que también le cobran al comerciante del 2 al 3 por ciento por el privilegio de aceptar la tarjeta.

La Figura 5.4 es del informe State of Bitcoin Q1 2014 de CoinDesk. Han identificado las empresas más probables a ser interrumpidas por Bitcoin.

Lo sorprendente de este análisis no es solo el tamaño de la industria a punto de ser interrumpido, sino que este análisis no incluye a los bancos. Recientemente, tuve que transferir dinero a un socio comercial en Europa. El costo para completar esta transacción en Bank of America fue de más de $ 50 y demoraría dos días hábiles, sin incluir mi tiempo para conducir hasta el banco y completar el papeleo. Elegí en su lugar enviar bitcoins: con un clic del mouse, el pago se envió de forma instantánea, sin ningún papeleo y de forma gratuita. La interrupción no es un experimento mental futurista; ya ha comenzado.

Capitalización de Mercado (millones) a 8 Abril 2014

Processors	Market Cap
Visa Inc	$104,744
American Express Co	$94,486
MasterCard Inc	$82,378
Capital One Financial Corp	$43,930
DISCOVER FINANCIAL SERVICES	$27,418
Alliance Data Systems Corp	$13,968
Total System Services Inc	$5,619
Global Payments Inc	$4,904
Euronet Worldwide Inc	$2,100
Heartland Payment Systems Inc	$1,440
Green Dot Corp	$732
Total	**$381,720**

Payment Hardware	Market Cap
NCR Corp	$5,921
MICROS Systems Inc	$3,892
VeriFone Systems Inc	$3,680
INGENICO	$4,807
Diebold Inc	$2,530
Outerwall Inc	$1,822
Wincor Nixdorf AG	$2,300
Agilysys Inc	$284
ON TRACK INNOVATIONS LTD	$74
Total	**$25,310**

Money Transfer/ATM Outsourcing	Market Cap
Western Union Co	$8,826
Euronet Worldwide Inc	$2,100
Cardtronics Inc	$1,670
MoneyGram International Inc	$1,195
Xoom Corp	$685
Total	**$14,476**

Bank Software	Market Cap
Fidelity National Information Services Inc	$15,455
Fiserv Inc	$14,582
Jack Henry & Associates Inc	$4,743
ACI Worldwide Inc	$2,251
Total	**$37,032**

Figura 5.4: Bitcoin pretende interrumpir una industria de $ 459bn +

FUENTE: CoinDesk, Wedbush Securities.

Cuando Western Union suplantó el Pony Express, fue porque proporcionaron un producto superior en la forma de una forma más rápida de transportar información. Del mismo modo, el caballo de acero y el carruaje sin caballos aumentaron la velocidad del transporte humano. La mayor facilidad y velocidad de transferencia de valor usando Bitcoin tiene el potencial de aumentar la velocidad del transporte de valor, también conocido como la economía global.

Cuando el mercado bursátil colapsó en 1929, las noticias se difundieron primero a través del ticker de Western Union, luego del telégrafo y finalmente al día siguiente en el periódico. Todos vimos los horrores del 11 de septiembre en nuestras pantallas de televisión e inmediatamente inundaron las redes de telefonía celular con llamadas. Cuando el Capitán Sullenberger condujo valientemente su avión enfermo al río Hudson, Twitter estaba allí para capturar el milagro.

En la escuela de negocios, lo primero que se enseña a un joven capitalista es que hay tres formas de ganar participación en el mercado: (1) hacer un producto superior, (2) vender un producto existente por más barato, o (3) hacer ambas cosas. El reciente incumplimiento de la red de tarjetas Target destaca por qué una red distribuida como Bitcoin es superior. Todos los datos de crédito que Target recopila se almacenan en una base de datos. Los ladrones solo necesitaban hackear un único punto para acceder a la información, un único punto de falla. La red bitcoin está descentralizada, lo que significa que la información no se almacena en una única base de datos. Cada transacción debe ser verificada por múltiples miembros de la red y su información personal nunca será necesaria. Bitcoin no solo ofrece un producto superior; también es más barato. De hecho, es gratis.

A medida que la velocidad y la facilidad de la transferencia de información aumentaron, también lo hizo el negocio de la tecnología de la información. Los telégrafos llevaban a las radios, que se transformaron en televisores, que se conectaron a Internet y nos dieron compañías como Netflix. Hace una década, pocos podían predecir que la televisión a la vista sería una industria multimillonaria. Del mismo modo, a medida que aumente la facilidad y la velocidad de la transferencia de valor, nacerán nuevas industrias y compañías.

5.4- Bancos Centrales

La transacción de bitcoin que realicé con un socio comercial en Europa es un territorio desconocido para los bancos centrales mundiales. Cuando se mira desde la perspectiva de la oferta de dinero, esta transacción redujo la oferta de dinero en los Estados Unidos y aumentó la oferta de dinero en Europa. Esto ocurrió sin el uso de la Reserva Federal, el Banco Central Europeo o bancos comerciales intermediarios. El único registro de esta transacción está en el blockchain, pero el blockchain no identifica si la transacción cruzó las fronteras nacionales. Por lo tanto, el único registro de que el dinero fluyó fuera de los Estados Unidos y hacia Europa son las palabras que he escrito.

Si bien es poco probable que mi única transacción tenga un impacto perjudicial en la política monetaria mundial, a medida que se realizan más transacciones con bitcoins, las estadísticas de suministro monetario pueden volverse inexactas. Los banqueros centrales que desarrollan modelos econométricos elaborados para orientar la política podrían estar perdiendo una parte importante de las transacciones internacionales. La implicación de los datos faltantes es que la política monetaria podría basarse en datos incorrectos y podría dar lugar a una mala política. Este

escenario puede asustar a algunos y deleitar a otros. Los puristas de la escuela austríaca pueden regocijarse en la libre circulación del capital, mientras que otros pueden clamar por la rendición de cuentas.

Este cambio no debe ser atemorizante, pero sí debe ser reconocido por los banqueros centrales. La economía y el ecosistema de Bitcoin es lo suficientemente pequeño como para no tener un impacto importante en el suministro de dinero. Los banqueros centrales tienen tiempo para incorporar transacciones de divisas alternativas en decisiones de política y modelos econométricos. Los primeros intentos pueden simplemente ser conjeturas, pero eso no debería impedir la inclusión futura. A medida que el sistema financiero avanza hacia la descentralización, el papel de los banqueros centrales puede cambiar drásticamente. Ya sabemos que las transacciones están cambiando los flujos de dinero globales. Los banqueros centrales deben comenzar a abrazar y comprender estos flujos.

5.5- Bitcoin es el catalizador

Nunca sabremos si Satoshi Nakamoto pensó en las implicaciones de su invención. Después de todo, los primeros informáticos que usaron líneas telefónicas para enviar archivos de datos simplemente intentaban hacerles la vida más fácil; no se dieron cuenta de que estaban inventando Internet. Si bien Internet tardó en desarrollarse en su forma actual, la revolución fue que la información descentralizada de Internet. La información descentralizada fue la chispa que encendió el horno para organizaciones como Google y Wikipedia. Estas organizaciones interrumpieron los medios, publicaciones, publicidad e incluso su biblioteca local. Sin embargo, la información descentralizada también tenía un problema; es decir, cualquiera podría publicar información inválida. Este problema significaba que un tipo de información (transacciones financieras) no se podía descentralizar, hasta Bitcoin.

Bitcoin resolvió el problema de enviar información financiera a través de Internet sin un intermediario, y podría servir como el catalizador que descentraliza los servicios financieros. Dentro de una década, la industria de servicios financieros puede emplear una fracción de su fuerza laboral actual, pero también será mucho más eficiente. Este es un cambio que es paralelo al paso de una economía agraria a una industrial. El catalizador para este cambio es Bitcoin y la solución que proporciona. A través de la automatización, la economía global prosperó durante la Revolución Industrial. De manera similar, Bitcoin, la tecnología blockchain y los mineros automatizan muchas de las funciones de nuestros intermediarios financieros actuales. Además, la automatización se distribuye a cualquier persona que tenga una conexión a Internet. Transferir el rol del tercero de confianza de los intermediarios financieros a individuos no ocurrirá sin tremendas angustias y reticencias.

Aquellos que abrazan el cambio pueden ser recompensados como los primeros industriales. Henry Ford y Andrew Carnegie reconocieron un cambio y se hicieron con un lugar en el salón de la fama de los negocios. Quizás se abra un lugar en el salón de la fama para aquellos que aprovechan el Bitcoin Big Bang, o quizás los intermediarios financieros se adaptarán. Lo que está claro es que en la próxima década, la destrucción creativa será el mantra dentro de los servicios financieros, y todo se deberá a un genio anónimo que regaló su invención de forma gratuita.

Capítulo 6

> [Monedas virtuales] pueden ser prometedoras a largo plazo, especialmente si las innovaciones promueven un sistema de pago más rápido, más seguro y eficiente.
>
> -Ben Bernanke

6.1- ¿Qué es un Minero Bitcoin? Un banquero

El sol asoma sobre el horizonte y la niebla se está despegando de la bahía. Su taza de café caliente sube por el parabrisas mientras su automóvil lucha por comenzar. Hace frío, está oscuro y son las 11 a.m. Bienvenido a las minas bitcoin de Reykjanesbaer, Islandia. Después de registrarse con un guardia protegido por un cristal a prueba de balas, ingresa a la trampa del hombre, una cámara que normalmente se encuentra en una penitenciaría. La puerta se cierra de golpe y piensas: "Ya no estamos en Kansas" ... o tal vez lo estés. Emmanuel Abiodun tiene una configuración similar en Kansas City. El Sr. Abiodun es el CEO de treinta y tantos años y fundador de CloudHashing, una compañía global de minería de bitcoin.

Emmanuel Abiodun estaba trabajando en HSBC en Londres cuando se enteró de una "estafa" que se llamaba minería bitcoin. Así es, el fundador de una de las mayores operaciones mineras de bitcoin en el mundo pensó que era una estafa cuando escuchó por primera vez sobre Bitcoin. ¿Quién podría culparlo? Un programador anónimo de computadoras escribió 31,000 líneas de código para que cada 10 minutos cualquier computadora conectada a la red pudiera aventurar una ecuación matemática compleja. Si la computadora adivinó correctamente, se enviaron 50 bitcoins a la billetera que reside en el disco duro. Si tomó más de 10 minutos adivinar la respuesta, el código del software ajustó la ecuación para que fuera más fácil de resolver.

Entre enero y marzo de 2013, el precio de un solo bitcoin comenzó a subir de $ 15 a $ 45, y esto llamó la atención del Sr. Abiodun, ya que tenía el mío. Instaló una computadora en la habitación de invitados de su casa suburbana de Londres, descargó el Bitcoin-QT y se convirtió en un minero de bitcoin. A medida que el precio ascendió a $ 100 en su camino a $ 260 en abril de 2013, el entusiasmo de Emmanuel Abiodun por el proyecto se disparó. Desafortunadamente, también lo hizo su factura de electricidad.

Cuanto más avanzaba en la minería bitcoin, más se daba cuenta de que para ganar dinero real se necesitaría una computadora más rápida que ejecutara constantemente el software de minería. El Sr. Abiodun continuó trabajando en su trabajo diario, mientras pasaba las noches agregando tarjetas gráficas a su "plataforma" minera y reparando el ventilador sobrecalentado. La operación se volvió tan compleja y generó tanto calor que sus suegros ya no visitarían. No poder visitar a sus padres fue la gota que colmó el vaso para la Sra. Abiodun. Dio un ultimátum: o las computadoras se fueron o ella lo hizo.

Emmanuel Abiodun no es el único minero bitcoin que tiene un problema con el calor y una factura alta de electricidad. Un profesor de química en Minnesota ha instalado su plataforma minera en el sótano junto a la chimenea para ayudar a ventilar algo del calor. Un joven en Las Vegas tuvo que comprar un segundo acondicionador de aire solo para mantener su departamento habitable. Cuando su factura mensual de electricidad pasó de $ 250 a $ 700, su esposa expresó su escepticismo.

Pero, ¿por qué estos mineros existen? Seguramente deben tener alguna función para ser tan generosamente recompensados por molestar a sus esposas. Para explicar la función de los mineros, es mejor analizar las agallas de una transacción de Bitcoin. Advertencia justa para el lector: Vamos a usar términos como nonces, hashes criptográficos y bloques. No se preocupe, lo haremos lo menos doloroso posible, pero es un mal necesario para continuar nuestro viaje.

6.2- ¿Cómo funciona una transacción de Bitcoin?

Comenzaremos con la simple transacción entre Keith y Alan. A estos dos jóvenes les gustaría realizar una transacción de Bitcoin; de hecho, Keith desea enviar a Alan un bitcoin como pago por el paisajismo completado por Alan. Tanto Keith como Alan tienen carteras de Bitcoin en sus computadoras, y es en estas carteras donde se almacenan sus direcciones. Su billetera es similar a su cuenta bancaria. Tiene tanto su saldo de bitcoin como sus direcciones. Una dirección de Bitcoin no es diferente a un cheque; contiene su número de ruta, número de cuenta y un número de cheque. Sin embargo, los usuarios de Bitcoin pueden crear tantas direcciones como quieran y pueden asignar cualquier cantidad de bitcoins a cada dirección. Ver la Tabla 6.1.

Una dirección de Bitcoin es una cadena alfanumérica de 27 a 34 caracteres que comienza con un 1 o un 3 y representa un destino en la red de Bitcoin. Una dirección típica de Bitcoin se ve así: 13uRbMgunUpShBVTewXjtQTBv5MndwfXhb.
Cuando Keith se sienta en su computadora, usa la billetera Bitcoin para crear una nueva dirección que contiene un bitcoin. Al mismo tiempo, Alan crea una dirección que le permite recibir el pago y envía esta cadena de números a Keith. En términos sencillos, la dirección de Alan dice: "Yo, envía mi bitcoin aquí". Keith golpea enviar, que ordena al software Bitcoin que envíe un bitcoin desde su dirección a la dirección de Alan.

Dentro de la billetera de Keith, el software está creando tanto una clave privada como una pública: esto se conoce como un par de claves criptográficas. La clave privada es como la llave de tu auto. Si está vendiendo su automóvil, debe transferirlo al comprador. En el mundo de Bitcoin, la clave privada muestra la propiedad del bitcoin. El software firma la transacción con la clave privada de Keith (conocida solo por la computadora de Keith) y luego transmite la clave pública a la red de Bitcoin. La clave pública permite que cualquier persona que escuche la red de Bitcoin verifique que la transacción proviene de la billetera de Keith. Cuando la clave pública y las claves privadas coinciden, voila -transacción verificado.

Cuadro 6.1: Componentes de Bitcoin y su Funcion

Componentes de Bitcoin	Funcion
- Billetera	Este es tu cuenta bancaria
- Direccion	Estos son tus cheques

¿Quiénes son estas personas que escuchan la red? Sí, lo adivinaste, mineros. Sin los mineros, nada se verifica. Las computadoras que Emmanuel Abiodun ejecuta en Islandia agrupan todas las transacciones de los últimos 10 minutos en un archivo llamado bloque. El trabajo de los mineros es similar al de un banquero. Transfieren la propiedad de un cliente a otro y verifican que ambos clientes tengan derecho a realizar transacciones.

Continuando con la transacción Keith y Alan, si este pago se realizó con un banco tradicional, el banquero verificará que Keith tenga suficientes fondos para ser transferidos y luego facilitará la transferencia. Utilizando el Sistema de Reserva Federal centralizado, el banquero debitaría una cuenta y acreditaría a la otra, por supuesto cobrando una tarifa por sus problemas. Con Bitcoin, la transacción es gratuita o casi gratuita. A los mineros se les paga con nuevas monedas acuñadas

por el software Bitcoin. Funcionalmente, no hay diferencia entre una transacción de bitcoin y un pago realizado con un cheque. En ambos casos, el dinero se transfiere de una parte a la otra. La diferencia revolucionaria es que Bitcoin permite la misma función sin el costo de un intermediario.

Pero espera, ¿no son los mineros los intermediarios?

Esto es de hecho cierto; el protocolo de Bitcoin reemplaza al banquero con el minero y, al hacerlo, elimina el costo de un intermediario. El papel tradicional del banquero era ser un tercero de confianza, ver cada transacción y verificar la validez. Satoshi Nakamoto diseñó una forma para que una computadora reemplace a un banquero. Bitcoin puede realizar esta tarea de forma segura a través del uso de la criptografía.

6.3- ¿Qué es criptografía?

La criptografía es una técnica utilizada para permitir la transmisión segura de información. En términos simples, la criptografía convierte la información de un estado legible en una tontería y luego proporciona un medio para descifrar el mensaje. Esta rama de las matemáticas ha existido durante siglos y ha crecido en sofisticación a medida que los científicos informáticos se han involucrado. Los predecesores de los criptólogos modernos fueron los rompedores de códigos empleados por los ejércitos en tiempos de guerra. Bitcoin utiliza la criptografía para codificar una transacción financiera, transmitirla a través de Internet y luego descifrarla cuando llega a la billetera del destinatario. Bitcoin usa una función hash criptográfica para realizar esta tarea.

La complejidad del término función hash criptográfica es el segundo después de la ecuación matemática que describe. Una función hash criptográfica no es más que una ecuación matemática que convierte las palabras en números. Toma cualquier mensaje redactado y lo convierte en una cadena única de números, piense en ello como una picadora de carne para los mensajes. El mensaje (carne) entra, sale la salchicha; pero en este caso, el carnicero puede usar las matemáticas para volver a convertir la salchicha en carne. Lo que es único de una función hash es que el mensaje o entrada puede ser de cualquier longitud, pero la salida es de longitud fija. Esto hace que enviar el mensaje sea seguro y eficiente.

Las funciones hash criptográficas no se inventaron con Bitcoin. Tienen una larga historia de uso en firmas digitales y comercio electrónico. De hecho, el software de Bitcoin es solo una manera muy segura de firmar digitalmente un cheque, y, de hecho, su firma digital es más difícil de falsificar que su firma habitual. Estas firmas digitales son tan únicas que la probabilidad de que alguien tenga la misma firma digital es increíblemente pequeña.

Una firma digital es una forma de firmar electrónicamente un mensaje. Cuando firmas algo con una firma digital, generas una clave de firma que es privada y una clave de verificación que es pública. Usando una función hash, su firma digital y su mensaje se convierten matemáticamente en una secuencia de números, que ahora es su mensaje firmado digitalmente. Para verificar el mensaje, el decodificador necesita el mensaje firmado y la clave de verificación. Ahora el verificador (o minero) trabaja hacia atrás usando la clave de verificación y el mensaje firmado. Utilizando las matemáticas de nuevo, el minero puede determinar si el mensaje firmado se puede hacer combinando su clave privada y firma digital. Dado que la firma es parte del mensaje, cada mensaje es único y este mensaje se transmite a la red de Bitcoin para su verificación.

Luego, los mineros van y revisan el blockchain para rastrear si esta firma digital se ha usado antes y qué mensaje se envió con ella. Si el mensaje es idéntico a un mensaje grabado en la cadena de

bloques, entonces los mineros saben que se ha utilizado antes y es falso. Si los mineros verifican que el mensaje es único y nunca se ha utilizado antes, entonces permiten la transacción.

¿Cómo sabemos que los mineros realmente hicieron su trabajo y no son perezosos? Altas facturas de electricidad. Para resolver el hash criptográfico, las computadoras de minería deben gastar una gran cantidad de potencia computacional, que usa mucha energía. En cada momento en el tiempo, la red Bitcoin está registrando cuánta potencia computacional se está utilizando para resolver el problema; esto se llama cantidad de hash. Cualquiera puede mirar la red y determinar que las computadoras de minería consumen mucha electricidad para resolver el problema: en Bitcoin y en criptografía, esto se llama prueba de trabajo.

La prueba de trabajo muestra que alguien participó en un esfuerzo computacional. Es un acertijo que, una vez resuelto, demuestra que hiciste el trabajo. Otro uso potencial para el concepto de prueba de trabajo es disuadir a SPAM. Si se necesita energía para enviar y decodificar un mensaje, costará dinero enviar SPAM. Puede costar una fracción de un centavo enviar un correo electrónico con prueba de trabajo, pero podría costar una fortuna enviar millones de esta manera.

El mensaje codificado enviado a la red de Bitcoin también se conoce como un desafío. Cuando la computadora de minería que escucha un mensaje escucha un desafío, se le ocurre una respuesta. Esta respuesta es esencialmente una conjetura sobre la respuesta a la ecuación matemática. La respuesta a la ecuación es tan rara que solo tiene una respuesta adecuada. Además, esa respuesta es tan difícil de encontrar que debe tomar la computadora más rápida de 10 minutos para llegar a la conjetura correcta.

El proceso de extracción se puede comparar con lanzar una moneda, excepto que los mineros lanzan una gran cantidad de monedas, alrededor de un billón, para determinar la cadena de respuesta correcta. La cadena correcta es lo que se llama resistencia a colisión, lo que significa que las posibilidades de que dos mensajes sean iguales o "colisionan" son matemáticamente muy bajas. El hash, o ecuación matemática, se aplica tanto al mensaje como a la respuesta. Si la función hash arroja el mismo resultado, entonces los mineros han verificado el mensaje.

El software Bitcoin utiliza una función hash criptográfica para convertir el bloque de transacciones en una cadena alfanumérica de tamaño fijo llamada valor hash. Ahora, lo especial de una función hash criptográfica es que cualquier cambio en la entrada crea un resultado completamente diferente, también llamado resumen. En la Tabla 6.2 usamos la función de cifrado de Bitcoin, conocida como SHA-256 para traducir tres mensajes ligeramente diferentes.

Cuadro 6.2: Función Hash Criptográfico SHA-256

Entrada	Funcion Hash Criptografica	Salida / Valor Hash
Envio $10	SHA-256	46ab27f445d603f5c33f2153f1faabdc9064fc72e503ec4ae9234c96eec651a6
Envio $20	SHA-256	d84d6c04b78f6f3ba2ab62426dc741e57e917c342461a0e54b2c6046f431796a
Envio $300.50	SHA-256	bfa7dfc4590dfd62647fca561103e4fee5631e9d0ff9329ff969e0e2a3146556

Lo primero que debes notar sobre los mensajes encriptados es que cambiar el mensaje de un personaje de "Enviar $ 10" a "Enviar $ 20" da como resultado una producción muy diferente. El pequeño cambio en la entrada que resulta en una transformación completa de la salida es una forma en que las transacciones de Bitcoin están garantizadas como únicas. La segunda cosa a notar es que incluso si cambiamos la longitud del mensaje de siete caracteres "Enviar $ 10" a once caracteres "Enviar $ 300.05", la salida solo tiene 64 caracteres. De hecho, cualquier mensaje de longitud se convertirá en 64 caracteres, lo que hace que enviar un mensaje encriptado sea muy

eficiente. Dado que el blockchain está almacenando todos los mensajes, usar una función hash criptográfica para reducir los mensajes a 64 caracteres ayuda a mantener los datos almacenados al mínimo.

Cada vez que el mensaje se pasa a través de la picadora de carne (o función de picadillo), se produce una salida diferente. Sin embargo, para que cada transacción sea única, el software de Bitcoin agrega a cada transacción un número aleatorio llamado nonce. Este número aleatorio crea una traducción única o valor hash para cada transacción.

Además, como nivel adicional de seguridad, el software Bitcoin requiere que el valor hash comience con un cierto número de ceros. Es imposible para los mineros predecir qué nonce producirá la cantidad correcta de ceros a la izquierda, así que los prueban todos. De hecho, cada segundo, todas las computadoras de minería en la red Bitcoin calculan 10 billones de hash de valores. Mediante la fuerza de cálculo bruto, los mineros finalmente encuentran un valor que coincide con el valor hash generado aleatoriamente de la transacción. Para que se confirme una transacción, seis mineros deben encontrar exactamente el mismo valor.

A medida que se agregan más transacciones a la cadena, cada bloque contiene una referencia al bloque anterior. Si alguien quisiera gastar el bitcoin que Keith le envió a Alan, no solo tendrían que realizar la laboriosa tarea de encontrar el valor hash correcto, sino que tendrían que retroceder y volver a calcular cada valor hash por cada transacción que se haya realizado alguna vez. lugar: una tarea prácticamente insuperable. Cuanto más grande es la cadena de bloques, más seguro se vuelve.

6.4- ¿Todavía quieres ser un minero?

Minería bitcoins no es solo una forma de lograr un consenso seguro; también es la forma en que se acuñan los bitcoins. El primer minero que encuentre el valor hash correcto se recompensará con un bloque de monedas. La recompensa original fue establecida por el software de Bitcoin en 50 monedas, y esta cantidad se reduce a la mitad cada 210,000 bloques. La recompensa actual es de 25 bitcoins. Además de las nuevas monedas, los mineros reciben una pequeña tarifa de transacción por su trabajo. Al ritmo actual, la tarifa de transacción es insignificante, pero a medida que se extraigan más monedas, la tarifa de transacción se convertirá en una parte más grande de la corriente de ingresos del minero.

Ahora puede tener una computadora de repuesto en su ático y está pensando en unirse a la fiebre del oro digital. Tal vez usted tiene un entendimiento significativo, o tal vez no le importa, no estoy aquí para juzgar. Desafortunadamente, el aumento meteórico en el precio de los bitcoins ha causado una avalancha de interés. Con todos los nuevos mineros, el nivel de dificultad de la red ha superado las simples plataformas mineras.

Recordemos cuando estábamos hablando de cómo seis mineros tenían que confirmar la transacción y el tiempo promedio era de unos 10 minutos; bueno, si seis mineros lo hacen más rápido que 10 minutos, entonces el software de Bitcoin dificulta aún más el problema matemático. Esto es lo que se conoce como dificultad de red. Ver la Figura 6.1.

La tasa de hash es la línea gris oscuro y es una estimación de cuántas ecuaciones se calculan cada segundo. Como puede ver, el aumento del precio atrajo a más mineros, lo que aumentó el número de ecuaciones que se calculan. Dado que el juego de la minería es competitivo, más jugadores implican verificaciones de transacciones más rápidas. El software luego se ajusta para hacer la

ecuación más difícil. Fue diseñado de esta manera para mantener la creación de las nuevas monedas a un ritmo constante.

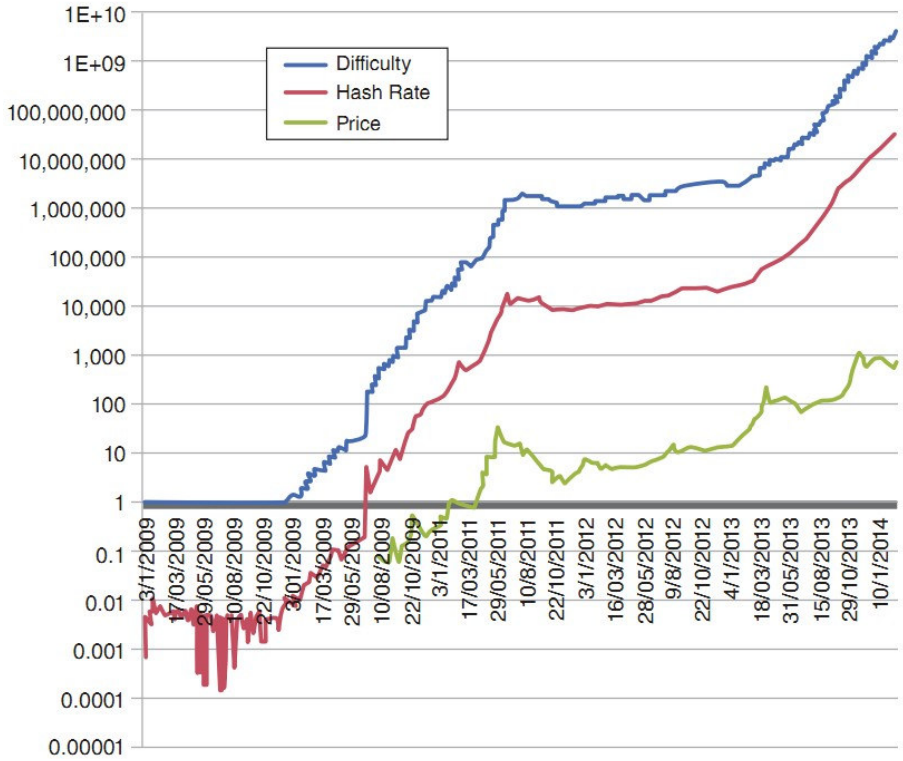

Figura 6.1: El precio Bitcoin vs Dificultad de la Red y la Tasa Hash

Con todos esos cálculos, podría pensar que todas las monedas se habrán ido para el momento en que lea estas páginas. Piensa otra vez. La combinación del ajuste de dificultad y la tasa de bloqueo a la mitad del bloque garantiza que el último bloque de bitcoins no se extraerá hasta 2140. Cada 210,000 bloques, la recompensa se reduce a la mitad. Esto se conoce como la tasa de bloqueo a la mitad. Pero voltee ese ceño fruncido; todavía hay tiempo para que hagas tu fortuna minera. Vamos a examinar lo que va a tomar.

Dado que Bitcoin solo ha existido desde 2009, hay una breve historia de la minería. Considera esta tu lección llamada "Una breve historia del tiempo de Bitcoin". Hace poco tiempo, en una galaxia que residía en Internet, los bitcoins fueron minados con computadoras simples; la unidad de procesamiento central (CPU) se usó para resolver el problema matemático. Entonces apareció un traficante joven y se dio cuenta de que los problemas matemáticos se podían resolver más rápido con una tarjeta gráfica, sí, mientras disfrutabas uno frío el 4 de julio, alguien estaba pensando en cómo resolver un hash criptográfico más rápido. ¿Empezando a ver por qué son millonarios?

Figura 6.2 Plataforma de Minería FPGA hecha en casa

La siguiente evolución en el historial de la plataforma minera fue FPGA o matrices de compuertas programables en campo (Figura 6.2). Si bien este nombre suena formidable, lo que realmente significa es que el hardware se puede comprar a granel, conectado entre sí y programado en el campo. Sería mejor pensar en esta evolución ya que los mineros de edad de MacGyver comprarían los FPGA y construirían una computadora que solo se usaba para resolver problemas matemáticos y recolectar bitcoins.

Actualmente estamos en la Era Dorada, donde Emmanuel Abiodun usa circuitos integrados específicos de la aplicación (ASIC) para generar valores de hash criptográficos a velocidades que adormecen la mente. Así es como la red puede completar 10 cuatrillones de cálculos por segundo. Los mineros ya no tienen que manipular las computadoras; los ASIC están fabricados en fábrica para funcionar. No es demasiado diferente a la historia de NASCAR: los moonshiners arreglaron los autos viejos para hacerlos correr más rápido. Eventualmente, los llevaron a la playa para competir. Los autos de carrera de hoy están muy lejos de los originales, pero la historia es la misma.

Figura 6.3: Dave Carlson en su estación de minería de Bitcoin de $8 millones por mes

Emmanuel Abiodun no es el único minero de bitcoin que construye una operación masiva. En el estado de Washington, Dave Carlson dirige una de las minas de bitcoin más grandes del mundo

(Figura 6.3). Carlson se sintió atraído por Washington porque esta región tiene algunas de las tarifas de electricidad más bajas, lo que le permite generar $ 8 millones al mes en ingresos de minería de bitcoin. Sí, ¡$ 8 millones por mes! Para generar estos ingresos, utiliza alrededor de 1,4 megavatios de electricidad, que también es suficiente para iluminar una ciudad pequeña.

¿Aún interesado? Digamos que ha adquirido la plataforma más grande y más mala conocida en el mundo de la minería; tal vez sea usted la persona que pagó $ 20,600 por una plataforma minera de $ 1,500 en eBay. Todavía puede tener dificultades para ganar dinero. Recuerde, la minería bitcoin es una carrera. El ganador obtiene el botín, y ganar significa tener la mayor potencia informática. Pero no pierdas la fe. Hay una manera de hacer un poco de masa: únete a un club. Más específicamente, únase a un grupo de minería.

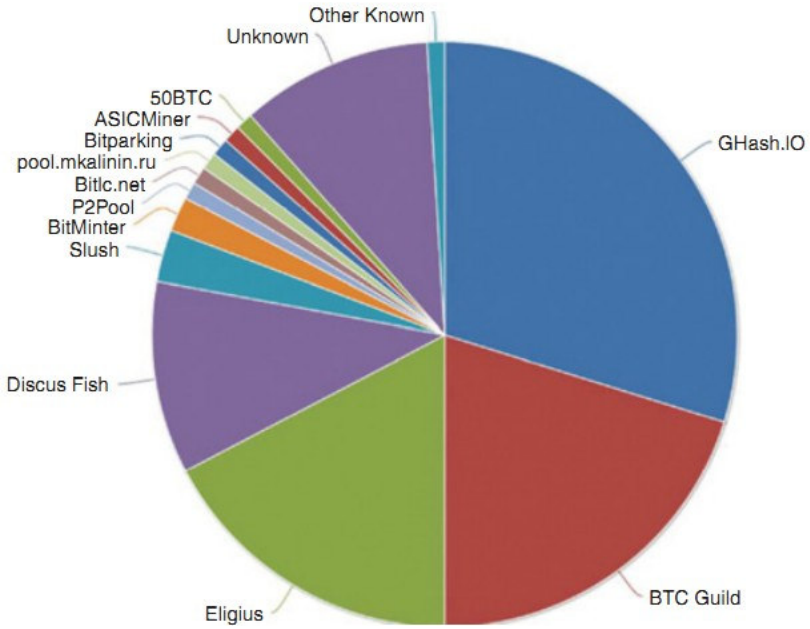

Figura 6.4: Participación de mercado en el pool de minera de Bitcoin

FUENTE: Blockchain.info, 10 de enero de 2014.

Un grupo de minería es un grupo de individuos que deciden agrupar su poder de cómputo para extraer bitcoins y dividir los beneficios. En el mundo de Bitcoin, estos se rigen por las organizaciones autónomas desconcentradas moniker clunky. No olvide este término, es clave para el futuro de Bitcoin. Por ahora, solo sé que el sistema de amigos funciona. Ver figura 6.4.

Y al igual que en el nivel cuántico, el nivel macro (pool) significa el grupo más grande con la mayor cantidad de potencia gana. Algunos de ustedes están intrigados, algunos de ustedes están a punto de quedarse dormidos, y otros ven una laguna. Antes que nada, DESPIERTA. De acuerdo, ahora a la laguna llamada ataque del 51 por ciento, que discutimos en el Capítulo 4.

Teóricamente, alguien o un conjunto podría reunir suficiente potencia informática para calcular el 51 por ciento de todas las ecuaciones. Si esto ocurriera, entonces este grupo sería el único que podría confirmar las transacciones, y obtendrían todas las monedas. Pero aún más nefastos, podrían confirmar transacciones dos veces por la misma moneda. No está mal, ¿verdad? No solo obtienen todas las monedas; ellos pueden gastarlos dos veces.

Eche otro vistazo a ese gráfico circular. ¿Ves el gran pastel azul? Es un grupo de minería llamado Ghash.io. En enero de 2014, representó el 42 por ciento de la capacidad informática en la red. La

comunidad de Bitcoin estaba agitada. ¿Qué iban a hacer? ¿Era este un grupo nefasto de bandidos o simplemente mineros bien intencionados de ideas afines? La primera reacción fue el boicot de un minero, y fiel a su naturaleza de autocontrol, los mineros con sombrero blanco comenzaron a eliminar su poder de computación de la piscina, reduciendo así su influencia. Finalmente, Ghosh.io emitió una declaración que decía que no tenían intención de orquestar un ataque del 51 por ciento y que tomaría medidas para evitar tal resultado.

Ahora con todos estos grupos y supercomputadoras, pensarías que los mineros están ganando dinero a manos llenas. Después de todo, una vez que el costo de la máquina está cubierto, literalmente debe "imprimir" dinero. No olvides que muchos de los que vinieron antes que tú se enfrentaron con un ultimátum de su pareja, ya sea que la máquina se vaya o se vayan. Eso es porque las máquinas están trabajando tan duro y usan tanta energía que emiten una gran cantidad de calor. Para mantener la operación en funcionamiento, los mineros usan ventiladores y aires acondicionados, y esta es también la razón por la cual el Sr. Abiodun se mudó a Islandia. ¿Qué tiene Islandia en abundancia y es esencialmente gratis? Aire frio. Por lo tanto, aunque los ingresos por operación de los mineros están disminuyendo, las operaciones que pueden usar menos energía para enfriar las máquinas tienen una ventaja.

Supongamos que no quieres dejar a tu familia y no están particularmente interesados en mudar la Islandia. ¿Se perdió toda esperanza? No, aún puede convertirse en un minero de criptomonedas eligiendo Litecoin u otra moneda digital. ¿Esperar lo? Hay más de un "bitcoin"? ¿Recuerdas cuando profundizamos en el cifrado de Bitcoin y hablamos hashes criptográficos? Seguro lo haces. Bueno, un ex empleado de Google llamado Charles Lee pensó que podría mejorar Bitcoin, y en 2011 creó y lanzó Litecoin.

Hay tres diferencias principales entre Litecoin y Bitcoin. Primero, los bloques de Litecoin se producen cada 2.5 minutos en vez de cada 10 minutos con Bitcoin. La ventaja de una creación de bloques más rápida es un tiempo de confirmación más rápido y, por lo tanto, menos tiempo para un ataque de gasto doble. La desventaja es que todos esos bloques forman una cadena muy grande; por lo tanto, la cantidad de datos que deben almacenarse es casi cuatro veces superior a la de Bitcoin. En segundo lugar, Litecoin eventualmente emitirá 84 millones de monedas (recuerde que Bitcoin tendrá un máximo de 21 millones de monedas). En tercer lugar, Litecoin utiliza scrypt como un protocolo de encriptación, lo que hace que sea más fácil extraer sin una tarjeta de gráficos sofisticada. La diferencia entre scrypt y SHA256 utilizada por Bitcoin es la forma en que la computadora procesa la ecuación matemática. Es esta facilidad de minería lo que ha llevado a la explosión de criptomonedas alternativas, también llamadas monedas alternativas, también llamados altcoin.

6.5- ¿Necesitamos otro Bitcoin?

Es posible que se pregunte por qué necesitamos otro Bitcoin, y aún más, ¿por qué alguien aceptaría Auroracoin, Dogecoin o incluso un BKoin? El profesor Robert Shiller ha opinado que existe un defecto en las monedas alternativas: ninguna de ellas resuelve un problema económico. Para el éxito a largo plazo, cualquier empresa debe resolver un problema. No me gustan las almendras y el coco? Bien, hay Montículos. Problema resuelto e imperio construido. Bitcoin resolvió el problema de los generales bizantinos, e indudablemente hay valor en ese logro. Sin embargo, si los mineros van a reemplazar al intermediario del servicio financiero, entonces las monedas que extraen deben tener un objetivo económico.

La otra crítica de Bitcoin y alt-coins es la falta de estabilidad. En un día cualquiera, el precio de Bitcoin puede fluctuar en más del 20 por ciento. Esta volatilidad limita su capacidad de actuar

como un medio de intercambio y una reserva de valor. Hay dos factores principales de la volatilidad: los especuladores y los mineros. Dado que los mineros necesitan pagar esas altas facturas de electricidad, constantemente están vendiendo y convirtiendo monedas digitales en fiat. Del otro lado están los especuladores que están sujetos a los caprichos de la emoción humana.

Hay un viejo dicho sobre el oro: una onza siempre te comprará un buen traje en Londres. Este adagio destaca la estabilidad del poder de compra del oro y es una de las razones principales por las que ha servido como moneda en los últimos 5.000 años. El consumidor y el comerciante desean esta estabilidad en el poder adquisitivo. Desde la perspectiva del consumidor, el poder adquisitivo estable significa que los ahorros pueden acumularse sin los efectos nocivos de la inflación. Un comerciante preferirá una moneda estable porque su margen de ganancia es una función directa del costo de sus suministros. Una moneda que fluctúa enormemente significa un costo salvajemente fluctuante de los bienes vendidos.

La estabilidad a largo plazo del oro se usa a menudo para criticar a Bitcoin en comparación. Servir como una tienda de valores es una de las tres funciones esenciales de una moneda. Si hubiera una forma de resolver este problema de "almacenamiento de valor", tal vez si estuviera involucrado un banco central. La comunidad de criptomonedas gritará blasfemia ante la mención de una figura de autoridad centralizada. Sin embargo, si alguien pudiera idear una forma de estabilizar una criptomoneda utilizando un algoritmo predeterminado, ¿entonces se resolvería el problema y se construiría un imperio? Quizás. En el siguiente capítulo, seguiremos mi creación del Nautiluscoin, la primera moneda con su propio fondo de estabilidad.

Capítulo 7

Todo el dinero es una cuestión de creencia.

-Adam Smith

7.1- Nautiluscoin — 0 a $1 millón en 60 días

La libertad es más preciosa que el oro ". Este fue el lema inscripto en la libra de Georgia de 1776. Cuando George Washington cruzó el Delaware, era poco probable que tuviera un bolsillo lleno de dólares de EE. UU. La moneda de la tierra era la moneda continental, o Continental, emitida por el Congreso Continental para pagar la Guerra Revolucionaria. Cuando el Congreso Continental emitió esta moneda, no estaban pisando tierra virgen. De hecho, seguían una larga historia de emisión de divisas que comenzó con la libra de Massachusetts en 1690. Los billetes de bacalao y las libras de Connecticut y Virginia estaban en circulación y se podían convertir a la moneda internacional de la época, que era en 1690 el Dólar molido español.

No fue hasta las Actas Bancarias Nacionales de 1863 y 1864 que el dólar de los Estados Unidos comenzó a actuar como la única moneda de la tierra. La Ley de 1863, también conocida como la Ley de la moneda nacional, fue diseñada para resolver el problema de la inflación causada por la abundancia de billetes emitidos por entidades privadas. La ley gravaba los pagarés emitidos por los bancos estatales y locales y los convertía efectivamente en moneda inferior. Gravar las monedas privadas finalmente las eliminó de la circulación.

El sistema de moneda emitida por el estado y la privada funcionó bien hasta que inevitablemente una desaceleración económica haría que fuera demasiado tentador imprimir más billetes. Los primeros 150 años de los Estados Unidos están marcados con muchos episodios de alta inflación debido a un exceso de oferta de dinero emitido por entidades privadas. Bitcoin resuelve el problema del exceso de oferta al limitar matemáticamente el número de monedas que alguna vez existirán. Es esta propiedad la que hace de Bitcoin un tema ideal para la emisión de dinero privado.

Una plétora de disertaciones doctorales han abogado por un mejor sistema de dinero, y algunas incluso han argumentado que el gobierno no debería tener el monopolio de emitir dinero. El defensor más conocido del dinero privado fue Friedrich Hayek. En su libro The Denationalization of Money (Instituto de Asuntos Económicos, 1976), Hayek defendió que el dinero debería emitirse de forma privada y competir por la aceptación. Hayek imaginó un mercado competitivo para el dinero privado que convergió en las monedas más estables. Supuso que una moneda que ganara poder adquisitivo perjudicaría a los deudores, mientras que una moneda devaluada perjudicaría a los acreedores. Concluyó que el mercado elegiría la moneda con el poder adquisitivo más estable.

No es sorprendente que la sugerencia de Hayek levantara algunas cejas y lo convirtiera en un pararrayos de críticas. La trampa de la economía como ciencia es que rara vez hay un laboratorio para probar la hipótesis. Por lo tanto, la teoría económica sigue siendo solo eso: teoría.

Hayek sugirió que un emisor privado de dinero debería establecer un piso sobre el precio de ese dinero para mantener la estabilidad. También sugirió que nunca se puede romper el piso mientras los especuladores crean que el banco central se capitalizó lo suficiente como para mantener ese piso. Esta teoría ha sido probada muchas veces con las monedas vinculadas a niveles predeterminados. La falla en las monedas vinculadas siempre ha sido la capitalización del banco

central. Una vez que se hace evidente que el banco central no podrá mantener la vinculación, se produce un ataque especulativo, lo que obliga al banco a dejar de comprar divisas.

Uno de los fallos más memorables, Black Wednesday, se produjo en el Reino Unido en 1992. Los especuladores de divisas, incluido George Soros, vendieron libras esterlinas británicas cortas y cosecharon ganancias de más de mil millones de dólares en un frenético período de 24 horas. En previsión de la Unión Económica y Monetaria, Europa creó el Mecanismo de Tipo de Cambio (MTC) para reducir la variabilidad del tipo de cambio. El ERM era un sistema semielaborado; es decir, se permitió a las monedas operar dentro de una banda predeterminada.

Cuando el ERM se estableció en 1979, el Reino Unido se negó a participar. Dado que la libra británica era de libre flotación, estaba sujeta a los caprichos de los flujos internacionales de divisas. Cuando Nigel Lawson se convirtió en canciller del Tesoro, abogó por un tipo de cambio fijo y utilizó el bajo récord de inflación de Alemania Occidental como su razonamiento. Esta admiración y creencia en una moneda estable dio lugar a una política semioficial de sombrear el alemán alemán deutsche de 1987 a 1988. Sin embargo, esta política y el ERM no fueron populares con el asesor económico de Margaret Thatcher, Alan Walters. Cuando Walters llamó al ERM "a medio hacer", Nigel Lawson renunció.

John Major sucedió a Lawson como Canciller del Tesoro y convenció al gobierno británico de ingresar al MTC en 1990. Cuando el Reino Unido entró en el MTC, el marco alemán se cotizaba a 2,95 libras esterlinas, lo que significaba que la tasa no podía fluctuar por encima de 3.127 o por debajo de 2.773. Cuando las monedas están vinculadas, significa que sus políticas económicas también están hermanadas. En ese momento, el Reino Unido estaba luchando contra la inflación y su economía estaba al borde de la recesión. Alemania también estaba luchando contra la inflación, pero su economía era más fuerte que la del Reino Unido. Para luchar contra la inflación, Alemania elevó sus tasas de interés al 15 por ciento, lo que exacerbó la debilidad de la economía británica.

A medida que la economía británica vaciló, la libra esterlina comenzó a caer al extremo inferior de su banda permitida. Esta disminución significó que el gobierno del Reino Unido tuvo que actuar o retirarse del ERM. Actuar significaba comprar libras esterlinas en el mercado abierto, y para lograr esto, Gran Bretaña necesitaba reservas en moneda extranjera. Al comprar una moneda extranjera, uno intercambia una moneda por otra; en este caso, los vendedores intercambiaban la libra esterlina por otras monedas como el marco alemán. Para facilitar este intercambio, el Reino Unido necesitaba un tesoro.

Sin embargo, John Major creía que la retirada del ERM y la posterior devaluación de la libra conducirían a niveles aún más altos de inflación. Por lo tanto, el movimiento inicial de John Major no fue retirarse del ERM o comprar libras británicas. Decidió elevar las tasas de interés al 10 por ciento en un intento por desalentar a los especuladores de vender la libra. No funcionó.

El 16 de septiembre de 1992, el Reino Unido anunció que aumentaría nuevamente las tasas de interés del 10 por ciento al 12 por ciento, pero la libra siguió cayendo. Más tarde ese mismo día, el gobierno prometió elevar las tasas al 15 por ciento, pero se perdió la credibilidad. A las 7:00 p.m. el Reino Unido anunció que dejaría el ERM y mantendría las tasas en un 12 por ciento.

Cuando se asentó el polvo, se estimó que el Tesoro del Reino Unido había perdido más de £ 3 mil millones tratando de defender la moneda. La crisis tomó peajes políticos y económicos, lo que llevó a muchos a creer que alimentó la recesión. Con el paso del tiempo, algunos llegaron a creer que el Miércoles Negro era necesario para reequilibrar la economía del Reino Unido.

Independientemente de la conclusión, este fue un ejemplo real de lo que puede suceder cuando un banco central pierde credibilidad.

7.2- Creando una moneda

Cuando concebí Nautiluscoin, era consciente de los peligros de una moneda vinculada, pero las monedas digitales aún necesitan un mecanismo para reducir la volatilidad. Mi solución fue crear la primera moneda digital con su propio "banco central". El único propósito del banco central era estabilizar la moneda. Estaba intrigado e inspirado por la posibilidad de probar la teoría de Friedrich Hayek de que los consumidores y los comerciantes convergerían en la moneda más estable. El Nautiluscoin Stability Fund es un "banco central" autofinanciado encargado de estabilizar la moneda, con el objetivo de un patrón de crecimiento sólido y estable, como un caparazón nautilus.

Lo que sigue es mi diario desde la creación hasta $ 1 millón en 60 días.

> 6 de marzo de 2014: hoy tuvimos la reunión de producción inicial para el segmento de Dinero rápido para crear la moneda. Envié diapositivas y definiciones al equipo de producción ayer, pero no fueron tan claras como pensaba. Tal vez escribir el libro y entrar en la esencia de las criptomonedas me tiene demasiado cerca del proyecto. El objetivo es crear un segmento de 90 segundos que presente el mundo de las monedas digitales e ilustre cómo se crean.
>
> El plan es crear la moneda usando Coingen.io, y luego voy a prever la moneda para crear el fondo que actuará como banco central. El segmento terminará con el principio premonitorio, y luego le corresponde al poder del banco central crear un mercado líquido y estable. He decidido renombrar el fondo de estabilidad como un "banco central". Creo que este es el más fácil de entender.
>
> También me di cuenta esta tarde que o bien necesito elegir un intercambio oficial o publicar un tipo de cambio oficial en el sitio web. Creo que hacer una oferta en cada intercambio en el que cotiza la moneda podría volverse insostenible si de hecho la moneda es exitosa. Por ahora, estoy dando vueltas alrededor de la idea de una tasa de cambio oficial publicada en el sitio web.
>
> 4 de abril de 2014-Han pasado algunas semanas, pero nos estamos acercando al lanzamiento de la moneda. Ahora tengo claro que tendré que elegir un intercambio oficial para que funcione el Fondo de Estabilidad Nautiluscoin (NSF). Tuve una excelente conversación con los fundadores de Austin Global Exchange. Parecen ser exactamente el tipo de socios emprendedores que funcionarían bien con Nautiluscoin.
>
> Austin Global será el intercambio oficial después del lanzamiento y la NSF operará en ese intercambio. NSF es el nombre del banco central que creé. Después de pensarlo mucho, parecía incongruente tener una moneda descentralizada con un banco "central". El NSF tendrá el único propósito de actuar como un tope de velocidad cuando la volatilidad aumenta.
>
> 12 de abril de 2014: filmamos el segmento de Fast Money esta semana y estamos listos para lanzar la moneda. Austin Global Exchange ha configurado

Nautiluscoin para que pueda comercializarse el día en que aireamos el segmento. Sigo creyendo que la creación de un mercado líquido y estable será la parte más difícil de este proceso. La única razón para comprar Nautiluscoin es la especulación de que será aceptado por los comerciantes. Si la NSF puede crear un mercado, entonces es más probable que los comerciantes lo acepten.

13 de abril de 2014: ¡Nautiluscoin acaba de sufrir un ataque al corazón! El equipo de Austin Global Exchange descubrió una falla importante en el código que permitirá a los mineros acumular todas las monedas dentro de las primeras dos semanas y luego controlar la cadena de bloques. No estoy seguro de entender realmente lo que han encontrado, ¡pero es mejor que aprenda rápido!

Actualización: Acabo de aprender una gran lección sobre "Bitcoin Time": así es como se mueven las cosas en este negocio. Cuando originalmente creé la moneda con Coingen, el software simplemente clonaba Bitcoin (o en el caso de Nautiluscoin, clonaba Litecoin). El problema es que el código original de Litecoin no tenía en cuenta los mineros de circuitos integrados específicos de la aplicación (ASIC). El código original ajusta el problema matemático cada dos semanas para asegurarse de que el problema se resuelve dentro del marco de tiempo de un minuto que especifiqué. Sin embargo, los nuevos mineros de ASIC pueden minar tan rápido que, antes de que se ajuste el problema, podrán extraer todas las monedas. Podrán explotar los bloques en cuestión de segundos, no el minuto que originalmente quería.

La solución para esto es algo llamado Kimoto Gravity Well (KGW): esta es la primera vez en mi vida que escucho estas palabras, y claramente estoy por encima de mi cabeza. Después de algunas investigaciones rápidas, aprendí que KGW cambia la dificultad del problema matemático después de cada bloqueo en lugar de cada dos semanas. Para que Nautiluscoin se convierta en algo más que un experimento, tendré que instalar KGW.

14 de abril de 2014: después de hablar con algunos desarrolladores de moneda digital, he determinado que KGW no podrá implementarse antes del lanzamiento. Tendré que lanzar la moneda con la falla y arriesgarme con los mineros. Al menos podré probar la eficacia de la NSF; si puedo crear un mercado estable y líquido con un gran defecto en el código, cuando se solucione la moneda será aún más fuerte.

18 de abril de 2014-Se lanzó la moneda, y sorprendentemente aún no ha sido destruida por los mineros. Si bien pude obtener mucha atención del segmento Fast Money, no creo que la comunidad minera conozca Nautiluscoin. Además, el precio puede no ser lo suficientemente alto como para atraer grandes mineros, lo que me puede dar tiempo para solucionar el problema.

Con ese fin, los fundadores de Austin Global Exchange me pusieron en contacto con los creadores de moneda de una moneda llamada DigiByte. Aparentemente, tienen una mejor solución que Kimoto Gravity Well, se llama DigiShield y se ha implementado en Dogecoin.

23 de abril de 2014: pasé los últimos días hablando con Jared Tate de DigiByte y estoy muy impresionado con él. El equipo de DigiByte implementará DigiShield en Nautiluscoin, pero tomará mucho más trabajo de lo que originalmente pensé.

El código anterior que recibí de Coingen no funcionará si quiero tener una moneda sólida que sea aceptada globalmente: el equipo de DigiByte tiene que recodificar por completo la moneda, y tendremos que volver a lanzar la moneda. Tengo que decir que el equipo de DigiByte es muy profesional y conocedor. Creo que compraré DigiByte, ya que son el verdadero negocio.

Ahora estoy aún más feliz de que poca gente sepa sobre Nautiluscoin, ya que un relanzamiento significa que las monedas originales no tendrán valor. Si una gran cantidad de grandes mineros tenían las monedas, habrían desperdiciado energía en la minería sin obtener ningún rendimiento. Tengo la mayoría de las monedas ya que soy el único minero en la red, por lo que un relanzamiento no me molestará.

26 de abril de 2014-Ahora que tengo un equipo de desarrollo trabajando en el código, puedo enfocarme en el marketing. Cuando originalmente lancé la moneda, el único lugar donde anuncié que estaba en CNBC, pero la comunidad de moneda digital aún no lo sabía. El lugar para anunciar el lanzamiento de una moneda es el foro de Bitcointalk. Nunca he usado esto y sospecho que enfrentaré otra curva de aprendizaje abrupta.

1 de mayo de 2014: ¡es el día de relanzamiento! Estamos empezando de nuevo en $ 0, pero el código es sólido y esta será la primera moneda en lanzarse con DigiShield. Jared Tate de DigiShield se ha puesto en contacto con algunos grupos de minería que estarán a bordo para el lanzamiento; sin estos grupos de minería, las transacciones no se verificarán y toda la red se detendrá. Aprendí que un lanzamiento justo es muy importante al establecer el valor de una moneda. El mundo de las monedas alternativas está lleno de esquemas de bombeo y descarga; por lo tanto, las nuevas monedas se ven con escepticismo. Además, las monedas pre-minadas son mal vistas, ya que la mayoría de la gente piensa que el desarrollador de la moneda simplemente va a tirar las monedas en el mercado para obtener una ganancia rápida.

He anunciado el lanzamiento de la charla de Bitcoin, y espero haber explicado lo suficiente a la NSF para que la gente entienda que es un concepto sin fines de lucro.

1 P.M.-¡La moneda se lanza! Acabo de comprar las primeras monedas a 0.00400 BTC, lo que le da una valoración inicial de aproximadamente $ 0.18. Esto es mucho más alto de lo que esperaba, pero ahora necesito otros especuladores que deseen comprar de la NSF para que pueda usar las bitcoins para soportar el precio.

2 de mayo de 2014: el precio se ha desplomado durante la noche de $ 0,18 a aproximadamente $ 0,9. Acabo de aprender una lección muy valiosa y descubrí un defecto en mi plan de estabilización. El concepto de NSF se basa en la suposición errónea de que todos los titulares de Nautiluscoin lo tienen por la misma razón: la especulación de que los comerciantes lo aceptarán en el futuro. Sin embargo, esta no es la motivación de los mineros: su motivación es obtener ganancias y pagar sus facturas de electricidad. A los mineros no les importa la estabilidad, y tan pronto como extraen la moneda, la venden. No anticipé la influencia de la venta de los mineros sobre el precio de la moneda.

10 de mayo de 2014: el precio de la moneda se ha estabilizado, aunque a un precio muy bajo. El funcionamiento de la NSF se ha convertido en un trabajo más de lo que esperaba: estos mercados están abiertos las 24 horas del día, los 7 días de la semana. Es sábado por la noche a las 11 P.M., y acabo de recibir noticias de que Austin Global Exchange ha sido pirateado y las existencias de la NSF están en peligro. El equipo de AGX ha eliminado el sitio para evitar problemas de seguridad adicionales; en este momento no tengo idea si las monedas NSF han sido robadas.

Actualización: 12 de la noche, Austin Global Exchange me ha dicho que las existencias de la NSF son seguras, pero es posible que me hayan robado algunos bitcoins. No tenía mucho valor en bitcoins en el intercambio, así que me alivia saber que fueron las únicas monedas robadas. El intercambio permanecerá cerrado hasta que descubran la violación de seguridad y cómo solucionarlo.

12 de mayo de 2014: Austin Global Exchange vuelve a funcionar y las monedas NSF que se depositaron en el intercambio se contabilizan. Me ha impresionado mucho la respuesta de Austin Global: han manejado esta brecha como verdaderos profesionales. Sin embargo, he aprendido otra lección valiosa: no importa cuán seguros parezcan ser los intercambios, son el eslabón débil en el mundo de las monedas digitales. Este es un problema que debe remediarse si las monedas digitales se convertirán en una nueva clase de activos.

Por suerte, Nautiluscoin se agregó a otro intercambio, Poloniex. Nunca había escuchado sobre este intercambio, pero la adición es bienvenida, ya que está claro que usar un intercambio para la operación NSF no es seguro.

16 de mayo de 2014: el precio de Nautiluscoin se ha más que duplicado en las últimas 24 horas, y la razón es que otro intercambio ha decidido incluir a Nautilus. El intercambio de Mintpal es uno de los intercambios de divisas digitales más grandes, y su cotización ha hecho que el precio salte de $ 0.12 a más de $ 0.25. Todavía me resulta curioso que el simple hecho de ser agregado a un intercambio agregue valor intrínseco, pero en la medida en que un mercado más líquido se agregue al efecto de red, supongo que hay un argumento que se debe hacer para una mayor valoración.

20 de mayo de 2014: creo que todas las cosas buenas llegan a su fin, incluso en monedas digitales: el precio de Nautiluscoin ha caído nuevamente en más del 50 por ciento. A medida que más mineros se unieron a la red, se acuñaron más monedas. Para pagar las facturas de electricidad, los mineros venden automáticamente las monedas recién acuñadas y las convierten en monedas fiduciarias. No anticipé la influencia de la venta de mineros sobre el precio de Nautiluscoin.

La NSF no puede seguir el ritmo de la venta, y se ha descubierto un error importante en mi lógica. Hice la suposición de que todos los titulares de Nautiluscoin estaban sosteniendo la moneda por la misma razón, es decir, la apreciación del capital. En base a esta suposición, pensé que controlar la volatilidad sería mucho más fácil de lo que parece. Mi error fue no incluir las ventas de los mineros en mi lógica; no les importa la apreciación del capital; lo único que les importa es obtener un beneficio a corto plazo.

A pesar de todos mis esfuerzos de marketing para explicar el NSF, los mineros continúan vendiendo automáticamente. Es probable que los mineros no tengan idea acerca de la NSF; simplemente están mirando una ecuación de rentabilidad. Estoy seguro de que miraré hacia atrás como un nuevo error flagrante: ¡vive y aprende!

En retrospectiva, debería haber cambiado la forma en que se extrae la moneda de una prueba de trabajo a una prueba de participación. El método de prueba de participación elimina a los mineros del proceso y permite que cualquier persona que tenga las monedas para extraer nuevas monedas simplemente compre abrázalas en su billetera.

12 de junio de 2014: el precio de Nautiluscoin ha bajado lentamente, y el NSF no puede suavizar el golpe.

Nos hemos visto afectados por una confluencia de eventos: primero, los mineros continúan acuñando nuevas monedas y arrojándolas al mercado; segundo, el precio del bitcoin ha caído un 12 por ciento en solo unos pocos días. Esto ha obligado a los mineros a vender aún más Nautiluscoin. Como Nautiluscoin no se puede convertir directamente en moneda fiduciaria, los mineros primero deben vender Nautiluscoin y recibir bitcoins. Una vez que reciben las bitcoins, las venden por dólares estadounidenses, euros, libras, etc. A medida que el precio del bitcoin desciende, los mineros necesitan vender más para pagar facturas y obtener ganancias. Este ciclo de retroalimentación negativa está afectando el precio de Nautiluscoin ya que los mineros venden más para obtener más bitcoin.

A menos que encuentre otro comprador "natural" de Nautiluscoin, irá disminuyendo lentamente. Necesito encontrar una razón para que la gente compre Nautiluscoin además de la especulación de que algún día un comerciante puede aceptarlo como pago.

17 de junio de 2014: The Goddess of Fortune sonrió a Nautiluscoin una vez más. La noche anterior, la estrella profesional de artes marciales Jon Fitch me contactó a través de Twitter. Recientemente se ha involucrado en monedas digitales y está buscando un patrocinador para su próxima pelea. La próxima pelea saldrá al aire el fin de semana del 4 de julio en NBC y tiene el potencial de llegar a millones de hogares. Cuando Dogecoin patrocinó un auto de carreras NASCAR, el precio de la moneda se duplicó.

18 de junio de 2014-Jon y yo hemos resuelto los detalles del patrocinio: el tamaño del logotipo es directamente proporcional a la cantidad de dinero que se paga. Quiero que la comunidad sea parte de esta promoción; esto permitirá a cualquier persona con Nautiluscoin ayudar a patrocinar al primer atleta profesional a pagar en monedas digitales.

Comenzaré la recaudación de fondos enviando 20,000 NAUT a Jon, y luego anunciaré a la comunidad que hemos llegado a este acuerdo y que cualquiera puede participar. Si podemos llegar a (Continuación)

$ 10,000 en dólares estadounidenses equivalentes, luego Nautiluscoin tendrá una ubicación privilegiada en los pantalones cortos, camisetas y pancartas para la pelea.

Aquí está el anuncio oficial:

Estamos muy contentos de anunciar que Nautiluscoin patrocinará a Jon Fitch, el No. 2 de las categorías mixtas de artes marciales (MMA) en el peso welter clasificado, en su próxima pelea el 5 de julio en NBC. Al igual que muchos de nosotros, Jon ha descubierto recientemente el error de la moneda digital y, con este patrocinio, se convertirá en el primer atleta profesional a quien se le pagará en una moneda digital.

Con este patrocinio, Nautiluscoin comienza su camino hacia la aceptación como medio de intercambio. En los próximos meses, los minoristas podrán aceptar Nautiluscoin para transacciones tanto en línea como fuera de línea. Además, se lanzarán varias nuevas empresas que utilizarán Nautiluscoin exclusivamente. Este es un momento emocionante para las monedas digitales, y Nautiluscoin tiene la suerte de contar con una comunidad de apoyo.

22 de junio de 2014-La promoción de Jon Fitch ha ido muy bien. No solo hemos recaudado casi $ 5,000 en Nautiluscoin, sino que el precio de la moneda Nautilus casi se ha duplicado desde el anuncio. Hemos tomado el valor de mercado total de Nautiluscoin de $ 0 el 1 de mayo de 2014 a $ 500,000 el 22 de junio de 2014.

Si bien todo parece estar yendo en la dirección correcta externamente, internamente la moneda está teniendo problemas. El código de DigiShield que utilizamos para proteger contra los mineros que sabotean la moneda está siendo jugado por esos mismos mineros. Los mineros están esperando que la ecuación matemática sea muy fácil, y luego lanzan toda su potencia de cálculo a la moneda en un intento de extraer más monedas. Cuando los mineros cambian el poder de cómputo hacia Nautiluscoin, DigiShield comienza a hacer la ecuación más difícil y los mineros se retiran. El problema ocurre cuando los mineros se retiran. La ecuación matemática se mantiene difícil durante un período demasiado largo, y sin la potencia extra de extracción, las transacciones no se procesan. En lugar de tomarse un minuto para procesar las transacciones, lleva horas.

Hay dos soluciones al problema. El primero es para mí convertirme en minero y mantener la red. El mayor obstáculo aquí es que no tengo las computadoras mineras de alta potencia, y si lo hiciera, ¡no estoy seguro de que sabría cómo operarlas! La otra solución es pasar de la prueba de trabajo a la prueba de participación. En la prueba de participación, los mineros son reemplazados por los titulares de la moneda, siempre que puedan demostrar que han retenido la moneda, luego su computadora se utiliza para procesar las transacciones. Me inclino a avanzar hacia la prueba de participación, ya que permite a Nautiluscoin pagar un "dividendo".

Dado que mi objetivo es hacer de Nautiluscoin la inversión elegida por los inversores profesionales que ingresan al espacio de moneda digital, creo que la prueba de participación y el "dividendo" serán fáciles de entender. Además, significa que la moneda no está a merced de los mineros.

5 de julio de 2014-Es el día de la gran pelea, y aunque no recaudamos el equivalente de $ 10,000, Jon Fitch ha decidido cubrir la otra mitad y hacer de Nautiluscoin su principal patrocinador para esta pelea. Esperaba tener el nuevo

> código de prueba de participación implementado por ahora, pero está tardando más de lo esperado. No obstante, el precio de la moneda se ha disparado, y en 60 días hemos alcanzado un límite de mercado de $ 1 millón, y Nautiluscoin es la moneda digital número 35 más valiosa en el mundo entre más de 300 monedas.
>
> Este parece ser un lugar apropiado para terminar este diario. Ha sido un lanzamiento exitoso, y no podría estar más feliz con el apoyo que Nautiluscoin ha recibido. La comunidad construida alrededor de la moneda es tremenda, y he aprendido que construir una comunidad fuerte es esencial para lograr el éxito.
>
> Si bien hemos logrado que Nautiluscoin sea reconocido, aún queda mucho trabajo por hacer. El siguiente paso es construir el ecosistema Nautiluscoin: esto llevará a toda la comunidad a lograrlo. Actualmente hay dos proyectos que conozco que se están construyendo en torno a Nautiluscoin como medio exclusivo de pago.
>
> El desafío para mí ahora es construir una economía esencialmente desde cero. Esta tarea es estimulante y desalentadora...

7.3- ¿Funcionó?

La creación de Nautiluscoin comenzó con mi deseo de probar la hipótesis económica de Friedrich Hayek. Las monedas digitales son el laboratorio perfecto para poner a prueba su afirmación de que los consumidores y los comerciantes gravitarán hacia la moneda más estable. En el caso de Nautiluscoin, hubo algunos éxitos y fracasos. Nautiluscoin creció con éxito de decenas de miles de líneas de código a una de las monedas digitales más valiosas que existen. A partir del 1 de mayo de 2014, Nautiluscoin tenía una capitalización de mercado de $ 0, y solo una cotización estaba cotizando la moneda. La comunidad especulativa de moneda digital adoptó la idea de una moneda estable y empujó a Nautiluscoin a $ 1 millón en capitalización de mercado en julio de 2014. En 60 días, ocho intercambios diferentes cambiaron a Nautiluscoin y varias otras monedas se desarrollaron para negociar exclusivamente con Nautiluscoin. En mi opinión, esto es extraordinario e ilustra que hay algo de mérito en la afirmación de Hayek.

Sin embargo, no pude reconocer el impacto de los mineros que venden Nautiluscoin para obtener una ganancia rápida. Supuse incorrectamente que todos los titulares de la moneda tenían el mismo horizonte de tiempo y el mismo motivo de tenencia. Esta suposición falsa hizo Nautiluscoin mucho más volátil de lo que esperaba. Sin embargo, mi error en la lógica no hace que todo el experimento sea un fracaso; simplemente significa que, en el futuro, el fondo de estabilidad debe tener en cuenta a todas las partes interesadas en Nautiluscoin. En varias ocasiones, el fondo de estabilidad pudo detener una caída vertiginosa del precio. El simple hecho de colocar una gran orden de compra en los intercambios hizo que los vendedores ajustaran su comportamiento.

Al construir la economía de Nautiluscoin, el fondo de estabilidad se modificará con las lecciones aprendidas en esta fase inicial. En particular, el papel de los mineros puede eliminarse cambiando el código a lo que se conoce como prueba de participación. En un sistema de prueba de participación, los titulares de la moneda hacen la extracción. De hecho, uno debe tener monedas en su billetera para demostrar que tiene una participación en Nautiluscoin, y solo entonces se les permite verificar y procesar las transacciones. Un sistema de prueba de participación premia a los titulares de las monedas por procesar las transacciones y elimina a los mineros. Otra característica del sistema de prueba de participación es que se puede pagar un "dividendo". Es decir que si un individuo retiene la moneda durante un período de tiempo predeterminado y participa en el

procesamiento de las transacciones, se le paga en monedas recién acuñadas, también conocido como "dividendo".

La economía de Nautiluscoin se construirá alrededor de una moneda estable. La fase inicial se transformó en algo mucho más que un experimento. Hay suficiente evidencia para sugerir que la afirmación de Hayek sí cambió el comportamiento humano. Ahora la tarea es construir una economía alrededor de este hallazgo y explorar más a fondo la función del mundo real de esta teoría.

Capítulo 8

La verdad es que ninguna base de datos en línea reemplazará su periódico diario.

-Clifford Stoll, Newsweek, 1995

8.1- Construyendo la economía Nautiluscoin

Las monedas han evolucionado en los últimos cinco milenios desde los productos respaldados por el respaldo del gobierno. Las conchas marinas, pieles de animales y rocas brillantes han servido como moneda y el tercero de facto de confianza. A medida que los gobiernos ganaron riqueza y poder, reemplazaron a las mercancías como intermediarios. Sin embargo, la tentación de devaluar las monedas fiduciarias ha demostrado ser el talón de Aquiles de todos los medios de cambio respaldados por el gobierno. Esta amenaza de devaluación hace que la moneda fiduciaria sea un depósito de valor inferior. Desde la crisis financiera de 2008, muchos inversores han vuelto a la protección del oro como una reserva de valor.

Si bien el oro tiene una larga historia de aceptación como medio de intercambio, su valor se basa completamente en la creencia de que puede convertirse en un fiat y ser aceptado para los bienes y servicios. Puede haber un valor de escasez de oro, pero como lo demuestra la desaparición de wampum, la escasez no es el principal impulsor de una moneda basada en los productos básicos. Cuando los operadores globales necesitaban realizar transacciones fuera de América del Norte, rápidamente abandonaron wampum a favor de una moneda que fue ampliamente aceptada. Curiosamente, a pesar de la creencia en el oro como moneda, no es ampliamente aceptado por los comerciantes. De hecho, las monedas digitales se aceptan de manera más amplia que el oro y se transportan fácilmente.

Los atributos de la aceptación comercial global y el fácil transporte convierten a las monedas digitales en un sustituto ideal no solo para el oro sino también para las monedas fiduciarias. Para ser claros, las monedas digitales no necesitan reemplazar el oro o el fiat para tener éxito, simplemente necesitan competir y complementar los medios de intercambio existentes. Si las monedas digitales solo pueden tomar una fracción de la cuota de mercado actualmente en manos del oro y del fiat, entonces serán un éxito rotundo.

Nautiluscoin fue creado para resolver un problema y probar una hipótesis. El problema para el que fue diseñado fue mi falta de conocimiento sobre el funcionamiento interno de las monedas digitales. Antes de crear Nautiluscoin, tenía muy poco conocimiento de las funciones hash y de los algoritmos criptográficos seguros. Necesitaba ensuciarme las manos y aprender el oficio. Lo que no anticipé es cuánto absorbería. Como parte de la creación de Nautiluscoin, decidí probar la hipótesis de Friedrich Hayek sobre las monedas privadas. En particular, quería poner a prueba su afirmación de que la moneda más estable sería la moneda más atractiva. Durante la fase inicial del experimento, descubrí que Hayek estaba realmente interesado en algo, ya que los inversores adoptaron la idea de una moneda estable.

Ahora que he establecido un mercado líquido y relativamente estable, la próxima tarea es desarrollar una economía en torno a esta moneda. Esto está rezagado de cómo se han desarrollado las economías tradicionales y los medios de intercambio. Por lo general, una economía se desarrolla en torno al sistema de trueque y luego avanza lentamente hacia una economía basada en la moneda. En este caso, tengo una moneda en busca de una economía. Supongo que podría sacar un anuncio personal para Nautiluscoin que diga algo como esto:

NUEVO NIÑO EN EL BLOQUE, BUSCANDO EL ECOSISTEMA CORRECTO

Tengo una personalidad relativamente estable y disfruto de carreras largas para aumentar mi poder adquisitivo. Estoy lo suficientemente seguro para usarlo en transacciones serias y estoy buscando una relación profesional.

-GetNauti

Utilizando el método de anuncio personal, Nautiluscoin puede encontrar una combinación económica o podría ir en interminables fechas improductivas. La alternativa es ir orgánica y permitir que el ecosistema correcto se desarrolle en torno a esta personalidad estable. Crear un ambiente fértil para que una economía se desarrolle requiere la búsqueda continua de la estabilidad.

La búsqueda de la estabilidad no se trata solo de reducir las fluctuaciones diarias de los precios. Para que Nautiluscoin sea verdaderamente exitoso, debe preservar e incrementar el poder adquisitivo. La estabilidad diaria de precios es importante para los consumidores y los comerciantes para realizar transacciones, pero el éxito a largo plazo de cualquier moneda es una función del poder adquisitivo. Si los usuarios de una moneda creen que su capacidad para comprar bienes y servicios en el futuro disminuirá, entonces es menos probable que tengan y usen la moneda. Hay innumerables ejemplos de monedas soberanas que han seguido el camino del pájaro dodo debido a una política monetaria débil. Por lo tanto, el objetivo más importante para Nautiluscoin será mantener una moneda fuerte con un poder adquisitivo estable y creciente.

Con el fin de lograr nuestro objetivo de moneda fuerte, Nautiluscoin competirá con la economía. Tradicionalmente, los bancos centrales con una política cambiaria fuerte tienen la responsabilidad de proporcionar un ancla para la economía mediante el uso de objetivos de oferta monetaria, objetivos de tasas de interés y / o objetivos de tipo de cambio. La historia económica ha demostrado que estos objetivos requieren que el banco central tenga recursos significativos para lograr los objetivos de manera creíble. La mayoría de las políticas de segmentación exitosas se basan en un recurso ilimitado, que es clásicamente la capacidad de imprimir o pedir prestado dinero. En el caso de Nautiluscoin, el suministro de dinero está fijado por el código de software y no existen mercados de deuda pública para usar como objetivos de tasa de interés. Sin embargo, esto no significa que le falten flechas en el carcaj.

Debido a que el suministro de dinero se fija y se libera con el tiempo, tenemos la capacidad de establecer la tasa de crecimiento de la oferta monetaria. Además, la red de Nautiluscoin se protegerá mediante el método de prueba de participación, lo que nos permite pagar intereses a aquellos que deseen tener Nautiluscoins. Finalmente, el proceso de extracción nos permite respaldar el tipo de cambio mediante el uso de ganancias mineras para comprar Nautiluscoin. Usando estas tres flechas, Nautiluscoin competirá con la economía del sonido y se convertirá en la moneda digital de "blue-chip".

8.2- Prueba de participación dinámica

Actualmente, Nautiluscoin usa un método de prueba de trabajo (PoW) para verificar y transmitir transacciones que son similares a Bitcoin. Los métodos PoW requieren que los mineros resuelvan una ecuación matemática muy difícil para procesar transacciones; por su esfuerzo, son recompensados con Nautiluscoins recién acuñadas. En un sistema de prueba de participación

(PoS), los titulares de las monedas desempeñan el papel del banquero / minero, y son estos titulares quienes son recompensados con monedas recién acuñadas.

Por ejemplo, supongamos que un comerciante tiene 10,000 Nautiluscoins que recibió de la venta de un producto. En un sistema PoS, ella es recompensada por sostener esas monedas y transmitir su propiedad a la red. La difusión de la propiedad se almacena en el blockchain y se utiliza para verificar una transacción válida cuando elige gastar Nautiluscoins. En la práctica, el comerciante puede mantener las monedas en su billetera durante siete días; esta información se registra para que todos sepan que estas monedas pertenecen al comerciante. La información sobre su participación en las monedas es valiosa para la red, y este valor se recompensa con más monedas. En este caso, después de siete días, el comerciante puede recibir 1,000 Nautiluscoins más, lo que haría que sus tenencias netas sean 11,000 Nautiluscoins. De esta forma, el comerciante recibió un pago de intereses del 10 por ciento en siete días, lo cual no está nada mal. Al mismo tiempo, el "banco central", que es el código informático, ha aumentado el suministro de dinero en 1.000 Nautiluscoins.

Siguiendo con este ejemplo, se deduce que si el poder adquisitivo de Nautiluscoin se ha mantenido estable o aumentado, entonces el comerciante ha recibido un beneficio económico al ayudar a verificar y procesar las transacciones. Si el poder adquisitivo aumenta y el comerciante recibió un pago de intereses, entonces se le puede alentar a gastar el ingreso adicional. Es este ciclo de incentivo y retroalimentación el que se utilizará para apuntar a una tasa de crecimiento para la economía de Nautiluscoin.

Nautiluscoin Producto interno bruto objetivo

El objetivo de todos los bancos centrales es promover el crecimiento económico. Por lo general, los banqueros centrales eligen un objetivo de pleno empleo y estabilidad del nivel de precios para apuntar a una tasa de crecimiento económico. En términos simples, la cadena de causalidad para la política monetaria se parece al gráfico que se muestra en la Figura 8.1.

La suposición simple en este modelo básico de banca central es que el crecimiento de la oferta monetaria tiene un impacto lineal directo sobre el crecimiento económico. La experiencia del mundo real refuta esta suposición y sugiere que la relación es dinámica. Además, el objetivo de aumentar la oferta monetaria puede definirse mejor como el aumento del poder adquisitivo. Por ejemplo, si un paquete de chicle cuesta $ 1 hoy y la Reserva Federal de EE. UU. Dobla el suministro de dinero de la noche a la mañana, el paquete de chicle puede costar $ 2 mañana. Al mismo tiempo, sin embargo, los consumidores tienen el doble de la cantidad de dinero, lo que significa que el paquete de $ 2 de goma cuesta lo mismo que el paquete de $ 1 de goma de mascar. Si un consumidor tiene solo $ 1 hoy y le dan otro $ 1 durante la noche, y el precio del chicle aumenta a $ 2, el consumidor tiene exactamente el mismo poder adquisitivo que el día anterior.

La relación dinámica no lineal entre el suministro de dinero y el crecimiento económico es la razón por la cual la oferta monetaria de Nautiluscoin se ajustará dinámicamente al crecimiento de la economía. Una característica única de las monedas digitales es que cada vez que se procesa un bloque de transacciones, el software registra el número de transacciones que se han producido. Nautiluscoin procesa un bloque de transacciones por minuto, lo que significa que cada 60 segundos podremos saber si la economía está creciendo o desacelerándose. El rico conjunto de datos es una ventaja masiva sobre las monedas fiduciarias y permite un conjunto predeterminado de reglas para controlar la oferta de dinero.

No es práctico ni deseable ajustar de manera funcional la oferta de dinero cada minuto ya que la volatilidad en la cantidad de transacción generaría demasiado ruido para tomar una decisión

informada. En el caso de Nautiluscoin, una vez al mes se analizará el volumen de transacciones para determinar si la economía está creciendo o disminuyendo. Si la economía está creciendo a la tasa meta o cerca de ella, entonces la oferta monetaria se mantendrá sin cambios. Sin embargo, si la economía se desacelera, la oferta monetaria se ajustará para aumentar el poder adquisitivo.

Figura 8.1: Cadena de causalidad para la política monetaria

Este tipo de enfoque algorítmico de la política monetaria rara vez ha sido probado en el mundo real y vive principalmente en libros de texto económicos. Una vez más, las monedas digitales están liderando el camino como el laboratorio perfecto para experimentar con la política monetaria algorítmica.

Política monetaria algorítmica

En el caso de la economía Nautiluscoin, el objetivo de la política monetaria será aumentar o disminuir el poder adquisitivo en respuesta a la fortaleza o debilidad relativa de la economía. Con ese fin, el objetivo inicial para el crecimiento económico de Nautiluscoin se establecerá en 5 por ciento anual. Si el crecimiento económico no alcanza este objetivo, la tasa de interés y la oferta monetaria se ajustarán para aumentar el poder adquisitivo.

Funcionalmente, cómo funcionará esto puede parecer contradictorio, ya que aumentar el poder adquisitivo significa elevar las tasas de interés. Recuerde que el pago de intereses se realiza a quienes poseen y poseen Nautiluscoin; por lo tanto, elevar la tasa de interés alentará a más usuarios a comprar y mantener Nautiluscoin. Los nuevos compradores atraídos por la mayor tasa de interés también deben mantener sus monedas durante un período de tiempo predeterminado. Este período de retención eliminará el suministro de los mercados de tipos de cambio y, junto con los nuevos compradores sensibles a las tasas de interés, debería aumentar el precio de Nautiluscoin. De esta forma, elevar las tasas de interés no solo aumenta la oferta monetaria, sino que también aumenta la tasa de cambio, lo que en conjunto generará un aumento en el poder adquisitivo.

Si la economía crece más rápido que la tasa objetivo, entonces las tasas de interés disminuirán. Disminuir la tasa de interés reduce el crecimiento de la oferta de dinero y puede alentar a algunos tenedores a vender sus monedas. A medida que los titulares sensibles a la tasa de interés reducen la exposición, la tasa de cambio debería caer, lo que da como resultado una disminución del poder adquisitivo. El objetivo de la política monetaria algorítmica dinámica es crear un patrón de crecimiento económico sin problemas a largo plazo, como se muestra en la Figura 8.2.

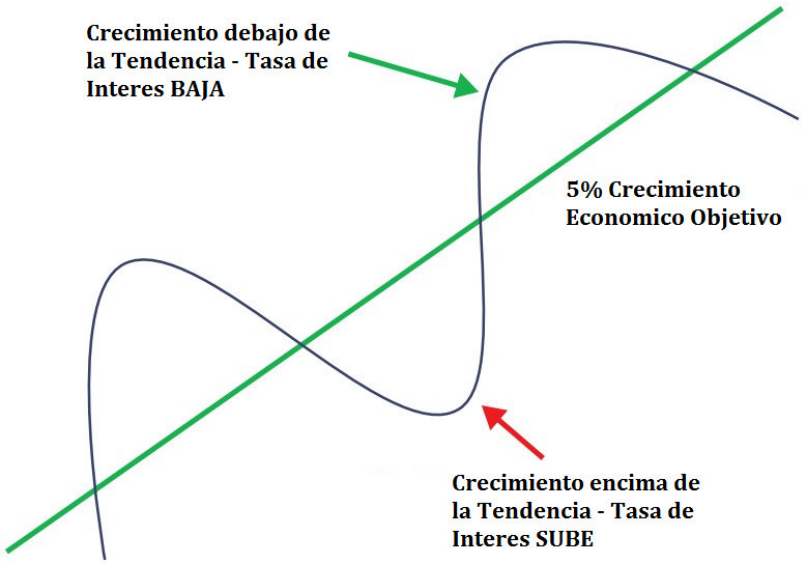

Figura 8.2: La política monetaria algorítmica dinámica crea un patrón de crecimiento económico uniforme en el largo plazo

Este sistema de PoS dinámico es posible solo porque el software de moneda digital registra constantemente la transacción que tiene lugar en la economía de Nautiluscoin. Actualmente, los bancos centrales confían en las agencias gubernamentales para recopilar y estimar datos económicos. Típicamente, este proceso se caracteriza por ajustes frecuentes de los datos por un único punto de falla. Si el Departamento de Trabajo de EE. UU. Calcula mal la tasa de desempleo, la política monetaria podría volverse inútil. Con las monedas digitales, los datos sobre la economía son continuos y seguros. Eso no quiere decir que las monedas digitales puedan mejorar la política monetaria, solo que el conjunto de datos es más preciso.

8.3- Otras herramientas políticas

Además del sistema de PoS dinámico que se implementará en Nautiluscoin, hay otras dos herramientas que se pueden utilizar para promover el crecimiento económico y el poder adquisitivo. La primera de estas herramientas ya existe en forma del Fondo de Estabilidad Nautiluscoin (NSF), mientras que la segunda herramienta, un multipool PoS, se implementará con el cambio al sistema de PoS dinámico.

El NSF fue concebido para estabilizar el precio de Nautiluscoin y, en última instancia, aumentar el poder adquisitivo de los usuarios y los titulares de la moneda. Sin embargo, descubrí un error en mi lógica cuando los mineros comenzaron a vender indiscriminadamente sus tenencias de Nautiluscoin. Supuse incorrectamente que todos los titulares de la moneda tenían la misma motivación, es decir, que estaban sosteniendo la moneda para obtener un retorno de la inversión. No tuve en cuenta el hecho de que la motivación de los mineros es convertir la moneda digital a fiat lo más rápido posible para financiar la operación minera.

El cambio a un sistema PoS eliminará a los mineros y permitirá que la NSF cumpla con su función de un tope de velocidad para una volatilidad excesiva. La NSF funcionará de manera similar a como lo hace un creador de mercado en los mercados financieros. El fondo proporcionará liquidez cuando sea necesario, con el objetivo de respaldar continuamente el poder adquisitivo. La operación de la NSF en los mercados de tasa de cambio no elimina el potencial de pánico o euforia;

esas son cualidades exclusivamente humanas. Sin embargo, la NSF puede proporcionar un nivel imparcial de cabeza durante tiempos de comportamiento humano extremo.

La segunda herramienta que se utilizará es un PoS multipool. Aunque el método PoS elimina la extracción, no nos impide extraer otras monedas digitales. Recuerde que un grupo de minería es un grupo de mineros que combinan recursos informáticos. La combinación es más poderosa que los mineros individuales y, por lo tanto, aumenta las posibilidades de ser el primero en resolver el problema matemático y recibir la recompensa.

Originalmente, los fondos mineros se centraban en una moneda y, por lo tanto, los beneficios eran una función de la fluctuación en el precio de la moneda. Eventualmente, los mineros desarrollaron pools multinúcleo como una forma de aumentar la rentabilidad y reducir la exposición a las fluctuaciones de la tasa de cambio. Un grupo multinúcleo utiliza un algoritmo para extraer las monedas más rentables. El algoritmo calcula las probabilidades de éxito para resolver el problema matemático y el precio al que se pueden vender las monedas de recompensa. Estos grupos multinúcleo están cambiando constantemente las operaciones mineras entre las monedas más rentables.

En un pool multinivel típico, los beneficios de la moneda se convierten inmediatamente en bitcoins o en moneda fiduciaria para que la operación minera pueda seguir siendo financiada. Un multipool PoS no convierte las ganancias de la moneda en moneda fiduciaria; en cambio, usa los beneficios para comprar la moneda PoS. En el caso de Nautiluscoin, un multipool minará otras monedas y las ganancias se usarán para comprar Nautiluscoin. De esta forma, habrá un flujo continuo de compras en el mercado de tasa de cambio. Este flujo continuo de compras combinado con la operación NSF debería proporcionar una poderosa herramienta para aumentar el poder adquisitivo.

8.4- Alternativa al oro

A medida que se implementen las herramientas de política monetaria, Nautiluscoin debería atraer la atracción tanto de los comerciantes como de los consumidores. La amplia aceptación de Nautiluscoin por los bienes y servicios le dará una clara ventaja sobre el oro. Además, el enfoque de tres flechas para la política monetaria algorítmica podría proporcionar a Nautiluscoin más estabilidad que el oro. Con ese fin, a medida que se desarrollen los mercados, la NSF se utilizará para mantener la volatilidad de Nautiluscoin por debajo de la volatilidad del oro. La baja volatilidad, el aumento del poder de compra y la aceptación del comerciante, permitirán a Nautiluscoin competir contra el oro como moneda alternativa.

La capacidad de Nautiluscoin para tomar cuota de mercado del oro tendrá un impacto dramático en el precio de la moneda y, por extensión, su poder adquisitivo. A partir de 2013, se estima que ha habido 171,000 toneladas de oro extraídas en la historia del mundo. Como el oro no se deteriora, todo este oro aún existe. En una tonelada de oro, hay 35,274 onzas, lo que significa que a $ 1,300 por onza el valor total de todo el oro en el mundo es de $ 7,8 billones de dólares.

La propuesta de valor de Nautiluscoin es que no se deteriora, tiene una política monetaria que mejora su función como depósito de valor y puede utilizarse como un medio de intercambio. El oro no tiene una política monetaria de apoyo; de hecho, el valor del oro es una función de la percepción. Además, como medio de intercambio, el oro se queda corto ya que muy pocos comerciantes aceptan el oro directamente. La propuesta de valor permitirá a Nautiluscoin competir por la cuota de mercado con oro.

La Tabla 8.1 ilustra el valor implícito de Nautiluscoin en diferentes niveles de participación en el mercado del oro.

Si Nautiluscoin atrae solo el 1.0 por ciento del valor del oro, entonces el precio implícito de Nautiluscoin es de $ 15,682. Es decir, si el 1 por ciento de los tenedores de oro decide que Nautiluscoin es una mejor reserva de valor y decide convertir su oro en Nautiluscoin, la valuación implícita sería superior a $ 15,000 (suponiendo un total de 5 millones de monedas).

Cuadro 8.1: Valor Implicito de Nautiluscoin

Porcentaje Participacion Mercado	Participacion Mercado en USD	Valor Implicito en Nautiluscoin
0.10%	$7.8 mil millones	$1,568.20
0.50%	$39.2 mil millones	$7,841.00
1.00%	78.4 mil millones	$15,682

¿Podría ocurrir este aumento en el valor de mercado? Si la hipótesis de Hayek es correcta y la política monetaria algorítmica es efectiva, entonces es posible atraer una parte de los dólares de inversión del oro. Dado que todas las monedas son una cuestión de fe, puede tomar algún esfuerzo mover esos dólares de inversión. Sin embargo, a medida que los mercados se desarrollan y la regulación atrae a los inversores institucionales, la probabilidad de éxito debería aumentar.

8.5- Dinero, hecho mejor

En última instancia, el impacto de todas estas herramientas de política monetaria será proporcionar el terreno fértil para que una economía se construya en torno a una moneda que sea económicamente sólida con una política transparente. Sin duda, la economía es más que una política monetaria algorítmica y un poder adquisitivo cada vez mayor. En esencia, la economía es una ciencia social que busca influir en el comportamiento humano. Como participante de 20 años en los mercados financieros, soy escéptico de que el comportamiento humano pueda controlarse. Sin embargo, al igual que la mariposa que bate sus alas y causa un huracán, pequeños cambios en la política monetaria pueden tener un impacto a corto plazo en el comportamiento humano.

La política monetaria fuerte de Nautiluscoin contará con el respaldo de tres herramientas para la política monetaria: prueba de participación dinámica, un fondo de estabilidad y un grupo de minería multinivel, como se muestra en la Figura 8.3.

Estas herramientas de política tienen dos canales por los que pueden influir en el poder adquisitivo; pueden operar a través del canal de tasa de cambio o el canal de tasa de interés. Debido a que Nautiluscoin no es una moneda de reserva, el determinante final del poder adquisitivo será la tasa de cambio con monedas fiduciarias y bitcoin.

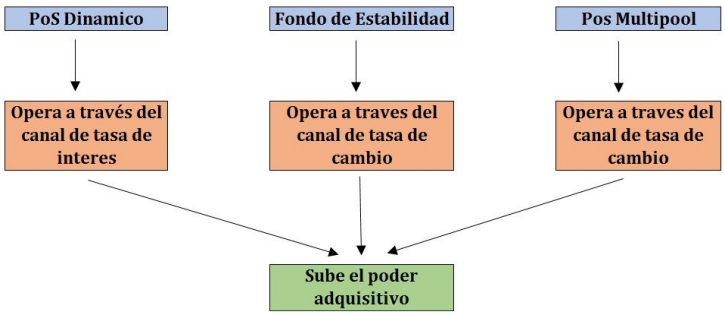

Figura 8.3: Herramientas Politicas de Nautiluscoin

A medida que se perfecciona la política, la hipótesis económica de Hayek sugiere que la aceptación del consumidor y del comerciante debería crecer. A medida que la aceptación crezca, el ecosistema debería seguir y el negocio específico de Nautiluscoin se puede formar en torno a este dinero estable y sólido. Si tiene éxito, Nautiluscoin no solo tendrá una economía sólida con un crecimiento constante, sino que también será un momento único en la historia económica en que se habrá implementado una teoría de la moneda privada.

8.6- Integración del mercado financiero

Como Nautiluscoin desarrolla su reputación como la moneda privada que es una alternativa al oro, también debe atraer la atención tanto de los comerciantes como de los consumidores. Ambos grupos de usuarios deberían gravitar hacia Nautiluscoin como una moneda estable con un poder adquisitivo creciente que beneficia a ambos. Sin embargo, Bitcoin tiene una ventaja significativa en toda la competencia de las transacciones minoristas tradicionales. Si bien Nautiluscoin puede competir tecnológicamente, el efecto de red de Bitcoin es una barrera formidable para la entrada. Por lo tanto, Nautiluscoin necesitará encontrar un nicho para competir.

El estado del dólar de EE. UU. Como moneda de reserva global lo ha convertido en la moneda de referencia para poner precio a los productos básicos internacionales y los mercados financieros. Sin embargo, la naturaleza centralizada actual de la red de dólares de EE. UU. Se caracteriza por intermediarios, comisiones bancarias y riesgo de tipo de cambio. Cada uno de estos puntos de fricción representa una razón por la cual el dólar de EE. UU. No es la moneda más apropiada para los mercados financieros internacionales. Además, cada uno de los puntos de fricción representa una oportunidad para Nautiluscoin.

Para entender cómo puede funcionar esto, usemos el ejemplo de un productor de petróleo en Canadá que quiere vender su petróleo a un comprador en China. Bajo el sistema actual, el precio global del petróleo se cotiza en dólares estadounidenses. El comprador chino debe convertir el renminbi en dólares estadounidenses para comprar el petróleo canadiense. Además, los productores de petróleo canadienses deben convertir esos dólares de EE. UU. En dólares canadienses para pagarles a sus empleados. Por supuesto, cada vez que se realiza una conversión de moneda, un banco internacional de divisas se coloca en el medio y cobra una tarifa. Además, el comprador y el vendedor están perdiendo dinero en el diferencial de compra / venta en los mercados de divisas extranjeras.

Si el precio global del petróleo se denominara en Nautiluscoin, entonces el comprador y el vendedor del petróleo podrían pasar por alto a muchos de los intermediarios en los mercados financieros internacionales. Sin duda, aún existiría un riesgo de tipo de cambio al convertir nuevamente a la moneda local, pero los tres mecanismos de estabilidad para Nautiluscoin deberían reducir ese riesgo. Además, se podría adjuntar un contrato inteligente a cada transacción que especifica cuándo y dónde se transfiere el valor. Cuando el petrolero llega al puerto chino, el contrato inteligente daría lugar al pago. Esto eliminaría el riesgo de que el comprador chino pague por el petróleo que nunca llega.

Para facilitar la integración de Nautiluscoin en los mercados financieros, necesitaremos establecer índices para usar como referencia. La función de estos índices será estandarizar los precios de los productos básicos y los mercados financieros mundiales de dólares estadounidenses a Nautiluscoin. De esta forma, podemos establecer un punto de referencia para el precio de los mercados financieros en moneda digital y eliminar parte de la fricción del sistema.

8.7- Derechos especiales de giro

El concepto de una moneda de reserva global se ha intentado anteriormente, específicamente con la creación de los Derechos Especiales de Giro (DEG) del Fondo Monetario Internacional (FMI). Creado en 1969 para ayudar a apoyar el Acuerdo de Bretton Woods de tipos de cambio fijos, los DEG permiten a los países miembros intercambiar libremente tenencias de DEG para monedas fiduciarias utilizables. Los DEG se diseñaron para ayudar a los países con fuertes finanzas a ayudar a los países con finanzas débiles y facilitar el flujo de divisas entre los miembros del FMI. Esto podría hacerse voluntariamente, o el FMI podría instruir a sus miembros a comprar SDR de países que necesitan divisas.

Las monedas digitales y los DEG comparten características comunes, en particular que ambos dependen de una red de usuarios dispuestos a aceptar la moneda a cambio de un bien o servicio. Sin embargo, los DEG están limitados por la falta de liquidez y el requisito de ser parte del FMI. Además, la centralización de la moneda dentro de la estructura del FMI no lo hace ideal para las transacciones internacionales. Finalmente, el propósito de los DEG era facilitar los préstamos entre los miembros del FMI, que es una función completamente diferente de una moneda de reserva mundial.

Las monedas digitales, específicamente Nautiluscoin, están en una posición única para resolver el problema de la fricción dentro de los mercados financieros internacionales.

8.8- ¿Por qué NAUT?

La etapa inicial del ecosistema de la moneda digital se ha caracterizado por nuevas monedas con mejoras tecnológicas. Si bien esta evolución tecnológica es necesaria, la competencia en este nicho es feroz. Afortunadamente, debido a la naturaleza de código abierto de las monedas digitales, Nautiluscoin puede adaptar la tecnología más prometedora. La gran y diversa comunidad que apoya a Bitcoin hace que sea difícil para esta moneda digital original ser flexible y adaptar las nuevas tecnologías. La flexibilidad es una ventaja para Nautiluscoin.

Además, la tradición del anonimato en las monedas digitales puede haber sido útil durante el desarrollo, pero la etapa de inversión profesional requerirá transparencia. Dada la creación de alto perfil de Nautiluscoin, goza de un nivel de transparencia que no tiene precedentes en las monedas digitales.

Finalmente, la economía de Nautiluscoin se construirá en torno a los sólidos principios económicos de una moneda estable y el aumento del poder adquisitivo. La política monetaria algorítmica única le dará a Nautiluscoin una ventaja económica sobre otras monedas digitales.

Si bien Nautiluscoin puede haber sido creado como un experimento, ha cobrado vida propia. Nautiluscoin ha tenido la suerte de contar con una comunidad fuerte y activa de inversionistas en divisas digitales que han ayudado a construir el ecosistema primitivo. Como administrador de este ecosistema, mi trabajo es posicionar a Nautiluscoin como la principal inversión en la clase de activos de moneda digital. El plan de negocios para Nautiluscoin se basa en los tres pilares de mejora continua, transparencia y economía sólida.

Capítulo 9

> Con e-currency basado en pruebas criptográficas, sin la necesidad de confiar en un tercero intermediario, el dinero puede ser seguro y las transacciones fáciles.
>
> -Satoshi Nakamoto

9.1- Invertir y tradear monedas alternativas

En el verano de 1944, mientras la guerra continuaba devastando Europa, 730 delegados de las 44 naciones aliadas se reunieron en las serenas Montañas Blancas de New Hampshire. La Conferencia de Bretton Woods, llamada así porque se celebró en el Hotel Mount Washington en Bretton Woods, New Hampshire, fue convocada para diseñar el sistema global de dinero después del final de la Segunda Guerra Mundial. Esta conferencia no solo estableció el Banco Mundial y el Fondo Monetario Internacional, también creó un sistema global de tipos de cambio fijos. Se consideró que el dólar de EE. UU. Era la moneda de reserva global, ya que se podía convertir directamente en oro. Todas las demás monedas se vincularon al dólar estadounidense para darles estabilidad.

En la relativa calma de la época de la posguerra, el sistema de Bretton Woods logró mantener la estabilidad monetaria mundial. El Plan Marshall permitió reconstruir tanto a Alemania como a Japón y creó una gran demanda para los productos estadounidenses y, por extensión, para el dólar de EE. UU. Sin embargo, el éxito del sistema de Bretton Woods sería su caída. Como resultado de la demanda de dólares de EE. UU., La moneda se sobrevaloró y Estados Unidos se volvió menos competitivo. En la primavera de 1971, Alemania Occidental fue el primer país en abandonar el sistema de tipo de cambio fijo y el valor del dólar cayó un 7,5 por ciento de mayo a julio de 1971. La caída del valor del dólar llevó a los países con grandes tenencias de dólares a convertir a oro Cuando Suiza y Francia canjearon una gran cantidad de dólares de EE. UU. Por oro, la presión se intensificó para devaluar el dólar de EE. UU. De hecho, el Congreso de EE. UU. Publicó un informe que recomendaba solo esta acción.

Durante una frenética reunión secreta en Camp David, el presidente Richard Nixon reunió a sus asesores, y llegaron a la conclusión de que Estados Unidos debería suspender unilateralmente la convertibilidad del dólar de EE. UU. En oro. El domingo 15 de agosto de 1971, el presidente Nixon tomó las ondas de televisión y anunció que había quitado a los Estados Unidos del patrón oro. Esta orden ejecutiva terminó efectivamente el Acuerdo de Bretton Woods.

Apodado el Nixon Shock, el colapso del Acuerdo de Bretton Woods significó que las monedas que alguna vez fueron vinculadas al dólar ahora son de libre flotación. Con los tipos de cambio flotantes vino el desarrollo de los mercados de divisas. Estos mercados no estaban regulados, fragmentados e ilíquidos según los estándares actuales. En particular, estas mismas características describen el estado actual de los mercados de divisas digitales. En los 40 años que siguieron al Acuerdo de Bretton Woods, el mercado de divisas se convirtió en el mayor mercado por volumen en todo el mundo. Durante este tiempo, las fortunas se han hecho y perdido, recuerdan el triunfo de mil millones de dólares de George Soros sobre el Banco de Inglaterra.

En su forma actual, el mercado de divisas digital se asemeja a los mercados de divisas fiduciarios durante la década de 1970: la fragmentación, la falta de liquidez y la falta de regulación fueron todas características de los mercados fiduciarios. A pesar de sus humildes comienzos, el mercado de divisas se convirtió en el financiero más grande y poderoso del mundo. De hecho, el Banco de Pagos Internacionales informó que en 2013 los mercados cambiarios intercambiaron $ 5.2

billones por día. En la actualidad, las monedas extranjeras representan una forma para que los inversionistas diversifiquen las tenencias de los mercados financieros tradicionales. Las monedas digitales tienen un potencial similar para convertirse no solo en un importante mercado financiero sino también en una nueva clase de inversión.

El Bitcoin Big Bang puede llegar a ser otro momento en la historia como el Nixon Shock. A medida que las economías de las monedas digitales evolucionen, se abrirán nuevas oportunidades de inversión. Las monedas digitales en realidad no son diferentes de sus primos fiduciarios: apoyan la transferencia de valor en una economía al proporcionar un medio de cambio, una unidad de cuenta y una reserva de valor. Además, a medida que los datos de estas economías digitales se hacen más accesibles, estas monedas digitales se pueden analizar de la misma manera que las monedas fiduciarias. No sería sorprendente ver que las monedas digitales se conviertan en una parte integral de la planificación de inversión.

Una nueva clase de inversión

En 1952, Harry Markowitz introdujo Portfolio Theory (ahora conocida como Modern Portfolio Theory), que sugería que los inversores deben tener en cuenta cómo fluctuaban cada una de sus inversiones. Markowitz demostró que los inversores que asignan fondos de inversión basados en el movimiento del precio relativo de una clase de activos con otra superarán a los inversores que simplemente se centraron en la selección de valores individuales. La teoría de la cartera moderna es la base de casi todos los modelos de asignación de activos actualmente en uso. En esencia, el principio sugiere que la volatilidad de una cartera de inversiones se puede reducir mezclando diferentes clases de activos juntos. Además, los inversores no solo deberían considerar el rendimiento absoluto sino también la cantidad de riesgo que se suponía que generaría el rendimiento de la inversión.

El modelo de asignación de activos más simple es la cartera 60/40, que coloca el 60 por ciento de los activos en acciones y el 40 por ciento de los activos en bonos. Usando esta fórmula para la asignación de activos, un inversor habría realizado un rendimiento del 10 por ciento anual entre 1990 y 2011 con una fluctuación de la cartera del 10 por ciento anual. Es decir, la cartera podría aumentar o disminuir su valor en un promedio del 10 por ciento en cualquier momento del año. En comparación, el S & P 500 generalmente fluctúa el 19 por ciento por año. La clave para reducir la volatilidad es crear una cartera de activos no correlacionados. Por ejemplo, utilizando el fondo cotizado SPDR S & P 500 (ETF; SPY) y el iShares 20+ US Treasury Bond ETF (TLT) como representantes de acciones y bonos, respectivamente, podemos crear un portafolio de $ 100,000 que se invierta $ 60,000 en SPY y $ 40,000 en TLT. Ver la Figura 9.1.

Figure 9.1: Un Portfolio de $100,000 que está invertido con $60,000 en SPY y $40,000 en TLT.

Desde 2010, la cartera 60/40 arrojó un promedio de 9,39 por ciento, mientras que la cartera de acciones solo obtuvo un promedio de 13,69 por ciento. Ver la Tabla 9.1.

Sin embargo, la cartera de acciones solo fue siete veces más volátil que la cartera que se asignó al mercado de bonos. Como sugirió Markowitz, esto se debe a que las acciones y los bonos son activos no correlacionados, cuando las acciones suben, los bonos tienden a caer y viceversa. Desafortunadamente, hay un error en la teoría moderna de la cartera que ha salido a la luz desde la Gran Recesión. Desde que la Reserva Federal se ha embarcado en la flexibilización cuantitativa, tanto las acciones como los bonos han aumentado juntos. En la práctica, esto significa que estas dos clases de activos ya no están correlacionadas y los beneficios de la diversificación se han reducido.

Cuadro 9.1: Retorno de la estrategia 60/40 y solo acciones

Year	60/40	SPY
2010	8.50%	11.79%
2011	11.02%	-0.20%
2012	7.41%	13.47%
2013	10.65%	29.69%
Retorno Promedio	9.39%	13.69%
Retorno por Volatilidad	1.73%	12.28%

The Wall Street Journal, CNBC y Burton Malkiel, el padre de Random Walk, han expresado su preocupación por la correlación cambiante. En una entrevista con CNBC, Malkiel declaró que la cartera 60/40 era francamente peligrosa en este entorno. Como muestra el gráfico de la Figura 9.2, la correlación de tres meses entre acciones y bonos se ha correlacionado positivamente, mientras que para una diversificación ideal, una correlación negativa es la mejor.

Figura 9.2: Correlación de 6 meses entre S&P 500 y Bono Tesoro 10 años

Cuadro 9.2: Correlación diaria del Bitcoin con otros Activos 2010-2013

S&P 500	Nasdaq Composite	Bono Tesoso 10 años	Oro
0.803	0.8419	0.3007	-0.692

En otras palabras, los bonos ya no brindan la protección de diversificación que alguna vez tuvieron. Bitcoin y las monedas digitales en general ofrecen una nueva clase de activos de rendimientos potencialmente no correlacionados, lo que podría aumentar la diversificación de la cartera. Consulte la Tabla 9.2 para la correlación diaria de Bitcoin con otros activos entre 2010 y 2013.

En los últimos tres años, la correlación de bitcoin y el S & P 500 se ha vuelto muy positiva, lo que indica que el bitcoin puede no ser una ayuda para la diversificación. Sin embargo, de septiembre a noviembre de 2012, el S & P 500 cayó casi un 7 por ciento, pero el precio del bitcoin aumentó un 17,3 por ciento. La divergencia en el rendimiento dio como resultado que la correlación entre el S & P 500 y el bitcoin se volviera negativa. La implicación es que la correlación altamente positiva actual puede ser simplemente una coincidencia. Sin duda, esto es evidencia anecdótica y el tamaño de la muestra es aún demasiado pequeño para hacer una declaración estadística sólida. No obstante, las economías emergentes de monedas digitales tienen el potencial de mejorar la diversificación de la cartera.

Esta nueva clase de inversión debe convertirse en su promesa, ya que actualmente carece de todo el potencial como dinero. En general, los economistas aceptan que el "dinero" tiene tres funciones: un medio de intercambio, un depósito de valor y una unidad de cuenta. Como medio de cambio, las monedas digitales cumplen con los requisitos de dinero; actualmente, más de 45,000 empresas aceptan Bitcoin. Las empresas emergentes aparecen cada día con el único propósito de facilitarles a los consumidores y comerciantes el uso de monedas digitales. Además, la aceptación de la moneda digital se acelerará con el efecto de red.

Una unidad de cuenta significa que se puede cambiar una cierta cantidad de dinero por una canasta de bienes. Por ejemplo, si su factura de comestibles es de $ 100 por semana, podría decir que las cuentas de 100 unidades de billetes de dólares para una canasta de comestibles. La trampa de todas las monedas fiduciarias o en papel es que la inflación erosiona el poder de compra, por lo que en 10 años su canasta de comestibles puede costar $ 200. Los economistas han argumentado que la inflación es el resultado de la creación de más unidades de cuenta; en otras palabras, imprimir más dinero proporciona un azúcar temporal alto a una economía en quiebra, pero finalmente conduce a la inflación. Argumentar la causa de la inflación está más allá del alcance de este libro; sin embargo, las monedas digitales hacen imposible imprimir más unidades. Recuerde que la minería libera lentamente nuevas unidades en el ecosistema. Es este flujo

constante de unidades lo que hace que las monedas digitales sean una opción superior como unidad de cuenta.

Algunos han argumentado que Bitcoin no es dinero real porque su precio fluctúa violentamente. Los detractores sostienen que la volatilidad impide que Bitcoin funcione como una reserva de valor. Sin embargo, los escépticos pasan por alto el hecho de que, como experimentamos inflación con papel moneda, la estabilidad de un dólar es una ilusión. Cualquiera que solía frecuentar una tienda de golosinas sabe que el dólar de EE. UU. No ha mantenido un valor estable. Debido a que la mayoría de las naciones desarrolladas experimentan una inflación de menos del 5 por ciento por año, los críticos tienen una amplia munición cuando el precio del bitcoin fluctúa del 5 al 10 por ciento por día. Sin embargo, con el tiempo, el dólar de EE. UU. Ha fallado como un depósito estable de valor, y la muerte por mil recortes de papel tiene el mismo resultado que un ataque cardíaco fatal.

La volatilidad del precio de bitcoin probablemente disminuirá con la aceptación, de hecho, el aumento del uso ya está teniendo un efecto de amortiguación. A medida que el precio se estabiliza, existe un fuerte argumento para que los productos mundiales tengan un precio en monedas digitales. Debido a que las monedas digitales no tienen un banco central o un gobierno adjunto, no existen obstáculos políticos o monetarios para la aceptación. Los productores de petróleo de Arabia Saudita acumulan miles de millones de dólares estadounidenses, pero no tienen control sobre la Reserva Federal o el Tesoro. En cualquier momento, las autoridades monetarias de EE. UU. Podrían decidir devaluar la moneda. Los que tienen miles de millones se verían desproporcionadamente lastimados. El suministro de dinero para monedas digitales se fija desde el momento en que se escribe el código. Eso no quiere decir que las fuerzas del mercado no puedan mover el precio de la moneda hacia arriba o hacia abajo debido a las fluctuaciones en la demanda, pero las autoridades monetarias no pueden cambiar la oferta.

La falta de una autoridad monetaria y la subsiguiente incapacidad para pagar impuestos en monedas digitales es otro argumento en contra de las monedas digitales como dinero "real". La réplica a esta crítica es que un ciudadano de Estados Unidos no puede pagar al IRS con yenes o euros, sin embargo, todavía son monedas. La autoridad para imponer impuestos depende de la aplicación de los derechos de propiedad, que normalmente es el papel de un gobierno central. Si los impuestos no se pagan, el gobierno tiene derecho a tomar su propiedad, ya sea un gravamen sobre su casa o un embargo sobre su salario. Si un comerciante trabaja y no recibe el pago, puede colocar un gravamen de comerciante, que será aplicado por los tribunales. Estas son las reglas que nosotros, como comunidad, hemos acordado vivir. Dado que Bitcoin no tiene un gobierno central o un ejército para hacer cumplir las reglas, nunca puede ser una moneda ... o eso dice el argumento.

Lo que se pasa por alto es que Bitcoin tiene su propio mecanismo de aplicación incorporado que de alguna manera puede ser superior a nuestro sistema actual. Dentro del protocolo Bitcoin hay una marca de tiempo que le permite programar en el momento en que se realiza el pago, muy similar a programar un pago en línea con su cuenta bancaria. Sin embargo, Bitcoin va un paso más allá y le permite adjuntar un contrato a ese pago, y tanto el contrato como el pago se registran en el libro mayor. Dado que las transacciones de bitcoin son irreversibles una vez que la transacción y el contrato están firmados y grabados digitalmente, no hay forma de incumplir el acuerdo.

Acordar pagar sus impuestos o una factura de un plomero es un contrato. Es posible que no lo haya firmado, pero todavía es ejecutable por el gobierno. Bitcoin elimina al intermediario (gobierno) y programa la ejecución del contrato (pago) directamente en el libro mayor. Este concepto es lo que se conoce como un contrato inteligente o propiedad inteligente. Aprenderemos mucho más sobre contratos inteligentes más adelante, pero por ahora es importante saber que el

aspecto de dinero inteligente de Bitcoin es lo que hace que la aplicación sea mejor que nuestro sistema actual.

Para estar seguro, Bitcoin es una moneda joven y una nueva tecnología, que es a la vez amenazante e intrigante. Wall Street siempre ha considerado favorablemente las nuevas tecnologías en otros campos, pero se adapta lentamente a los cambios estructurales dentro de su propia industria. Hubo un tiempo en que el comercio electrónico se consideró poco ético: se suponía que los "caballeros" debían comerciar por teléfono o cara a cara, pero ahora hay una carrera armamentista para crear los sistemas de comercio electrónico más grandes y rápidos.

La visión actual de Wall Street es que Bitcoin no es una moneda, pero podría ser una nueva clase de activos, que es el término de Wall Street que dice "podemos cobrar una tarifa" por esto. Si de hecho nace una nueva clase de activos, entonces hay nuevas divisiones para crear, nuevos informes de investigación para emitir, y servicios de asesoría para ser vendidos. En mi opinión, eventualmente habrá un fondo mutuo de divisas digital y su asesor financiero tendrá un gráfico circular realmente agradable que le mostrará cuánto debe invertir en monedas alternativas como clase de activos.

9.3- Valuación

Ya sea que las monedas digitales sean un nuevo tipo de activo o una moneda, aún deben valorarse. Dado que las monedas digitales no tienen un flujo de efectivo asociado (todavía), el uso de un análisis de flujo de efectivo descontado no es muy útil. Es mejor valorarlos como monedas tradicionales. Es decir, el valor debe reflejar el tamaño y el crecimiento de la economía subyacente. Dado que la aceptación del comerciante es un gran impulsor de valor, existe un aspecto de moneda emergente para las monedas digitales. Si consideramos que una moneda emergente es un proxy para el bien o servicio subyacente provisto, se deduce que a medida que el bien proporcionado por la economía emergente sea más ampliamente aceptado, el valor de la moneda emergente aumenta. Por ejemplo, mire el país de Chile, el mayor productor mundial de cobre. La superposición del peso chileno con el precio del cobre ilustra que el valor del peso chileno fluctúa casi directamente con el precio del cobre, como se muestra en la figura 9.3.

Las monedas digitales se pueden pensar de una manera similar. A medida que la economía subyacente crece, es decir, más comerciantes aceptan la moneda, el valor de la moneda debería crecer. En otras palabras, una mayor aceptación del comerciante proporciona una demanda natural de la moneda de los nuevos participantes en el mercado. La figura 9.4 ilustra que el precio de bitcoin ha aumentado con la cantidad de comerciantes que aceptan bitcoins. Las líneas suaves son un mecanismo de suavizado exponencial aplicado a cada serie. Las líneas de tendencia exponencial indican cuál está creciendo a un ritmo más rápido, el precio de bitcoin o la aceptación del comerciante.

Lo interesante es que la influencia de la aceptación del comerciante está disminuyendo. La línea punteada que sube rápidamente muestra que el precio se está apreciando a una tasa mucho más alta que el número de transacciones (línea suave). Utilizando este indicador simple, se puede concluir que el precio del bitcoin actualmente está impulsado por la especulación. Este fenómeno podría significar que el éxito de Bitcoin podría ser su desaparición, al menos en lo que se refiere al precio.

Figura 9.3: HGY100 Cobre - grafico diario.

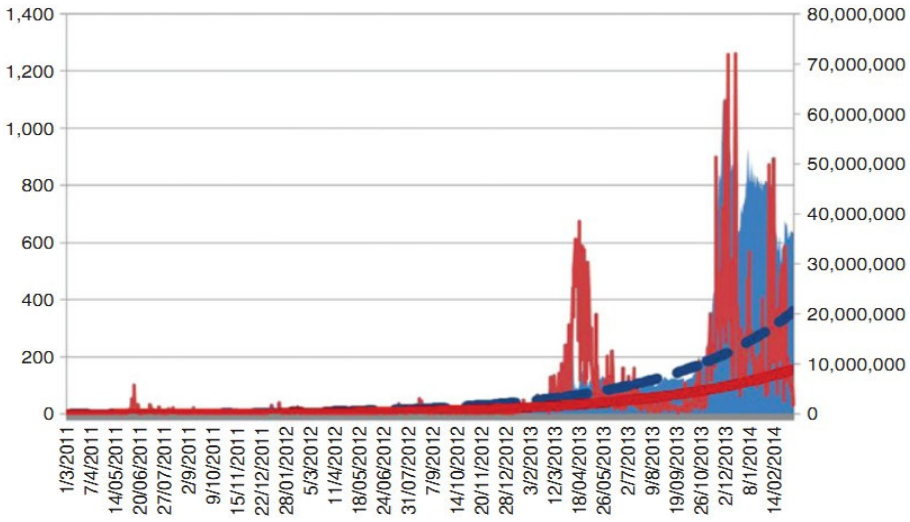

Figura 9.4: Precio en el Bitcoin sube

Para explorar por qué el éxito de Bitcoin podría ser perjudicial para el precio, supongamos, in extremis, que cada comerciante en el mundo acepta bitcoins y que cada consumidor tiene exactamente el número de bitcoins que desea. Bajo este escenario, la nueva demanda natural se evapora. Al mismo tiempo, la especulación será sofocada por la aceptación saturada del comerciante. Eliminar el soporte de estos dos compradores naturales podría tener un efecto perjudicial en el precio de bitcoin. Por supuesto, no sabemos cuándo ni dónde ocurrirá esto, podría suceder a $ 1,000 o $ 1 millón.

Esto trae a colación un punto interesante sobre Bitcoin que lo prepara para una burbuja. Al realizar transacciones, los consumidores y comerciantes no se preocupan por el precio del bitcoin, lo importante es que, durante el tiempo en que transfieren el valor, el precio se mantenga estable. Esto significa que los compradores principales de bitcoin en este momento (los consumidores) son independientes de los precios. Los compradores que son agnósticos al precio son un bloque de construcción de una burbuja. Además, existe una infraestructura emergente que respalda el comercio de márgenes, que es otro ingrediente esencial para una burbuja especulativa. La combinación de compradores que son independientes del precio y la capacidad de los especuladores para usar el crédito para comprar es en lo que se basan todas las burbujas. Es muy

probable que el bitcoin alcance las condiciones de burbuja en algún momento de su vida -todos los mercados lo hacen-, ya que es un hecho indiscutible que los humanos extrapolan las tendencias actuales en el futuro, a menudo con un crecimiento exponencial. En algún punto, estas expectativas se vuelven tan divorciadas de la realidad económica que surge la burbuja.

¿Ha comenzado la burbuja? Nop. La aceptación del comerciante está creciendo, pero ni siquiera está cerca de completarse; por lo tanto, el precio de bitcoin tiene un largo camino por recorrer antes de que las expectativas puedan separarse de la realidad. Esto también significa que hay tiempo para que los inversionistas agreguen monedas digitales a su cartera, lo que implica lidiar con un intercambio o un vehículo de inversión privada. El Bitcoin Investment Trust es uno de los vehículos de inversión privada para bitcoin y ha publicado una tabla interesante sobre el potencial al alza de la valoración de bitcoin, que se muestra en la Tabla 9.3.

Esta comparación de valuación ilustra claramente el increíble potencial alcista para el precio de bitcoin. Usando suposiciones conservadoras, la valoración de bitcoin tiene el potencial de aumentar de 10 a 100 veces su valor actual. Esta comparación de valoración también se puede usar para evaluar otras monedas digitales. Bitcoin puede tener el efecto de red como viento de cola, pero eso no significa que otra moneda digital no pueda derrocar al rey reinante. A modo de comparación, Google es una de las compañías más grandes del mundo y líder indiscutible de la búsqueda en Internet. Esta compañía, que es omnipresente en nuestras vidas, ni siquiera existía cuando Internet se hizo popular en 1994. De hecho, en 1999, Google tenía solo ocho empleados. Si consideramos Bitcoin como una prueba de concepto, entonces es más fácil ver cómo una nueva moneda digital podría convertirse en el líder.

Cuadro 9.3: Potencial alza de la valuación del Bitcoin

Bitcoin al alza...			
Si Bitcoin es igual al valor de...	**Base de Comparaion**	**Valor Actual**	**Precio Implicito del Bitcoin**
Paypal	Lider de pago online	$30 mil millones	$3,750
Base monetaria de Turquia	Divisa de mercado emergente	$96 mil millones	$12,015
5% del oro	Reserva de valor global	$376 mil millones	$47,010
Valuacion Actual Bitcoin		$8 mil millones	-600

En este punto, puede estar buscando su chequera, listo para invertir en la moneda digital que puede convertirse en el próximo Google. Bueno, frenar, vaquero. Invertir en monedas digitales requiere algunos pasos para ingresar al ecosistema. En primer lugar, deberá convertir su moneda fiduciaria (dólares, euros, yen, etc.) en monedas digitales, lo que se puede hacer en algunos servicios de bolsas y monederos. Una vez que tiene bitcoin, comprar y vender otras monedas digitales es tan fácil como ingresar una orden para comprar las acciones de Google.

Intercambios (Exchanges)

Los intercambios de divisas digitales actúan como un intermediario y un intercambio. Además, se pueden dividir en intercambios solo de bitcoin e intercambios de divisas alternativos (también conocidos como intercambios de monedas alternativas). Los intercambios solo de bitcoin hacen exactamente lo que parece, solo intercambian Bitcoin. Bueno, en realidad, generalmente intercambian algunas de las monedas alternativas más grandes, como Litecoin y Ripple. Los intercambios de divisas alternativos negocian todo lo demás, como Nautiluscoin.

Para comprar Bitcoin necesitará usar un servicio de billetera / monedero digital como Coinbase y depositar monedas fiduciarias. Una vez que se acepte su depósito, puede comprar bitcoins. Como titular de bitcoins, ahora forma parte del ecosistema de moneda digital y puede enviar esos

bitcoins a cualquier intercambio que elija. Una vez en el intercambio, puede comprar una gran cantidad de monedas digitales usando bitcoins. La mayoría de los mercados de valores cotizan monedas digitales en bitcoin o Litecoin, pero a medida que el ecosistema ha crecido, algunas otras monedas se están utilizando para valorar las monedas digitales. Por ejemplo, AllCrypt cotiza varias monedas digitales en términos de Nautiluscoin.

Mientras estamos en el tema de los intercambios, hablemos de los más infames: Mt Gox. En su apogeo, el intercambio de Mt Gox fue el mayor intercambio de bitcoins en el mundo, y su implosión le costó a la gente millones de dólares. ¿Recuerdas cuando hicimos alusión a las billeteras frías y calientes en un capítulo anterior? Seguro lo haces. Bueno, aquí es donde juegan un papel.

Una billetera caliente es una billetera de moneda digital que está conectada a Internet. Esto le permite enviar cualquier moneda digital a través de Internet en cuestión de segundos. El riesgo es que estar conectado a Internet expone la billetera a los piratas informáticos. Esta es la razón por la cual la mayoría de la gente guarda grandes sumas de monedas digitales en lo que se conoce como billeteras frías. Una billetera fría no está conectada a Internet; puede ser una computadora portátil que no está conectada o conectada a Wi-Fi. Alternativamente, una billetera fría puede ser un servidor independiente y sin conexión con el mundo exterior. Una billetera fría incluso puede ser una memoria USB que está conectada a una computadora solo cuando desea transferir moneda. El punto clave es que una billetera caliente está conectada a Internet y es vulnerable, mientras que una billetera fría no es vulnerable a un ataque cibernético.

¿Cómo se relaciona esto con Mt Gox? Me alegro de que preguntaras. La mayoría de los intercambios tienen la mayoría de las monedas digitales depositadas en billeteras frías. Las monedas digitales se transfieren a una billetera caliente solo cuando alguien quiere hacer un intercambio. Por lo general, los intercambios contienen del 80 al 90 por ciento de sus depósitos en billeteras frías, y el resto es utilizado por los comerciantes activos. En el caso de Mt Gox, tenían una gran cantidad de bitcoins en sus billeteras calientes, lo que los exponía a un ataque cibernético. Además, Mt Gox carecía de suficientes registros y un protocolo para determinar dónde residían todos los depósitos. Cuando se corrió la voz de que Mt Gox había sido pirateado, todos se apresuraron a sacar sus monedas del intercambio. Sin embargo, sin registros suficientes era difícil determinar dónde estaban todas las monedas, no tenían idea de cuántas monedas había en la billetera caliente y cuántas habían sido robadas.

9.5- Vehículos de inversión

Para algunos, la idea de una billetera caliente o fría y la posibilidad de un ataque cibernético es más información o riesgo de lo que desean. La solución es invertir en un vehículo regulado que haga toda la seguridad y el intercambio por usted. Hay dos vehículos principales de inversión para aquellos que desean tener bitcoins: uno aún espera la aprobación y el otro está en funcionamiento.

Winkelvoss ETF

Los gemelos Winkelvoss, sí, los mismos de la saga de Facebook, han aplicado para crear un ETF que cotice en bolsa que albergará bitcoins. El proceso de aprobación para cualquier ETF es largo, y un ETF basado en bitcoins probablemente reciba un control adicional. La ventaja de esta estructura, cuando se aprueba, es que proporcionará un vehículo comercial líquido para bitcoins. En lugar de aventurarse en intercambios de divisas digitales no regulados, el ETF de Bitcoin permitirá que cualquier persona con una cuenta de corretaje de los EE. UU. Compre, venda y negocie bitcoins. Por supuesto, al igual que el ETF de oro, este producto no está diseñado para ser "cobrado"; esto es simplemente una forma de participar en las fluctuaciones de precios de bitcoin.

Bitcoin Investment Trust

Si no puede esperar a que la Comisión de Bolsa y Valores apruebe un ETF de Bitcoin y no desea la molestia de comprar y almacenar de manera segura una gran suma de bitcoins, entonces Bitcoin Investment Trust (BIT) puede ser para usted. El Bitcoin Investment Trust es un producto ofrecido a través de una subsidiaria de SecondMarket y está dirigido a personas de alto patrimonio que desean obtener exposición a Bitcoin. El principal beneficio de este fondo es que comprar y almacenar puede ser una tarea laboriosa, especialmente para los no iniciados. Descargar una billetera y luego vincular una cuenta bancaria a un intercambio puede ser desalentador. El BIT ofrece una manera simple de exponerse a bitcoin en dólares estadounidenses sin la necesidad de convertirse en un experto en moneda digital. Este es el vehículo de inversión perfecto para aquellos que quieren ser los primeros en adoptar sin la curva de aprendizaje de billeteras frías y calientes, almacenamiento seguro y códigos de seguridad.

Hay algunas características únicas del BIT que lo hacen ideal para inversores sofisticados. Actualmente, si desea comprar cualquier cantidad de bitcoins, debe lidiar con varias empresas no registradas y no registradas. Los operadores de muchos intercambios de divisas digitales no son muy visibles por diseño, y a menudo operan desde países con leyes cuestionables. Sin duda, algunos de los intercambios más grandes y nuevos están comenzando a salir de las sombras, pero todavía es un negocio de entidades no reguladas. Al mismo tiempo, el mercado de bitcoins y especialmente de monedas alternativas está muy fragmentado, lo que dificulta la compra de grandes sumas de bitcoins. En un esfuerzo por sortear muchos de estos desafíos, el operador de BIT adquiere y almacena bitcoins sin tener que lidiar con los jugadores antes mencionados.

El BIT es comercializado y distribuido por SecondMarket Inc., un broker-dealer registrado en los EE. UU. Y la Autoridad Reguladora de la Industria Financiera (FINRA). Además, el BIT está estructurado para que su propiedad esté en acciones de la confianza no directamente en bitcoins. De estructura similar al SPDR Gold ETF, el valor de las acciones de BIT se deriva de las bitcoins subyacentes que el vehículo de inversión mantiene pasivamente. El beneficio de esta estructura es que el título de propiedad es claro y se puede usar para fines de planificación patrimonial. Además, debido a que las acciones del BIT son valores, pueden mantenerse en algunas cuentas de jubilación con ventajas impositivas, así como en cuentas de corretaje. Esto hace que la obtención de la exposición a bitcoins en su cartera de inversiones sea tan sencilla como ordenar a su corredor de cuenta de jubilación comprar acciones en el BIT.

La desventaja de esta estructura es que no es líquida. Como se trata de títulos privados, existen ciertas limitaciones sobre cuándo y cómo pueden venderse. Eventualmente, a medida que las acciones en el BIT maduren, serán elegibles para la negociación por parte del público en general. SecondMarket tiene un amplio conocimiento de los mercados de valores privados y es más conocido por manejar gran parte de los intercambios de ofertas públicas preiniciales en acciones de Facebook.

9.6- Crecimiento en los clases de activos

Independientemente de cómo elija invertir, esta nueva clase de activos está comenzando a crecer. Cuando el choque de Nixon liberó las monedas fiduciarias para flotar con las fuerzas del mercado, los mercados de divisas apenas se desarrollaron. Eventualmente, a medida que ingresaba más liquidez en los mercados de divisas y se desarrollaban más productos, el crecimiento del mercado de divisas explotó. Desde el comercio por teléfono hasta las computadoras rápidas, ahora se puede enviar divisas al mundo literalmente a la velocidad de la luz. Además, existen fondos mutuos

dedicados, fondos de cobertura e intermediarios financieros que se han desarrollado en los últimos 40 años.

Las lecciones aprendidas del crecimiento de los mercados de divisas se pueden aplicar a las monedas digitales, y dado que existe una plantilla preexistente, es probable que los mercados de divisas digitales se desarrollen más rápido.

Cuando colapsó el sistema de Bretton Woods, los mercados de futuros y opciones no existían, sin embargo, mientras se escriben estas palabras, se están desarrollando futuros en monedas digitales. Finalmente, la rápida aceptación de los inversionistas institucionales vendrá solo con claridad regulatoria. La incertidumbre actual sobre la legitimidad de las monedas digitales es un obstáculo para una aceptación más amplia. Los fondos de pensiones, las compañías de seguros y otros inversionistas institucionales tienen la responsabilidad fiduciaria de invertir en clases de activos con una estructura legal clara. A medida que esta estructura legal se desarrolle para las monedas digitales, los inversores profesionales tendrán más probabilidades de ingresar al mercado.

Capítulo 10

Tira de la cuerda, y seguirá donde quieras. Presiónalo, y no irá a ninguna parte.

-Dwight D. Eisenhower

10.1- Regulación

El tema de la regulación monetaria digital no es solo controvertido; puede ser francamente inflamatorio para los puristas de monedas digitales.

Bitcoin fue creado para eliminar a terceros del sistema financiero, ya sean agencias gubernamentales o bancos del centro monetario. Como defensor del capitalismo de libre mercado, preferiría que el mercado se autorregulara y muchos tradicionalistas de la moneda digital consideran que el código matemático autorregulador en el corazón de estas monedas es superior a cualquier regulación gubernamental. Este argumento tiene mérito pero también tiene un defecto en su lógica. Si bien el código matemático hace un trabajo excepcional para eliminar a los intermediarios financieros, no aborda el problema de la codicia y el engaño humanos.

Como creador de una moneda digital, he visto a la industria madurar desde un niño terrible con una inclinación por lo ilícito hasta un adolescente rebelde con un futuro brillante. Para que las monedas digitales cumplan la promesa de la adultez, necesitan algunas reglas para vivir, un protocolo, si se quiere.

Por primera vez en la historia de la humanidad, las monedas digitales y la tecnología blockchain les permite a las personas enviar información segura a través de una red no segura sin un tercero de confianza. El uso más obvio para esta tecnología es para transacciones financieras. Convenientemente, la industria centralizada de servicios financieros está lista para la desintermediación. Desde la fundación del Banco de Inglaterra en 1694, nuestro sistema financiero ha consistido en intermediarios que orbitan alrededor de los bancos centrales. Esta web era necesaria para garantizar la transferencia segura de valor entre dos partes que no tienen forma de confiarse mutuamente. El tercero de confianza, o intermediario, desempeñó una función esencial verificando la legitimidad de la transacción financiera y transfiriendo el valor.

Sin embargo, las monedas digitales y el blockchain son más que solo un medio de intercambio; representan una base de datos segura abierta a cualquier persona que tenga una conexión a Internet. Internet abrió una cantidad de información sin precedentes a la sociedad, pero carecía de un mecanismo para verificar la información. La tecnología blockchain es el mecanismo por el cual cualquier información puede rastrearse hasta su origen. Esta tecnología es demasiado importante para acechar en las sombras.

La aplicación de la ley, las autoridades impositivas y las agencias reguladoras del mercado financiero han expresado interés en definir las reglas para las monedas digitales. Todavía es muy temprano en el juego, y muchos de estos reguladores están empezando a comprender el alcance de las monedas digitales. La buena noticia para los defensores de la moneda digital es que cualquier tipo de regulación será un guiño implícito de legitimidad. Con solo deslizar un lápiz, estas agencias tienen la capacidad de declarar monedas digitales ilegales, pero un conjunto de reglas significa que la clase de activos llegó para quedarse.

10.2- Agencias regulatorias

Dependiendo de la ubicación geográfica, la regulación de la moneda digital ha abarcado desde prohibiciones absolutas hasta enfoques de laissez-faire. Islandia y Vietnam son los dos países en los que están prohibidas las monedas digitales y Bitcoin. Estas prohibiciones son más sobre los flujos de capital internacionales que la prohibición de la tecnología. Durante la crisis financiera de 2008, Islandia sufrió una fuga de capital de la economía cuando el sistema bancario implosionó. Para evitar otra crisis, Islandia prohíbe la transferencia de moneda digital fuera del país. Curiosamente, existe una moneda digital diseñada para ser utilizada dentro de las fronteras de Islandia; Auroracoin es legal en Islandia porque está especificado para ser utilizado solo en Islandia.

Los dos países más influyentes en la regulación de la moneda digital son China y los Estados Unidos. Gran parte del movimiento extremo en Bitcoin durante 2013 fue el resultado de ciudadanos chinos que compraron Bitcoin para sacar dinero del país. Dado que China tiene un sistema fijo de tasa de cambio fiduciaria y restringe los flujos de capital, las monedas digitales ofrecieron un camino alrededor de las autoridades. Sin embargo, el gobierno chino se apresuró a detener los flujos de capital advirtiendo a los bancos estatales que no trabajen con los intercambios de divisas digitales. En diciembre de 2013, el Banco Popular de China también bloqueó que los procesadores de pagos se ocupen de los intercambios de divisas digitales. Estos movimientos efectivamente frenaron la salida masiva de dinero de China y el precio del bitcoin cayó más del 50 por ciento. Esta fue la vorágine que convirtió mi "can not-lose trade" en la burbuja de Bitcoin en una inversión a largo plazo y fue un catalizador para escribir este libro.

En los Estados Unidos, varias agencias tanto a nivel estatal como nacional han dado un golpe en la regulación y la aplicación de la ley. En marzo de 2014, el Servicio de Impuestos Internos emitió una guía sobre el tratamiento fiscal para las monedas virtuales. En efecto, esta guía trata las monedas digitales como una propiedad, como acciones, en lugar de una moneda. Esta decisión es positiva para los inversionistas por dos razones. En primer lugar, aclara las implicaciones fiscales de invertir en monedas digitales como una clase de activos. Debería alentar a las instituciones a moverse en el espacio y crear una nueva fuente de demanda de bitcoin. Dado que el valor total de bitcoin es pequeño en relación con otras clases de activos, no sería necesario que muchos inversores de tamaño institucional elevaran sustancialmente el precio. En segundo lugar, los inversores de EE. UU. Que posean bitcoin durante más de un año tributarán a la tasa del impuesto a las ganancias de capital. Si se considerara Bitcoin como una moneda "real", los inversores recibirían impuestos a su tasa de impuesto ordinaria independientemente del período de tenencia. Esto debería alentar la tenencia de monedas digitales a largo plazo y tiene el potencial de reducir la volatilidad.

Es interesante comparar el dictamen del IRS con la orientación normativa de Dinamarca. El 17 de diciembre de 2013, la Autoridad de Supervisión Financiera (FSA) de Dinamarca emitió un comunicado que decía que las monedas digitales no estarían reguladas por la FSA. Además, el 25 de marzo de 2014, la red de TV2 en Dinamarca informó que las autoridades tributarias determinaron que las ganancias en monedas virtuales no serían gravadas. El tratamiento fiscal variable de un activo que no tiene una residencia legal destaca uno de los desafíos en la regulación de activos digitales.

Otro desafío a la regulación se puede encontrar en la saga de SatoshiDice, un sitio de apuestas en línea de Bitcoin. En 2012, el fundador de SatoshiDice, Erik Voorhees, lanzó una oferta pública inicial (OPI) para recaudar dinero para desarrollar el sitio. En este caso, el capital recaudado estaba en bitcoins, no en moneda fiduciaria. Además, las acciones emitidas a SatoshiDice se cotizan en una bolsa llamada MPEx, que tiene su sede en Rumania y negocia solo acciones de

compañías que tienen un precio en bitcoin. Dado que las acciones fueron ofrecidas a inversores estadounidenses (entre otros países), la Comisión de Bolsa y Valores de los Estados Unidos (SEC) acusó a Erik Voorhees de violar la Ley de Valores de 1913. Esta ley requiere el registro de OPI ante la SEC. A pesar de que Voorhees solo emitió activos digitales y generó bitcoin, la SEC descubrió que, independientemente de la moneda utilizada, ofrecer una inversión a un ciudadano de los EE. UU. Requiere registro. Voorhees pagó una multa de $ 50,000 y vendió el sitio web a un comprador anónimo por casi $ 12 millones.

FINCEN

La primera agencia reguladora de los EE. UU. Que ofreció orientación y normas sobre monedas digitales fue la División de Ejecución de Delitos Financieros del Tesoro de los EE. UU. (FINCEN). La guía de FINCEN fue diseñada para prevenir fraudes y delitos financieros y se enfocó principalmente en negocios de servicios monetarios. Un negocio de servicios de dinero es cualquier entidad que acepta dinero y realiza un servicio de transmisión de dinero. Esencialmente, estas pautas son un intento de restringir el uso de las monedas digitales por aquellos que desean ofuscar transacciones potencialmente ilegales.

> Guía de FINCEN para prevenir el fraude y los delitos financieros
>
> Un administrador o intercambiador que (1) acepte y transmita una moneda virtual convertible o (2) compre o venda moneda virtual convertible por cualquier razón es un transmisor de dinero bajo las regulaciones de FinCEN, a menos que una limitación o exención de la definición se aplique a la persona. Las regulaciones de FinCEN definen el término transmisor de dinero como una persona que proporciona servicios de transmisión de dinero, o cualquier otra persona involucrada en la transferencia de fondos. El término servicios de transmisión de dinero significa "la aceptación de dinero, fondos u otro valor que sustituye a la moneda de una persona y la transmisión de dinero, fondos u otro valor que sustituya la moneda por otra ubicación o persona por cualquier medio".
>
> La definición de un transmisor de dinero no diferencia entre las monedas reales y las monedas virtuales convertibles. Aceptar y transmitir cualquier cosa de valor que sustituya a la moneda hace que una persona sea un transmisor de dinero según las normas que implementan la BSA. FinCEN ha revisado diferentes actividades que involucran moneda virtual y ha hecho determinaciones con respecto al tratamiento regulatorio apropiado de administradores e intercambiadores bajo tres escenarios: corredores y distribuidores de monedas electrónicas y metales preciosos electrónicos; monedas virtuales convertibles centralizadas; y monedas virtuales convertibles descentralizadas.

La consecuencia involuntaria de estas pautas es que desplazó parte de la carga regulatoria a las agencias bancarias estatales. Al hacerlo, las directrices de FINCEN establecieron como requisito que las empresas de servicios monetarios dedicadas a transacciones en moneda digital tendrían que registrarse en las 50 agencias bancarias estatales. Si bien la guía de FINCEN fue bien recibida por la comunidad de capital de riesgo cuando comenzó a cristalizar el panorama regulatorio, ha impuesto una carga innecesaria a muchas empresas y tiene el potencial de frenar la innovación.

Departamento de Finanzas de Nueva York

Fomentar la innovación se mencionó específicamente cuando en julio de 2014 el Departamento de Finanzas de Nueva York se convirtió en la primera agencia reguladora del estado en presentar leyes propuestas sobre monedas digitales con el anuncio de BitLicense. El superintendente Benjamin Lawsky asumió el liderazgo en la regulación de negocios de divisas digitales con el objetivo de proteger a los consumidores al tiempo que fomenta la innovación. La ley propuesta exige que las empresas de divisas digitales con sede en Nueva York obtengan BitLicense. BitLicense haría que las empresas no solo mantengan registros de los clientes sino que también mantengan ciertos niveles de capital. Una vez más, la amenaza de consecuencias involuntarias podría descarrilar el espíritu emprendedor en las monedas digitales. En particular, los requisitos de cumplimiento, capital y mantenimiento de registros tienen el potencial de impulsar negocios de moneda digital desde el estado de Nueva York.

> Sección 200.7 Cumplimiento
>
> (a) En general. Se requiere que cada licenciatario cumpla con todas las leyes, normas y reglamentos federales y estatales aplicables.
> (b) Oficial de cumplimiento. Cada licenciatario deberá designar a una persona o individuos calificados responsables de coordinar y monitorear el cumplimiento de esta Parte y todas las demás leyes, normas y reglamentos federales y estatales aplicables.
> (c) Política de cumplimiento. Cada licenciatario deberá mantener y aplicar las políticas de cumplimiento escritas, incluidas las políticas relacionadas con la lucha contra el fraude, el blanqueo de dinero, la seguridad cibernética, la privacidad y la seguridad de la información y cualquier otra política requerida en esta Parte, que debe ser revisada y aprobada por el licenciatario. consejo de administración u órgano de gobierno equivalente.
>
> Autoridad Estatutaria: Ley de Servicios Financieros, secciones 102, 301 y 302

Pocos argumentarían que el cumplimiento de las normas contra el lavado de dinero es un impedimento para la innovación, pero el requisito de designar un oficial de cumplimiento y mantener una política escrita de cumplimiento hará desagradable la idea de comenzar un negocio en Nueva York. A menos que estas reglas sean adoptadas por los 50 estados, los empresarios simplemente optarán por establecerse fuera del estado de Nueva York.

Además, el requisito de mantener ciertos niveles de capital es demasiado ambiguo y amplio para ser útil. No hay duda de que a cualquier empresa que ofrezca salvaguardar los activos del público en general se le debe exigir que mantenga niveles de solvencia. Sin embargo, incluso las reglas establecidas por más de 300 años de banca central no evitaron la crisis financiera de 2008 y el fraude conmensurado.

> Sección 200.8 Requerimientos de capital
>
> (a) Cada Licenciatario deberá mantener en todo momento el capital que el superintendente determine que sea suficiente para garantizar la integridad financiera del Licenciatario y sus operaciones en curso. Al determinar la cantidad mínima de capital que debe mantener un licenciatario, el superintendente considerará una variedad de factores, que incluyen pero no se limitan a:
> (1) la composición de los activos totales del licenciatario, incluida la posición, el tamaño, la liquidez, la exposición al riesgo y la volatilidad del precio de cada tipo de activo;

(2) la composición del pasivo total del licenciatario, incluido el tamaño y el tiempo de amortización de cada tipo de responsabilidad;
(3) el volumen real y esperado de la actividad comercial de moneda virtual del licenciatario;
(4) si el licenciatario ya cuenta con licencia o está regulado por el superintendente según la Ley de servicios financieros, la Ley bancaria o la Ley de seguros, o está sujeto a leyes como el proveedor de un producto o servicio financiero, y si el licenciatario está en buen estado. de pie en tal capacidad;
(5) el monto de apalancamiento empleado por el licenciatario;
(6) la posición de liquidez del licenciatario; y
(7) la protección financiera que el licenciatario proporciona a sus clientes a través de su cuenta fiduciaria o fianza.

El Departamento de Finanzas de Nueva York estaría mejor servido al adoptar las reglas que ya rigen en los negocios de servicios financieros. Esto permitiría a las empresas de divisas digitales competir en pie de igualdad con el sistema bancario existente.

Finalmente, el requisito de mantener un registro de cada transacción es simplemente un comienzo para casi cualquier negocio nuevo.

(1) Registros de transacciones de moneda virtual
Cada Licenciatario mantendrá la siguiente información para todas las transacciones que impliquen el pago, recibo, cambio o conversión, compra, venta, transferencia o transmisión de Moneda Virtual: la identidad y las direcciones físicas de las partes involucradas, la cantidad o el valor de la transacción, incluyendo en qué denominación se compró, vendió o transfirió, el método de pago, la (s) fecha (s) en que se inició y completó la transacción, y una descripción de la transacción.
(2) Informes sobre transacciones
Cuando un licenciatario participa en una transacción o serie de transacciones para el recibo, intercambio, conversión, compra, venta, transferencia o transmisión de moneda virtual, en un monto total que excede el valor en dólares estadounidenses de $ 10,000 en un día, en uno Persona, el licenciatario deberá notificar al Departamento, de la manera prescrita por el superintendente, dentro de las 24 horas.

Si cada transacción que tuvo lugar necesitara incluir la dirección física de las partes involucradas, entonces muy pocas transacciones de moneda digital tendrían lugar en el estado de Nueva York. El objetivo de las monedas digitales es que son un medio eficiente para transferir valor. Si dos partes acuerdan intercambiar valor, no es necesario intercambiar direcciones físicas. Si de hecho el requisito de los registros lo convierte en la ley final, se producirán dos resultados: primero, muy pocas empresas solicitarán una BitLicense; y, en segundo lugar, las empresas que sí soliciten incurrirán en grandes tarifas legales y de mantenimiento de registros.

Finalmente, estas reglas se cumplirían mejor si estuvieran acompañadas por una exención de impuestos para aquellos que reciben BitLicense. El estado de Nueva York ya ofrece zonas libres de impuestos con hasta 10 años de operaciones libres de impuestos, la combinación de estas zonas con zonas BitLicense compensaría algunos de los costos onerosos.

10.3- Desafíos a la Regulación

La fuerza de las monedas digitales es que existen en millones de computadoras distribuidas a través de las fronteras locales e internacionales. Esta distribución presenta un desafío para los reguladores ya que la aplicación a través de las fronteras locales e internacionales es virtualmente imposible. Idealmente, las regulaciones serán lo suficientemente ligeras como para alentar a quienes están en el espacio monetario digital a someterse voluntariamente a la regulación. BitLicense necesita ser un sello de legitimidad buscado por aquellos operadores con la mayor integridad. Además, las críticas a la regulación seguramente señalarán el potencial de mayores costos. Esta crítica no carece de fundamento y es la razón por la cual es fundamental para el Departamento de Finanzas de Nueva York cumplir con su compromiso de no sofocar la innovación. La regulación ligera para proteger a los consumidores y permitir que más personas experimenten los beneficios de las monedas digitales es una adición bienvenida al ecosistema.

La regulación de las monedas digitales puede parecer un anatema para aquellos que se suscriben a la forma más pura de la creación de código abierto de Nakamoto. La naturaleza de fuente abierta de las monedas digitales proporciona un mecanismo autorregulador incorporado, pero ese mecanismo no protege contra la avaricia humana. Para que las monedas digitales crezcan, necesitan un conjunto de reglas que les permita emprender mientras que fomentan y protegen a los nuevos usuarios. La regulación realizada correctamente no solo puede ampliar la base de usuarios, sino también legitimar implícitamente las monedas digitales.

La industria de activos digitales ha formado un grupo llamado Autoridad de Transferencia de Activos Digitales (DATA), que pretende ser un enlace de la industria con los reguladores globales. DATA trabaja con los líderes de la industria y los reguladores para facilitar las mejores prácticas dentro de la industria de activos digitales. Son entidades como DATA las que se convertirán en la FINRA de los activos digitales.

10.4- Tirando de la cuerda

Con todos los nuevos productos de inversión que se están desarrollando, es solo cuestión de tiempo antes de que más regulaciones formen parte del ecosistema.

Los ataques cibernéticos en los principales intercambios de divisas digitales han amenazado con hacer fracasar el crecimiento de la tecnología blockchain. Además, muchos capitalistas de riesgo han estado esperando claridad regulatoria para financiar la creación de nuevas monedas digitales. A medida que se desarrollen las regulaciones, será esencial que la comunidad de moneda digital tenga un rol integral.

Los reguladores no solo están luchando con la forma de hacer cumplir las reglas sobre las monedas que no tienen una jurisdicción legal o están patrocinadas por un gobierno soberano, sino que también están tratando de comprender la tecnología detrás de las monedas digitales y los activos digitales. Las regulaciones deben ser lo suficientemente flexibles como para permitir la innovación y alentar a los desarrolladores de divisas digitales a permanecer dentro de una jurisdicción legal. Al mismo tiempo, el espacio de moneda digital está listo para el fraude, ya que hay una ventaja de información para los desarrolladores nefastos.

El entorno normativo ideal será aquel en el que la comunidad de moneda digital global acuerde un conjunto de reglas que definan buenas prácticas. Estas buenas prácticas deben ser adoptadas por todos los desarrolladores con sombrero blanco y deben ser demandadas por los usuarios de moneda digital. Es importante que la comunidad de la moneda digital reconozca que es mejor

trabajar con los reguladores que presionar contra ellos. Las agencias de autorregulación que ya existen en los mercados financieros se pueden usar como plantilla para las monedas digitales.

La próxima etapa de crecimiento para las monedas digitales implicará la aceptación del público en general, lo que hace imperativo que se adopte un conjunto de buenas prácticas. La tecnología blockchain es revolucionaria y puede utilizarse para más aplicaciones que la simple transferencia de valores. Es un desarrollo demasiado importante para ser usurpado por los no-hacer-pozos. Internet comenzó como una forma de enviar archivos entre computadoras y se convirtió en una tecnología que permite a los médicos realizar cirugías que salvan vidas a distancia. El potencial de blockchain es tan grande como Internet. Con el panorama regulatorio enfocado, puede comenzar el viaje hacia la adultez de las monedas digitales.

Capítulo 11

> Creo que Internet será una de las principales fuerzas para reducir el papel del gobierno. Lo único que falta, pero que pronto se desarrollará, es un efectivo electrónico confiable.
>
> -Milton Friedman

11.1- Dinero inteligente: configúralo y olvídate

Ron Popeil hizo una fortuna con un tostador de pollo y una frase: "¡Prepáralo y olvídate!". El asador Showtime hizo la vida más fácil y resolvió el problema que todos tenemos, no el tiempo suficiente para cocinar una comida sana y asequible. Con su rotisserie y una frase, Popeil prometió que podrías hacer una comida deliciosa y saludable en dos sencillos pasos. Una vez que preparó el pollo, simplemente puso en marcha la máquina y se olvidó de ella hasta que el temporizador emitió un zumbido. Puedes hacer algo similar con Bitcoin. No, no cocinará un pollo, pero puede "configurarlo y olvidarlo". A través de las funciones de dinero inteligente de Bitcoin, puede establecer literalmente una transacción y olvidarla: el software Bitcoin hace el resto.

Pero espera hay más. También puede adjuntar un contrato o propiedad a la transacción y la red de Bitcoin verificará que usted es el propietario y la transferirá cuando desee a quien desee.

A medida que se escriben estas páginas, los codificadores emprendedores trabajan arduamente en funciones denominadas contratos inteligentes y propiedad inteligente. Los contratos inteligentes son documentos legales que se adjuntan a una transacción de bitcoins. Estos contratos estipulan a quién pagar, cuándo pagar y qué se intercambia, y son increíblemente eficientes. Además, dado que la transacción de bitcoins es irreversible y se adjunta un contrato firmado, la resolución de disputas se reducirá drásticamente.

La propiedad inteligente es cualquier propiedad que se puede identificar digitalmente. Por ejemplo, cada seguridad en América del Norte puede ser identificada por su Comité sobre el número de Procedimientos Uniformes de Identificación de Valores (CUSIP). Este código alfanumérico de nueve caracteres se usa para liquidar y transferir valores. Actualmente, el proceso de distribución del número es propiedad de American Bankers Association y es operado por S & P Capital IQ. Cuando se transfiere un valor entre dos partes, el número CUSIP identifica la propiedad (acción) y el centro de intercambio de información lleno de personas y computadoras completa la transferencia. Todo este proceso se puede simplificar adjuntando el número CUSIP a una transacción bitcoin. Un certificado de acciones que se transfiere a través de la red de Bitcoin es un ejemplo simple de propiedad inteligente.

Los contratos inteligentes y la propiedad son parte del creciente ecosistema de Bitcoin que está fortaleciendo la columna vertebral del dinero inteligente. Esta parte del ecosistema de Bitcoin se está moviendo tan rápido que muchos se están refiriendo a la velocidad del cambio como "tiempo de Bitcoin". Sin embargo, antes de seguir adelante, debemos hacer un viaje atrás en el tiempo.

En los viejos tiempos, allá por la década de 1960, existía un correo electrónico para que los científicos informáticos se comunicaran entre sí sobre las computadoras centrales cerradas específicas. Una década después, la Agencia de Proyectos de Investigación Avanzada (ARPA, DARPA) del gobierno de EE. UU. Decidió interconectar diferentes sistemas informáticos y llamarlo ARPANET. Para todos los efectos, el establecimiento de ARPANET fue el nacimiento de Internet. Ahora que los sistemas informáticos estaban interconectados, la Agencia de Proyectos de

Investigación Avanzada de Defensa (DARPA) necesitaba una forma de comunicarse a través de diferentes plataformas. Los sistemas de correo electrónico anteriores estaban cerrados al resto de Internet porque cada red hablaba un idioma diferente y operaba bajo un conjunto diferente de reglas llamadas protocolos.

A principios de la década de 1970, se desarrolló el Protocolo simple de transferencia de correo (SMTP) que permitió la comunicación de diferentes sistemas informáticos. El conjunto estandarizado de reglas de DARPA era similar a los estándares aceptados para construir ferrocarriles en los Estados Unidos. La aceptación del "indicador estándar" de George Stephenson permitió a los vagones viajar por todo el país sin la necesidad de cambiar de carril. La proliferación de SMTP permitió que la comunicación viajara a través de los sistemas informáticos.

El dinero es similar al correo electrónico: ambos transmiten un mensaje y ambos requieren un conjunto de reglas para transferir ese mensaje de una persona a otra. El mensaje de dinero es valor; al enviar dinero estás transfiriendo valor de una persona a otra. Si compra una camisa por $ 35, está enviando este mensaje a su banco:

> Estimado Banco,
> Actualmente estoy de compras en la casa de las camisas impresionantes de Rudy y he encontrado una camiseta que realmente me gusta, de hecho, es increíble. Esta camiseta cuesta $ 35 y deseo tener esta camisa más de lo que deseo tener $ 35. Por favor, transfiera $ 35 a la Casa de Camisas Impresionantes de Rudy de mi cuenta para que pueda dejar la tienda con esta increíble camiseta en mi poder.
>
> Saludos.

Una vez que su banco recibe este mensaje, hay un conjunto de reglas que sigue para realizar la transferencia a la Casa de las impresionantes camisas de Rudy. Por supuesto, nunca se ve toda esta comunicación porque una tarjeta de débito lo hace parecer fácil, pero tenga la seguridad de que hay mensajes volando a través del ciberespacio asegurándose de obtener su increíble camiseta.

El sistema financiero actual ha desarrollado estos protocolos o reglas para que los diferentes bancos puedan comunicarse y transferir valor. A medida que los bancos se globalizaban, se necesitaba otro conjunto de reglas para que el dinero hablara el mismo idioma; es decir, el mensaje "Por favor transfiera $ 35" podría traducirse fácilmente a otras monedas. Estos protocolos rigen las finanzas modernas, pero en el sistema financiero de Bitcoin, estas reglas recién se están desarrollando.

11.2- Reglas del camino

Hoy en día, hay tres protocolos que compiten para convertirse en el próximo SMTP. Ripple, MasterCoin y ColoredCoin están tratando de hacer una transferencia de valores perfecta en computadoras, monedas y fronteras nacionales. Ripple es una moneda y un protocolo, y su objetivo es hacer posible la transferencia de cualquier tipo de valor a través de una red distribuida. Lo llaman correo electrónico por dinero. Lo que hace único a Ripple es que compite con Bitcoin como moneda. Con Ripple, el valor se puede transferir instantáneamente y de forma gratuita ya sea que ese valor se almacene en euros, dólares estadounidenses, bitcoins u ondulaciones.

MasterCoin y ColoredCoin están adoptando un enfoque diferente: al usar la red bitcoin existente, están diseñando productos que van por encima. Tanto ColoredCoin como MasterCoin les permiten a los usuarios finales crear su propia moneda.

11.3- Contratos inteligentes y propiedad

Una vez que se establezcan las reglas del camino del dinero, podremos transferir virtualmente cualquier cosa de valor. El correo electrónico nos permitió enviar cualquier mensaje a cualquier persona que estuviera conectada a Internet. Debido a que el protocolo Bitcoin ha resuelto el problema de transferir información segura a través de una red insegura, se puede usar para enviar valor a través de Internet. Sin embargo, necesitaremos algunas reglas para guiarnos, pero esta vez ya existen, solo necesitan ser convertidas en código de computadora.

En su forma más simple, los contratos son el conjunto de reglas que deben seguirse cuando dos personas deciden intercambiar algo de valor. El contrato que firme al comprar una casa contiene instrucciones tanto para el comprador como para el vendedor. Cuando se trata de usar contratos en conjunto con Bitcoin, los contratos deben ir a la escuela y convertirse en contratos inteligentes. Los contratos inteligentes son contratos que se integran en la propiedad y convierten a la propiedad anteriormente tonta en propiedad inteligente.

Su teléfono móvil es un gran ejemplo de un contrato integrado en una propiedad, lo que hace que su teléfono sea una propiedad inteligente. Para verificar que el usuario del teléfono es el verdadero propietario, su teléfono móvil solo funciona si ingresa el número de identificación personal (PIN) correcto: incrustado en el software del teléfono hay un contrato que establece que el teléfono solo funcionará para el legítimo propietario. La clave para probar que usted es el propietario legítimo es su PIN. Pero también tiene un contrato inteligente con su proveedor de servicios móviles. Has firmado un contrato con AT & T, Verizon o Sprint en el que aceptaron proporcionar cobertura de telefonía móvil a cambio de un pago. Si su pago no llega según lo acordado, su teléfono móvil se desconectará.

Otro ejemplo real del concepto de propiedad inteligente / contrato es un inmovilizador para automóvil. Este dispositivo electrónico evita que el motor funcione a menos que esté presente la "clave" correcta. Esta clave puede ser un código o PIN o incluso usar criptografía para crear un cifrado seguro. Estos dispositivos han sido obligatorios en Alemania, el Reino Unido y Finlandia desde 1998. En Australia, donde los inmovilizadores han sido obligatorios desde 2001, han reducido el robo de automóviles en un 45 por ciento. Si el token o código correcto no está presente, el dispositivo no permite que el combustible fluya hacia el motor, de esta manera evita que un automóvil se caliente después de que se haya accedido.

Dado que las bitcoins se pueden dividir en ocho decimales, es factible que la denominación más pequeña de bitcoin (un Satoshi) pueda integrarse en cada automóvil que salga de una línea de ensamblaje. Cuando el automóvil se transfiere al concesionario, esa transacción se registrará en el blockchain, y cuando usted compra el automóvil, la transferencia también se registra en el libro mayor central. Esto crearía un solo registro de propiedad y podría eliminar los números de identificación del vehículo. Además, cualquier persona que posteriormente compró el automóvil simplemente podría mirar la cadena de bloques para determinar a todos los propietarios del vehículo. La tergiversación de la verdadera propiedad por vendedores inescrupulosos sería eliminada.

La primera persona en proponer la idea de un contrato inteligente fue el profesor de derecho Nick Szabo-yep, ese Nick Szabo, el que todos habían señalado una vez como Satoshi Nakamoto. En

1997, Nick Szabo escribió un artículo llamado "La idea de los contratos inteligentes", en el que describía las cláusulas contractuales integradas digitalmente en la propiedad. De hecho, en este documento, no solo describe la idea de un inmovilizador de automóviles, sino que también examina cómo se podrían usar los contratos inteligentes para los préstamos P2P (peer-to-peer). Dado que los contratos inteligentes se adjuntan a cualquier garantía que se prestaría si el prestatario incumple el acuerdo, la propiedad de la propiedad simplemente se revertiría al prestamista.

Bitcoin permite que este simple proceso de contrato se integre en prácticamente cualquier cosa que pueda identificarse digitalmente. El requisito de identificación digital no es tan siniestro como suena, podría ser tan simple como colocar un código de barras en un objeto, ya sea una lámpara antigua o una casa. Siempre que ese código de barras no se pueda eliminar de la propiedad, la propiedad se puede transferir utilizando la red de Bitcoin. La ventaja de usar Bitcoin es que el protocolo tiene seguridad incorporada y no requiere un abogado para redactar el contrato. Esta es solo otra forma en que Bitcoin podría desintermediar una industria de servicios.

Estos contratos inteligentes también se pueden usar para eliminar al intermediario del sistema bancario, que sería una extensión de la tesis original de Nick Szabo sobre préstamos entre pares. En un préstamo de automóvil típico, el banco le presta dinero para comprar un automóvil, y si el préstamo no se cancela según lo programado, el banco contrata a un agente de repo para recuperar su garantía. Al usar las propiedades de contrato inteligente de Bitcoin, el contrato de préstamo podría incluirse en su clave: si su préstamo no se reembolsa de acuerdo con el acuerdo, la clave no arrancará el automóvil. Además, usando el GPS, el banco podría ubicar el automóvil y enviar a un representante con una nueva llave para alejar el vehículo, sin necesidad de repo.

Por supuesto, con este nivel de control sobre la garantía, uno no necesita ser un banco para hacer este préstamo. Las personas con dinero en efectivo para prestar tienen una oportunidad sin precedentes de prestar dinero de manera segura sin intermediarios. Este es un enorme avance para los préstamos peer-to-peer (P2P). El problema con los préstamos P2P es que el prestamista no tiene una seguridad razonable de que pueda recuperar la garantía si se infringe el acuerdo. Si alguien no le devuelve el dinero ahora, debe presentar un reclamo legal ante el tribunal. Hay un costo asociado no solo a la contratación de un abogado, sino también al tiempo dedicado a documentar la transacción.

Para ver cómo funcionaría esto, supongamos que me presta dinero para comprar un automóvil y acordamos que cada mes le pagaré $ 300. Escribimos este contrato en nuestra transacción de Bitcoin y lo transmitimos a la red para registrarlo y verificarlo. Ahora tenemos un registro digital irreversible de nuestra transacción. También escribimos en nuestra transacción que si no le pago, tiene derecho a recuperar mi automóvil. Como vimos con el ejemplo del banco, recuperar las garantías es bastante simple con Bitcoin. Cuando mi pago no llega según lo acordado, nuestro contrato digital apaga mi automóvil y desactiva la llave. Según nuestro contrato, la propiedad se transfiere a usted y se programa una nueva clave: usted mantiene esta nueva clave y ahora es el propietario legítimo del vehículo. Por supuesto, todavía necesita encontrar el automóvil, pero la tecnología de posicionamiento moderna puede ayudar con eso.

Considerar la idea de combinar contratos inteligentes con automóviles no tiene por qué ser un ejercicio de impagos y embargos de préstamos. Imagine que posee un nuevo Tesla y que está tomando un viaje de negocios a Los Ángeles. Supongamos también que Tesla ha adoptado Bitcoin y cada nuevo Tesla está integrado con un Satoshi de bitcoin durante el proceso de fabricación. La prueba de su propiedad se registrará en el blockchain, pero no es necesario transferir la propiedad completa para obtener un beneficio de la tecnología de Bitcoin. Usando un contrato inteligente conectado a su Tesla, podría vender tiempo de uso en su automóvil, un servicio de tiempo

compartido para automóviles P2P. En lugar de alquilar un auto de Hertz o Avis, podría cambiar el uso de su Tesla en Nueva York por el uso de un Tesla en Los Ángeles. Esto podría revolucionar la forma en que se venden los automóviles. Es posible que los concesionarios pronto se pregunten: "¿Desea la opción de alquiler con su compra?" No solo cambiaría la forma en que se venden los automóviles; también proporcionaría una nueva clase de activos para que Wall Street negocie, empaquete y revenda.

La propiedad inteligente y los contratos también podrían usarse en servicios financieros. Las compañías fiduciarias, como U.S. Trust y Bank of New York, ofrecen a los clientes un tercero neutral que transferirá activos (valor) cuando se cumplan ciertas condiciones, generalmente a la edad de 21 años o al morir. Por lo general, una persona que desea transferir riqueza generacional contratará a un abogado para redactar los documentos del fideicomiso. Luego, los activos a transferir se colocarían en la confianza de un tercero neutral. Una vez que se hayan cumplido las condiciones del documento del fideicomiso, el tercero transferirá los activos. En cada una de las coyunturas, tanto el otorgante como el beneficiario cobran honorarios. Usando un contrato inteligente con una marca de tiempo, la misma transacción podría llevarse a cabo prácticamente sin cargo.

Puede ser necesario un abogado para escribir originalmente los documentos del fideicomiso, pero una vez que está codificado en un bitcoin, la transacción se realiza en piloto automático. El documento de confianza se registrará en el blockchain con una serie de declaraciones if-then. Por ejemplo, si el beneficiario cumple 21 años, entonces recibe 100 bitcoins. Cuando el reloj marca la medianoche en su cumpleaños, la propiedad se transfiere automáticamente: el propietario original de los bitcoins lo configuró literalmente y lo olvidó.

11.4- Ethereum

Llevando este concepto al siguiente nivel está el equipo de Ethereum. El líder Vitalik Buterin, Ethereum está desarrollando una cadena de bloques y un lenguaje de programación que permitirá a cualquier persona crear una aplicación de contrato inteligente. Ethereum se ha llamado Bitcoin 2.0, pero ese es un nombre inapropiado; Bitcoin claramente ha ido por el camino de un medio de intercambio. Está en camino de convertirse en otra moneda global. Sin embargo, Ethereum está intentando convertirse en la "tienda de aplicaciones" del mundo de las monedas digitales. Su objetivo es desarrollar el lenguaje informático que será la columna vertebral de los contratos inteligentes y las aplicaciones de propiedad. Aún más, se han establecido como una organización sin fines de lucro y planean dar esta tecnología revolucionaria de forma gratuita.

Antes de profundizar en lo que es Ethereum, necesitamos saber quién es Ethereum. ¿Por qué esta organización sin fines de lucro va a cambiar el mundo? El cofundador y el mascarón de proa de la organización es Vitalik Buterin, un informático de 20 años que también fundó la revista Bitcoin. Buterin es una de las jóvenes armas en el mundo de las monedas digitales, donde también ha trabajado en proyectos como Dark Wallet, una billetera de Bitcoin que pretende agregar otra capa de anonimato a la economía de Bitcoin. También acaba de recibir una Beca Thiel, que proporciona $ 100,000 a 20 de los desarrolladores más prometedores del mundo. Si el nombre de Thiel suena, es porque la fundación fue creada por Peter Thiel, el fundador de PayPal, el primer inversor en Facebook y el gran capitalista de riesgo que apoya los proyectos de Bitcoin.

Junto con Vitalik Buterin, el equipo fundador está repleto de una lista de estrellas de científicos informáticos, criptógrafos y expertos en monedas digitales. El único nombre que sobresale es Ralph Merkle, que es un consejero de Ethereum. ¿Quién es Ralph Merkel? Él es la persona que inventó las funciones hash criptográficas. La complicada ecuación matemática que encripta y

protege la red de Bitcoin se basa en una invención que Ralph Merkle desarrolló para un proyecto de pregrado. También es uno de los inventores de la criptografía de clave pública y ahora es un investigador de nanotecnología. Si estás construyendo una plataforma de aplicaciones basada en la tecnología blockchain y la criptografía, Ralph Merkle es un tipo que quieres tener en tu equipo.

A medida que el precio de bitcoin subió gran parte de la atención se ha centrado en usar bitcoin como moneda. El concepto de un blockchain ha encontrado un hogar exitoso como una manera de transferir de forma segura el valor a través de Internet. Sin embargo, usar la tecnología blockchain para crear un medio de intercambio es solo un uso, es como usar electricidad solo para encender una lámpara. El concepto blockchain se puede usar para aplicaciones que van más allá del dinero, por ejemplo, se puede usar para establecer y almacenar la propiedad de cualquier activo físico que tenga una firma digital (propiedad inteligente). La tecnología blockchain también se puede usar para transferir estos activos mediante contratos inteligentes con reglas predeterminadas de transferencia de propiedad. Una extensión lógica de este concepto es utilizar la tecnología blockchain para crear y comercializar derivados financieros como certificados por diferencia. Además, la tecnología se está utilizando para crear intercambios descentralizados que facilitarán la transferencia de propiedad, almacenarán la transacción y actuarán como una cámara de compensación descentralizada.

A medida que se desarrollan estos tipos de aplicaciones, hay dos obstáculos importantes que superar: primero, Bitcoin tiene una escalabilidad limitada y, en segundo lugar, debe haber un lenguaje común. Ya hemos discutido las limitaciones de transacciones de Bitcoin, pero también hay un problema de almacenamiento. Recuerde que para mantener la red de Bitcoin funcionando de manera segura depende de que los mineros descarguen cada transacción que haya tenido lugar alguna vez. A medida que se agregan más transacciones a la cadena de bloques, es necesario almacenar más datos en la computadora de cada minero. La fuerza de una red distribuida descentralizada es que cualquier nodo en la red almacena la información, y si un nodo falla, los otros nodos continúan funcionando sin interrupción. Sin embargo, a medida que crece la cadena de bloques, la realidad económica de almacenar todos los datos significa que solo los mineros con la capacidad financiera para almacenar los datos en bases de datos masivas podrán actuar como un nodo completo.

Bitcoin ya ha alcanzado el punto en que solo unas pocas grandes corporaciones pueden permitirse explotar minas de manera rentable. Estas grandes operaciones mineras son esenciales para el funcionamiento de la red, pero el hecho de que la explotación minera rentable requiere una inversión financiera significativa significa que la red se está centralizando cada vez más. De hecho, tiende hacia el sistema financiero que ya tenemos, donde los grandes bancos comerciales son esenciales para el funcionamiento del sistema. El grupo de minería más grande ya procesa cerca del 50 por ciento de las transacciones en la red; esto es casi tan lejos como la red puede obtener del concepto original de Satoshi de un sistema financiero descentralizado.

La tendencia hacia la centralización de los mineros se produce cuando la red está procesando y almacenando solo transacciones financieras. Cuando se desarrollan y despliegan otras aplicaciones de la tecnología blockchain, el problema se verá exacerbado. Los mineros ya no procesarán compras en Overstock, sino que también procesarán y almacenarán contratos de derivados financieros, mercados de predicción y resultados de votación. En resumen, cuanto mayor sea el crecimiento de la red Bitcoin, más centralizado se volverá.

Ethereum está tratando de resolver este problema creando una blockchain completamente nueva que está específicamente diseñada para manejar aplicaciones descentralizadas. Ethereum no está tratando de competir con Bitcoin, simplemente se está desarrollando para cumplir la promesa del concepto de blockchain. Ethereum está abordando el problema de la centralización de la minería

eligiendo un algoritmo de minería que permitirá que cualquier computadora procese transacciones en la red. En el lenguaje de divisas digital, esto se conoce como algoritmo resistente a ASIC. Esto significa que el algoritmo que utiliza Ethereum no dará una ventaja a los mineros con la computadora más cara. Esto en sí mismo podría ser revolucionario en el mundo de las monedas digitales, ya que revertiría la tendencia hacia la centralización.

El segundo problema que Ethereum está abordando es el de la estandarización, particularmente en el lenguaje de la computadora que se usa para desarrollar nuevas aplicaciones. Una manera fácil de pensar sobre esto es la diferencia entre el sistema operativo Android de Google y el iOS de Apple; ambos se pueden usar para desarrollar aplicaciones, pero se debe escribir una aplicación completamente nueva en ambos idiomas para que funcione en cualquiera de los sistemas. Ethereum está desarrollando un lenguaje llamado EVM, que significa código de máquina virtual Ethereum. EVM permitirá a cualquier persona crear una aplicación descentralizada utilizando cualquier lenguaje de computadora que elija. Una vez que se completa la aplicación, EVM estandarizará el código para que funcione sin problemas en la red de Ethereum.

El objetivo de Ethereum es hacer posible que cualquier desarrollador escriba un contrato inteligente que operará en la cadena de bloques de Ethereum. Una vez más, el impacto de esta tecnología no debe subestimarse. La capacidad de crear y distribuir aplicaciones descentralizadas tiene el potencial de perturbar una gran cantidad de empresas, no solo en la industria financiera.

El grupo Ethereum imagina tres tipos de aplicaciones que utilizarán la cadena de bloques: aplicaciones financieras, aplicaciones semifinancieras y aplicaciones no monetarias. Las aplicaciones financieras son las más simples ya que existen en otra forma. Un contrato de opciones es un ejemplo de un candidato principal para la descentralización a través de Ethereum.

Un contrato de opción financiera le da al comprador el derecho, no la obligación, de comprar o vender un valor a un precio predeterminado. Esencialmente, es un contrato entre comprador y vendedor que establece que el 30 de junio (fecha de vencimiento) el comprador de una opción de compra tiene derecho a comprar acciones XYZ a $ 75, y el vendedor de la opción call tiene la obligación de vender acciones XYZ a $ 75. Bajo el sistema actual, el contrato se liquida al vencimiento de Options Clearing Corporation, una cámara de compensación centralizada. Si el precio de las acciones de XYZ es de $ 80 el 30 de junio, entonces el comprador de la opción de compra ejercerá su derecho a comprar XYZ a $ 75. The Options Clearing Corporation se asegura de que el vendedor de la opción entregue acciones de XYZ a $ 75.

Usando Ethereum y el blockchain, el contrato entre el comprador y el vendedor de la opción se puede programar y almacenar en la base de datos que se conoce como blockchain. Tanto el comprador como el vendedor reservan fondos en custodia para liquidar la transacción, si al vencimiento la acción XYZ es de $ 80, la cadena de bloques Ethereum transfiere automáticamente la propiedad de XYZ del vendedor al comprador y acredita la cuenta de los compradores con la diferencia de $ 5 entre precio acordado $ 75 y el precio actual $ 80. Esto se puede lograr con solo unas pocas líneas de código de computadora, eliminando a Options Clearing Corporation y muchos otros intermediarios en el negocio de compensación. Es rápido, eficiente y se ofrece de forma gratuita.

El tipo de aplicación semifinanciera implica un premio o bonificación por trabajo computacional. Por ejemplo, los proyectos actuales de SETI son candidatos para la descentralización usando Ethereum. La Búsqueda de Inteligencia Extraterrestre (SETI) es el nombre de una colección de proyectos que buscan la vida en el espacio exterior. El más famoso es SETI @ Home dirigido por la Universidad de California-Berkeley. Bajo este proyecto, cualquier persona puede ayudar a procesar los datos recopilados mediante el uso voluntario de la computadora de su hogar con fines

computacionales. Los proyectos de SETI @ Home envían "unidades de trabajo" a las computadoras que se ofrecieron como voluntarios, y cuando se completa el procesamiento, los resultados se envían a la Universidad de California-Berkley. Si bien este proyecto ya es un proyecto de computación distribuida, depende de voluntarios. Usando Ethereum, el proyecto SETI @ Home podría ofrecer recompensas o hacer micropagos para recursos computacionales. De esta manera, la transacción es financiera, pero el resultado podría beneficiar a la sociedad por un tiempo (o daño, dependiendo de su opinión de ET).

Finalmente, las aplicaciones no monetarias pueden involucrar aplicaciones de votación o mercados predicativos. Estos mercados de predicción podrían usarse para gobernar, interrumpir los sistemas políticos representativos que gobiernan la mayor parte del mundo. Supongamos que a un pueblo le gustaría construir un nuevo parque y ha asignado $ 100,000 del presupuesto del pueblo para completar este trabajo. Sin embargo, antes de que se pueda hacer el trabajo, debe ser aprobado por los ciudadanos. Usando EVM, la ciudad podría distribuir tokens a cada ciudadano y luego configurar una dirección YES y una dirección NO. Los ciudadanos emitirían su voto enviando el token a la dirección SÍ o NO. Esta información sería procesada, asegurada y almacenada por la cadena de bloques de Ethereum. Al final del tiempo de votación predeterminado, la ciudad simplemente miraría qué billetera tenía más fichas; si SÍ tenía más fichas, entonces el parque se construiría. Esto eliminaría inmediatamente cualquier alteración de votos ya que el suministro de tokens sería fijo, por lo tanto, se reconocería que cualquier token adicional es fraudulento.

11.5- Criptoactivos: un nuevo tipo de inversión

La posibilidad de adjuntar un contrato a una transacción de moneda digital abre la posibilidad de que haya nacido una nueva clase de activo. Cuando un inversor compra un bono, está celebrando un acuerdo contractual con la empresa emisora para prestar dinero a una tasa predeterminada. Además, cuando el inversor compra una acción, tiene derecho a una parte de los beneficios proporcional a su inversión. Ambos acuerdos contractuales se pueden lograr fácilmente mediante contratos inteligentes. Curiosamente, esta nueva clase de activos se puede crear sin el uso de un banco de inversión u otros intermediarios financieros.

Estas criptomonedas y criptomonedas son realmente un híbrido de las acciones tradicionales y los bonos cruzados con una moneda. Funcionan como una acción o un bono en el sentido de que otorgan al titular un derecho sobre ciertos flujos de efectivo, pero al mismo tiempo pueden utilizarse como medio de intercambio. Por ejemplo, si Ford creó un FordCoin, podría usar un contrato inteligente para otorgarle el derecho al titular de una parte de las ganancias como las acciones de Ford. El titular de FordCoin también podría usar la moneda para comprar un vehículo nuevo. Cuando Ford recibió el FordCoin, podría convertirlo inmediatamente en moneda fiduciaria o podría mantenerlo como una inversión. Si Ford decidiera mantener la moneda para la inversión, sería similar a una recompra de acciones, donde la moneda se mantendría en el tesoro de Ford, y nunca se lanzaría a los mercados públicos. Eliminar el suministro del mercado debería tener un efecto positivo en el precio, lo que podría permitir que más clientes de Ford con FordCoins compren un automóvil.

Alternativamente, estas criptoequidades podrían usarse al igual que las ofertas públicas iniciales tradicionales. Una empresa que desee recaudar capital podría precaver una parte de la moneda como lo hicimos con Nautiluscoin y usar las ganancias de vender las monedas preestablecidas como capital para operar el negocio. Una vez más, esto se puede lograr sin un banco de inversión y sin regulación. Dicho esto, la regulación es probable que se convierta en parte del ecosistema de moneda alternativa, pero al principio tiende a ser menos onerosa que las leyes de valores tradicionales.

El problema que deben enfrentar los reguladores es que las monedas alternativas no son entidades legales y los titulares de las monedas no son parte del equipo de gestión. Esto hace que la aplicación de las regulaciones sea prácticamente imposible. Además, las monedas digitales no están domiciliadas en ningún país en particular, lo que significa que no están sujetas a ningún sistema legal. Cómo y dónde regular las monedas digitales es el mayor desafío que enfrentan los gobiernos y las agencias reguladoras.

11.6- Organizaciones Autónomas Descentralizadas (DAO)

Llevar el concepto al siguiente nivel es la noción de una organización autónoma descentralizada, DAO para abreviar. Un DAO es un grupo de personas afines que se reúnen para completar una tarea predeterminada. Estas son entidades virtuales que replican la función de una corporación sin la estructura legal. Un DAO se compone de miembros que tienen cada uno un cierto número de acciones en la organización. Los miembros de DAO tienen derecho a gastar los recursos de la organización para llevar a cabo la tarea predeterminada. Esto se puede lograr usando el sistema de votación descrito para el parque del pueblo, o puede preprogramarse durante la creación del DAO.

Los recursos del DAO pueden ser monetarios o algo físico, como el poder computacional. De hecho, al igual que una corporación legal, los tipos de recursos son ilimitados. Un uso monetario de un DAO podría proporcionar un seguro para un grupo que puede no ser elegible. En esencia, una compañía de seguros funciona como un conjunto de dinero: recauda dinero de sus miembros, invierte el dinero y paga los reclamos del grupo. Supongamos que hay un grupo que no puede obtener un seguro. Podrían formar un DAO y cada depósito una cantidad predeterminada. A continuación, el código informático instruirá a la DAO para que invierta el dinero en bonos del gobierno y pague los intereses recibidos a los accionistas de la DAO. Además, el código de computadora del DAO podría configurarse para pagar reclamos de seguro. Esto no solo eliminaría a las compañías de seguros, sino que protegería a los grupos que anteriormente no eran asegurables.

Siento que continúo escribiendo la misma frase: las implicaciones de esta tecnología (DAO en este caso) no pueden subestimarse. La tecnología DAO y blockchain no necesita eliminar por completo a las empresas, pero se pueden usar para hacerlas más eficientes. Las estructuras organizativas pueden hacerse más planas, se puede llegar a decisiones consensuadas sin interminables correos electrónicos y políticas de oficina, y los recursos se pueden asignar de manera más poderosa.

11.7- Profesor Dinero

El concepto de dinero inteligente tiene amplias implicaciones, desde la interrupción de la profesión legal y la banca hasta el replanteamiento de las estructuras organizativas corporativas. La naturaleza descentralizada de Bitcoin se está extrapolando para redefinir los principios probados y verdaderos de los negocios. La maximización de los beneficios está cediendo a la maximización de los recursos y las monedas digitales están impulsando este cambio.

Al mismo tiempo que están surgiendo las monedas digitales, la economía colaborativa está floreciendo y el concepto de blockchain es la tecnología ideal para alimentar este nuevo paradigma empresarial. Las empresas necesitarán reexaminar la maximización de los beneficios como un impulsor de valor porque con las monedas digitales, el valor puede derivarse mediante la maximización de los recursos. Es una nueva forma de ver el negocio que debe ser adoptada por la próxima generación de líderes.

Capítulo 12

He visto el futuro y funciona.

-Lincoln Steffans

12.1- Todo lo que sabe sobre negocios está mal

Todo lo que aprendió sobre los negocios está mal. Esta declaración es impactante, verdadera y está destinada a transmitir los deslumbrantes desarrollos que está generando la red descentralizada de Bitcoin distribuida. El Big Bang de Bitcoin no es una revuelta anarquista hacia un sistema económico socialista; es, de hecho, un restaurador para el capitalismo y la democracia. La descentralización pone el poder económico en manos de los ciudadanos y elimina muchas de las regulaciones que impiden que el capitalismo funcione de manera eficiente. Bitcoin, las monedas alternativas y el blockchain son las herramientas que se pueden utilizar para extraer las influencias positivas del capitalismo. Estas herramientas se pueden utilizar para crear nuevas empresas o reemplazar regímenes de divisas rotos. Además, el concepto blockchain se puede utilizar en aplicaciones más allá de la economía.

Los estudiantes de primer año de negocios aprenden que las corporaciones existen para obtener ganancias. Lo que se echa de menos es la "esperanza" implícita que se encuentra dentro del motivo de la ganancia. Las corporaciones se concibieron para unir el riesgo de largos viajes al extranjero y proteger a los inversores de pérdidas personales más allá de la inversión original. Si bien estas entidades están alimentadas por el afán de lucro, su existencia continua depende totalmente de si la sociedad valora sus productos. El valor se deriva de la función del producto final. Al final, cualquier producto que no ayude a la supervivencia humana es un bien de lujo. La esperanza implícita es que una corporación proporcionará un bien o servicio que contribuya a la evolución del ecosistema humano.

Determinar si un producto o servicio se agrega al ecosistema humano es más fácil de lo que parece, solo se necesita ver la demanda del producto. Un producto que está en alta demanda por definición se agrega al desarrollo humano. El iPhone puede parecer inicialmente un bien de lujo, pero ahora se usa para controlar la salud y la seguridad personal. La energía utilizada para extraer bitcoins puede parecer desperdiciada, pero el bitcoin se está utilizando para ayudar a los que no tienen acceso a servicios bancarios, eliminar el robo de identidad y reconstruir el sistema financiero. Una corporación puede parecer abiertamente como un calamar vampiro chupa-ganancias, pero su verdadero propósito es resolver un problema. En esencia, una corporación es simplemente un grupo de personas que acuerdan trabajar juntas para lograr un objetivo común. Este objetivo podría ser encontrar la cura para el cáncer o ganar dinero en el mercado de valores. Si este grupo falla en su tarea o su objetivo declarado ya no es valorado por la sociedad, la empresa fracasa.

La corporación moderna es un laberinto centralizado de estructuras organizativas: los vicepresidentes supervisan a los empleados, mientras que los vicepresidentes superiores supervisan a los vicepresidentes, y el CEO está a cargo de todo. Además, estas organizaciones se dividen en diferentes redes, cada una con su propia tarea específica, como contabilidad, ventas, marketing y distribución. A medida que la organización crece, la estructura se vuelve más compleja. La solución a esta complejidad ha sido la centralización; una persona, un policía de tránsito, si lo desea, dirige cada división. El defecto en esta estructura es que crea un único punto de falla. Si el CEO o el gerente no hacen su trabajo, o peor, es negligente o sin escrúpulos, entonces todo el sistema falla.

Los anales de la historia comercial están repletos de historias de advertencia sobre puntos únicos de falla. Desde Enron hasta Bernie Madoff, cuando un punto en la red controla toda la organización, el fracaso es solo un pensamiento criminal. Pero, ¿necesitamos esta complejidad? ¿Qué pasaría si las "corporaciones" o grupos de personas pudieran convocar espontáneamente y aceptar resolver un problema? ¿Cómo funcionaría? De hecho, hay un precedente histórico para las corporaciones "espontáneas". Durante el siglo XVI, se formaron entidades para viajes únicos durante los días de ensalada del comercio de especias. Cuando el barco regresó del viaje, la entidad se disolvió y las ganancias se dividieron entre los accionistas. Antes de la formación de Dutch East India Company, la primera organización multinacional, el mundo de los negocios era un sistema descentralizado que consistía en nodos formados espontáneamente para completar una tarea: el viaje. La Compañía Holandesa de las Indias Orientales cambió la forma en que se realizaban los negocios, ya que fue diseñada para sobrevivir a múltiples viajes y operar en todo el mundo. En resumen, marcó el comienzo de la era de la corporación multinacional global.

El Big Bang de Bitcoin es otro momento en el tiempo donde el mundo de los negocios tal como lo conocemos está a punto de cambiar. Durante 400 años, el péndulo se ha inclinado hacia las organizaciones empresariales multinacionales globales. Las tres empresas más grandes del mundo por capitalización bursátil son Apple, Exxon, Mobil y Microsoft; operan en todos los países del mundo y tienen más de $ 1 billón en capitalización bursátil. En conjunto, estas tres corporaciones producen más ingresos que el 87 por ciento de las economías mundiales y se ubicarían en el puesto 30 en la lista del producto interno bruto por país. La era de la organización multinacional puede haber oscilado a un extremo.

Retroceder hacia el sistema económico descentralizado de un solo viaje es la promesa de Bitcoin. El equivalente moderno de las corporaciones de un solo viaje es la organización autónoma descentralizada (DAO). El DAO es exactamente el tipo de organización que surge cuando un grupo se reúne para realizar una tarea. Utilizando el concepto blockchain y los contratos inteligentes, estos individuos pueden asignar valor a una tarea y transferir el resultado (valor) de esa tarea a cualquier persona, instantáneamente y de forma gratuita. Sin embargo, hay una gran diferencia entre los DAO y las corporaciones de un solo viaje del siglo dieciséis: estas "corporaciones" no son propiedad de nadie y existen solo en virtud de la tarea en cuestión. No hay un CEO, vicepresidente o gerente; en resumen, no hay un solo punto de falla.

En este punto, puede burlarse y replicar que en un sistema capitalista el grupo no tendría motivación sin la promesa de ganancias, y por lo tanto una organización autónoma descentralizada nunca funcionaría. Bueno, ya lo hacen.

Los mineros de Bitcoin se unen en grupos y comparten el poder de la computación con el objetivo de resolver ecuaciones matemáticas. La red bitcoin depende de estos mineros para verificar que los bitcoins no se gasten el doble. Por su esfuerzo, los mineros son recompensados con bitcoins. Estos grupos mineros dividen las ganancias entre los miembros en proporción a los recursos comprometidos. Las organizaciones no tienen un CEO, no están registradas en ningún gobierno ni tienen nómina, pero sí existen.

El motivo de ganancia todavía existe en los DAO, pero el concepto de la cadena de bloques y la recompensa de monedas para la minería crean un motor de ganancias autónomo. Siempre que los mineros tengan un ecosistema para convertir las monedas de recompensa en bienes y servicios, la entidad puede continuar alimentando el trabajo necesario para completar la tarea. Los cuatro pilares de los que depende una economía monetaria digital son la cadena de bloques, las recompensas mineras, los comerciantes y los intercambios. El blockchain es el mecanismo de transferencia de valor, mientras que las recompensas mineras proporcionan ganancias en forma

de monedas recién acuñadas. Sin embargo, estas monedas no tienen valor a menos que los comerciantes las acepten o los especuladores estén dispuestos a comprarlas.

Es esencial que las cuatro partes de la economía monetaria digital funcionen sin problemas ya que representan colectivamente el motor del sistema. Cada pieza es necesaria para crear el motivo de ganancia autosustentable en el corazón del ecosistema digital. Estos cuatro pilares son como los instrumentos en una orquesta, por separado, sus partes pueden parecer inconexas, pero cuando trabajan juntas, producen una sinfonía. Esto también hace que una economía monetaria digital sea más colectiva en el sentido de que se necesita una comunidad para que prospere. La colaboración, el intercambio y la combinación de recursos son todos sellos distintivos de la economía digital o criptonomics.

Criptonomics (Criptonomia)

El termino de criptonomia es el estudio y análisis de la economía de la moneda digital. Como hemos visto, la economía digital requiere un esfuerzo de colaboración para existir y puede diferir de la economía tradicional en el concepto del afán de lucro. En la economía tradicional, el motivo del beneficio es simple de determinar: uno simplemente necesita preguntar si los consumidores comprarán el producto final a un precio superior a los costos de producción. Si la respuesta es sí, comienza la producción y el organismo corporativo cobra vida. El marketing, el diseño, la fabricación y las ventas trabajan para obtener ganancias, ganar participación de mercado y garantizar que la corporación sea una entidad en marcha.

Sin embargo, en criptonomics, el producto final puede no ser algo que se ofrece a la venta; puede ser un bien social que se regala gratis. Esto es similar a cómo Google realiza negocios. Produce un bien y lo regala de forma gratuita y luego se beneficia del valor creado. Por ejemplo, el sistema operativo móvil de Google es de código abierto y gratuito, sin embargo, Google utiliza los datos que recopila para alimentar a más del 50 por ciento de los teléfonos móviles del mundo para vender anuncios. Las ganancias de Google se eliminan al menos un paso de su producto. Esto ocurre en criptonomics: la ganancia está separada del éxito financiero del producto final; el beneficio es una función de la interacción entre mineros, comerciantes e intercambios.

Separar el beneficio de la viabilidad financiera del producto final es un cambio radical en el capitalismo, pero no es sin precedentes. El software de fuente abierta y la economía colaborativa son las raíces de las cuales ha crecido la criptonomía. El proceso típico de toma de decisiones para una entidad que busca ganancias comienza con un análisis del mercado final, luego las entidades que buscan ganancias necesitan saber cuánto producto fabricar, a qué precio venderlo y cómo mantener la competitividad para determinar si los recursos deben ser asignados. Sin embargo, en criptonomics, el proceso de toma de decisiones se invierte: la entidad comienza con el beneficio y luego decide qué producir.

Nautiluscoin es un ejemplo perfecto del proceso de toma de decisiones criptoeconómicas. Dentro de los primeros 60 días de existencia, pudimos crear una "entidad" que tenía una capitalización de mercado de $ 1 millón sin producir un solo producto. Nautiluscoin no obtiene ganancias; no tiene un organigrama, no tiene nómina, no tiene sede y no es una entidad legal. Sin embargo, los inversores de divisas alternativas compraron la moneda y aumentaron el precio creando $ 1 millón en valor en 60 días. Ahora que se ha creado el valor, podemos tomar una decisión sobre qué producir, lo que, por supuesto, está completamente revertido de la economía tradicional. Algunas monedas deciden usar la ganancia para llevar agua a quienes la necesitan, mientras que otras deciden financiar la investigación del cáncer. Otra opción es usar los beneficios para financiar otro negocio que pueda tener un producto rentable pero que necesite capital inicial.

Transferir capital de aquellos que lo tienen a aquellos que lo necesitan es la esencia del capitalismo. Bitcoin y las monedas alternativas proporcionan el camino para devolver el sistema económico capitalista a su base.

Los proyectos y productos financiados a través de monedas alternativas tienen un motivo de ganancia, pero están separados del resultado final. Además, las monedas alternativas y los DAO pueden cumplir objetivos sin una estructura corporativa cuyo único propósito es garantizar la rentabilidad y la sostenibilidad. Si una organización puede existir para completar una tarea y no tiene una estructura corporativa, entonces el concepto de un afán de lucro se ve radicalmente alterado.

La idea del afán de lucro proviene de la teoría de la elección racional, que postula que los individuos tienden a perseguir sus propios intereses. Esta es la columna vertebral del capitalismo de libre mercado y ha impulsado la economía mundial durante siglos, para bien o para mal. Esta es también una teoría sobre la que he desarrollado mis negocios. El llamado modelo comercial "come lo que matas" alimenta gran parte de Wall Street, y es por eso que Wall Street es más una colección de empresarios que un oligopolio de grandes instituciones financieras.

Desde la crisis financiera de 2008, las firmas de Wall Street no han podido ilustrar a Main Street que gran parte de la compensación para los participantes del mercado financiero es en forma de una bonificación de rendimiento. Si un comerciante en un importante banco de Wall Street no funciona, ella no recibe ningún pago. Además, si el banco completo no funciona, el grupo de bonificación se reduce. Lamentablemente, se ha prestado demasiada atención a algunos malos actores. Todos los sistemas tienen fallas, y la crisis financiera de 2008 arrojó una luz dura sobre los defectos del sistema capitalista de libre mercado, pero, como dicen, la luz del sol es el mejor desinfectante.

Si el concepto del afán de lucro es defectuoso, ¿pueden existir corporaciones o una organización para atender las necesidades de las personas? La falla en el afán de lucro es que asume que si una empresa no es rentable, la sociedad no la valora. Por supuesto, la sociedad valora muchas cosas pero no son rentables: los servicios de emergencia y las vías públicas son dos "negocios" extremadamente valiosos que no son rentables. Ha habido algunos intentos de privatizar carreteras, pero en general estos intentos no han producido resultados espectaculares.

El desarrollo de monedas digitales, o criptomonedas, tiene el potencial de desarrollar un nuevo tipo de sistema económico. La evolución comienza con un sistema financiero descentralizado donde los jugadores del centro están desintermediados. Eliminar la fricción de los engranajes del sistema financiero permite que las nuevas entidades operen sin problemas y que los nuevos sistemas socioeconómicos broten. La Criptonomía destruye los conceptos del afán de lucro, el esfuerzo colaborativo y los bienes sociales. Las monedas digitales pueden engendrar microeconomías donde los bienes públicos de hecho pueden generar ganancias. Los DAO son el catalizador transformacional: el objetivo de un DAO puede ser obtener un beneficio, o puede ser lograr un objetivo que sea importante para un subconjunto de la sociedad. El factor distintivo de un DAO es que no tiene una estructura corporativa para financiar. Es decir, los salarios no necesitan ser pagados, los costos de atención médica son cero, y los costos de infraestructura nacen de los accionistas de la DAO. La eliminación de la mayoría de los costos organizacionales puede hacer que muchos esfuerzos no rentables sean rentables y podría potencialmente cambiar la forma en que se estructura y analiza el negocio.

El Boston Consulting Group, fundado por Bruce Henderson, es una de las tres principales firmas de consultoría empresarial y es famoso por tres estructuras que desarrollaron para ayudar a las empresas a ser más rentables y competitivas. The Growth Share Matrix, Experience Curve Effects

y Advantage Matrix están en la caja de herramientas de cada consultor. Mientras que las Tres Estrategias Genéricas de Michael Porter han guiado el proceso de toma de decisiones de muchos ejecutivos. Sin embargo, el proceso inverso de toma de decisiones de criptonomics puede volverlos irrelevantes.

12.3- Matriz de crecimiento participación – Matriz BCG

Bruce Henderson no solo hizo una fortuna al fundar el Boston Consulting Group, sino que también ayudó a otros a hacer fortuna a través de su agudo sentido de la dinámica empresarial. Henderson ha creado una amplia gama de estructuras para ayudar a los ejecutivos a conceptualizar cada parte de su negocio y analizar la rentabilidad. La más famosa de las estructuras es la Matriz de Crecimiento Compartido, también conocida como la Matriz BCG o la Matriz Boston. La Matriz de participación de crecimiento consta de cuatro cuadrantes denominados vacas lecheras, perros, signos de interrogación y estrellas, como se muestra en la figura 12.1.

Los ejes de la matriz se denominan Crecimiento de mercado y Cuota de mercado relativa. Las estrellas residen en el cuadrante que tiene un alto crecimiento del mercado, y el negocio tiene una gran cuota de mercado. Los interrogantes son líneas de negocio con un alto crecimiento del mercado, pero por alguna razón la corporación no tiene una gran participación de mercado. Los perros son líneas comerciales que tienen un bajo crecimiento del mercado y la corporación tiene una pequeña participación en el mercado. Finalmente, las vacas de efectivo son líneas de negocios que tienen mercados de crecimiento lento, pero la corporación tiene una alta participación de mercado y por lo tanto disfruta de beneficios saludables.

Figura 12.1: La matriz de participación de crecimiento

Toda la matriz está diseñada para ayudar a las empresas a asignar recursos a las empresas más rentables. Las vacas lecheras deben ser ordeñadas el mayor tiempo posible, mientras que los perros deben ser descartados (lo siento, amantes de los perros). Los signos de interrogación merecen atención solo si la organización cree que puede ganar participación de mercado y ser

más rentable. Finalmente, se supone que la mayoría de los recursos de una corporación se asignan a las estrellas, también conocidas como las empresas más rentables.

La criptonomía hace que esta matriz sea irrelevante por el simple hecho de que su premisa subyacente es que las corporaciones existen para obtener ganancias. En la criptoeconomía, existen organizaciones para completar una tarea considerada valiosa por los interesados en el DAO. Esto puede ser para obtener un beneficio, o puede ser para llevar agua fresca a una aldea. Además, aplanando la estructura organizacional podría realinear los gastos de tal manera que los perros se conviertan en una empresa rentable. Quizás es cierto que todos los perros tienen su día.

12.4- Efectos de Curva de Aprendizaje

La curva de aprendizaje se propuso y observó por primera vez durante los experimentos con humanos que memorizan números. A medida que los sujetos se volvieron más expertos en la memorización, pudieron memorizar más números más rápido. Este concepto luego se reformuló en el efecto de la curva de experiencia en 1936 en la Base de la Fuerza Aérea Wright, donde se observó que a medida que la producción de aeronaves se duplicaba, se necesitaba entre 10 y 15 por ciento menos de trabajo para producir una aeronave. Los mecánicos de la aeronave aprendían de la experiencia y lo aplicaban a su trabajo y se volvían más eficientes.

Una vez más, Bruce Henderson de BCG formalizó la curva de aprendizaje en Experience Curve. Sus primeros trabajos usaron el ejemplo de la producción del Ford Modelo T de 1906 a 1916. Vea la Figura 12.2.

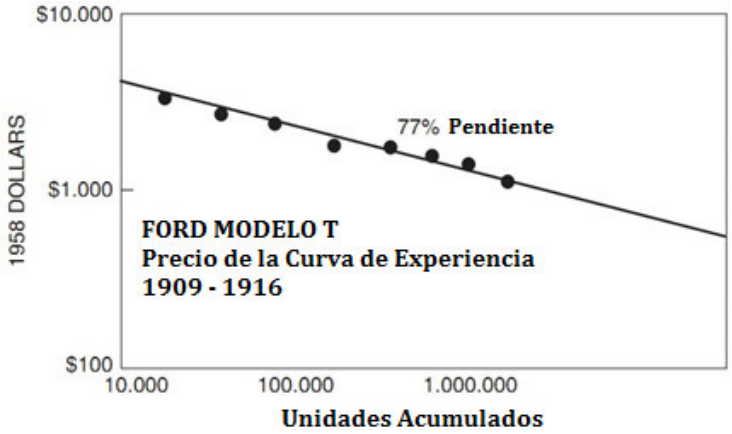

Figura 12.2: FORD MODELO T – Precio de la Curva de Experiencia: 1909 - 1916

Henderson observó que el costo de producción del Modelo T disminuía a medida que aumentaba el volumen de la unidad. Mientras su trabajo original ilustraba una relación lineal, modificó posteriormente la Curva de experiencia para incluir una función de ley de potencia. Es decir, a medida que la producción aumentaba, el costo disminuía a un ritmo cada vez mayor.

BCG utilizó esta Curva de Experiencia para asesorar a los clientes para maximizar la producción, ya que reduciría los costos y aumentaría las ganancias. El fundamento de esta observación es que la entidad está diseñada para ser continua. En el caso de una corporación, esta es una suposición válida, ya que la incorporación es indefinida. Sin embargo, en la criptonomía, los DAO pueden organizarse espontáneamente para completar una tarea, a veces con fines de lucro y, en ocasiones, de beneficio social. Dado que el objetivo del DAO es Inite, no hay una suposición de una entidad en curso y, por lo tanto, pocas tareas repetitivas para adquirir experiencia. Esto no quiere decir que la Curva de experiencia no es válida; simplemente no es una herramienta útil en criptonomia.

12.5- Las 3 Estrategias Genéricas de Porter

Michael Porter ha escrito 18 libros sobre estrategia comercial. Es un reconocido profesor de estrategia y competitividad en la Universidad de Harvard, y generalmente se le considera la autoridad en todas las cuestiones de la estrategia comercial. Es mejor conocido por sus Tres Estrategias Genéricas, que en términos simples describen cómo una empresa puede obtener una ventaja competitiva, como se muestra en la Figura 12.3.

Su matriz describe tres formas básicas para que un negocio compita: diferenciación, liderazgo de costos y enfoque estratégico. Si una empresa diferencia su producto de los demás en el mercado, entonces los consumidores pueden ser persuadidos a comprar más de este producto, y más ventas significa más beneficio. Una vez más, las suposiciones pueden ser válidas en un mundo que maximiza los beneficios, pero en criptonomics, el objetivo de la organización puede no ser la maximización del beneficio. Además, enfocarse en un nicho de mercado o reducir los costos de hecho puede permitirle a una corporación convertirse en los jugadores dominantes en la industria. Sin embargo, esto supone que tanto la industria como la corporación continuarán.

Criptonomía no necesariamente hace la suposición de preocupación en curso. Un DAO puede tener una vida útil ilimitada, pero es igualmente probable que se cancele una vez que se complete su tarea o se haya alcanzado el objetivo. En este caso, hay poca necesidad de ser el líder del mercado u obtener una ventaja competitiva ya que el mercado puede desaparecer como resultado directo de que el DAO resuelva un problema.

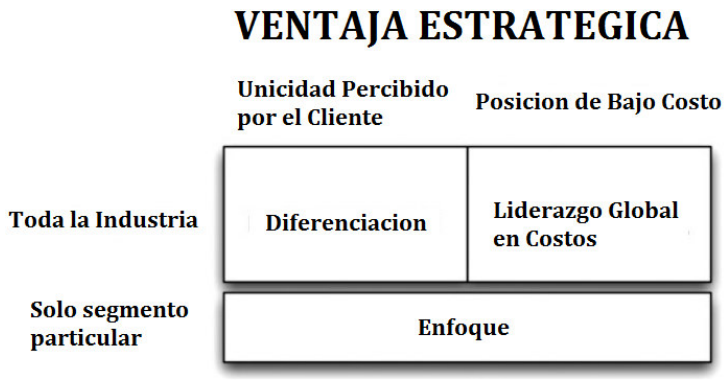

Figura 12.3: Tres estrategias genéricas

12.6- Gestión de recursos humanos

La Sociedad para la Gestión de Recursos Humanos (SHRM) fue fundada en 1948 y ha crecido hasta convertirse en la organización de comercio de recursos humanos más grande del mundo. SHRM tiene 275,000 miembros en 160 países. Menciono esto no porque me gusta escribir estadísticas, sino porque la tecnología blockchain y los DAO tienen el potencial de afectar a todo este grupo. La administración de recursos humanos se encarga de garantizar que los empleados reciban un pago y reciban un trato justo y, en general, proporcionen un lugar de trabajo saludable. Pero con un DAO no hay empleados; cada parte interesada en el DAO es un contratista independiente. Sin humanos, hay poca necesidad de administrar esos recursos.

Alternativamente, puede ser necesario integrar los DAO con las corporaciones tradicionales. La tendencia en los negocios ya es contratar tantos contratistas independientes como sea posible

para reducir los costos adicionales. Si una empresa puede contratar un DAO para resolver un problema, entonces esa relación comercial debería integrarse en la estructura organizativa actual.

La disrupción no siempre tiene que significar que las industrias se destruyen, sino que también puede significar que evolucionan.

12.7- Alimentando la Economía Compartida

Desde la crisis financiera de 2008, otra evolución económica que se ha producido es el aumento de la llamada economía colaborativa. La economía colaborativa se rige por muchos apodos, incluida la economía entre pares, la economía de malla y el consumo colaborativo, que describen un sistema económico que comparte activos humanos y físicos. La columna vertebral de la economía colaborativa es la premisa de que cuando se comparten los recursos, no solo se pueden asignar de manera más eficiente, sino que también pueden ganar valor gracias a la mayor cantidad de personas y empresas que tienen acceso. El principio principal es que los recursos no utilizados son un valor desperdiciado.

El concepto de la economía colaborativa ganó popularidad a principios de la década de 2000, cuando el software de código abierto se hizo cada vez más frecuente. La economía colaborativa busca resolver el problema de la tragedia de los bienes comunes, que afecta al modelo económico de libre mercado, es decir, cuando todos actuamos en nuestro propio interés, tendemos a reducir y desperdiciar recursos. Está más allá del alcance de este libro ahondar en si el motivo del beneficio egoísta es responsable de los defectos del capitalismo, pero lo importante es que las monedas alternativas han agregado un motor de ganancias a la economía colaborativa. Las monedas alternativas permiten que el motivo de ganancia con intereses propios impulse la economía de intercambio.

Algunas de las empresas exitosas de intercambio temprano han utilizado un modelo de negocio de alquiler / arrendamiento. Por ejemplo, tanto ZipCar como AirBnB brindan una plataforma para alquilar / arrendar horas y apartamentos de vehículos no utilizados. Este modelo funciona porque los recursos se comparten fácilmente y quienes usan el servicio obtienen utilidad del producto, es decir, el usuario de ZipCar obtiene del punto A al punto B y el cliente de AirBnB tiene un lugar para descansar. Sin embargo, cuando la utilidad es menos evidente, el modelo ha contado con la bondad de los extraños como lo hace Kickstarter.

Para los que no están familiarizados, Kickstarter es la plataforma de crowdsourcing más grande del mundo para proyectos creativos. Los proyectos creativos financiados tienen una utilidad menos obvia o amplia y, por lo tanto, se limitan a la financiación por parte de entusiastas verdaderos. Este tipo de microfinanciación es una revolución en sí misma, pero solo es escalable en la medida en que haya suficientes donantes para respaldar estos microecosistemas. Uno todavía se encuentra con el problema de vincular los beneficios o la "utilidad" con el producto final. Las monedas alternativas tienen el potencial de cambiar esta dinámica.

Si pensamos en una campaña de Kickstarter como DAO, entonces podemos aplicar todos los beneficios de criptonomia al proyecto. Supongamos que una comunidad forma espontáneamente una organización con el objetivo de producir una película documental, y para financiar la película recurren a una plataforma de crowdfunding como Kickstarter. Una campaña de recaudación de fondos exitosa requiere un número mínimo de partes interesadas con dinero para donar a fin de apoyar el proyecto. Sin embargo, con las monedas alternativas, los "donantes" no tienen por qué tener un interés personal en el proyecto en absoluto.

Si el DAO crea una moneda para apoyar el proyecto y utiliza contratos inteligentes para distribuir las ganancias futuras del documental, ampliará su potencial de recaudación de capital. Aquellos que compren la moneda alternativa recibirán una porción del flujo de efectivo de la película y tendrán el potencial para la apreciación del capital de la moneda digital. De esta manera, las monedas alternativas rompen juntos el aspecto motivacional positivo de las ganancias con motivos altruistas de apoyar un proyecto creativo. Sin embargo, esto no es solo una forma para que los especuladores de divisas se sientan bien consigo mismos; en realidad es una mejora del sistema capitalista.

El capitalismo es el mejor sistema que los humanos hemos desarrollado para asignar recursos eficientemente, hasta ahora. El mero hecho de que haya recursos no utilizados para compartir es evidencia de que el capitalismo no está funcionando tan eficientemente como puede. La economía colaborativa buscó resolver este problema de recursos desperdiciados, y con la adición de monedas alternativas, este nuevo sistema socioeconómico puede aprovechar la emoción humana primordial de la codicia.

En la clásica película de Oliver Stone, Wall Street, el villano principal es Gordon Gekko, que es reverenciado por su modelo empresarial egoísta e implacable. En un discurso seminal, frecuentemente repetido por los prometedores titanes de Wall Street, Gordon Gekko expone sobre la virtud de la codicia.

El punto es, señoras y señores, que la codicia, por falta de una palabra mejor, es buena.
La codicia es correcta
La codicia funciona
La codicia aclara, atraviesa y captura la esencia del espíritu evolutivo.
La avaricia, en todas sus formas -la codicia de la vida, del dinero, del amor, del conocimiento- ha marcado la oleada ascendente de la humanidad.

Mientras que la película era aparentemente sobre la codicia por el dinero, hay una lección que la economía compartida puede tomar de Gordon Gekko. Nos guste o no, la codicia es un gran motivador. El desarrollo de monedas alternativas junto con la interacción de la economía colaborativa y los especuladores ha creado un entorno en el que la codicia y el altruismo pueden existir juntos. De hecho, no solo pueden existir sino que pueden prosperar.

12.8- El futuro podría funcionar

Lincoln Steffens era un fanático del cambio de siglo que abogaba por la revolución política sobre la reforma. Sus puntos de vista fueron sin duda controvertidos, especialmente cuando regresó de una visita de tres semanas a la Unión Soviética en 1919. Se dice que Steffens llamó a la Rusia soviética "un gobierno revolucionario con un plan evolutivo". Su entusiasmo por la revolución soviética resultó en su frecuente frase citada "He visto el futuro, y funciona". Creía que la Revolución Soviética estaba a punto de cambiar el mundo y que a través de la colaboración y el intercambio de recursos, el futuro funcionaría mejor. Sin embargo, en el momento de su muerte en 1936, ya no estaba tan entusiasmado con la Revolución de Octubre.

El principal cambio en la Unión Soviética desde la visita de Steffen fue la muerte de Lenin y el nombramiento de Joseph Stalin como Secretario General del Comité Central. El desarrollo que es importante para Bitcoin y la criptoeconomía es que con este nombramiento se convirtió en un único punto de falla. Las atrocidades cometidas por Stalin no tenían nada que ver con el sistema económico particular elegido. Un gobierno central nefasto puede cometer crímenes de lesa

humanidad bajo el capitalismo, el comunismo o cualquier otro sistema. La centralización del poder político y financiero es el eslabón más débil.

La clave del éxito de cualquier sistema económico es una estructura política lo suficientemente flexible como para gobernar eficientemente y descentralizar el poder para los ciudadanos. La democracia es esencial para que el capitalismo cumpla su promesa de asignar de manera eficiente los recursos para atender las necesidades de la sociedad. Sin la capacidad de corregir excesos, cualquier sistema puede ser secuestrado por los poderosos política y financieramente. El concepto de un sistema transparente que permite a las partes interesadas confiar entre sí sin conocerse es un gran paso adelante en la evolución de los sistemas económicos y políticos.

La idea de una cadena de bloques transparente que se puede usar para asignar recursos colectivamente, votar y resolver problemas es la esencia de la democracia: un ser humano, un voto. Las democracias representativas que existen actualmente eran logísticamente necesarias, ya que era imposible que una nación entera votara sobre cada una de las leyes. Si bien elegimos representantes para cuidar nuestros intereses, este sistema una vez más crea un único punto de falla y actualmente desvía los incentivos hacia el interés propio.

A medida que el concepto distribuido descentralizado del blockchain nos mueva hacia los conceptos fundadores de la democracia, el sistema económico y político se volverá menos concentrado. Todos los sistemas tienen límites más allá de los cuales se rompen; en los sistemas políticos y económicos, ese límite es una centralización excesiva. Monedas alternativas; el blockchain; y el sistema transparente y sin confianza que han creado tiene el potencial de hacer retroceder el péndulo hacia un sistema económico y político más democrático.

El Big Bang de Bitcoin es una revolución social y económica que impulsará la próxima oleada de desarrollo humano. Aprovechará lo que hemos aprendido sobre el capitalismo y lo fusionará con el consumo colaborativo para producir un sistema socioeconómico impulsado por el afán de lucro pero que satisfaga las necesidades de la sociedad. La crisis financiera de 2008 fertilizó el terreno para el cambio económico. La crisis puso de relieve nuestras verrugas económicas y llevó el concepto de centralización a su punto de quiebre. A medida que el péndulo comenzó a oscilar hacia un sistema económico descentralizado, Bitcoin surgió en el momento. Bitcoin y el blockchain jugarán un papel protagonista en la nueva economía. Liberará y acelerará los sistemas financieros reconstruidos, y resolverá problemas que quizás no sepamos que tenemos. En resumen, Bitcoin es la idea correcta en el momento adecuado.

Parafraseando a Lincoln Steffens, hemos visto el futuro, y podría funcionar.