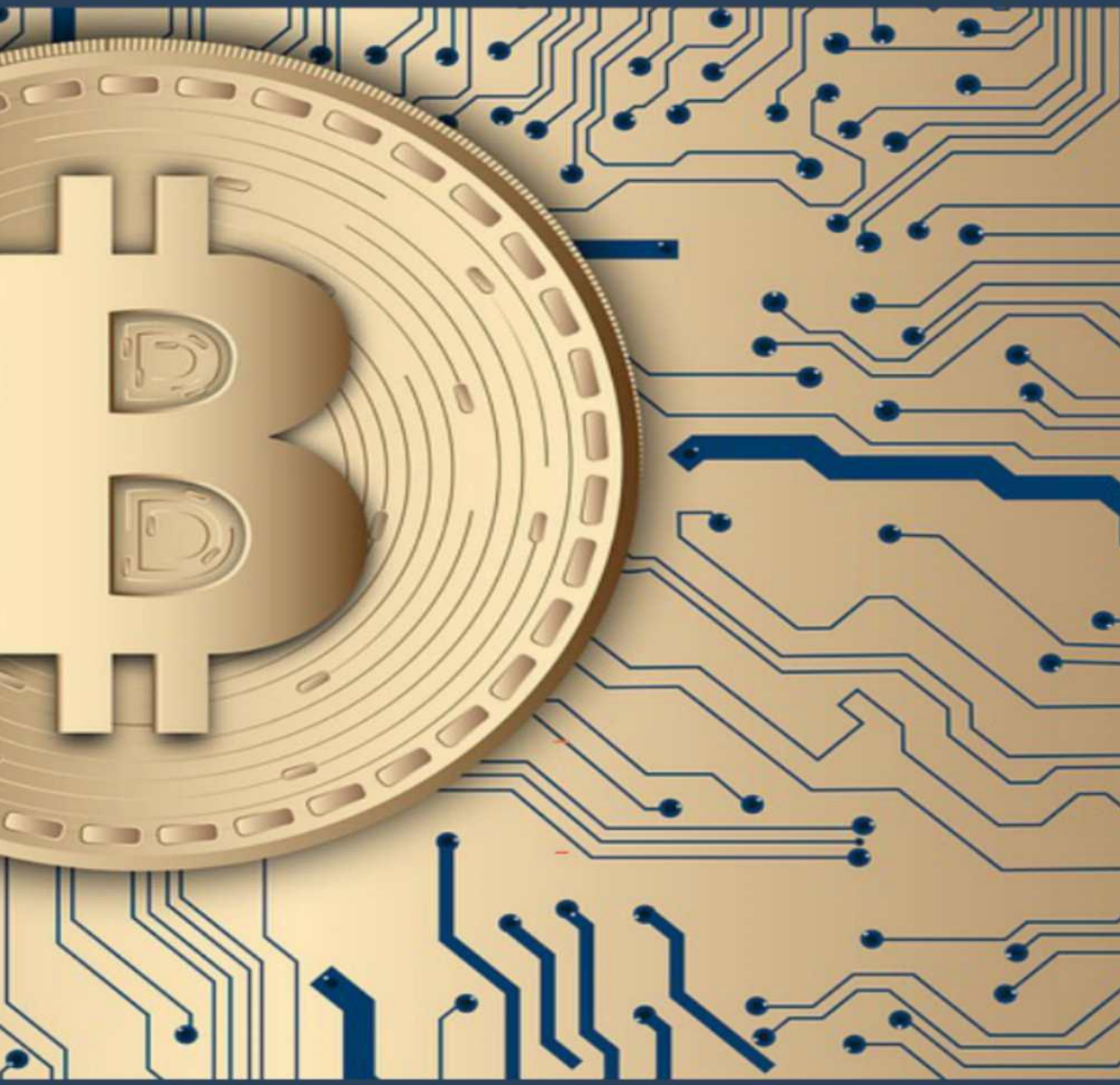
El Bitcoin...
lo que hay mas allá.



Federico Quiroz

EL BITCOIN

LO QUE HAY MAS ALLA

Federico Quiroz

El Bitcoin lo que hay más allá
@FedericoQuiroz

Coordinación y producción editorial
Carmen Valverde

Diseño y diagramación
Maride Hernández
Diseño portada
Luis palacios
Corrección de texto
Maguaría Quiroz

DEDICATORIA

A mis hijos

Federico Quiroz

A Guillermina

Mi especial socia y mujer

A todos mis colaboradores, y a todos mis lectores y alumnos

Contenido

Capítulo 1

Introducción

En las últimas dos décadas, Internet combinada con la revolución de los teléfonos inteligentes ha creado un mundo conectado permanentemente que trasciende las fronteras nacionales, las diferencias horarias y la distancia geográfica. De esta manera, Internet se ha convertido en la columna vertebral de la mayoría de nuestras actividades, no solo de comunicación y entretenimiento, sino también de actividades económicas, como el comercio o el trabajo. Para la década de 2018, se ha vuelto realmente difícil, si no imposible, vivir sin usar

Internet de una forma u otra.

El progreso tecnológico también afectó cómo almacenamos nuestro dinero y cómo pagamos por los bienes y servicios que necesitamos. Lo más intrigante es que estamos cambiando nuestra percepción de lo que el dinero es, o puede ser, y estamos empezando a experimentar con tipos de dinero que no se han visto antes en la historia de la humanidad: las monedas digitales. Las monedas digitales solo viven en el mundo virtual de Internet, las computadoras o los teléfonos inteligentes. Tienen nombres que suenan extraños, se rigen por reglas a menudo desconocidas y nos exigen que

adoptemos nuevos hábitos si queremos usarlos. Algunas de las monedas digitales provienen de emisores con los que estamos familiarizados, por ejemplo, redes sociales como Facebook o plataformas comerciales como Amazon. Otros pertenecen al misterioso grupo de criptomonedas: las monedas digitales que no tienen ninguna persona o institución que administre su emisión, no tienen autoridad que las regule y operan a través de una red descentralizada de igual a igual.

Si bien las monedas emitidas por empresas como Amazon y Facebook son posiblemente más importantes en la economía, son las criptomonedas las que

impulsan el interés de las personas en las monedas digitales. Ciertamente merecen la atención debido a la innovación técnica que representan. Por ejemplo, Bitcoin incluye un algoritmo sofisticado que resuelve un enigma informático de larga data, conocido como

"El problema de los generales bizantinos". A pesar del nombre colorido del problema, relativamente pocas personas han oído hablar de él. Y sin embargo, la mayoría de nosotros hemos oído hablar de Bitcoin. Esto se debe a la tentadora implicación de una solución al oscuro problema con un nombre colorido: la posibilidad de que

los sistemas de pago, o incluso las monedas, operen en una red distribuida, sin emisores o instituciones que los controlen o administren y con suficiente seguridad para resistir los intentos maliciosos de infiltrarse. Como veremos, esta innovación tiene el potencial de cambiar significativamente la economía, desde la forma en que se envían las remesas transfronterizas, a hacer que los micropagos sean económicamente sostenibles, a ofrecer una manera de realizar transacciones en línea que proteja la privacidad mejor que cualquier otro método, a cambiar La forma en que se hacen cumplir los contratos.

El momento de la innovación no podría haber sido mejor. Casi al mismo tiempo, el mundo experimentó la mayor crisis financiera global en la historia moderna. La crisis llevó a algunas personas a cuestionar la administración de las monedas emitidas por el estado y las instituciones involucradas en ella, en particular, el sector financiero y el gobierno. Los bancos en dificultades y, de hecho, las operaciones bancarias reales destacaron el potencial la fragilidad de las instituciones financieras tradicionales como lugares seguros para los depósitos de las personas, mientras que la deuda gubernamental extraordinaria en muchos

países planteaba dudas sobre el valor futuro de las monedas emitidas por el estado. Esto llevó a algunos a la conclusión de que había llegado el momento de crear un sistema de dinero seguro, práctico para las interacciones económicas globales y, lo que es más importante, independiente de las grandes instituciones financieras y gobiernos existentes. Un aspecto importante de la justificación económica de un sistema monetario de este tipo se ha basado en el argumento de que los sistemas de transferencia internacional actuales son caros e inflexibles, lo que impone costos no razonables a individuos y empresas. Más allá de estas razones económicas, algunas personas, quizás influenciadas

por un ideal libertario, también sintieron la necesidad de un sistema de dinero que, simplemente, está fuera de la vista de los gobiernos.

Bitcoin ha captado la atención de los medios también debido a su asociación con la economía sumergida. Algunas personas siempre han buscado el secreto y el anonimato en un sistema de pago alternativo con el fin de escapar de la ley. Desde su aparición, Internet y el comercio electrónico se han utilizado para actividades ilegales, principalmente para el comercio de armas y drogas.

El tamaño de este comercio ilegal es difícil de estimar, pero su orden de

magnitud es de miles de millones de dólares estadounidenses. Uno de los elementos más conocidos de esa economía sumergida fue Silk Road, ampliamente cubierto por los medios de comunicación, especialmente después de octubre de 2013, cuando la policía estadounidense cerró el sistema y arrestó a su fundador, Ross William Ulbricht. En 2015, Ulbricht fue condenado por administrar el sitio y condenado a cadena perpetua. Silk Road fue solo uno de los muchos, aunque posiblemente uno de los más grandes, sitios web que se especializaron en hacer coincidir compradores y vendedores de productos ilegales, operando en la llamada "red oscura",

una capa de Internet donde la actividad no se puede rastrear (fácilmente) De vuelta a las ubicaciones físicas de sus participantes. Para las personas involucradas en tales actividades ilegales. Las actividades comerciales, un sistema de pago que garantiza el secreto y el anonimato siempre ha sido una propuesta muy atractiva.

Lo que alimentó el frenesí de los medios fue la mística que rodea al primer sistema de criptomonedas, Bitcoin. Bitcoin fue introducido en 2008 por un misterioso personaje llamado Satoshi Nakamoto, cuya identidad real es desconocida. Con una adopción rápida y relativamente amplia, la criptomonedas

estaba experimentando un éxito fenomenal, al menos hasta 2013.

Desde entonces, ha sufrido una serie de reveses debido a una variedad de factores interrelacionados, que incluyen una caída del mercado, fraude, problemas de seguridad y desafíos regulatorios de varios gobiernos. Más importante aún, el éxito inicial de Bitcoin ha llevado a una proliferación increíble de criptomonedas competidoras. Hoy en día, el complejo ecosistema que surgió enfrenta una considerable incertidumbre, lo que plantea la pregunta: ¿Cómo será el futuro de las finanzas después de la "explosión cámbrica" de las

criptomonedas?

Antes de siquiera considerar esta pregunta, hay que darse cuenta de que el universo de las monedas digitales va mucho más allá de las criptomonedas. De hecho, ha surgido una nueva familia de monedas digitales paralelamente a Bitcoin y sus competidores. El aumento de estas monedas también está estrechamente relacionado con el surgimiento de Internet, y ha sido motivado por las necesidades de las grandes empresas de Internet: Amazon, Facebook, Tencent, etc.

La conectividad permanente y ubicua proporcionada por Internet también ha dado lugar a estas nuevas empresas que

permiten que una gran cantidad de personas interactúen de manera sofisticada. Las redes sociales, las plataformas de comercio electrónico, las plataformas de juegos en línea o los mundos virtuales se denominan

"Plataformas de transacciones" que crean valor al facilitar el intercambio entre sus miembros, que a menudo representan diferentes grupos de consumidores: compradores, vendedores, anunciantes o desarrolladores. La naturaleza del intercambio, ya sea es social / comercial, ya sea para entretenimiento o para un propósito profesional / comercial en particular, a menudo define

el modelo de negocio de la plataforma, incluida su propuesta de valor y la forma en que la plataforma obtiene sus ingresos. Si bien estas propuestas de valor y modelos de ingresos varían sustancialmente entre las plataformas de transacción, es bastante natural que la mayoría de ellos ofrezcan la posibilidad de un intercambio económico entre sus miembros y entre estos miembros y la plataforma en sí. Esto plantea la cuestión de la necesidad de un medio de intercambio, esencialmente un sistema de pago eficiente, que pueda adaptarse a las necesidades especiales de la plataforma. Muchas empresas de plataformas han considerado introducir una moneda especial para proporcionar

una. Las monedas basadas en plataformas son, por definición, monedas centralizadas donde las plataformas controlan (en la medida de lo posible) las "reglas" que rigen el uso de sus monedas.

Curiosamente, los problemas centrales que guían la introducción de estas monedas basadas en plataformas son muy diferentes de las de las criptomonedas. Mientras que en este último caso, el objetivo es Cree una moneda completamente funcional para reemplazar las monedas emitidas por el estado, las monedas basadas en plataformas intentan diseñar sus sistemas de pago a propósito con

objetivos específicos en mente. Esto generalmente se reduce a restringir algunas de las funcionalidades de sus monedas.

Sin embargo, a pesar de estas restricciones, las monedas basadas en plataformas capturaron la imaginación del público en la misma medida en que lo hizo Bitcoin, sin duda en parte debido a estas plataformas. Gran tamaño y naturaleza global. Por ejemplo, cuando Facebook avanzó con sus Créditos de Facebook en 2011, los comentaristas los vieron como una amenaza para las monedas emitidas por el estado. "¿Podría un gigantesco no soberano, como Facebook algún día lanzar una

moneda real para competir con el dólar, el euro, el yen y similares?", Escribió Matthew Yglesias (2012).

De manera similar, el reconocido economista de pagos David Evans (2012) escribió: “Las compañías de juegos sociales podrían pagar a los desarrolladores de todo el mundo con créditos de Facebook y los pequeños empresarios podrían aceptar créditos de Facebook porque podrían usarlos para comprar otras cosas que necesiten o recompensar a los clientes con ellos. En algunos países (especialmente aquellos con deudas nacionales que son mayores que sus PIB), los créditos de Facebook podrían convertirse en una moneda más

segura que la moneda nacional". Se expresaron preocupaciones similares cuando Amazon introdujo Amazon Coins en 2013. Market Watch, afiliado al Wall Street Journal, Yo escribí: "Pero a largo plazo, lo que más debería preocupar a los [bancos centrales] es perder su monopolio en la emisión de dinero.

Empieza a surgir una nueva generación de monedas virtuales, y algunos de los gigantes de la industria de la web, como Amazon.com Inc., están entrando en el mercado". Como veremos más adelante, muchas de estas preocupaciones son exageradas, incluso si en algunos casos, las monedas basadas en plataformas han tenido un impacto mucho más allá del

negocio de sus emisores.

El objetivo de este libro es explorar el universo joven y dinámico de las monedas digitales para comprender sus orígenes y su significado para nuestras economías. Nos acercamos a estas monedas desde el punto de vista de los economistas, analizando las necesidades que satisfacen para los clientes y comerciantes, los incentivos que crean para sus usuarios y la forma en que compiten con otras monedas potenciales en el mercado. Siempre que sea posible, lo haremos de una manera que abstraiga los detalles técnicos de cómo funcionan las monedas digitales, haciendo que este libro sea adecuado para personas con

poca experiencia o educación en informática, criptografía, etc.

A veces no podemos evitar hablar de los aspectos técnicos de una moneda, por ejemplo, apenas podemos evitar discutir el ingenioso algoritmo que subyace en las criptomonedas como Bitcoin, pero intentará hacerlo de la manera más accesible posible. En lugar de crear un manual técnico, pretendemos describir las fuerzas económicas que rigen la evolución de las monedas digitales.

El objetivo es comprender por qué ciertos modelos parecen tener éxito sobre otros: qué impulsa la competencia entre monedas alternativas, qué moneda es probable que prevalezca si una

moneda puede reemplazar a otra, y qué características de diseño (o restricciones) tienen sentido en contextos económicos o empresariales determinados.

Con este fin, comenzaremos desde el principio: describiremos cómo las sociedades humanas inventaron el dinero, cómo el dinero facilitó las transacciones y cómo las debilidades en el diseño del dinero llevaron a la innovación y mejoras en la forma en que pagamos por las cosas. Las monedas digitales pueden parecer muy alejadas de esa historia, o incluso de la prehistoria, del dinero.

Sin embargo, este resumen histórico nos

permite identificar algunas de las fuerzas económicas centrales que impulsan el uso de diferentes tipos de dinero, resaltar las necesidades específicas que sirve el dinero e ilustrar los atributos clave que debe tener el dinero. Estas necesidades y atributos son notablemente universales, y son tan importantes ahora como lo fueron hace siglos. Su análisis sentará las bases para nuestra posterior discusión sobre las monedas digitales y nos dará un marco para analizarlas.

Tal marco es de importancia crítica. Sin ella, puede ser difícil entender qué está sucediendo exactamente en el universo de la moneda digital. Gran parte de la

narrativa que rodea a las monedas digitales es un poco sensacionalista, sin duda influenciada por los tumultuosos eventos que rodean la introducción de las monedas digitales, o los espectaculares desarrollos en Bitcoin, no solo su ascenso a una inmensa popularidad sino también los episodios menos optimistas del cierre de la Ruta de la Seda. O el cierre del monte. Intercambio de Gox. Comenzar con un marco económico nos ayudará a ver a través de la confusión para comprender mejor el fenómeno de las monedas digitales y su potencial para cambiar nuestra economía.

En la siguiente parte del libro, usaremos

este marco para explorar el universo de las monedas digitales basadas en plataformas que son administradas centralmente por las empresas que las han introducido. Analizaremos las fuerzas económicas que lo hicieron atractivo para que Amazon emita la Moneda de Amazon o para que Facebook emita los Créditos de Facebook, y por qué Facebook decidió cerrarla poco después. Aquí, también discutiremos qué impulsa la elección de la plataforma de características de diseño particulares para su moneda.

Resulta que las monedas digitales basadas en plataformas difícilmente podrían funcionar como dinero en el

sentido amplio de la palabra: no porque sean inherentemente defectuosos, sino porque las plataformas que los emiten hacen un gran esfuerzo para desactivar las funciones principales que son necesarias para una moneda ampliamente adoptada.

Veremos que esto no debería sorprender: tales restricciones encajan bien con los modelos de negocios de las plataformas y hacen que sus monedas sean más útiles para generar un mayor beneficio para la plataforma.

Una adopción generalizada, y tal vez incluso desplazando a las monedas emitidas por el estado, es algo que se discute a menudo en el contexto de las

monedas digitales descentralizadas, o criptomonedas como Bitcoin. Discutimos estas innovaciones en la última parte del libro. Nos fijamos en la evolución en curso de su diseño, el valor que proporcionan más allá de las alternativas existentes y algunos de los desafíos que enfrentan actualmente.

Volvemos de nuevo a nuestro marco económico y mostramos que muchas de las características de las criptomonedas están diseñadas específicamente para abordar una necesidad económica particular que en el pasado ha sido satisfecha por una característica correspondiente del dinero tradicional, es decir, no digital. Esto nos ayuda

identifique características que pueden ser llamativas y ampliamente discutidas pero que no cambian la economía de una criptomonedas y que hacen que una nueva criptomonedas, para todos los propósitos prácticos, sea tan útil o tan prometedora como la anterior.

También observamos el ecosistema en el que existen las criptomonedas, centrándonos en sus partes más significativas desde el punto de vista económico. Por ejemplo, analizamos la evolución y el papel de los intercambios de criptomonedas en línea y analizamos la eficacia con la que funcionan como parte de la infraestructura de criptomonedas.

Finalmente, discutimos la competencia entre varias criptomonedas (en el momento de escribir este artículo, hay unos cientos de ellas que se negocian activamente) y, quizás de manera más tentadora, la competencia entre una criptomonedas y las monedas tradicionales emitidas por el estado, tales como Dólar estadounidense.

Tales discusiones a menudo se convierten en especulaciones sobre el futuro, una tentación que no hemos podido resistir. Al mismo tiempo, reconocemos claramente que es demasiado pronto para pintar una imagen exacta, dada la experimentación a gran escala que aún está en curso. Más

importante aún, tales pronósticos son particularmente difíciles a la luz de la incertidumbre sobre cómo responderán los gobiernos al surgimiento de las monedas digitales. En este sentido, nuestro libro no es una pieza de política sobre banca central o regulación de divisas. Más bien, es un análisis de las fuerzas económicas que impulsan el surgimiento y el uso eficiente de los sistemas de dinero competidores aplicados al mundo digital.

Capítulo 2

Medio de intercambio: Competencia siempre presente

Las monedas digitales son solo una innovación reciente, y su uso generalizado sigue siendo una cosa del futuro. Es conveniente, sin embargo, comenzar nuestra investigación mirando el pasado.

De hecho, no solo comenzaremos mucho antes de la era digital, sino también antes del desarrollo del dinero. No tenemos la intención de proporcionar una descripción completa de la historia del dinero aquí.1 Más bien, en nuestra

discusión nos centraremos en los atributos de las diferentes monedas y las diversas necesidades económicas a las que sirve el dinero. En una perspectiva histórica, podemos analizar las fuerzas competitivas que hacen que algunos medios de intercambio sean más exitosos que otros para satisfacer esas necesidades. Más adelante veremos que las monedas digitales pueden ser exitosas solo si satisfacen dichas necesidades, así como, o mejor que, las monedas tradicionales que ya tenemos en uso.

También haremos un resumen de los diversos objetos y tecnologías que han servido como dinero o, más

ampliamente, como medio de intercambio. Veremos ejemplos de la coexistencia de varias monedas, episodios que sugieren una posibilidad tentadora de que, en el futuro, las monedas digitales no puedan coexistir. Solo junto a otras monedas digitales pero también al lado del dinero tradicional.

Finalmente, hablaremos de la competencia entre diferentes monedas. Nuevamente, las ideas de este análisis serán útiles en una discusión posterior. Por ejemplo, las monedas digitales se están introduciendo junto con el dinero tradicional, y necesariamente deben competir con él. Eventualmente, si las

monedas digitales ganan una adopción más generalizada, es posible que debamos revertir estos argumentos y usarlos para discutir si el dinero tradicional puede sobrevivir a largo plazo en presencia de las monedas digitales.

Con esta hoja de ruta en mente, avancemos y comencemos con una breve historia de cómo operamos.

2.1. El medio de intercambio—Panorama histórico

Si les preguntara a sus amigos por qué las economías modernas necesitan dinero, lo más probable es que respondan "para comprar cosas". Esta respuesta sería tan simple como

engañosa. Es cierto que necesitamos dinero para facilitar el comercio, pero hubo un momento en la historia de la humanidad en el que las transacciones ocurrieron sin dinero. La mayoría de nosotros hemos escuchado sobre el trueque, el intercambio de un producto o servicio directamente por otro producto, sin el uso de dinero. Pero las primeras transacciones económicas probablemente son anteriores incluso a ese desarrollo. En esencia, las primeras transacciones se basaron en la confianza. No había necesidad de dinero en los grupos de cazadores-recolectores preagrarios.2 Los miembros del grupo eran todos responsables de la provisión comunitaria de bienes. El grupo realizó

un seguimiento de la contribución de cada miembro e impuso multas para minimizar el potencial de free-riding. La memoria colectiva del grupo sirvió como un libro de contabilidad o quizás una cuenta bancaria prehistórica. Miembros que contribuyeron al bienestar del grupo podría contar con ser correspondido en el futuro. El beneficio colateral de este arreglo simple pero ingenioso fue el crédito. Un miembro de un grupo podría contar con la posibilidad de recibir bienes y servicios, incluso si aún no ha obtenido suficientes "puntos brownie" para justificarlos. Mientras el grupo se acordara de la transacción, podrían

esperar que el miembro la pague con buenas acciones en el futuro. Si el miembro no lo hizo, entonces el grupo podría presumiblemente disciplinar al miembro al no permitirle participar en el sistema en el futuro.

Por supuesto, contar con memoria colectiva solo funciona si el grupo es de un tamaño relativamente pequeño. Con el tiempo, los grupos se hicieron más grandes; por ejemplo, la gente comenzó a establecerse en las primeras ciudades. Con el tiempo, las personas no pudieron realizar un seguimiento de las contribuciones individuales. Además, a medida que los diferentes grupos comenzaron a comerciar entre sí, se hizo

necesario comerciar con personas que no estaban familiarizadas, y por lo tanto, cuyas contribuciones anteriores eran desconocidas y que difícilmente podrían ser disciplinadas por no pagar un producto en el futuro.

Sin la ayuda de la memoria colectiva y la disciplina impuesta por el grupo, las transacciones se volvieron riesgosas: ya no podría estar seguro de que las personas con las que comerciar le pagarían más tarde. No obstante, cuando las personas ven ganancias suficientemente grandes del comercio, por lo general encuentran una manera de realizarlas. La forma más sencilla de hacerlo es intercambiar bienes

inmediatamente, sin esperar un reembolso incierto en el futuro. Por lo tanto, la falta de familiaridad de los comerciantes no detuvo las transacciones por completo, sino que las obligó a basarse en un intercambio inmediato de bienes por bienes: el trueque.

El trueque funciona muy bien, siempre que encuentre un vendedor que ofrezca algo que quiere y si al mismo tiempo tiene algo que el vendedor quiere a cambio. En la práctica, esta "doble coincidencia de deseos" puede ocurrir con poca frecuencia.3 Este es un problema importante que limita el comercio. Si desea obtener un bien

particular, puede que ya sea difícil para usted encontrar a alguien que tenga ese bien que ofrecer; será aún más raro que tengas algo que esa persona quiera a cambio.

Es posible que deba depender de cadenas más largas de compradores y vendedores: para obtener algo que la persona **A** quiere, primero tengo que comerciar con la persona **B**. Pero, por supuesto, puede ser aún más difícil encontrar a tres o más personas con participaciones y deseos adecuadamente alineados y hacer que lleguen al mismo lugar al mismo tiempo. Afectar a todos los comercios al mismo tiempo también es más seguro.

Con más partidos, la primera persona en entregar su bien es la última en recibir el bien negociado. Existe el riesgo de que algo salga mal en el camino, y la primera persona en la cadena puede perder su bien original y no recibir mucho a cambio.

El trueque tiene un inconveniente más: la coincidencia de tiempo.

Por ejemplo, muchos productos son estacionales y pueden ser difíciles de almacenar por períodos de tiempo más largos. En el otoño, es posible que tenga algunas bayas que le agradaría intercambiar por carne cuando llegue el invierno, pero como todavía faltan unos meses para el invierno, no podrá

cambiar las mercancías en una transacción de trueque. Por lo tanto, para que una transacción de trueque sea exitosa, las dos partes no solo necesitan desear sus productos respectivos, sino que también deben quererlos y tenerlos disponibles al mismo tiempo. Debido a tales fricciones, muchos intercambios potenciales pueden no ocurrir, dejando a las partes que se hubieran beneficiado del comercio en una situación peor.

A medida que las sociedades se hicieron más grandes y surgieron nuevas oportunidades comerciales entre varios grupos, aumentaron estas fricciones y los beneficios perdidos del comercio.. Esto ilustra la función principal del

dinero, intuitivamente obvia para la mayoría de las personas: el dinero está ahí para facilitar el comercio, para superar la doble coincidencia y los problemas de tiempo y nos permite obtener los bienes y servicios que necesitamos.

Esas primeras sociedades que coordinaron el uso de tokens o bienes intermedios tuvieron más oportunidades para comerciar. Los tipos más tempranos de tales bienes intermedios, que se remontan al menos a aproximadamente 3000 AC, estaban relacionados con productos alimenticios como la cebada. El uso de alimentos populares ayudó a aliviar el primer

problema, la coincidencia de necesidades. Todos en una sociedad consumían alimentos similares, lo que los convertía en un producto atractivo para todos los miembros de la sociedad ("todos podríamos usar más cebada"). Por supuesto, la innovación fue que las personas comenzaron a aceptar la cebada no solo para su propio consumo, sino también con la expectativa de usar la cebada para otras transacciones futuras. Es probable que esta innovación no haya sido decretada por un gobernante ("todos usaremos cebada como dinero"), sino que ocurrió de manera orgánica. En cualquiera de los dos casos, el dinero, en el sentido en que normalmente lo llamamos hoy en

día, nació. Sin embargo, este primer dinero también sirvió otro papel útil: era la comida.

Los productos alimenticios utilizados para facilitar el comercio diferían entre las sociedades. La cebada, probablemente el primer ejemplo histórico, se usó en la antigua Mesopotamia. La sal se ha utilizado en China en el siglo XIII y en Etiopía desde el siglo XVI hasta el siglo XX, mientras que el imperio azteca adoptó los granos de cacao. Todos estos ejemplos comparten algunos rasgos importantes. Primero, eran relativamente uniformes y fáciles de dividir. Uno puede hacer unidades más pequeñas o más grandes,

por peso o volumen (apenas), rompiendo trozos cada vez más grandes (sal) o recolectando cantidades más pequeñas o más grandes (granos de cacao). Si mide la cebada con una taza estándar, la taza tendrá una cantidad similar de la Sólo los alimentos relativamente duraderos fueron adoptados como dinero. En esto, claramente dominaron otros artículos de alimentos tales como frutas perecederas, pescado o leche. No obstante, no pudieron almacenarse indefinidamente, y en ocasiones duraron solo una temporada o, como mucho, unas pocas temporadas.

Los productos alimenticios se deterioran

rápidamente por varias razones. El dinero del alimento podría perecer cuando se expone a los elementos o, más prosaicamente, podría ser consumido por los animales.

El dinero siguió evolucionando y, alrededor del año 1200 a. C., apareció una innovación: dinero basado en fichas que no estaban relacionadas con los alimentos. Quizás el más conocido de estos tokens fueron las carcasas cowry, de uso generalizado en África durante cientos de años. El rango de tal dinero era, sin embargo, mucho mayor. Para dar solo dos ejemplos más coloridos, hasta que los dientes de ballena del siglo XIX sirvieron como dinero en Fiji y, en las

Islas del Almirantazgo, los dientes de perro desempeñaron el mismo papel hasta el siglo XX.4

Este dinero basado en fichas tenía claras ventajas con respecto a los productos alimenticios. Las fichas se mantendrían durante mucho más tiempo que una temporada. También eran más fáciles de almacenar o transportar en distancias más largas. Una característica importante de las monedas basadas en fichas era que las fichas representaban el valor de una manera más abstracta y simbólica que la cebada o el cacao, ya que tenían menos valor intrínseco que la comida. Por lo general, tenían un significado cultural, y también se

utilizaban para la decoración.

Curiosamente, no está claro si se convirtieron en moneda porque tenían un significado cultural o si obtuvieron el significado porque podían usarse en intercambios y, por lo tanto, representaban más valor.

A lo largo de estas ventajas, hubo algunos inconvenientes distintos. Mientras que los alimentos que se usaban como monedas eran relativamente uniformes, los tokens usados como dinero variaban mucho en formas, tamaños y colores. Estas diferencias, que ocurren naturalmente en conchas, dientes, etc., lo hicieron más difícil. Moneda del producto alimenticio

este año y el próximo, en su hogar o en una aldea vecina. Sólo los alimentos relativamente duraderos fueron adoptados como dinero. En esto, claramente dominaron otros artículos de alimentos tales como frutas perecederas, pescado o leche. No obstante, no pudieron almacenarse indefinidamente, y en ocasiones duraron solo una temporada o, como mucho, unas pocas temporadas.

Los productos alimenticios se deterioran rápidamente por varias razones. El dinero del alimento podría perecer cuando se expone a los elementos o, más prosaicamente, podría ser consumido por los animales.

El dinero siguió evolucionando y, alrededor del año 1200 a. C., apareció una innovación: dinero basado en fichas que no estaban relacionadas con los alimentos. Quizás el más conocido de estos tokens fueron las carcasas cowry, de uso generalizado en África durante cientos de años. El rango de tal dinero era, sin embargo, mucho mayor. Para dar solo dos ejemplos más coloridos, hasta que los dientes de ballena del siglo XIX sirvieron como dinero en Fiji y, en las Islas del Almirantazgo, los dientes de perro desempeñaron el mismo papel hasta el siglo XX.4

Este dinero basado en fichas tenía claras ventajas con respecto a los productos

alimenticios. Las fichas se mantendrían durante mucho más tiempo que una temporada. También eran más fáciles de almacenar o transportar en distancias más largas. Una característica importante de las monedas basadas en fichas era que las fichas representaban el valor de una manera más abstracta y simbólica que la cebada o el cacao, ya que tenían menos valor intrínseco que la comida. Por lo general, tenían un significado cultural, y también se utilizaban para la decoración.

Curiosamente, no está claro si se convirtieron en moneda porque tenían un significado cultural o si e obtuvieron el significado porque podían usarse en

intercambios y, por lo tanto, representaban más valor.

A lo largo de estas ventajas, hubo algunos inconvenientes distintos. Mientras que los alimentos que se usaban como monedas eran relativamente uniformes, los tokens usados como dinero variaban mucho en formas, tamaños y colores. Estas diferencias, que ocurren naturalmente en conchas, dientes, etc., lo hicieron más difícil. Para las personas que usan la moneda para acordar qué "precios" ellos representaban Por ejemplo, un pez podría valer tres dientes de perro, pero tal vez el vendedor exigiría cuatro dientes si los dientes fueran

particularmente pequeños. En algunos casos, tales diferencias entre los tokens se utilizaron para la ventaja. Por ejemplo, en la Isla Yap, las conchas de vaqueros de labios azules, un tipo más raro que el tipo más popular de labios amarillos, sirvieron como moneda de "denominación más alta".

Un tipo particular de dinero simbólico eran piezas de metal.

El primer uso del metal como moneda que conocemos ocurrió en la antigua Mesopotamia, en 2500 a. C. El metal demostró ser incluso más duradero que las conchas o los dientes. También era fácilmente divisible en unidades más pequeñas, y estas unidades podrían

compararse directamente entre sí en función de su peso. Esto representó una mejora sobre las conchas o dientes naturales.

No obstante, los metales no habían resuelto completamente el problema de las unidades no uniformes. Si bien era fácil pesar piezas de metal, había varios tipos de metales de uso común: cobre, plata y, por supuesto, oro. Además, incluso un tipo de metal puede tener una pureza diferente. Estas diferencias causaron dificultades y riesgos adicionales al realizar transacciones, particularmente cuando las personas sin conocimiento especializado utilizaban el dinero de metal.

El riesgo en torno al valor del pago recibido haría que algunos vendedores desconfiaran, y podrían evitar algunas operaciones que de otra manera podrían ser beneficiosas.

El problema de las unidades no uniformes fue el impulsor de la próxima innovación: las monedas basadas en metales. Estas piezas uniformes de metal, con un sello que certifica indirectamente el peso y la pureza, representan unidades uniformes. Dos monedas con el mismo sello fueron consideradas equivalentes; diferentes sellos fueron reconocidos fácilmente como indicadores acordados del peso de la moneda o tipo de metal. Esto hizo

transacciones/intercambios de metal para mercancías, mucho más fácil. Uno no necesitaba tener escalas a mano y saber cómo usarlas o tener experiencia para juzgar la pureza del metal. Uno podría confiar en el sello como indicador de valor. Esto, por supuesto, funcionó bien cuando las personas confiaban en el sello. Típicamente, las mentas serían controladas directa o indirectamente por el soberano. El beneficio de la moneda dependía entonces de la confianza de la gente en la autoridad e integridad del gobernante. Cuando las personas no confiaban en el sello, volvieron a los métodos más antiguos de pesar y verificar la pureza del metal.

Las primeras monedas fueron introducidas en el reino de Lydian en el siglo séptimo antes de Cristo. Fueron acuñados de electrum, una mezcla natural de oro y plata, pero pronto siguieron las monedas de plata y oro. Una innovación interesante en ese momento era que las monedas de Lydian eran relativamente pequeñas, lo que facilitaba el almacenamiento y el transporte de la moneda. Mientras que el metal anterior se usaba para transacciones de gran valor, cada moneda valía unos pocos días de la mano de obra Trabajo o una pequeña parte de una cosecha. Esto abrió lo que podría llamarse un mercado minorista a

más oportunidades comerciales.

La invención de Lydian resultó ser más atractiva que los tipos de dinero anteriores. La invención se extendió rápidamente por todo el Mediterráneo, y las monedas de metal de diferentes valores y tamaños se convirtieron en la principal herramienta del comercio en el mundo occidental hasta el Renacimiento. El modelo básico se mantuvo sin cambios hasta ahora. Las monedas siguen siendo discos de metal con un sello que certifica el valor de la pieza.

La siguiente innovación significativa en dinero fue el papel moneda. Históricamente, se introdujo por primera vez en China en el siglo VIII. Es posible

que Marco Polo haya llevado la idea del papel moneda a Europa. En Europa, el papel moneda se hizo popular durante el Renacimiento, cuando los banqueros italianos presentaron facturas de crédito. Tanto en China como en Europa, el papel fue sustituido por el metal. Porque el papel era más barato, más fácil y más seguro de transportar.

Una persona que llevaba papel moneda era menos visible que un carro con metal valioso. Por lo tanto, las compañías de papel moneda tenían menos probabilidades de ser atacadas en las carreteras. Tanto debido al menor riesgo de ataque como a que solo la persona que llevaba el papel necesitaba

protección y no el carro con piezas de metal, uno necesitaba contratar menos guardias para viajar con seguridad que cuando se transportaba el mismo valor de metal.

Durante varios siglos, el dinero en papel representaba un reclamo sobre el dinero metálico. Se realizó a través de diferentes tipos de pagarés. Los recibos de depósitos son los más simples. Cuando una persona depositaba oro en un orfebre-banquero renacentista, él (generalmente él en ese momento) recibía un recibo. Con este recibo el oro podría ser retirado del orfebre. Originalmente, los recibos eran personales, pero luego se hicieron

pagaderos al portador. Eso permitía la transferibilidad y, por lo tanto, los recibos podían usarse en transacciones en lugar del oro en sí.

Más tarde, cuando los bancos emitían billetes, la tenencia de un billete en dólares del Banco de Augusta, Georgia, significaba que el Banco de Augusta en cualquier momento canjearía esa nota por especie; Es decir, monedas de oro o plata. Era cierto, en principio, hasta que el patrón oro fue abandonado en 1970.7 Después de que se eliminó el estándar de oro, el dinero en papel ya no era un reclamo sobre el metal o cualquier otro bien. Se convirtió en dinero fiduciario, dinero "por decirlo así". Los países los

convirtieron en moneda de curso legal, en el sentido de que fueron aceptados como pago de impuestos y deudas. Los comerciantes debían aceptarlo, a menos que declararan explícitamente que no lo harían. Pero lo más importante es que se acepta el papel moneda porque los vendedores saben que pueden gastarlo como dinero. No tiene valor intrínseco, a menos que cuente el valor de reciclaje del papel. Su valor es puramente simbólico. Es cierto no solo sobre el papel moneda. A pesar de que el metal puede tener un valor más intrínseco que el papel, el valor de las monedas modernas se deriva del número estampado en ellas. Las monedas ya no se acuñan de oro y plata, sino que se

acuñan con metales de menor valor, como el cobre y el níquel. El valor simbólico de la mayoría de las monedas es mayor que el valor del metal en ellas. Pero en algunos casos, cuesta más hacerlos que su valor nominal. Por esta razón, la Casa de la Moneda canadiense dejó de emitir monedas de un centavo en 2013.

Si bien hoy aceptamos el papel moneda como una de las formas de moneda más comunes, históricamente no fue así. A menudo había problemas para introducir papel moneda, por ejemplo, porque la población no lo consideraba tan confiable como las monedas de metal y posiblemente temía una emisión

excesiva. En algunas regiones, especialmente en China, el papel moneda que representa el dinero metálico se introdujo con éxito porque fue impuesto y garantizado por el estado. De hecho, el estado recurrió a la ejecución de personas que se negaron a cumplir y a confiscar otros medios potenciales de pago, como el metal y las gemas.

En Europa, el papel moneda tenía más dificultades para ser adoptado en general. Los estados europeos no imponían una aplicación tan fuerte, ni tampoco garantizaban el valor del papel moneda. Hubo varios casos de gobiernos que emitieron en exceso papel

moneda que luego no se canjearon por el valor prometido. Esto generó desconfianza en el papel moneda y dificultó su adopción generalizada.

El desarrollo final, que nos lleva a los tiempos actuales, es el dinero electrónico. La mayoría de las veces, cuando las personas piensan en dinero electrónico, piensan en tarjetas de crédito. Las tarjetas de crédito no comenzaron como electrónicas. Ni siquiera comenzaron como plástico.

Comenzaron como tarjetas de cartón en la década de 1950. Los sistemas de tarjetas de crédito se basan en un libro de contabilidad. Las transacciones se registran y reportan a una institución que

posee el libro mayor y la cuentas La institución, generalmente un banco, verifica si los fondos que se van a gastar están disponibles, agrupa las transacciones para facturar al titular de la cuenta y, por lo general, también ofrece servicios de crédito. La tarjeta de crédito proporciona información sobre la cuenta y el sistema donde se guarda la cuenta.

La introducción de tecnologías digitales permitió el reporte electrónico de las transacciones, aceleró la autorización y disminuyó el fraude. Pero en última instancia, es una forma digital de mover dinero que tiene una contraparte física. Un tipo diferente de dinero digital, el

enfoque de los siguientes capítulos, es el dinero que solo existe digitalmente. Libre de la contraparte física, puede tener diferentes propiedades que el dinero que conocemos de la historia.

La adopción generalizada de las formas más modernas de dinero (monedas de metal, papel moneda y, cada vez más, dinero electrónico) se debe a sus ventajas sobre las formas anteriores. Pero incluso hoy en día, todavía hay situaciones en las que reaparecen los tipos anteriores de dinero. Por ejemplo, la escasez de la moneda habitual en los campos de prisioneros de guerra llevó al uso de cigarrillos como moneda simbólica. El mismo símbolo ha sido

adoptado como moneda en las economías informales en las cárceles. Curiosamente, cuando se prohibió fumar en algunas cárceles, los cigarrillos desaparecieron, pero el dinero no: los prisioneros comenzaron a usar latas de caballa como moneda.

2.2. ¿Qué roles sirve el dinero?

El papel clave del dinero es facilitar el comercio. El comercio voluntario significa que cada parte prefiere recibir los bienes que la otra parte tiene en lugar de retener los bienes que originalmente tenían. Por lo tanto, tal comercio mejora El bienestar de las partes comerciales. Sin embargo, como

vimos en nuestro resumen histórico, existen importantes fricciones que limitan el comercio o lo hacen más difícil. El dinero es una innovación importante porque alivia algunas de esas fricciones. La adopción de un tipo de dinero determinado dependerá de qué tan bien los atributos del dinero satisfagan las necesidades económicas de los consumidores. Discutimos una serie de tales atributos, por ejemplo, divisibilidad, facilidad de almacenamiento y transporte

Ahora los discutimos más sistemáticamente.

Los economistas a menudo usan la siguiente definición de dinero en tres

partes:

(1) Unidad de cuenta, (2) medio de intercambio y (3) almacenamiento de valor. Esta definición significa que dos personas pueden acordar cuánto vale un bien en términos de dinero (eso es la parte 1); las personas aceptan el dinero cuando venden el bien, porque creen que será aceptado en otro lugar cuando quieran cambiarlo por un bien que quieran comprar (parte 2); y el dinero no perderá su valor drásticamente entre el momento en que las personas lo obtienen y el tiempo que lo gastan para comprar otra cosa (parte 3).

Estas tres características hacen posible que el dinero facilite el comercio. Cada

una de estas dimensiones es importante.

Si sabemos que incluso falta uno, probablemente no aceptaríamos una determinada cantidad de dinero en una transacción.

Hay, sin embargo, algunos problemas con esta definición.

En primer lugar, es algo circular. En esencia, dice que el dinero es algo que se usa como dinero. En este sentido, simplemente describe un equilibrio. Lo que no puede hacer es decirnos. Si una lata de caballa o un dólar zimbabuense es dinero. Además, la definición suena como tres preguntas de sí o no, lo que sugiere que si responde

"Sí" tres veces, lo que estás evaluando

es dinero.

Ese no es el caso.

Por ejemplo, no hay nada que pueda servir como medio de intercambio en todas las transacciones y nada que pueda almacenar valor para siempre. Si tomamos esta interpretación, de repente, las monedas buenas no satisfacen la definición. Toma el euro o la corona sueca o el zloty polaco. ¿Son una buena tienda de valor para los próximos 300 años? Eso es dudoso. De manera similar, el dólar confederado era dinero cuando se usaba, pero resultó no ser una buena reserva de valor, ya que no tenía valor después de la Guerra Civil. La moneda debe almacenar el valor durante

el tiempo suficiente para que la persona que obtiene la moneda pueda creer razonablemente que puede gastarla (unos días, semanas, meses... la definición es deliberadamente un poco vaga en los detalles aquí). De lo contrario, simplemente no sería un buen medio de intercambio.

Además, esta definición está destinada a aplicarse a un entorno particular, por ejemplo, un área geográfica. Consideremos por ejemplo la corona sueca. Pocas personas negarían que la corona sea dinero. Ciertamente satisface la definición del libro de texto, que sirve como una unidad de cuenta, una reserva de valor y un medio de

intercambio, con una calificación. Puede realizar transacciones fácilmente en coronas suecas en Suecia, pero es posible que no se acepten de manera general en otros lugares. Es muy poco probable que pueda usarlos en una tienda de la esquina en los Estados Unidos.

Vemos que la definición del libro de texto tiene un inconveniente importante: no establece los límites, no define el entorno al que debe aplicarse. No podemos aplicarlo universalmente, ya que eso lo haría completamente vacío. Por ejemplo, incluso el dólar estadounidense, la moneda más global que tenemos, no se acepta en todas

partes. En el extranjero, uno podría cambiarlo por la moneda local, pero no todas las tiendas e instituciones locales aceptarían los dólares americanos directamente como medio de pago.

Por lo tanto, hay todo un espectro de cuán amplia o estrechamente se aplica esta definición. De hecho, argumentaríamos que algunas innovaciones merecen ser llamadas dinero a pesar de que su alcance se limita a unos pocos tipos de transacciones en particular.

Como veremos, muchas monedas digitales operan con tales Las restricciones están limitadas a un tipo particular de entorno (digital) y solo a

algunos productos específicos que puede realizar o usar en ese entorno, por ejemplo, una espada para su avatar en el juego en línea de jugadores múltiples World of Warcraft. Los puristas podrían argumentar que esto descalifica tales monedas digitales como "dinero"; después de todo, no son un medio de intercambio generalmente aceptado para todas, o incluso la mayoría de las transacciones. Pero entonces, ¿en qué se diferencia de la corona sueca?

El dinero debería facilitar el comercio. Puede facilitar el comercio en alguna área geográfica o facilitar solo un tipo específico de comercio. Cuanto más limitado sea el comercio que puede

facilitar, más limitada será la moneda. En algún momento se puede decir que es tan limitado que ya no es una moneda. Desafortunadamente, decidir dónde radica ese punto podría convertirse fácilmente en una cuestión semántica, especialmente en un área tan nueva, dinámica y llena de casos límite como las monedas digitales.

Dados los límites a la definición de dinero del libro de texto:

Limitar una moneda a la región geográfica o al tipo de transacción: es fácil ver cómo podrían coexistir al mismo tiempo varios tipos diferentes de dinero, algo que ha ocurrido varias veces en el pasado, como veremos en la

siguiente sección.

¿Qué hace buen dinero?

Es importante destacar que estas limitaciones no restan valor a la increíble utilidad de la definición. Trabajar con esta definición y analizar los rasgos que debe mostrar el dinero, ha permitido a los economistas explicar por qué algunos bienes son más aptos para ser utilizados como dinero que otros.

Por ejemplo, la cebada es una buena unidad de cuenta, porque es divisible. Pero no es duradero y podría perder valor entre una transacción y otra; Por lo tanto, no es un muy buen almacén de valor. Las casas son dinero

inconveniente para diferentes razones. Aunque son muy duraderos, apenas son divisibles y, a menudo, son incomparables, lo que los convierte en una unidad de cuenta deficiente. También es complicado intercambiar la propiedad de una casa, al menos, más difícil que entregar piezas de metal. Así que los bienes raíces son también un medio de intercambio pobre. Esta es la razón por la cual los bienes útiles que son lo suficientemente pequeños para llevarlos a otra persona y para pasarlos a otra, sirven mejor a la función.

Podemos ver cómo los diferentes atributos de los diferentes tipos de dinero se relacionan con qué tan bien se

cumple cada una de las tres funciones. Si las unidades son uniformes o no uniformes afecta la función de la unidad de cuenta. La misma incertidumbre sobre si un pez vale tres o cuatro dientes de perro, dependiendo de la calidad de los dientes, hace que sea difícil evaluar y comparar el valor de diferentes productos de manera sistemática. Esta incertidumbre puede aumentar la necesidad de negociación y hace que las transacciones consuman más tiempo. Por lo tanto, tales bienes no facilitan el comercio, así como otros bienes similares que son uniformes en todas las unidades. En esta dimensión, la cebada puede ser mejor que los dientes de perro. Y como la cebada de diferentes

campos puede tener cualidades ligeramente diferentes, las monedas y los billetes que usamos hoy en día son mejores que la cebada.

De manera similar, otros atributos influyen en la eficacia de una moneda potencial como depósito de valor. Los bienes que son duraderos y fáciles de almacenar de manera segura se desempeñan mejor como monedas. Para tomar un ejemplo extremo, un elemento radioactivo con una vida media corta daría lugar a una moneda muy pobre (aunque, sin duda, su fracaso como depósito de valor puede no ser el mayor problema con él).

Otros atributos influyen en el papel de

un bien como medio de intercambio. Claramente, un medio de intercambio que funcione bien debería ser fácilmente divisible. Algunas operaciones pueden no ser posibles si no hay suficientes denominaciones. Los bienes que son livianos y fáciles de transportar funcionan bien como medio de intercambio: llevar piezas de metal pesadas y difíciles de manejar es inconveniente, lo que hace que sea tentador dejar ese dinero en casa, lo que a su vez puede hacer que pierda muchas oportunidades para realizar transacciones. Un buen medio de intercambio tampoco es demasiado susceptible al fraude, es decir, es difícil de falsificar o duplicar. La escasez es

importante tanto para un medio de intercambio como para una reserva de valor. Si hay abundancia de un bien particular, y es fácil obtenerlo en cantidades ilimitadas, este bien no sería bueno. Consideremos, por ejemplo, el caso de la arena en una playa.

¿Por qué un vendedor renunciaría a un bien por la arena si pudiera obtener fácilmente la arena y mantener la buena? Para ser escasos, el dinero debe ser costoso de producir: extraer, recolectar o crecer. Por ejemplo, los metales que funcionan bien como el dinero, el oro y la plata, son costosos para la mina. No era tanto el caso del dinero de los alimentos, como la cebada. No obstante,

todavía podría funcionar como dinero porque no duró mucho. Se consumió o pereció de otra manera, y la cantidad de dinero para alimentos se debía reponer cada año solo para mantener el mismo nivel. Para que el metal, que es duradero y dura siglos, sea lo suficientemente escaso como para ser dinero, debe ser más costoso de producir, de modo que solo se agregue una pequeña cantidad cada año. Si cada año se añadiera tanto oro como cebada, el oro perdería rápidamente su valor.

La durabilidad del metal también proporcionó una oferta monetaria más estable. La cosecha de cebada puede ser más o menos abundante cada año. Y

como la oferta de dinero fluctúa, también lo harán los precios. En un año de buena cosecha, hay mucha cebada en todas partes y los precios de los productos que no son de cebada aumentan.

La oferta inestable (es decir, cambiante y no administrada) conduce a una mayor variabilidad en los precios. Tal variabilidad intensifica la incertidumbre, que a su vez puede crear fricciones en el comercio. Fabrica metal, con su suministro más estable, más preferido. Como dinero Por supuesto, incluso la oferta de dinero de metal puede experimentar grandes fluctuaciones. El ejemplo principal es el

descubrimiento de las Américas, que trajo grandes cantidades de oro y plata a la economía europea.

Para la mayor parte de la historia del dinero, las personas pueden elegir entre "producir" dinero o producir bienes y servicios que podrían intercambiarse por dinero. El cultivo de cebada, la minería de metales o la búsqueda de cáscaras cowry es la forma en que se podría producir dinero directamente. Pero para eso, uno tendría que tomar la decisión de cultivar más cebada en lugar de pastar vacas, o abandonar su granja para buscar oro en los ríos de California. Tal elección ya no era posible con la introducción del papel

moneda. El papel moneda era barato de producir, y su escasez provenía de la regulación estatal en forma de fuertes restricciones sobre quién podía producir dinero y cuánto. Por lo tanto, la escasez de papel moneda se impuso artificialmente, mientras que la escasez de dinero anterior resultó del costo de su producción. Como veremos más adelante, el problema de la escasez es muy importante para los esquemas de moneda digital, ya que a veces el dinero digital podría hacerse "con un clic del ratón". Este problema fue especialmente difícil para los sistemas de dinero digital descentralizados.

Todas las transacciones tienen algún

elemento de costos inherente a ellas. Los costos pueden venir de muchos conductores. Quizás el más obvio sea el tiempo necesario para realizar una transacción. Ya vimos la importancia de este costo en las comunidades humanas más tempranas, ya que era uno de los costos más importantes del trueque: es posible que deba pasar mucho tiempo para encontrar a alguien dispuesto a cambiar algo que tiene por algo que desea. En menor medida, los costos de tiempo hicieron que las piezas de metal sin pintar fueran inferiores a los tipos de dinero posteriores: tenía que pasar el tiempo pesando una pieza de metal o dividiéndola en piezas más pequeñas. Otro tipo de costo está relacionado con

el esfuerzo por cambiar la propiedad del medio de intercambio. Por ejemplo, el dinero que es particularmente pesado o difícil de transportar sería costoso entregar al vendedor.

Otros costos importantes son los costos mentales, por ejemplo, tener que realizar una aritmética relativamente más complicada para completar una transacción que usa muchas unidades diferentes de una moneda o varias monedas diferentes. Un costo relacionado es la probabilidad de cometer un error, por ejemplo, al decidir cuánto cambio devolver, o al distinguir diferentes cualidades en dientes de perro o piezas de metal que

podrían influir en su valor.

Además de estos costos, existen costos de transacción que son más indirectos. Después de una transacción completada, el vendedor puede necesitar asegurar el dinero que acaba de obtener, el ejemplo obvio aquí es la protección contra el robo, por ejemplo, contratar guardias al transferir dinero, construir cajas fuertes para almacenar metal, etc. Los ejemplos menos obvios, más relevantes para las monedas basadas en productos básicos, son la necesidad de protección contra los elementos y parásitos, o la necesidad de construir grandes almacenes para almacenar su dinero; Ambos son muy importantes cuando el dinero es, por

ejemplo, la cebada.

Finalmente, las oportunidades perdidas (transacciones perdidas que no ocurrieron) son otro tipo de costo de transacción.

El dinero que no satisface bien sus tres roles puede no ser capaz de facilitar tantas transacciones, y cada transacción que no ocurre es una pérdida para el comprador y vendedor potencial y para la economía en general. Los atributos del bien que sirve como dinero pueden contribuir a la pérdida de transacciones, por ejemplo, pesadez o uso de metales desconocidos.

Debido a estos atributos, los socios comerciales potenciales pueden ver la

transacción como demasiado costosa de realizar, o quizás demasiado arriesgada, y decidir no seguir adelante con ella. Las transacciones pueden perderse también cuando las unidades de la moneda no son eficientemente divisibles. Por ejemplo, si un pez en particular vale 4,25 dientes de perro para el vendedor y 4,75 dientes para el comprador, su comercio sería beneficioso para ambos lados, pero no ocurrirá porque los dientes de perro no son divisibles. Se puede realizar una transacción por 4 dientes o quizás por 5 dientes: pero no lo hará, ya que cualquiera de las dos opciones haría que una de las partes se encuentre en peor sentido que no realizar ninguna

transacción.

El argumento de los costos de transacción nos ayuda a comprender por qué el oro ha sido un ganador durante mucho tiempo en el campo del dinero.

El oro es duradero y divisible, puede ponderarse para una unidad de cuenta uniforme. Además, el oro ha sido culturalmente valioso, porque no cambia su apariencia con el tiempo. Confianza y falsificación

El oro nos ayuda a resaltar un atributo particular del dinero que cobrará importancia con las monedas digitales: la confianza. El dinero debe ser una buena reserva de valor, y se suele pensar que la escasez garantiza el valor

a lo largo del tiempo.

También es relativamente más difícil de falsificar o, al menos, se desarrollaron herramientas como la piedra de toque para verificar la pureza del oro.

Confiar en que una moneda es genuina es un requisito previo importante para realizar una transacción. Aunque hoy en día solemos pensar en la falsificación en el contexto del papel moneda, este procedimiento infame es mucho más antiguo que eso. Por ejemplo, las monedas de metal a menudo eran "recortadas", haciéndolas de menor peso de lo que deberían estar de acuerdo con su sello. Para evitar la degradación, los bordes de las monedas se estamparon o

se bordearon, lo que facilitó a los usuarios identificar si las piezas de metal se cortaron de una moneda, cambiando su peso y su valor. Hoy en día el valor de las monedas ya no proviene de su peso. No obstante, muchas monedas contemporáneas tienen bordes bordeados, debido a este legado. En otro tipo de falsificación, las monedas de metal o las piezas de metal sin pintar podrían contener un metal de menor valor en el interior, ocultado por el metal correcto en el exterior. Imagina, por ejemplo, un núcleo de cobre cubierto con un revestimiento de plata para imitar una moneda de plata. El ingenio humano es ilimitado. Incluso el dinero basado en materias primas fue

falsificado.

Consideremos el cacao, usado en el imperio azteca como dinero. Los asesores falsificaron esa moneda al llenar una cáscara de cacao vacía con barro y sellarla.

Las consideraciones de falsificación son particularmente importantes en el contexto de las monedas digitales. La tecnología digital hace que sea muy fácil y económico hacer copias perfectas de información almacenada digitalmente: archivos, códigos, contraseñas, direcciones, etc. En la industria de la música, resultó en una piratería a gran escala, que cambió la forma en que esta industria opera En el contexto del

dinero, da lugar al llamado problema de doble gasto.

En los próximos capítulos, analizaremos los distintos roles del dinero en el contexto de las monedas digitales. Luego veremos que muchos de los atributos son tan importantes para las monedas tradicionales (físicas) como para las digitales. Veremos que el dinero digital puede tener ventajas significativas cuando se trata de facilitar el comercio, haciéndolo más barato y más rápido.

También veremos que el fraude, y por lo tanto la falta de confianza, ha sido un desafío particular para los intentos de crear dinero en el mundo digital.

2.3. Dinero en competencia

La mayoría de nosotros estamos acostumbrados a un tipo particular de dinero (por ejemplo, dólares estadounidenses), y pensamos que ese "dinero" es simplemente está allí. No hay nada de malo en esta percepción; en la mayoría de los lugares, en un momento y lugar dado, solo una moneda en particular está en uso. Pero como con cualquier otro producto, el dinero compite con otro dinero. Si miramos de cerca, veremos esta competencia todo el tiempo. En el contexto histórico, la plata compitió con la cebada, las monedas de metal compitieron con el metal no acuñado y el papel moneda compitió con el oro. Curiosamente, muchas monedas

en competencia a menudo coexistían, aunque solo fuera por un tiempo. Los ducados venecianos y los florines de Florencia compitieron con otras monedas en toda la Europa medieval, y ahora el euro y el dólar estadounidense compiten en las transacciones internacionales. De hecho, sin competencia no habría cambio: una nueva moneda o una nueva forma de dinero se introducen en una economía que normalmente ya tiene una moneda predominante. La nueva innovación solo puede sobrevivir, y tal vez eventualmente ganar una adopción generalizada, si puede competir con éxito con los titulares.

Pero entonces, ¿qué determina el resultado de tal competencia?

2.3.1. La convivencia es costosa

Hay costos claros para tener múltiples monedas dentro de una economía. Podemos dividir estos costos en dos categorías amplias: costos cognitivos y costos de intercambio.

Los costos cognitivos surgen de la dificultad mental de tener que comparar precios y valores cotizados en varias monedas. Es necesario no solo comparar diferentes unidades al decidir si comprar algo, sino también realizar un cálculo mental al seleccionar los billetes y monedas para pagar la compra o al aceptar un cambio de la compra.

Consideremos por ejemplo el sistema de acuñación en Inglaterra. Históricamente, ese sistema incluía pozos, centavos, chelines, coronas, libras y guineas, algunos de metales diferentes, y por lo tanto cambian de valor entre sí. Finalmente, el valor relativo de estas diferentes unidades se fijó en 1717. Por ejemplo, el valor de una guinea había fluctuado entre 20 y 30 chelines, antes de fijarse en 21 chelines en 1717. Una libra contenía 20 chelines, por lo que una guinea valía 1 libra y 1 chelín. Un chelín contenía 12 peniques, y cada penique contenía 4 pozos (y, en épocas anteriores, variaba entre 8 y 4 pozos a un centavo). Una corona era un cuarto de libra.

Otros países europeos también utilizaron unidades múltiples. Por ejemplo, la Francia prerrevolucionaria tenía un sistema de moneda que rivalizaba con el inglés en términos de su complejidad. La unidad central del sistema era el luis d'or, que consistía en 10 libras. Cada libra constaba de 20 soles. Cada sol constaba de 12 negadores. Y esas eran solo monedas de oro.

Entre las de plata, 60 sous constituyeron 1 ecu de plata. El valor relativo de las monedas de oro y plata estaba cambiando con el tiempo. Tal multiplicidad creaba fricciones. La población local debe haber estado acostumbrada a esta mezcla. Sin

embargo, uno sospecha que esta multiplicidad de tipos de acuñación creó mucho margen para errores y confusión. Y con sistemas igualmente complicados e incompatibles en otros países, hizo que el comercio internacional fuera más confuso.

Eventualmente, tales fricciones se resolvieron adoptando el sistema métrico. La adopción del sistema métrico para la acuñación de monedas comenzó con los Estados Unidos y Francia a finales del siglo XVIII. El Reino Unido había sido un obstáculo en su negativa de larga data a adoptar el sistema métrico en su moneda. El sistema con libra como una unidad y 100

(nuevos) centavos por libra, dejando caer otras unidades, como Guinea y objetos de valor, solo se introdujo en 1971. El cambio del sistema métrico también se puede ver a la luz del costo mental de manejo de dinero: si uno opera en sistema decimal, es mucho más fácil sumar, restar o multiplicar los valores expresados en monedas cotizadas en la base de 100 (en oposición a, digamos, 21, el número de chelines en una guinea).

La tecnología puede ayudar a disminuir estos costos, aunque posiblemente no los elimine. Por ejemplo, los teléfonos celulares y la amplia cobertura de Internet facilitan la conversión de los

precios cotizados en una moneda extranjera a su moneda local. Sin embargo, hay, y probablemente siempre habrá, algún inconveniente en, digamos, tener que recurrir a su teléfono celular cada vez que quiera comprar algo. Además, incluso si la referencia a su teléfono celular no presenta complicaciones, no excluye la segunda gran categoría de costos: los costos de intercambio.

En economías que usan múltiples monedas diferentes, las personas asumen el costo de tener que cambiar una moneda por otra. Este costo no se puede evitar a nivel de la economía en general: incluso si decide aceptar y gastar un

solo tipo de moneda, algunas de las partes con las que realice transacciones deberán cambiar su moneda favorecida por la moneda de su elección. Clientes o proveedores Para ilustrar mejor los costos de múltiples monedas diferentes que circulan en una economía, consideremos la era de la banca estatal de los Estados Unidos en el período entre 1786 y 1963. En aquellos primeros días del país, los Estados Unidos

El gobierno acuñó monedas pero no emitió papel moneda.

La razón de esta configuración fue que el dinero impreso por el gobierno estaba sujeto a controversia luego de la emisión excesiva de Continental durante

la Guerra de Independencia.

A pesar de que el gobierno de los Estados Unidos se abstuvo de emitir papel moneda, los bancos privados imprimieron su propio papel moneda, y eventualmente le proporcionaron al mercado una gran cantidad de varios billetes. Los bancos privados emisores se establecieron sobre la base de la legislación de los estados individuales, y prácticamente todos los bancos privados emitieron sus propios billetes. La escala de este fenómeno refleja el hecho de que en 1860 había más de 1,500 bancos en los Estados Unidos, de los cuales 54 estaban en la ciudad de Nueva York.

A los bancos no se les permitió simplemente imprimir dinero a voluntad. Por requerimiento de la legislatura, las notas que emitían tenían que estar respaldadas por activos, y el banco emisor tenía la obligación de canjear las notas por especie, es decir, monedas de metal. La falta de canje de las notas traídas para la redención en especie fue un delito grave, y podría ser una causa para el fracaso del banco. En promedio, el 0.5 por ciento de los bancos fallaba anualmente, aunque hubo años en los que incluso el 5 por ciento de los bancos falló.

Con miles de diferentes tipos de billetes que circulan en la economía, no todos

los billetes fueron tratados por igual.

Por ejemplo, rápidamente quedó claro que un billete de cinco dólares de un banco podría valer menos que un billete de cinco dólares de otro banco. Estos descuentos hicieron que el intercambio de billetes y el comercio fuera más costoso.

La razón de la diferente valoración de las notas a menudo se relaciona con la dificultad y el riesgo de una redención exitosa de las notas. Nota para la especie. Para canjear la nota uno tenía que ir al banco que la emitió. Esto puede haber sido fácil para su banco local, pero habría sido difícil y quizás demasiado costoso si tuviera un billete

emitido por un banco muy lejano. Si todavía emprendiste el viaje y si tuviste una mala suerte, es posible que hayas descubierto que el banco al que ibas había fallado cuando llegaste allí. De hecho, los investigadores encontraron que los descuentos variaban geográficamente, y los descuentos eran generalmente más bajos para los bancos que eran locales y, por lo tanto, más conocidos para las personas que viven en un área determinada. El descuento también capturó el riesgo de una quiebra bancaria. Si tal riesgo era alto, era menos seguro que el billete podría ser canjeado. Los bancos en quiebra no canjearían las notas en absoluto o las canjearían a una fracción del valor

nominal. Por lo tanto, aceptar las notas de algunos bancos se consideró más riesgoso que aceptar las notas de otros bancos. Puede provenir del conocimiento general de que un banco en particular estaba en problemas, pero también de la falta de familiaridad con el banco. Es posible que alguien que vivió en Filadelfia haya tenido menos información sobre los bancos de Boston y haya estado menos dispuesto a aceptar los billetes emitidos por esos bancos. Esta fue otra razón por la que las notas de bancos lejanos se negociaron con un descuento mayor.

La incertidumbre sobre el valor de un billete se relaciona con otro fenómeno:

la falsificación. La falsificación era rampante. Con la multitud de diseños de notas, era difícil hacer un seguimiento de cómo debería ser una nota genuina de un banco en particular. Nuevamente, era más probable que los billetes desde lejos fueran falsificados, ya que las personas estaban menos familiarizadas con su diseño. Más colorido, los falsificadores a veces componen bancos enteros y billetes emitidos por estos bancos (ficticios). En un entorno con cientos de emisores diferentes, los falsificadores a veces lograron salirse con la suya, pero en última instancia contribuyeron a Aversión general a billetes menos populares o billetes de lugares geográficamente distantes.

Puede imaginar que la mayoría de las personas simplemente no pudieron realizar un seguimiento de todos estos problemas y matices. No es sorprendente que aparecieran corredores que estuvieran dispuestos a aceptar varios billetes y canjearlos entre sí, por un precio. Los corredores en muchas ciudades publicarán semanalmente, quincenalmente o mensualmente "detectores de falsificación" o "reporteros de billetes", publicaciones que enumeran falsificaciones conocidas y, a menudo, cotizan descuentos para el intercambio de billetes genuinos de diferentes bancos. En esas publicaciones, los

comerciantes encontrarían consejos como "mejor rechazar los 5s" del Webster Bank of Boston, Massachusetts, o "cuidado con todas las denominaciones del antiguo banco fraudulento de este nombre" para el New York Exchange Bank. Estos reporteros estaban disponibles para El público una vez más, por un precio. Pero incluso si tenía uno, consultarlo consumía mucho tiempo para los comerciantes y otros que los estaban usando.

En general, los costos de tener esta multitud de billetes fueron altos. Incluían costos tanto cognitivos como económicos. El último incluía los costos

directos de realizar transacciones (por ejemplo, tener que comprar un reportero de moneda) y los costos de asumir el riesgo e incertidumbre adicionales cuando se trata de varios billetes. Todo esto creó fricciones en el comercio y una carga para la economía en general.

El deseo de evitar estos costos es un importante impulsor de la competencia entre las monedas y puede eventualmente empujar a la economía a una moneda generalmente adoptada. Como resultado, también hay otro incentivo poderoso que opera en la misma dirección: los efectos de red.

2.3.2. Efectos de red

La competencia entre monedas es

diferente de la competencia entre la mayoría de los bienes, y un aspecto juega un papel clave papel aquí: el dinero exhibe lo que en economía se denomina “Efectos de red”. En pocas palabras, un objeto es más útil como dinero si otras personas lo usan también como dinero.

Los efectos de red se reconocieron por primera vez en la literatura económica en la década de 1980. Para usar el ejemplo más clásico, considere la red telefónica. No tiene sentido ser dueño de un teléfono si usted es el único. El valor de un teléfono aumenta a medida que más personas compran teléfonos, es decir, hay más teléfonos en la red.

En las últimas décadas, el estudio de los efectos de red se convirtió en un subcampo vibrante de la economía. Las herramientas que los economistas desarrollaron para estudiar redes se han utilizado para analizar, explicar y comprender una variedad de tecnologías modernas: consolas de videojuegos, computadoras o teléfonos inteligentes.

Las aplicaciones son particularmente relevantes en el contexto de las tecnologías de la comunicación. De hecho, se ha observado que lo que se ha denominado "efectos de red" no necesita una red física. No hay necesidad de cables como los de la red telefónica para que se produzcan efectos de red.

Resulta que el argumento de los efectos de red se aplica fácilmente al dinero. Supongamos que quieres introducir una nueva forma de dinero. Inicialmente, usted es el único que reconoce y acepta ese dinero, lo que hace que sea muy difícil persuadir a otra persona para que también lo adopte. Después de todo, si lo hace, inicialmente solo tendrá a ti con quien intercambiar. Las cosas son más fáciles si ya hay una parte más grande de la sociedad, con suerte incluyendo tanto a compradores potenciales como a vendedores, que están listos para usar la moneda.

Con los efectos de red, a menudo vemos un "ganador se lo lleva todo" dinámica.

Si dos redes son similares pero una es más grande, la más grande será más atractiva para los nuevos usuarios.

Los usuarios de la red más pequeña también pueden preferir cambiar a la red más grande. El más grande crecerá aún más, mientras que el más pequeño incluso puede desaparecer. Así, el ganador. Se lleva todo el mercado. A menudo, un mercado de este tipo es eficiente, ya que todos los usuarios pueden aprovechar el efecto de red máximo.

Debido a eso, la investigación económica a menudo encuentra que es socialmente óptima cuando todos usamos la misma tecnología que genera

efectos de red.

Con frecuencia vemos este tipo de dinámicas del ganador se lo lleva todo en el contexto del dinero. Al igual que con otras tecnologías que generan efectos de red, el dinero aceptado por un mayor número de personas es más útil que el dinero utilizado por unos pocos. Y dado que una moneda es más útil cuando más personas la adoptan, el beneficio se maximiza cuando todos usan la misma moneda.

En nuestro resumen histórico anterior, discutimos la aparición de monedas en Lydia en el siglo séptimo antes de Cristo.

Había buenas razones por las que las

monedas eran una tecnología superior al metal no extraído; por ejemplo, las monedas con la misma marca eran uniformes, todas valían lo mismo y todos sabían lo que valían. Ahorraron tiempo dedicado a pesar y disminuyeron la probabilidad de hacer trampa. Por lo tanto, cuando dos partes comerciales podían usar monedas o metal sin pintar, ambos preferían usar monedas.

Además, el vendedor sabía que le sería más fácil usar monedas en lugar de metales no acuñados en futuras transacciones, por lo que estaba más dispuesto a aceptarlas. Y a medida que más personas usaban monedas, menos personas querían usar metal sin pintar.

Es decir, a medida que las monedas se hicieron más populares, su atractivo creció y aumentó aún más su popularidad. Con el tiempo, las monedas tomaron el mercado para la mayoría de las transacciones. El metal no acuñado se usaba cuando las monedas no estaban disponibles o cuando el valor de una transacción era muy grande y una placa de metal era más práctica que muchas monedas.

El Renacimiento nos da otro ejemplo de la dinámica del ganador que se lleva todo en dinero. Durante el Renacimiento, la banca italiana, especialmente florentina y veneciana, se extendió por toda Europa, haciendo que

las monedas de Florencia (florín) y de Venecia (ducado) las monedas de elección incluso en lugares muy alejados de Italia. Con el crédito de las casas bancarias italianas, muchas operaciones se realizaron en esas monedas y la gente se familiarizó con ellas. Cuando los comerciantes tenían la oportunidad de realizar intercambios comerciales de florines y ducados o en algunas otras monedas, preferían los florines y ducados. Por lo tanto, los florines y ducados se estaban volviendo más populares, convirtiéndose en las monedas dominantes de Europa, y expulsando a otras monedas.

Nuestro último ejemplo es el de la thaler

María Theresa. El thaler (un nombre del cual se deriva la palabra "dólar") se introdujo en 1773 en honor a la emperatriz austriaca, la esposa del santo emperador romano Francisco I. Rápidamente se hizo muy popular, especialmente en el norte de África y en el Medio Oriente. La gente se mostró reacia a usar cualquier otra moneda. La razón por la que prefirieron a los thalers de María Theresa son precisamente los efectos de la red: prefirieron a los thalers porque sabían que todos los demás también preferirían intercambiar con los thalers de María Theresa, y pueden no estar tan inclinados a comerciar con otras monedas potenciales. Esta dinámica reforzó la

popularidad de los thalers de María Theresa en la región, expulsando otras monedas.

María Teresa murió en 1780, pero la moneda continuó siendo acuñada. Era una práctica inusual acuñar monedas con la imagen de un gobernante fallecido, por lo que todas las monedas acuñadas después de la muerte de María Teresa tuvieron la fecha de 1780. Siguieron siendo acuñadas después de que Napoleón aboliera el Sacro Imperio Romano en 1805 y después del Imperio Austro-Húngaro. Se desintegró después de la Primera Guerra Mundial. Más tarde, la República de Austria continuó acuñándolas hasta el Anschluss de

Hitler en 1937. Italia acuñó a los thalers de María Teresa a finales de los años 1930 para el uso en el territorio conquistado de Abisinia (la actual Etiopía). Es revelador que el gobierno de Mussolini decidió abastecer a los thalers porque la población local En Abisinia se negó a aceptar sustitutos. Estaban acostumbrados y confiaban en los thalers de María Teresa.

El efecto de "el ganador se lo lleva todo" fue tal que fue difícil para las monedas modernas introducirse con éxito en esa economía. El efecto no se limitó a Abisinia: el talero fue acuñado en mentas de Bombay y Bruselas a Utrecht y Viena. Incluso después de la

Segunda Guerra Mundial, Austria reanudó la acuñación de las monedas en 1956, y la última se acuñó en 1975. El número total de plata thalers de María Theresa acuñadas entre 1780 y 1975 se estima en unos 400 millones. Cada uno está fechado en 1780.

Con los efectos de la red empujando a la economía hacia una moneda única, ¿por qué observamos episodios prolongados en los que se utilizan múltiples monedas, por ejemplo, la multitud de billetes durante la era de la banca estatal en los Estados Unidos, como se describió anteriormente? En el caso de la era bancaria, la razón fue el límite externo impuesto por la regulación. Las monedas

que ganaron el mercado, ya sean florines, ducados o los thalers de María Theresa, fueron acuñadas hasta el punto en que la oferta de las monedas coincidía con la demanda. En contraste, los bancos conforme a las leyes bancarias estatales se mantuvieron reducidos (por ejemplo, no pudieron fusionarse entre sí) y estaban limitados en el valor de los billetes que podían emitir.

La emisión estaba limitada por el capital de los bancos, que a su vez estaba limitado por la ley. Para algunas áreas pequeñas o escasamente pobladas, la oferta de billetes de un banco fue suficiente para satisfacer la demanda.

Pero para la mayoría de las áreas urbanas, la demanda de billetes era mucho mayor de lo que cualquier banco podía proporcionar legalmente. Esta restricción, y la situación a la que dio lugar, fueron perjudiciales para la economía en su conjunto y se necesitaba cierta estandarización. Como veremos más adelante, fue una autoridad central (esencialmente, una nueva regulación) la que resolvió el problema: el gobierno de los EE. UU. Obligó a todos los bancos y ciudadanos a usar el dólar estadounidense.

2.3.3. La dificultad de introducir una nueva moneda: el exceso de inercia

Una y otra vez vemos una innovación, digamos, una tecnología nueva y prometedora, que tiene problemas para penetrar en el mercado y ganar una cuota de mercado del operador tradicional que puede estar ofreciendo una tecnología menos eficiente. La economía de la red nos permite comprender mejor este tira y afloja entre popularidad y facilidad de uso. Esta interacción, tal como se identifica en la literatura económica, es uno de los rasgos característicos que deberíamos esperar en entornos con efectos de red. Dichos entornos a menudo son demasiado lentos para adaptar la nueva tecnología, y en ocasiones pueden dejar de adoptarla por

completo, aunque hubiera sido beneficioso hacerlo. Los economistas llaman a esto "inercia excesiva".

En nuestro resumen histórico, vimos innovaciones que se introdujeron sin problemas en la economía y que finalmente ganaron gran popularidad. Por ejemplo, las monedas se adoptaron rápidamente y eventualmente desplazaron las piezas de metal sin pintar del titular anterior. Sin embargo, otras innovaciones enfrentaron grandes fricciones, ralentizando la adopción o haciéndola totalmente imposible.

Dicha fricción de adopción estuvo presente en el caso del papel moneda. El dinero de papel proporciona una mejor

tecnología, en términos de conveniencia, que el dinero de metal. Por ejemplo, es más fácil de transportar. Sin embargo, el mundo occidental tardó mucho tiempo en adoptarlo. En contraste, China adoptó el papel moneda mucho antes debido a la implementación directa de esta innovación por parte del estado.

De manera similar, las tarjetas de crédito son más convenientes de usar que el efectivo, especialmente para transacciones de gran valor. Son atractivos para los clientes porque son más ligeros y seguros que el efectivo, y eliminan la necesidad de preocuparse por el cambio. Su atractivo es algo más limitado para comerciantes, que deben

pagar tarifas adicionales para poder aceptar tarjetas de crédito. No obstante, para transacciones de gran valor, el beneficio de una mayor seguridad puede superar el costo, porque, por ejemplo, el comerciante puede evitar llevar una gran cantidad de efectivo al banco. Además, al aceptar tarjetas de crédito, los comerciantes evitan el riesgo de que el intercambio no se realice porque el cliente no tiene suficiente efectivo en él.

Y, de hecho, las tarjetas de crédito se hicieron muy populares, al menos a principios de siglo. Sin embargo, la adopción inicial no fue muy enérgica. A pesar de las ventajas de la tecnología, fue más un impulso de las compañías de

tarjetas de crédito que un empuje de los clientes. Había mucha desconfianza, tanto por parte de los clientes como por parte de los comerciantes.

Para contrarrestar esa inercia, las compañías de tarjetas de crédito ponen mucho esfuerzo en educar a las personas y alentar el uso del sistema. Por ejemplo, otorgan premios por usar tarjetas de crédito y anuncian sus planes de protección contra el fraude. Las compañías de tarjetas de crédito no emiten tarjetas y administran los pagos solo por el bien social y los beneficios del mercado. Ellos están preocupados por su propio beneficio. Pero uno podría imaginar fácilmente que sin el papel

activo de las compañías de tarjetas de crédito, el mercado se mantendría durante más tiempo en el uso tradicional pero menos eficiente de una gran cantidad de efectivo. Alternativamente, la nueva tecnología podría haberse esfumado porque a cada lado le preocuparía que el nuevo sistema de pago no ganara suficiente tracción con el otro lado. Hoy en día podemos señalar la gran conveniencia de usar tarjetas de crédito en línea y pensar que el beneficio de la adopción es claro. Pero las tarjetas de crédito probablemente no se usarían en línea si no se hubieran adoptado antes para transacciones de ladrillo y mortero.

De los ejemplos anteriores, vemos que a veces la facilidad de uso es la fuerza predominante y la nueva tecnología. Se adopta sin problemas, como monedas. A veces se adopta con resistencia y fricciones debido al exceso de inercia, como con el papel moneda y las tarjetas de crédito. Y es posible que a veces no se adopte en absoluto. Simplemente no observamos a un entrante potencial fallido. Por ejemplo, puede ser que la popularidad del thaler María Theresa haya impedido la adopción de algunas mejores formas de moneda.

Nuestro ejemplo final de exceso de inercia proviene de los Estados Unidos en la década de 1860. Como se

describió anteriormente, hasta 1863, todos los billetes en circulación fueron proporcionados por bancos privados según las leyes bancarias estatales individuales. La falsificación era rampante, y ocasionalmente los bancos estaban fallando, inutilizando las notas o canjeando con un descuento muy alto.

En 1863, los bancos comenzaron a emitir notas bajo la nueva legislación, la Ley Nacional de Bancos. Los llamados "bancos nacionales" seguían siendo bancos privados, usualmente con una única ubicación de ladrillo y cemento. Pero las notas que emitieron tenían un diseño distinto y uniforme, lo que facilitaba el control contra las

falsificaciones. Además, los billetes nacionales estaban asegurados, lo que significaba que, incluso si el banco fallaba, las notas se canjearían totalmente por especie.

Dado que las notas de los bancos nacionales tenían menos riesgo que las notas de los bancos estatales, eran un dinero más confiable.

Al aprobar la ley, el gobierno esperaba que, con esa ventaja, los billetes nacionales se aceptaran de manera general, lo que dejaría obsoletos los billetes estatales. Sin embargo, después de dos años no hubo una disminución visible en el uso de billetes estatales. Dado que las fallas bancarias ocurrieron

solo ocasionalmente, las personas pueden haber considerado el riesgo como una parte natural de los costos de transacción, y no estaban buscando activamente minimizar esos costos. Es posible que hayan desconfiado del diseño desconocido y que no hayan sido plenamente conscientes de los beneficios de los billetes nacionales. Los billetes estatales eran más familiares, y la gente sabía que Fueron aceptados en su entorno inmediato. Así que los billetes del estado seguían siendo aceptados porque todos esperaban que fueran aceptados.

El gobierno efectivamente puso fin a los billetes del estado al imponer un

impuesto del 10 por ciento a los bancos que pagan los billetes del estado en el mostrador, incluso si fueran las propias notas del banco.22 Esto finalmente puso fin a la era de la banca estatal.

2.3.4. Coexistencia de varias monedas

A pesar de la dinámica del ganador se lo lleva todo y, a pesar del exceso de inercia, a veces diferentes formas de dinero, diferentes monedas, pueden coexistir en la economía. Esto sucede cuando las diferentes monedas sirven para diferentes propósitos.

Tenemos los primeros registros de plata usados como dinero de la antigua Mesopotamia. Reemplazó un tipo de dinero más antiguo cebada. El metal

tenía un valor más alto que el de la cebada: una pieza de plata valía más que el mismo volumen de cebada.

Esta es la razón por la cual la plata era más conveniente para transacciones que involucran grandes valores y distancias más largas (por ejemplo, una carga de productos de un barco). Para los intercambios locales cotidianos de valores mucho más pequeños, los metales eran demasiado valiosos. Esos intercambios todavía se realizaban con cebada. Por lo tanto, aunque el metal fue más práctico y se adoptó en toda Mesopotamia, la dinámica del ganador se lo lleva todo nos ha llevado a que el dinero del metal expulse por completo

el dinero de la cebada más vieja.

De manera similar, la introducción de monedas no ha eliminado por completo el uso de metal no acuñado en las transacciones, especialmente las de alto valor, donde una gran cantidad de monedas estandarizadas no sería fácil de manejar. Diferentes transacciones tienen diferentes "necesidades", y diferentes monedas pueden coexistir si sirven mejor a estas diferentes necesidades. Todavía hay costos de dinero paralelo: el intercambio de cebada por metal y viceversa. Por el contrario, pero los beneficios de combinar la funcionalidad con las necesidades pueden valer la pena. Los dos tipos de dinero sirven a

sus propósitos respectivos mejor que tener un solo tipo.

También podemos pensar en los billetes y monedas contemporáneos como dos tipos diferentes de moneda que coexisten porque sirven para diferentes propósitos. Tendemos a usar billetes y monedas para diferentes tipos de transacciones. Normalmente, usamos monedas para transacciones de pequeño valor y billetes de banco para transacciones de gran valor. Claro, hay superposición, pero si solo tuviéramos billetes o solo monedas, los intercambios serían más laboriosos. Y para sus respectivos roles, los dos tipos utilizan tecnología óptima. Los billetes

de banco de denominaciones muy pequeñas que circulan con mucha frecuencia se desgastarían demasiado rápido. Las monedas son más duraderas, pero son más pesadas que los billetes. Usar muchas monedas, incluso de denominaciones más altas, para transacciones de gran valor sería menos útil que usar billetes de las mismas denominaciones. Clientes necesitaría llevar menos monedas si hubiera más denominaciones disponibles. Para que eso funcione, los comerciantes tendrían que tener todas las denominaciones siempre disponibles, y con un número mayor de denominaciones, tendrían que amarrar más de su capital solo para tener el cambio listo. Los costos de

transacción también aumentarían porque uno tendría que buscar monedas entre más denominaciones.

Estas diferentes funciones que desempeñan las monedas y los billetes son evidentes desde el momento en que se introdujeron los billetes. Por ejemplo, algunos de los primeros billetes emitidos por el Banco de Inglaterra en el siglo XVIII fueron los billetes de diez y veinte libras. Estas cantidades, equivalentes a aproximadamente mil dólares en la actualidad, limitaron el uso de los billetes a los estratos más ricos de la sociedad. No es sorprendente que se usaran casi exclusivamente para

transacciones comerciales de gran valor y fueron particularmente populares entre las elites financieras de la Ciudad de Londres. En general, podemos resumir las fuerzas competitivas de la siguiente manera. Hay costos para múltiples monedas, que incluyen no solo los costos cognitivos sino también el costo del intercambio.

Existen diferentes monedas disponibles: algunas pueden ser mejores o peores que otras para un propósito en particular y otras pueden ser equivalentes. Las personas están dispuestas a usar múltiples monedas y asumir el costo de la compatibilidad y el intercambio si las monedas tienen propósitos diferentes y

si cada una es mejor para su propósito que otras. Pero la gente prefiere usar una moneda para un propósito determinado: los efectos de red son importantes para las monedas. Los efectos de la red inclinan a la economía hacia los resultados del ganador se lo lleva todo, donde una moneda única representa todas las transacciones en la economía. En tales casos, la moneda predominante puede obstaculizar la competencia, y la inercia evita que las personas adopten monedas nuevas (o múltiples) que podrían mejorar su bienestar.

2.4. ¿Dinero virtual?

Nuestro resumen de la historia del dinero nos lleva a los tiempos modernos

y al enfoque principal de este libro: las monedas digitales. Los antecedentes que cubrimos en este capítulo nos darán una mejor comprensión de estas innovaciones y nos ayudarán a resaltar las similitudes entre ellas y las etapas anteriores en la evolución del dinero. Esto es quizás más evidente en los términos ampliamente utilizados "dinero virtual" y “moneda virtual”. Muchos de los ejemplos históricos de dinero merecen ser llamados virtuales, comenzando con el primer sistema de intercambio basado en la memoria colectiva.

Quizás se podría pensar en este sistema colectivo basado en la memoria entre

los cazadores-recolectores como la primera moneda virtual. La "moneda" era virtual, ya que capturaba muchas de las funciones que juega el dinero hoy en día, aunque no existía físicamente. Las personas podían ganar el dinero. Moneda haciendo favores a otros o proporcionando bienes y servicios a otros. Los "ahorros" de cada persona se guardaron en la memoria colectiva, que se convirtió en el equivalente de una cuenta bancaria o transacciones leger.

"Virtual" se usa a menudo como un sustituto de "digital". Incluso esto, sin embargo, es una descripción amplia que puede capturar más de lo que se pretende. Por ejemplo, los fondos en una

cuenta bancaria se almacenan electrónicamente, por lo que pueden considerarse como

"Dinero digital": aunque, como son solo una versión digitalizada del dinero emitido por el gobierno, no son "moneda digital".

En los capítulos restantes, ahora nos centraremos en las monedas digitales, entendidas como dinero en una forma digital que no tiene contrapartida física y que generalmente tiene su propia unidad de cuenta. Actualmente, esas monedas también se pueden ver como juego y dinero marginal, en el sentido de operar en los márgenes de la economía. Analizaremos las fuerzas económicas

detrás de su desarrollo y las compararemos con el dinero tradicional que hoy en día es emitido casi exclusivamente por los gobiernos. Sobre la base de este análisis, también echaremos un vistazo al futuro de las monedas digitales.

Capítulo 3

Monedas basadas en plataforma

En los últimos años, muchas grandes compañías de Internet han introducido sus propias monedas digitales. La mayoría de estas compañías operan grandes plataformas que abarcan los medios, el entretenimiento y el comercio electrónico. El mercado ha visto monedas de Amazon, créditos de Facebook, Q-coins, Microsoft Points y Reddit gold, solo por nombrar algunos. Esto está por encima de los muchos videojuegos y plataformas de juego que tienen sus propias monedas, por

ejemplo, World of Warcraft gold, Linden dólares de Second Life o Interstellar Kredits de Eve Online.

Todas estas monedas han sido introducidas por grandes plataformas en línea que, de una forma u otra, ayudan a las interacciones entre sus grandes grupos de miembros diversos: compradores y vendedores, jugadores de juegos o simplemente personas que desean intercambiar imágenes y mensajes entre sí. Estas interacciones a menudo involucran algún tipo de comercio que puede ser ayudado por una moneda especial, hecha a la medida, que las plataformas en línea brindan para la conveniencia de sus miembros.

Es importante ver que en todos estos casos, la moneda está totalmente controlada por la plataforma, que puede establecer todas sus características y propiedades. En este capítulo, revisamos algunas de estas monedas "controladas centralmente" para comprender los impulsores clave de su diseño y las reglas que rigen su uso. El dinero para fines especiales introducido de manera centralizada y controlado por varias organizaciones, desde entidades comerciales hasta organizaciones gubernamentales locales o nacionales, no es completamente nuevo. Por ejemplo, las fichas de casino y el dinero de Monopoly han existido durante un

siglo. Además, si bien rara vez se les llama divisas, el mundo ha estado bastante acostumbrado a las millas de aerolínea canjeables por vuelos futuros, reservas de hoteles o alquiler de automóviles.

Las millas aéreas son solo un ejemplo de la familia de programas de fidelización en millones de tiendas o para una multitud de productos y servicios. Los gobiernos han introducido regularmente o han permitido la introducción privada de monedas reales restringidas a grupos sociales específicos, regiones geográficas o categorías de productos. Por ejemplo, hay varias monedas locales que

funcionan en diferentes regiones de los Estados Unidos, por ejemplo, Horas de Ítaca en el estado de Nueva York o BerkShares en el oeste de Massachusetts. Los cupones de alimentos son otro ejemplo de dinero para propósitos especiales: son esencialmente un sistema de pago restringido para uso de los pobres y solo para ciertos productos.

Sin embargo, lo que ha cambiado es que la era digital ofrece nuevas y enormes oportunidades y desafíos para la introducción y el uso de monedas para fines especiales. Primero, la naturaleza digital de estas monedas brinda infinitas oportunidades para el diseño de nuevas

funciones adaptadas a las necesidades específicas de la empresa que las introduce. Como veremos más adelante, estas necesidades variadas pueden explicar muchas de las diferencias entre las monedas basadas en plataformas de hoy. Además, además de la multiplicidad de características, la era digital también hace que sea mucho más rentable monitorear y restringir el uso de la moneda. Sin embargo, lo más importante es que muchas de las monedas digitales recientemente introducidas son globales. Las organizaciones que los ofrecen son a menudo grandes plataformas, que se extienden a través de muchas naciones.

Como tales, estas monedas pueden tener un impacto global. Este hecho no escapó a la atención. De los responsables políticos y comentaristas económicos. Matthew Yglesias (2012), mencionado anteriormente, estaba preocupado por los Créditos de Facebook que asumían las monedas emitidas por el estado, y sus preocupaciones se hicieron eco de los economistas que vieron la coincidencia de estas introducciones de moneda con el aumento de la deuda nacional de los países desarrollados después de la crisis financiera. Particularmente amenazante para las monedas emitidas por el estado. Se expresaron preocupaciones similares

cuando Amazon introdujo Amazon Coins en 2013.

Los expertos vieron un potencial para que estas monedas cuestionen el monopolio de los bancos centrales sobre la emisión de dinero. Además del contexto histórico de la crisis financiera, estas preocupaciones también se vieron impulsadas por el hecho de que Facebook y Amazon son grandes plataformas con un amplio alcance internacional y una gran base de clientes. Amazon tiene un estimado de 250 millones de clientes, y Facebook ha superado los mil millones de miembros, sin contar el hecho de que posee grandes plataformas en línea adicionales, como

Instagram y WhatsApp. A menudo se recuerda que, por su tamaño, si Facebook fuera un país, contaría como el tercero más poblado, después de China y la India.

Por ahora, estas preocupaciones han desaparecido en gran medida, no solo porque Facebook decidió abandonar los Créditos de Facebook. Como argumentaremos a continuación, ni los Créditos de Facebook ni las Monedas de Amazon tuvieron el potencial real de convertirse en monedas ampliamente aceptadas a pesar del gran tamaño de sus compañías patrocinadoras. La razón principal es que estas monedas están muy limitadas en su funcionalidad. Por

ejemplo, ni los créditos de Facebook ni las monedas de Amazon se pueden transferir a otros usuarios, y solo se pueden gastar en Facebook o Amazon. Las monedas de Amazon tienen restricciones adicionales sobre lo que pueden gastar, solo en aplicaciones seleccionadas en Amazon Kindle Fire. Con tales limitaciones, no podrían convertirse en un medio de pago que rivalice con el dólar, el euro o el yen. De hecho, la transferibilidad es necesaria, aunque no atributo suficiente para que una moneda basada en plataforma tenga un impacto más amplio. Sin embargo, las plataformas pueden encontrar en su mejor interés limitar esta funcionalidad.

Para ser justos, las preocupaciones de los comentaristas estaban algo justificadas. Primero, algunas plataformas introdujeron monedas con funcionalidades completas que pueden intercambiarse libremente por monedas emitidas por el estado; por ejemplo, los dólares Linden de Second Life pueden intercambiarse por dólares americanos. Si bien estas monedas no tuvieron una influencia importante en las monedas emitidas por el estado hasta el momento, esto se debe en gran parte al hecho de que las plataformas subyacentes no crecieron lo suficiente para tal impacto. Además, incluso las monedas locales limitadas pueden representar un desafío

para los reguladores, a quienes les resultará difícil coordinar a través de las fronteras nacionales para implementar la regulación. Sin embargo, con la flexibilidad en el diseño que hace posible la naturaleza digital de estas monedas, tal regulación podría ser cada vez más necesaria.

¿Qué impulsa este diseño? Para comprender el panorama más amplio de las monedas digitales, debemos examinar más detenidamente los incentivos de las empresas de Internet al emitir sus monedas. Las monedas para fines especiales o "locales" siempre se han introducido con objetivos específicos en mente.

Su diseño refleja estrechamente estos objetivos al tratar de evitar consecuencias no deseadas. Este también ha sido el caso de las monedas locales no digitales, como veremos a continuación. Entre nuestros ejemplos digitales, Amazon y Facebook ya habían crecido mucho antes de introducir sus monedas. Operan de acuerdo con sus modelos de negocios específicos, y su crecimiento espectacular puede ser un indicador de que estos modelos de negocios son exitosos. Nos aventuramos en la hipótesis de que las empresas solo introducen sus monedas si refuerza sus modelos de negocios. La idea principal es que la digitalización permite el

diseño de monedas para un sin precedentes, y las empresas están diseñando sus monedas al elegir los atributos de la moneda de tal manera que se adapten mejor a sus modelos de negocios.

En lo que sigue, primero revisamos algunos ejemplos clásicos de monedas locales introducidas centralmente y mostramos cómo sus características de diseño reflejan los objetivos subyacentes de las organizaciones que los han introducido. A continuación, observamos cuatro modelos de negocios típicos de grandes plataformas de Internet y analizamos cómo las características de sus monedas digitales

recientemente introducidas reflejan estos modelos de negocios.

Finalmente, discutimos los límites de la distinción que se puede hacer entre las monedas basadas en la plataforma y el dinero emitido por el estado y discutimos los desafíos que pueden representar las monedas digitales a gran escala.

En nuestro análisis de los siguientes ejemplos, nos centraremos en tres atributos principales, que la entidad que introduce la moneda puede establecer y controlar fácilmente. Podría decirse que estos atributos tienen un gran impacto sobre si la moneda puede facilitar el comercio (el propósito central de una

moneda) y en qué contexto específico puede hacerlo. El primer atributo de este tipo es la posibilidad de adquisición, o cómo se puede adquirir la moneda. El diseñador de la moneda puede, por ejemplo, requerir que la moneda solo se "gane" con ciertas actividades específicas o que se pueda "comprar" (canjear por) otras monedas o bienes. La segunda característica que examinamos es la transferibilidad, o cuáles son las restricciones, si las hay, sobre la transferencia de la moneda a otras. Normalmente, la pregunta es si se puede transferir a otros miembros en la plataforma. Finalmente, la tercera característica, la posibilidad de canjear, prescribe lo que la moneda puede

comprar. En particular, el interés central es si se puede cambiar por moneda emitida por el estado. En otras palabras, la capacidad de redención define las restricciones para gastar la moneda. Si una moneda no tiene restricciones en ninguno de los atributos, es decir, se puede comprar y ganar, se puede transferir a cualquier persona que participe en el sistema, se intercambiará por moneda emitida por el estado y se puede gastar en cualquier cosa dentro del sistema; llamamos a dicha moneda totalmente equipada. Las monedas emitidas por el estado pueden considerarse monedas totalmente equipadas, al menos dentro del país

cuyo gobierno las emitió. Sin embargo, la mayoría de las monedas digitales suelen estar restringidas en uno o varios atributos.

Esas restricciones se establecen deliberadamente para reforzar el modelo de negocio de la plataforma emisora. Consideremos varios ejemplos con más detalle, comenzando con algunos tradicionales, arraigados en el mundo no digital.

3.1. Monedas especiales del mundo off-line

Como se mencionó anteriormente, el diseño del dinero ha existido por un tiempo. Todo tipo de puntos de fidelidad, cupones de alimentos y

algunos de los productos bancarios son ejemplos de este tipo de diseño. A continuación, veremos tres ejemplos particulares:

BerkShares, cupones de alimentos e hipotecas, para analizar los desafíos de diseño que han enfrentado a la luz de los objetivos de sus emisores.

BerkShares

BerkShares se introdujo en 2006 en la región de Berkshires de Massachusetts con la intención de ayudar a la población local en una zona turística. La presencia de turistas aumentó los precios en la zona pero no necesariamente los salarios locales.

Algunas empresas locales se reunieron y

acordaron dar un descuento a la población local, en esencia, introduciendo un esquema de discriminación de precios efectivo. Esto se hizo a través de BerkShares, una moneda local. Podría obtener BerkShares en un banco local pagando 95 centavos de dólar por cada BerkShare. Pero las empresas participantes los aceptan a la par con el dólar. Dado que son una moneda de papel, cualquier restricción para transferirlos entre personas locales y no locales sería demasiado costosa de hacer cumplir. Además, cuando utiliza BerkShares, no necesita demostrar que es un local, ni siquiera pretender ser

local.

Uno podría imaginar el requisito de que necesita mostrar su licencia de conducir con una dirección local para usar BerkShares. Pero esto puede ser demasiado oneroso o provocar un sentimiento negativo de los turistas y puede ralentizar las transacciones. Dado que solo puede usarlos en las empresas participantes, BerkShares tiene restricciones sobre dónde puede gastarlos, pero no sobre quién puede gastarlos. Cualquiera puede comprarlos en un banco local. No están publicitados, por lo que no mucha gente los conoce.

Pero, por supuesto, es más probable que

los locales sepan sobre ellos. Esta ha sido probablemente la única barrera para que todos aprovechen el descuento. Seguramente, si demasiados turistas se aprovecharan de BerkShares, uno puede imaginar fácilmente restricciones adicionales para adquirir y gastar BerkShares. Dado que serían costosos de implementar, en el tiempo adicional y la carga que lleva completar las transacciones, no se implementarían hasta que no fuera necesario hacerlo. Por el contrario, para las monedas digitales, es mucho menos probable que dichas restricciones soporten estos costos de transacción adicionales. Podrían incorporarse al diseño desde el principio.

Cupones de alimentos

Las estampillas de comida son otro ejemplo de dinero diseñado, uno en el que las restricciones sobre el gasto están realmente en efecto.

Solo puede gastarlos en lugares particulares, en productos particulares, solo en alimentos y no en alcohol o tabaco. El propósito de los cupones de alimentos es que el gobierno provea alimentos a las familias con bajos ingresos. Dar a esas familias los mismos fondos en efectivo permitiría Para gastar ese dinero en bienes que no sean alimentos, incluidas las drogas o el

alcohol. Esto iría en contra del propósito del programa. La introducción de una moneda distinta con restricciones en su uso permite al gobierno lograr su objetivo: complementar los alimentos para aquellas familias necesitadas.

Originalmente, los cupones para alimentos tenían la forma de sellos o cupones de papel, similar al papel moneda. Fueron aceptados por las tiendas de alimentos participantes sin importar quién los estaba usando. Eso significaba que no había ninguna restricción para transferirlos (las familias elegibles podían pasar sus cupones de alimentos a familias no elegibles) y no había restricciones sobre

quién podía gastarlos. Su uso solo estaba restringido por el lugar donde podían gastarse y en qué productos.

Desde fines de la década de 1990, los sellos de papel fueron eliminados y reemplazados por un sistema de tarjeta de débito llamado Transferencia Electrónica de Beneficios (EBT, por sus siglas en inglés) administrada por bancos, probablemente para ahorrar costos. En 2008, el gobierno cambió el nombre de Programa de Cupones para Alimentos al Programa de Asistencia de Nutrición Suplementaria. Las tarjetas EBT se basan en el nombre y el gobierno entrega el nuevo saldo a la tarjeta de la persona elegible. Todavía

no hay una restricción particular sobre quién puede usar la tarjeta para realizar compras, ya que no hay ningún requisito de verificación de ID. Dado que los beneficios se otorgan al hogar, este acuerdo permite que diferentes miembros del hogar recojan los alimentos. No obstante, transferir el beneficio a otra persona se volvió más oneroso.

No puede simplemente entregarle a otra persona $ 5 en cupones de alimentos. Si entrega su tarjeta, no solo se separará de todo el saldo, sino también de los beneficios futuros.

Las hipotecas

Una hipoteca también se puede

considerar como una moneda con una restricción de gastos. (Es curioso, normalmente no pensamos en cupones de alimentos e hipotecas en la misma categoría). Obtener un crédito del banco. Normalmente, no puede tomar este dinero e ir de compras o irse de vacaciones.4 En general, solo puede gastarlo en una propiedad particular.

Además, la hipoteca no se puede transferir fácilmente: está restringida a una sola entidad, generalmente una persona o un individuo. En general, también existen otras restricciones en el uso de una hipoteca: dado que la garantía es a menudo la propiedad inmobiliaria específica en cuestión, es

posible que el titular de la hipoteca deba proporcionar algún seguro para la propiedad. Es posible que se impongan programas de pago específicos y multas por pagos atrasados y / o anticipados. Claramente, una hipoteca es una forma de pago bastante compleja. En los tres ejemplos anteriores, el sistema de dinero especial ha sido introducido por una entidad (un consorcio de compradores, el gobierno o un banco, respectivamente) con objetivos específicos en mente. Las reglas que rigen las monedas crean incentivos particulares para los miembros de la población objetivo. Las características de diseño de estas monedas privadas deben tener en cuenta estos incentivos

para respaldar los objetivos de la entidad.

Esto a menudo significa considerar cuidadosamente las compensaciones. Por ejemplo, en el caso de los cupones de alimentos, el gobierno se dio cuenta de que tenía que restringir la transferibilidad para asegurarse de que solo los grupos sociales objetivo se beneficiaban de los subsidios. Sin embargo, demasiada restricción en la transferibilidad (por ejemplo, proporcionar acceso solo al jefe de familia), hace que el uso del subsidio sea impráctico porque a menudo son los miembros de la familia quienes están a cargo de las compras. La solución de

tarjeta de débito EBT es un buen compromiso en este caso.

Otra consideración importante en la elección de características para una moneda es el costo de implementación de las características. La mayoría de las veces, estos Los costos no son triviales, no importa quién los lleve. Las comisiones bancarias cobradas por la administración de las tarjetas EBT absorben parte del valor de los cupones de alimentos, por lo que usar las tarjetas EBT para restringir la transferibilidad tiene un costo tanto para el emisor de la moneda como, indirectamente, para el usuario.

En lo que sigue, argumentamos que las

monedas digitales proporcionan mucha más flexibilidad para introducir características de diseño y hacen que el monitoreo de sus restricciones correspondientes sea mucho menos costoso. Esto debería significar que el tipo de empresas capaces de introducir monedas digitales de manera efectiva podrían usar esta flexibilidad para su beneficio. No obstante, el cambio que traen las monedas digitales es cuantitativo en lugar de cualitativo. No es una cosa completamente nueva sino un cambio de grado.

Sin embargo, no debemos descartarlo por falta de novedad. Todavía puede tener un gran impacto. El correo

electrónico es un ejemplo de un cambio tan cuantitativo, no cualitativo, que sin embargo ha impactado significativamente nuestro trabajo y la vida en general, creando un lugar de trabajo más conectado y "justo a tiempo". El correo electrónico es un correo más rápido. En lugar de días, recibimos correo electrónico en minutos o menos. Al principio, las personas verificaban su correo electrónico de vez en cuando y escribían correos electrónicos similares a las cartas tradicionales. (¿Recuerda cuándo necesitó conectarse a través del acceso telefónico para recibir su correo electrónico, tal vez una vez cada pocos días?)

Sin embargo, rápidamente, los mensajes se devolvieron con mayor frecuencia y se acortaron. Las conexiones a Internet mejoraron, y ahora generalmente enviamos mensajes cortos e informales todo el tiempo y los recibimos casi al instante. El correo electrónico pasó de una versión digital de letras a una versión digital de notas aprobadas en una clase. Del mismo modo, ¿quién sabe adónde nos puede llevar la proliferación de monedas digitales diferenciadas? Como lo demuestran los ejemplos anteriores, al explorar sistemas privados de moneda digital más recientes, debemos tener en cuenta que estos sistemas están impulsados por la

interacción entre los objetivos de las entidades que los introducen y los incentivos que ofrecen a los usuarios. A su vez, en el caso de las empresas privadas como las plataformas de Internet, los objetivos son impulsados por los modelos de negocios de estas empresas. No es de extrañar entonces que fundamentalmente los diferentes modelos de negocios conducen a monedas privadas con características de diseño muy diferentes.

3.2. Monedas basadas en plataforma en la era digital

La era digital ofrece una medida sin precedentes para controlar el diseño de la moneda. En ciertos casos, la

tecnología también ha reducido significativamente el costo de implementar diseños alternativos. En particular, la tecnología puede ajustar fácilmente las tres características de diseño fundamentales que hemos revisado anteriormente. Permite, por ejemplo, controlar fácilmente a quién se puede o no transferir la moneda (transferibilidad). La tecnología también puede controlar mejor cómo se puede adquirir la moneda (adquiribilidad) y cómo puede gastarse (canjeable).

Sin duda, es mejor Utilice estos activos para consumir más en la plataforma que para perderlos. Esto, por supuesto, es beneficioso para la plataforma,

especialmente si su modelo de negocio se basa en la intensidad de uso. Esta es la razón por la que muchas de las plataformas digitales (por ejemplo, World of Warcraft o Facebook) restringen el cobro simplemente por no permitir que sus monedas se conviertan en moneda emitida por el estado. Al mismo tiempo, restringir los fondos dentro de la plataforma también puede significar que las personas podrían estar menos inclinadas a inyectar fondos desde el exterior en la plataforma en primer lugar. Si tales "inversiones" son críticas, digamos para el desarrollo de la plataforma en sí, entonces esta consideración debe ser compensada con la lealtad del cliente. Este es el caso del

mundo virtual Second Life, que depende completamente de sus usuarios para construir todo el contenido en la plataforma, desde la textura de la tierra hasta las plantas, las casas y cualquier objeto que pueda imaginar. Entre las tres características clave, la transferibilidad es particularmente sutil. Por un lado, la transferibilidad es claramente necesaria si la plataforma quiere una interacción económica entre los miembros. Sin embargo, la transferibilidad crea una posibilidad para que algunas personas utilicen la plataforma para ganar dinero y exportarlo desde la plataforma, incluso si la plataforma no permite oficialmente

tal "retiro". Al analizar el caso del oro de World of Warcraft a continuación, se hará evidente que permitir la transferibilidad generalmente está en conflicto con fuertes restricciones para sacar fondos de la plataforma.

¿Qué podría explicar qué características de diseño se implementarían para la moneda de una plataforma en particular?

Sobre la base de los ejemplos y la discusión anterior, vemos que el modelo de negocio de las plataformas tiene un papel decisivo en la elección de las características. El modelo de negocio de la plataforma proporciona orientación sobre los incentivos que la plataforma desea reforzar para su base de

miembros. Claramente, puede haber muchos otros determinantes, tal vez prácticos, que necesitan ser considerado; Por ejemplo, restricciones tecnológicas o regulatorias. Pero la moneda digital, si se adopta, debe respaldar el modelo de negocios de la empresa. Sin embargo, el concepto de "modelo de negocio" es bastante complejo. Para ser más específicos, nos centraremos en dos de sus aspectos clave: la forma en que la plataforma crea valor para sus clientes / miembros (es decir, su propuesta de valor) y la forma en que la plataforma captura este valor (es decir, su modelo de ingresos). Argumentamos que estos dos aspectos del modelo de negocio tienen una gran

influencia en la elección de las características de diseño para la moneda digital de la plataforma.

La evolución dinámica de Internet ha generado muchos modelos de negocios diferentes, y el proceso de experimentación está lejos de terminar. Actualmente, hemos identificado cuatro modelos particulares que cubren una gran cantidad de negocios exitosos de plataformas digitales. Son los siguientes:

1. Videojuegos interactivos en línea, como World of Warcraft y Diablo.

2. Mundos virtuales, como Second Life y Eve Online

3. Redes sociales, como Facebook y Tencent

4. Plataformas de promoción de productos, como la plataforma de lector electrónico de Amazon o una plataforma de juegos como Steam.

Observamos cada uno de estos cuatro modelos de negocios. Al analizar sus diseños de moneda digital, nuestro objetivo es explorar cómo su proceso de creación de valor y su modelo de ingresos están vinculados al tipo de monedas que introdujeron.

Una advertencia importante es que lo que llamamos modelos de negocios "típicos" exhiben una buena cantidad de variación en sí mismos.

De hecho, la separación estricta de estas cuatro categorías es algo forzada porque hay muchas plataformas que se ubican en algún lugar entre las categorías. Los videojuegos interactivos en línea tienen una variedad increíble, desde relativamente Simples y estilizados a universos complejos. World of Warcraft, por ejemplo, puede verse legítimamente como un mundo virtual en lugar de un simple videojuego, dependiendo de la perspectiva de cada uno, y tendremos que ser más explícitos para dejar clara esta diferencia.

Por otro lado, Eve Online puede verse como un videojuego en lugar de un mundo virtual. De manera similar,

Tencent se puede ver legítimamente como una red social a pesar de que es una de las plataformas de juegos más grandes del mundo, albergando muchos de sus propios juegos.

En lo que sigue, proporcionamos una caracterización más precisa de estos modelos de negocios, pero es importante tener en cuenta que cualquier clasificación es algo artificial, dada la gran cantidad y variedad de plataformas digitales disponibles.

En un aspecto importante, estas plataformas son bastante similares: todas exhiben alguna forma de externalidad de consumo. En tales entornos, los consumidores se

benefician de otros consumidores que utilizan la misma plataforma. Como el propósito principal de las plataformas es facilitar las interacciones entre grupos de consumidores, es bastante natural que las externalidades de consumo estén presentes. A su vez, la reciente aparición de tales plataformas no es sorprendente dada la capacidad central de Internet para conectar a un gran número de personas. Como tal, las plataformas construidas en Internet naturalmente explotan esta característica.

Tomemos el caso de los videojuegos, por ejemplo. Aquí, cuanta más gente juegue el juego, más agradable será:

esto se traduce en más emociones y también en más oportunidades de colaboración. Del mismo modo, en las redes sociales, más personas que comparten contenido, significan que hay más contenido para consumir. Para un miembro individual que comparte su contenido, hay una audiencia más grande si la plataforma tiene un número mayor de miembros. En los mundos virtuales, más miembros significan un mundo más rico y complejo con más objetos presentes y más cosas que hacer.

Mientras que hay diferencias a través de plataformas en cómo exactamente estas externalidades, los juegos están presentes de una forma u otra, lo que

naturalmente lleva a los efectos de red. La presencia y la naturaleza de las externalidades de consumo a menudo se reflejan en el diseño de las monedas que adoptan las plataformas.

Finalmente, es importante señalar que las plataformas digitales y sus monedas son fenómenos relativamente nuevos, y lo que observamos hoy no es la forma definitiva de las monedas digitales de estas empresas. La experimentación en este dominio está lejos de terminar. De hecho, y lo que es más interesante, algunas de las monedas introducidas no funcionaron y tuvieron que ser abandonadas o necesitaron un rediseño sustancial durante su corta historia.

Estos casos son particularmente interesantes para comprender el vínculo entre las características de diseño de las monedas digitales y su papel en los modelos de negocios correspondientes de las plataformas.

3.2.1. Videojuegos en línea y World of Warcraft Gold World of Warcraft

Es el juego de rol multijugador masivo en línea más popular (MMORPG). Creado por Blizzard Entertainment, cuenta con más de 8 millones de jugadores que interactúan con sus avatares en este mundo virtual medieval. A medida que juegan, ganan habilidades y riqueza. Realizan misiones, solas o más comúnmente en grupos, para

enfrentar desafíos y obtener aún más habilidades y riqueza.

Las búsquedas son exigentes, y es importante para el éxito construir un equipo con la composición adecuada de habilidades complementarias para el desafío en particular. La moneda del reino es el oro de World of Warcraft (oro de WoW). Se puede transferir libremente entre los miembros del juego, pero de acuerdo con las reglas del juego, no se puede adquirir a cambio de una moneda emitida por el estado, ni se puede canjear por una moneda emitida por el estado. WoW Gold solo se puede ganar en el juego y solo se puede gastar en el juego Es fácil entender el

propósito de la mayoría de estas características de diseño. Permitir que las personas ganen oro les hace progresar en el juego. Junto con la regla que WoW.

El oro solo se puede gastar en el juego, este diseño crea lealtad. El diseño también es compatible con el modelo de ingresos de la empresa: una cuota mensual. Los fondos ganados y bloqueados aumentan la lealtad al juego. Esto es aún más importante porque el juego exhibe fuertes externalidades de consumo y efectos de red asociados: cuantas más personas juegan, más posibilidades hay de formar equipos o unirse a ellos y completar búsquedas de

mayor dificultad ficticia. En esta configuración, tiene sentido aumentar la base de usuarios, y esto se logra haciendo que la plataforma sea un poco complicada para aquellos que ya se han enganchado. Su presencia hará que el juego sea más atractivo para los nuevos jugadores que están considerando unirse.

La transferibilidad también es importante para la propuesta de valor de World of Warcraft. El juego se basa en las interacciones entre los jugadores al permitirles formar coaliciones para completar las misiones. Completar una misión suele ser recompensado con una recompensa. La transferibilidad

garantiza que la recompensa se puede compartir de manera adecuada entre los miembros de la coalición.

Esto puede suceder según las habilidades o la contribución a la búsqueda. La transferibilidad también ayuda a los miembros a intercambiar armas y otros objetos entre sí. Esto, el aspecto comercial del juego también refuerza los efectos de red.

Sin embargo, en un aspecto, este diseño de moneda puede parecer demasiado restrictivo: el oro de WoW no se puede comprar con la moneda emitida por el estado, solo se gana en el juego. ¿Por qué Blizzard no querría ganar dinero extra vendiendo oro WoW?

¿No atraería aún más miembros? Resulta que esto podría socavar la propuesta de valor de World of Warcraft para los miembros y, como resultado, los ingresos de Blizzard. Los ingresos de World of Warcraft provienen de los jugadores suscripciones Siguen pagando siempre que el juego ofrezca la satisfacción de alta calidad a la que se han suscrito. Como se mencionó anteriormente, la interacción con otros jugadores es crucial en el juego. Las misiones en niveles más altos requieren la colaboración de varias o incluso algunas docenas de jugadores.

Sin embargo, más allá del tamaño del equipo, las habilidades de los

colaboradores también son fundamentales para el éxito. Las habilidades de nivel superior son deseables, y las habilidades deben ser complementarias dentro del equipo. Sin embargo, la mayoría de las veces, cuando se seleccionan miembros del equipo para una búsqueda, el jugador no conoce bien a los posibles candidatos. Afortunadamente, el estado alcanzado en el juego, que solo se puede adivinar a partir de su ropa y accesorios visibles, es un buen indicador de la habilidad del jugador. Una búsqueda exitosa requiere un equipo con la combinación correcta de habilidades. Si todos los signos de estado se obtienen al progresar en el juego, entonces el estado es un buen

indicador de habilidad.

Si, por otro lado, la ropa y los accesorios se compraron con dinero ganado fuera del juego, el estado mostrado ya no se correlaciona con la habilidad, y el estado no solo es poco informativo sino que también es engañoso para los jugadores que intentan armar un equipo de búsqueda exitoso. Si Blizzard cambiara las reglas y permitiera a los jugadores nuevos (por lo tanto, sin experiencia) comprar el estado de otros, esto crearía una fuerte externalidad negativa para los otros jugadores ("honestos"). La presencia de tales impostores podría destruir rápidamente el juego si se rompe la

confianza en las habilidades de los jugadores pares. WoW Gold está diseñado para servir al modelo de negocio del juego. Ilustra cómo la restricción deliberada de ciertos atributos de la moneda puede ayudar a crear valor para los clientes. Sin embargo, es importante darse cuenta de que no todos los juegos interactivos encuentran estas restricciones óptimas. En particular, una gran proporción de juegos (la mayoría de los juegos sociales en teléfonos móviles, por ejemplo) adoptan el clásico modelo freemium". En el modelo freemium, uno puede jugar gratis, ganando un "crédito" (generalmente alguna moneda digital) cuando avanza en el juego, es decir,

alcanza un estado más alto. Choque de clanes, desarrollado por el estudio de juegos Supercell es un buen ejemplo. Se puede jugar en una PC o en un teléfono inteligente. El juego es bastante simple. Los jugadores son dueños de un pueblo y su objetivo es desarrollarlo tanto como sea posible. El desarrollo esencialmente significa construir un ejército con armas sofisticadas y sólidas defensas contra los asaltantes.

Los fondos para construir el ejército provienen de las actividades económicas de la aldea, que, con un poco de simplificación, se reducen a la búsqueda de oro. El oro a su vez puede comprar más armas y así sucesivamente.

Una parte interesante del juego es que uno puede usar su ejército para asaltar otras aldeas y robarles oro. De esta manera, todos luchan y todos intentan lograr un mejor "estado", medido como un rango entre los jugadores, ajustando sus estrategias en términos de las inversiones que realizan en sus ejércitos, defensas y tecnologías de excavación de oro. Sin embargo, los jugadores también pueden comprar crédito con una moneda emitida por el estado que acelerará su avance al proporcionarles fondos adicionales. En lugar de una tarifa de suscripción fija, son estas compras, que generalmente provienen de una proporción muy pequeña de los jugadores, lo que

representa la fuente principal de ingresos del juego. Choque de clanes es un ejemplo típico de un juego de freemium.

Curiosamente, los juegos de freemium no parecen sufrir por el hecho de que algunos jugadores pueden comprar el "estado". En estos juegos, mientras que los jugadores pueden interactuar de varias maneras:

Ayudándonos unos a otros, negociando unos con otros, por ejemplo; no dependen tan críticamente de las habilidades avanzadas de cada uno. De hecho, en Choque de clanes, cualquier compañero con un ejército grande es tan bueno como cualquier otro, no importa

si el ejército fue comprado o "ganado" a través de conquistas. Como tal, el valor de un socio no está estrechamente vinculado a la experiencia en el juego.

En otras palabras, el hecho de que el estado observado no esté necesariamente relacionado con la habilidad no perjudica a los otros jugadores. Por lo tanto, los jugadores inexpertos no crean una fuerte externalidad negativa para los demás. Los juegos de Freemium generalmente también tienen restricciones sobre el retiro de fondos creados o comprados en el juego; estos fondos no se pueden recuperar para la moneda emitida por el estado. Esta restricción mantiene a los

jugadores en el juego, lo que también ayuda a otros jugadores a unirse. Sin embargo, como veremos a continuación, no siempre es fácil para el propietario del juego hacer cumplir esta regla, y algunos jugadores se esfuerzan por romperla.

Fraude con moneda digital

Si bien las funciones digitales de los juegos son fáciles de implementar y monitorear en la plataforma, Internet ha hecho cada vez más fácil romper las reglas utilizando otras plataformas interactivas que facilitan el comercio, como eBay, por ejemplo.

En World of Warcraft, por ejemplo, a pesar de las reglas del juego que dicen

lo contrario, hay muchas transferencias externas entre jugadores. La gente está dispuesta a comprar oro de WoW, por dinero emitido por el estado, junto con los artículos que puedes comprar con oro, como armas o armaduras, para avanzar en el juego sin la inversión de tiempo. EBay prohibió el comercio de monedas y activos en el juego en enero de 2007, pero hay una serie de otros sitios donde se puede comprar WoW oro para moneda emitida por el estado. Esto indica que hay demanda de activos en el juego. Y estos no son solo oficios ocasionales.

Hay tanta demanda que algunas personas en los países en desarrollo lo convierten

en su trabajo diario para jugar un juego, recolectar oro de WoW y luego venderlo en una moneda emitida por el estado. Esta actividad se conoce popularmente como "minería de oro". En casos extremos, incluso condujo a casos infames de minería de oro forzada en los campos de trabajo chinos, donde los guardias hicieron que los prisioneros jugaran el juego por la noche, vendiendo lo recolectado creando, la existencia de estos “mercados negros”.

No ayudó la reputación del juego. Pero incluso sin estos casos extremos, como hemos visto anteriormente, los mercados negros dañan a los jugadores al inundar la plataforma con personas cuyo estado

no coincide con su habilidad, lo que arruina el juego. Curiosamente, los propios jugadores de World of Warcraft comenzaron a vigilar este comportamiento sospechoso e informarlo a los administradores del juego. Como consecuencia, Blizzard ha expulsado a varios jugadores por fraude, pero la práctica no ha desaparecido.

Los propios jugadores encontraron una mejor solución. El problema de los "jugadores falsos" se volvió tan molesto para ellos que decidieron ignorar la mayoría de las demostraciones tradicionales de estado y, en su lugar, confiar en los llamados Puntos de Matanza del Dragón (DKP) para evaluar

la habilidad de un posible compañero de búsqueda. Los DKP se adquieren participando en una misión que mata a un tipo particular de criatura, llamada jefe. Inicialmente los jefes eran principalmente dragones, de ahí el nombre. La criatura muerta deja un tesoro o un botín. Cuando hay muchas personas en la búsqueda, necesitan ponerse de acuerdo sobre cómo dividir el botín. Los juegos resolvieron este problema asignando los DKP a los participantes de una búsqueda exitosa y permitiéndoles usar esos puntos para comprar ciertos artículos.

Pero los DKP solo pueden comprar aquellos artículos que son

recompensados por matar a un jefe. Si un jugador no gasta sus DKP, se acumulan y se pueden gastar más tarde. En otras palabras, los DKP son una moneda alternativa con restricciones sobre en qué se puede gastar la moneda. Lo más importante es que los DKP no son transferibles. Los DKP tienen un uso mucho más limitado que el oro de WoW, y los DKP no pueden sustituir al oro de WoW en su papel económico en el juego.

Sin embargo, en presencia de los mercados negros para el oro de WoW, los DKP resultaron ser más útiles para la habilidad de señalización. Al principio, los DKP se asignaron

informalmente y se rastrearon dentro de Grupos de jugadores, llamados gremios, con el propósito de la asignación de bienes. A medida que ganaron importancia como herramienta de señalización de habilidades, Blizzard formalizó este sistema dual como el llamado sistema de Avance de Gremios, aparte del oro existente.

Experimentos y aprendizaje infructuosos Blizzard también experimentó con un diseño diferente de sistemas monetarios en otros juegos. No todos los experimentos tuvieron éxito. Dadas las crecientes ventas de oro y artículos en el juego en el "mercado negro", Blizzard decidió incorporar dicha funcionalidad

directamente en el juego para la tercera edición de su popular juego Diablo. En este juego, un jugador derrota a las criaturas enemigas en un nivel de desafío creciente.

En cada nivel, una criatura derrotada suelta armas (y oro) que ayudan al jugador a derrotar a una criatura más exigente en el futuro. La culminación del juego es una pelea con Diablo, el "señor del terror". El juego Diablo es menos interactivo que World of Warcraft, pero aún tiene algunos elementos cooperativos. Un jugador que tiene un excedente de un tipo de arma, armadura u otros elementos pero que necesita un tipo diferente puede comerciar con otros

jugadores directamente a través de los mercados del juego, las llamadas casas de subastas.

Los intercambios pueden realizarse utilizando oro en el juego (en las Casas de subastas de oro), o utilizando moneda emitida por el estado (en Casas de subastas de dinero real). Blizzard cobra una tarifa de transacción en dichas operaciones, ya sea que se realicen con monedas en el juego o emitidas por el estado. Además, Blizzard cobra una tarifa de retiro si un jugador saca dinero emitido por el estado fuera de la plataforma. A diferencia de World of Warcraft, Diablo no está basado en suscripciones. Solo hay una tarifa única

por comprar el juego. Por lo tanto, ganar dinero con las transacciones en efectivo de los usuarios dentro y fuera del juego tenía sentido desde la perspectiva del modelo de ingresos. Sin embargo, la posibilidad de que los jugadores sin experiencia compren estatus representaba un problema importante, incluso en este juego donde el nivel de cooperación, y por lo tanto, la evaluación de la habilidad de un compañero, no es tan crítico. El respaldo al comercio de divisas emitido por el estado dentro del juego eliminó los mercados negros e hizo que la compañía obtuviera más ingresos, pero también reforzó las externalidades negativas representadas por los

"jugadores falsos". En marzo de 2014, Blizzard cerró las casas de subastas, diciendo que fueron perjudiciales para el juego porque "cortocircuitaron" el título e hicieron que el juego fuera menos satisfactorio.

Blizzard pareció controlar el problema del diseño de moneda en otro juego llamado Guild Wars 2.

En este juego, hay tres tipos de moneda: gemas, oro y karma. Las gemas están directamente vinculadas al dinero emitido por el estado. Los jugadores pueden comprarlos con dinero emitido por el estado a una tasa fija. El oro se puede ganar en el juego o comprar con gemas. Sin embargo, el oro se compra

en un mercado impulsado por el jugador. Eso significa que la plataforma no establece el tipo de cambio gemas-oro.

En cambio, la tasa depende de la oferta relativa y la demanda de oro y gemas. El Karma, por otro lado, se gana a través de las tareas del juego y no se puede comprar ni transferir. La mayoría delas micro- transacciones y compras en el juego, ya sea desde la plataforma o directamente entre los jugadores, se realizan en oro totalmente transferible. Pero el karma se usa para comprar premios únicos. Así, mientras que el oro y las gemas se pueden usar para adornar los avatares, solo las recompensas compradas con karma no transferible

indican directamente la habilidad del jugador.

Estos ejemplos de juegos de Blizzard muestran la importancia de la transferibilidad para la moneda. La transferibilidad hace que sea más fácil eludir otras restricciones, como las restricciones de compra y retiro, si a los usuarios les resulta beneficioso hacerlo. Si es importante para el valor de la plataforma que los usuarios no compren la moneda, como en el caso de la señalización de habilidades en World of Warcraft y Guild Wars 2, la plataforma debe contar con una moneda que no sea transferible. Esto puede crear conflicto si, al mismo tiempo, una de las

atracciones de la actividad en la plataforma son las interacciones económicas entre los usuarios. Estas actividades económicas en la plataforma usualmente requieren una moneda transferible. Como muestra el ejemplo de Blizzard, una posible solución es un sistema dual que permita comprar la moneda transferible, formalizar un estado de facto, y al mismo tiempo operar una moneda independiente no transferible obtenida en el juego y, por lo tanto, señalar la habilidad.

3.2.2. Mundos virtuales y dólares Linden

Los ejemplos anteriores analizaron la restricción de las funciones de moneda.

Pero el diseño óptimo para algunas empresas de plataforma puede apuntar a una moneda totalmente equipada. Un ejemplo de una moneda sin restricciones de este tipo es el dólar Linden, la moneda utilizada en un mundo virtual llamado Second Life. En este punto, es importante preguntar, ¿cuál es la diferencia entre un "mundo virtual" y un videojuego complejo como World of Warcraft? La respuesta corta es que los mundos virtuales son “MMORPG sin propósito”.

Los MMORPG clásicos representan un mundo bien definido con reglas bien definidas y una apariencia visual consistente. Lo más importante, tienen

objetivos bien definidos para sus jugadores. Los jugadores se enfrentan a misiones específicas, hay una jerarquía conocida entre ellos, y todos saben lo que hay que hacer para lograr los objetivos.

En Second Life se define muy poco. Uno puede elegir hacer lo que quiera, y las personas terminan haciendo cosas muy diferentes. Estas pueden ser actividades muy complejas, como ejecutar un bar virtual (con bebidas virtuales y música real mezclada por un DJ, representado por su avatar), construir y vender naves espaciales sofisticadas u operar una galería con hermosos cuadros. A diferencia de las actividades también

pueden ser realmente simples y no requieren mucho esfuerzo, como pasar el rato con amigos (tal vez en un bar), decorar el avatar de uno, solo visitar lugares en el mundo virtual, etc. De hecho, el mundo virtual en sí mismo tampoco está definido: se pueden visitar universos completamente diferentes y conocer avatares con aspectos muy diferentes. En una región, por ejemplo, algunos miembros han reconstruido todo el universo de la película Avatar, con islas flotantes y vegetación espectacular. Otras regiones fueron construidas para parecerse a un desierto industrial abandonado. Todos los aspectos del entorno, desde la forma de la tierra hasta la vegetación, los edificios, las

criaturas, etc., deben ser construidos desde cero por los miembros del mundo virtual.

Second Life es probablemente el mundo virtual más extremo en el sentido de que casi nada está definido en él; brinda posibilidades ilimitadas. En este sentido, es lo opuesto a World of Warcraft, que es un mundo virtual totalmente codificado. Los mundos virtuales representan un continuo entre estos extremos, con muchas plataformas situadas en algún lugar en el medio. Eve Online, por ejemplo, es un mundo virtual utópico inspirado por las ideas de Ayn Rand de un universo libertario. Si bien también permite una libertad casi

ilimitada para sus miembros, el entorno es algo más definido que el de Second Life. Sin embargo, en un aspecto, Eve Online es "más libre" que Second Life: no tiene derechos de propiedad, necesita estar organizado para hacer cumplir estos. En Second Life, los derechos de propiedad están bien controlados por el juego, y solo hackeando la plataforma puede alguien robar propiedad virtual de otros.

Dada esta libertad, habrá muchas personas diferentes en la plataforma con gustos y actividades diferentes. De hecho, los mundos virtuales están construidos para ser economías totalmente funcionales. En cambio, los

miembros tienen muchas oportunidades para recaudar ingresos de sus miembros. Un impuesto general sobre la actividad económica parece ser una buena manera de recaudar ingresos. En el caso de Second Life, donde el mundo estaría virtualmente vacío sin los objetos construidos por los residentes, un buen sustituto de la actividad económica es la propiedad de la tierra, ya que solo tiene sentido pagarlo si algo se construye en la tierra. La aplicación de impuestos a la tierra virtual está alineada con el costo de la plataforma de atender a los clientes, ya que más tierra y más objetos en la tierra significan más memoria utilizada por el sistema de tecnología de la información de la plataforma.

No es sorprendente entonces que el modelo de ingresos de Second Life esté estrechamente vinculado a la actividad económica en la plataforma. Específicamente, el modelo tiene tres fuentes principales de ingresos.

Primero, recauda ingresos de usuarios "avanzados", que tienen el derecho de construir cosas. Esencialmente, cobra una cuota de membresía. En segundo lugar, Second Life también recolecta los ingresos de las ventas de terrenos virtuales. Se puede comprar una isla pequeña por un pago único de aproximadamente $ 1,000 seguido de un alquiler continuo, generalmente de $ 200. Finalmente, Second Life cobra una

tarifa de transacción del intercambio entre dólares Linden y la moneda emitida por el estado. Todos estos ingresos están ampliamente vinculados a las diversas actividades económicas en la plataforma.

La moneda de Second Life, el dólar Linden, es una moneda totalmente equipada. Se puede ganar dentro de la plataforma, generalmente trabajando para alguien, pero también se puede comprar con moneda emitida por el estado. Puede transferirse a cualquier persona o gastarse dentro de la plataforma para comprar cualquier cosa que esté a la venta.

Finalmente, también se puede cambiar

de nuevo a la moneda emitida por el estado y sacarse de la plataforma. Esta última característica es algo desconcertante. ¿Por qué Second Life permite que las personas saquen su dinero de la plataforma? Como hemos visto antes, esto puede alentar a las personas a abandonar la plataforma, ya que, simplemente, no hay costo en dejar la plataforma. Cuando uno quiere probar otras cosas o porque la gente puede querer "retirar" después de haber tenido éxito. Claramente, esto no necesariamente beneficia a Second Life, especialmente en vista de las fuertes y positivas externalidades de consumo presentes en los mundos virtuales. ¿Por qué permitirlo entonces?

En resumen, en la política de "retiro" tiene que ver con la provisión de incentivos para "invertir" en la plataforma mediante la creación de contenido en ella.

Si Linden Labs, el propietario de Second Life, desea tener una comunidad interactiva vibrante en la plataforma, incluida una economía compleja, debe proporcionar incentivos para que las personas inviertan, y esto es para una base de miembros muy heterogénea. Primero, la gente necesita construir cosas. Para objetos complejos, como un avión, un instrumento musical o un centro comercial, la construcción puede requerir la colaboración de varias

personas o una combinación de elementos múltiples ya disponibles de otros.

Las "misiones" no están disponibles, la colaboración a menudo requiere la contratación de mano de obra. Además, al igual que en el mundo real, para funcionar bien en Second Life, se necesita un amplio comercio.

La mayoría de los objetos complejos requieren grandes inversiones de tiempo. No es razonable esperar que todos puedan pasar este tiempo en el juego, por lo que la plataforma debe alentar la inversión en términos de dinero. Para todos los propósitos prácticos, Second Life es como una

economía real, con mercados de inversión, mano de obra y productos con derechos de propiedad claros. De hecho, se ha señalado que una de las razones por las cuales los usuarios estaban dispuestos a construir una gran variedad de cosas para poblar el mundo virtual fue que, la plataforma declaró que los residentes (como se llama a los usuarios de Second Life) eran propietarios de los activos virtuales que crearon en el juego, y los residentes podrían vender libremente estos activos.

En este sentido, Second Life no es un juego como el MMOR-R. PGs que hemos revisado anteriormente. En 2008, muchos de sus residentes trasladaron

parte de sus vidas profesionales a Second Life, ganar Linden dólares construyendo cosas, abriendo y administrando tiendas, o simplemente trabajando para otras empresas virtuales. En consecuencia, el Servicio de Impuestos Internos declaró que las ganancias en dólares Linden estaban sujetas a impuestos y muchos otros gobiernos hicieron anuncios similares. Si bien para la mayoría de las personas estas ganancias eran efímeras, algunas personas hicieron una fortuna real vendiendo productos digitales en Second Life. Muchas empresas del mundo real, desde minoristas como American Apparel, compañías de medios como Reuters hasta, quizás más

naturalmente, compañías de tecnología como Sun Microsystems: decidió construir una presencia en Second Life. Fueron seguidos por otras organizaciones (escuelas, universidades y gobiernos locales o nacionales) que iniciaron actividades serias en el mundo virtual con la esperanza de que eventualmente se convirtiera en una plataforma de Internet dominante.

Eve Online

El mundo virtual Eve Online, mencionado anteriormente, también es un mundo virtual típico en el que poco se define para sus miembros, que pueden elegir libremente sus actividades. La configuración del espacio exterior de

ciencia ficción de Eve Online está más definida que la de Second Life. Pero las actividades de los miembros de la plataforma se suman a una economía bastante compleja que, en muchos aspectos, es incluso más libre que la de Second Life. Como se mencionó anteriormente, los derechos de propiedad no se aplican de manera centralizada, y en su lugar, los miembros deben organizarse para proteger su propiedad mediante la contratación de guardias y así sucesivamente. Eve Online es más "impulsado por el mercado" que Second Life, en el sentido de que el comercio, en lugar de contenido generado por el usuario, constituye una parte más importante del

juego. Si bien hay más restricciones para crear bienes virtuales en Eve Online, el comercio es más complejo y requiere habilidades especiales adquiridas en el juego. Esencialmente, se relaciona con la capacidad del comerciante para ver más oportunidades de arbitraje que otros jugadores que pueden haber invertido en el desarrollo de otras habilidades, como luchar o construir. Sin embargo, todas estas pequeñas diferencias entre Eve Online y Second Life no son importantes para el panorama general, es decir, que ambas plataformas tienen una economía compleja. En consecuencia, ambos mundos virtuales deben proporcionar

incentivos de inversión para sus miembros.

En consecuencia, no es sorprendente que Eve Online también tenga una moneda totalmente equipada, denominada Interstellar Kredits. Se abrevia como ISK, que es algo confuso, no solo porque la corona islandesa también se abrevia como ISK, sino porque la compañía de desarrollo de Eve Online, CCP Games, también tiene su sede en Reykjavik.

Impacto fuera de la plataforma. Si bien Second Life y Eve Online han introducido divisas totalmente equipadas, no hay restricciones para comprarlas, ganarlas, regalarlas o

transferirlas a la moneda emitida por el estado, ni los dólares Linden ni ISK han tenido importantes Impacto fuera de sus respectivas plataformas. Probablemente, la razón principal es que ninguna de las plataformas logró atraer a una comunidad muy grande. Hay más de 20 millones de cuentas de Second Life registradas, pero se estima que alrededor de 600,000 de ellas representan jugadores activos. La población de juegos de Eve Online se estima en 30,000 a 40,000 jugadores. Claramente, estas cifras son pequeñas en comparación con más de mil millones de miembros en Facebook, por ejemplo.

Sin embargo, a los primeros

comentaristas les preocupaba sobre todo el hecho de que las monedas de los mundos virtuales estuvieran completamente equipadas, por lo que tenían el potencial de reemplazar las monedas emitidas por el estado. Sin embargo, es erróneo preocuparse por el impacto de la moneda fuera de la plataforma prevista simplemente porque está completamente equipada. Como Fung y Halaburda. (2014), la moneda no necesita estar completamente equipada para tener un impacto potencial fuera de la plataforma. Solo necesita ser transferible. Una vez transferibles, los usuarios pueden manipular las restricciones en cuanto a la adquisividad y la capacidad de reembolso.

Este fue el caso de WoWel oro, que se negoció ampliamente fuera de la plataforma de World of Warcraft a pesar de carecer de algunas características clave que los dólares Linden tenían.

Con la capacidad de transferencia completa, si los usuarios desean adquirir o canjear la moneda por una moneda emitida por el estado, pueden encontrar una vía para el comercio mixto, donde una parte de la transacción se realiza en la plataforma y la otra, fuera de ella.

Una vez que la moneda se comercializa fuera de la plataforma, se puede utilizar para operaciones distintas de las previstas por la plataforma. El hecho de

que tenga un impacto fuera de la plataforma depende fundamentalmente de si los usuarios tienen un incentivo para usarlo en lugar de otras monedas disponibles.

Por lo tanto, esto se convierte en un problema típico de la competencia de divisas, que precede a la era digital. Puede haber algunos países donde las personas prefieren usar dólares estadounidenses en lugar de la moneda local. Argentina es a menudo señalada como una de ellas. Al mismo tiempo, coexisten monedas que satisfacen su rol; por ejemplo, dólares estadounidenses y canadienses.

Aunque no hay restricciones, los

canadienses no tienen necesidad de usar dólares estadounidenses en Canadá, y los estadounidenses no tienen necesidad de usar dólares canadienses en los Estados Unidos. Las mismas fuerzas juegan con las monedas digitales. Incluso con la transferibilidad, las monedas solo se adoptan fuera de la plataforma si cumplen algunas funciones mejor que las alternativas existentes. Por lo que sabemos, esto no ocurre con el oro de WoW, ni con los dólares de Linden. Pero hay un ejemplo bien documentado lo que ocurrió con las monedas Q, la moneda de Tencent, una red social china, que presentamos más adelante en este capítulo.

3.2.3. Redes sociales y créditos de Facebook Las redes sociales

Son el tercer modelo de negocio prototípico que ha surgido para las plataformas de Internet. En estas grandes plataformas con cientos de millones de usuarios, los miembros interactúan principalmente al compartir contenido entre ellos. El modelo de ingresos suele basarse en la publicidad, aunque ha habido otras fuentes de ingresos que pueden aportar contribuciones significativas, por ejemplo, los ingresos de los desarrolladores de aplicaciones o desarrolladores de juegos. Facebook es, con diferencia, la red social más grande del mundo, con casi 1.5. Mil millones de

usuarios activos. También posee una variedad de otras plataformas sociales líderes que están más o menos conectadas a Facebook, como Instagram, WhatsApp o Facebook Messenger. Es importante darse cuenta de que Facebook no es simplemente una plataforma para que sus miembros interactúen con el contenido generado por el usuario. Es una llamada plataforma de múltiples lados, donde una gran parte del contenido es proporcionado por terceros, ya sea sitios de medios, desarrolladores de juegos o aplicaciones, o simplemente marcas de productos.

Las categorías comunes de este

contenido de terceros consisten en videos, artículos y juegos.

En 2009, Facebook introdujo los créditos de Facebook, que en 2011 se convirtieron en la moneda obligatoria para todas las aplicaciones y juegos en la plataforma de Facebook que querían cobrar a los miembros.

El crédito de Facebook usó denominaciones no estadounidenses y esencialmente funcionó como una billetera virtual. Puede agregar fondos en línea o comprar tarjetas de regalo en las grandes tiendas. Desde entonces, el sistema se retiró en 2013 a favor de un sistema de pago que utiliza directamente las monedas emitidas por el estado.

Como se mencionó anteriormente, los créditos de Facebook no se pudieron transferir entre usuarios de Facebook. Tampoco se pudieron cambiar por moneda emitida por el estado, como dólares, euros o yenes. Los créditos se pueden gastar en cualquier cosa en Facebook, ya sea que el contenido se haya incluido directamente proporcionado por Facebook o por un desarrollador externo, siempre que los desarrolladores acepten los Créditos de Facebook. Entre 2009 y 2011, los desarrolladores podrían cobrar a los usuarios en créditos de Facebook o en monedas emitidas por el estado. Desde el 2011, hasta 2013, los desarrolladores

ya no tenían otra opción y tenían que usar los créditos de Facebook si querían cobrar a los usuarios.

En términos de capacidad de adquisición, los usuarios pueden comprar créditos de Facebook utilizando monedas emitidas por el estado. El precio era de unos 10, créditos de Facebook por dólar estadounidense, con una cantidad de descuentos por cantidad; por ejemplo, por $ 10 hubo un 5 por ciento de bonificación y uno recibió 105 créditos de Facebook.

Los usuarios también pueden obtener créditos de Facebook, por ejemplo, probando un juego o realizando una

encuesta. Gans y Halaburda (2015) muestran cómo restringir la funcionalidad de la moneda de tal manera era óptimo para Facebook. La clave aquí es el hecho de que la principal fuente de ingresos de Facebook es la publicidad. Los ingresos por publicidad están directamente relacionados con el tiempo que los usuarios pasan en la plataforma. Los créditos de Facebook se diseñaron de manera óptima para inducir a los usuarios a pasar más tiempo en la plataforma.

Una importante fuerza motriz proviene del hecho de que el "consumo" de Facebook exhibe complementariedades

del consumo. Es decir, cuanto más tiempo pasen mis amigos en Facebook, escribiendo publicaciones y comentando mis fotos, más divertido será para mí pasar el tiempo en Facebook, publicando fotos y comentando sus publicaciones. Esto a su vez da lugar a efectos de red positivos: cuantas más personas están activas en Facebook, más utilidad se obtiene al pasar tiempo en Facebook. Como vimos, esta es una propiedad muy común para las compañías de Internet y una muy valiosa.

Si Facebook puede inducir a un usuario a pasar más tiempo en la plataforma, ese usuario tendrá un efecto multiplicador

debido a estas complementariedades de consumo, e inducirá a otras personas a pasar más tiempo y tal vez atraer nuevas personas para unirse a Facebook. Los créditos de Facebook se diseñaron para atraer a los usuarios a pasar más tiempo en la plataforma, brindándoles una forma de mejorar su experiencia en Facebook. Por ejemplo, con los créditos de Facebook, los usuarios pueden enviar flores virtuales a un amigo o pueden obtener opciones adicionales en un juego; por ejemplo, compre fertilizante para plantas virtuales para aumentar la cosecha en su granja virtual, obtener una mejor alimentación para su mascota virtual, etc.

Todas estas actividades hicieron que pasar tiempo en Facebook fuera más placentero y, por lo tanto, inducía a las personas a pasar más tiempo.

Al permitir la compra y la ganancia, Facebook se aseguró de que los créditos de Facebook fueran accesibles tanto para los usuarios que tenían más dinero que tiempo en sus manos (dinero en efectivo) como para aquellos que tenían más tiempo que dinero (tiempo rico).

A su vez, permitir transferencias entre usuarios o intercambiar créditos de Facebook por moneda emitida por el estado solo socavaría este objetivo. Permitir el intercambio de Créditos de Facebook por moneda emitida por el

estado permitiría a los usuarios vender los Créditos de Facebook ganados a Facebook.

Permitir las transferencias entre los usuarios podría dar lugar a una situación en la que los usuarios ricos en tiempo ganen y vendan créditos de Facebook a usuarios ricos en efectivo. Para asegurarse de que los usuarios ricos en efectivo prefieran comprarles sus créditos de Facebook en lugar de hacerlo directamente desde Facebook, los usuarios ricos en tiempo podrían cobrar un precio más bajo que la tarifa oficial de Facebook.

En consecuencia, los usuarios ricos en tiempo venderían créditos de Facebook

en lugar de usarlos para aumentar su propia actividad de Facebook. Si bien los usuarios a menudo pasan tiempo en Facebook cuando obtienen créditos de Facebook, la mayoría de los créditos que ganan presencia no contribuyen a los ingresos publicitarios. Además, si los usuarios ricos en tiempo no pasan más tiempo en las actividades de Facebook, este pierde el efecto multiplicador de atraer a otros usuarios para que pasen más tiempo. Por lo tanto, equipar los créditos de Facebook con transferibilidad sería menos beneficioso para Facebook ¿Por qué se cerraron los créditos de Facebook? curiosamente, los créditos de Facebook se eliminaron a finales de 2013. ¿Fue porque estaban

mal diseñados?

Desde la perspectiva de Facebook, no necesariamente. Ciertamente, en su introducción, los usuarios se quejaron del nivel agregado de complejidad. Muchas de las aplicaciones de Facebook ya tenían sus propias monedas. Por ejemplo, Zynga, un gran desarrollador de juegos, tenía zCoin, como su moneda interna que podía usarse en los juegos de Zynga. Después de que los Créditos de Facebook se volvieran obligatorios para que las aplicaciones los usaran, los usuarios necesitaban intercambiar sus dólares por Créditos de Facebook y luego intercambiar Créditos de Facebook por

zCoins o FarmVille Dollars.

Facebook intentó presionar a los desarrolladores de aplicaciones para que utilizaran los Créditos de Facebook como moneda de la aplicación, pero solo tuvieron un éxito muy limitado. Los desarrolladores de aplicaciones como Zynga preferían sus propias monedas, porque esto bloqueaba a los usuarios a su aplicación particular. Los créditos de Facebook, a la inversa, podrían moverse entre aplicaciones. Muchas de estas aplicaciones eran juegos que, como vimos anteriormente, se preocupaban mucho por la lealtad del consumidor. En otras palabras, al requerir que todas las aplicaciones usen los Créditos de

Facebook, Facebook hizo que el cambio de consumidor entre aplicaciones de Facebook sea más fácil. De esta manera Facebook creó una mayor competencia para sus desarrolladores de aplicaciones.

Más competencia entre los desarrolladores de aplicaciones podría haber sido algo bueno para los miembros de Facebook. Con menores costos de cambio, esto podría haber alentado a los usuarios a consumir más contenido en Facebook, lo que a su vez habría dado lugar a más ingresos por publicidad, y así sucesivamente.

Sin embargo, este argumento no tiene en cuenta que Facebook es una plataforma

de múltiples lados. Para crear un ecosistema saludable de aplicaciones, debe proporcionar incentivos suficientes para que los desarrolladores de aplicaciones inviertan en contenido de calidad. Si los desarrolladores de aplicaciones pueden capturar muy poco excedente, pueden buscar ingresos en otros lugares, dejando a Facebook y, en general, aportando menos contenido a la plataforma. Zynga por ejemplo, ha sido uno de los mayores desarrolladores de juegos de Facebook y durante mucho tiempo fue la mayor fuente de ingresos de Facebook. Sin embargo, Zynga y la mayoría de los otros desarrolladores de juegos tenían sus propias plataformas que operaban fuera de Facebook.

Curiosamente, el mismo razonamiento que hizo a los créditos de Facebook beneficiosos para Facebook, evitó que los desarrolladores de aplicaciones cambiaran sus propias monedas a los Créditos de Facebook.

La moneda Q de Tencent

Tencent es una red social china. Si bien cumple una función similar a la de Facebook en Occidente, Tencent se diferencia de Facebook de muchas maneras. Hasta 2014, sus ingresos provenían principalmente de las ventas de productos digitales que las personas utilizan para construir avatares, decorar sus páginas, jugar juegos o dar regalos digitales entre sí. En comparación con

las redes sociales occidentales, Tencent se basa menos en la publicidad. Tencent también tiene su propia moneda, llamada Q-coin. Sin embargo, a diferencia de los créditos de Facebook, desde el principio, los miembros de Tencent han usado Q-coins fuera de la plataforma. Si bien esta no era una característica prevista, Tencent no había tomado medidas contra dicho uso hasta que los reguladores estatales lo solicitaron.

Aunque es una red social, en muchos aspectos Tencent se parece a un juego freemium, donde los jugadores pueden participar de forma gratuita, pero pueden comprar una mejor experiencia si gastan dinero en la plataforma.

Cuando los usuarios abren un perfil, comienzan a ganar monedas Q en proporción a sus actividades. Estas monedas Q son proporcionadas por la propia plataforma. Los usuarios también obtienen un estado que está vinculado a su "influencia" lo que depende de la apariencia de su página, actividades y conexión. Los usuarios también pueden comprar Q-coins con moneda emitida por el estado, esencialmente el estado de compra, que es nuevamente similar a los juegos freemium. Si bien es solo una pequeña proporción de los miembros que compran monedas Q, esos miembros son responsables de la gran mayoría de los ingresos de Tencent.

Las monedas Q se pueden usar para jugar una gran variedad de juegos en la plataforma. De hecho, Tencent es una de las plataformas de juegos más grandes del mundo y desarrolla muchos juegos originales.

La moneda Q de Tencent se introdujo a principios de la década de 2000. Como se mencionó anteriormente, las monedas Q se pueden ganar o comprar. En teoría, las monedas Q están vinculadas a la cuenta de cada usuario y no se pueden transferir directamente. No obstante, hay formas de transferirlos dentro de la plataforma con relativa facilidad. Además, las monedas Q no pueden, oficialmente, ser devueltas por la

moneda emitida por el estado.

A los pocos años de su introducción, Q-coin obtuvo una importante tracción fuera de la propia plataforma de Tencent.

Originalmente solo para compras de bienes y servicios virtuales, Q-coins se hizo popular para pagos de igual a igual. Inicialmente, la gente usaba monedas Q entre amigos cercanos para transacciones simples, por ejemplo, dividir una factura en un restaurante o enviar regalos en efectivo, una costumbre china popular. Poco a poco, los comerciantes en línea comenzaron a aceptar Q-coins como pago. Algunos comerciantes de ladrillo y mortero

también lo siguieron. Se informó que podría comprar comestibles u obtener un corte de cabello y pagar con Q-coins utilizando su cuenta de Tencent.

El banco central chino, el Banco Popular de China, comenzó a expresar sus preocupaciones sobre el impacto de Q-coin en el yuan en 2006, y esas preocupaciones se hicieron más fuertes a medida que aumentaba el valor del comercio con monedas Q. Los gerentes de Tencent señalaron las restricciones en la funcionalidad de la moneda como importantes factores mitigantes. En febrero de 2007, el Shanghai Daily informó que Song Yang, un asistente del gerente de relaciones públicas en

Tencent, dijo: "El hecho de que las monedas Q no se puedan cambiar oficialmente de nuevo en dinero las hace menos perjudiciales para el mercado financiero".

Sin embargo, como mencionamos anteriormente, la funcionalidad completa no es necesaria para que una moneda digital tenga un impacto fuera de la plataforma prevista. En cambio, una condición necesaria, aunque no suficiente, es la transferibilidad. Con la transferibilidad, los usuarios pueden canjear indirectamente las Q-coins al transferirlas entre sí dentro de la plataforma e intercambiar moneda emitida por el estado fuera de la

plataforma. Como vimos, este fue el caso de los mercados negros para el oro de WoW. Además, si las monedas Q son canjeables por bienes y servicios, puede que no haya necesidad de cambiarlas por la moneda emitida por el estado. De hecho, el comercio con monedas Q continuó aumentando y, según informes, alcanzó varios miles de millones de renminbi en 2008. Al año siguiente, el gobierno chino introdujo un reglamento que prohíbe el intercambio de una moneda digital por bienes y servicios reales, con el fin de "limitar su posible impacto en el sistema financiero real". Sin embargo, hoy en día todavía hay un mercado secundario para las monedas Q donde las personas las venden por

dinero emitido por el estado. En la redacción de este libro, en Taobao, una plataforma comercial, vimos a un vendedor que ofrecía 50 monedas Q por 47.44 renminbi, mientras que la "tasa oficial" es de 1 a 1. Si uno busca el término "comprar moneda Q" Aparecen más de setecientos mil resultados; en otras palabras, el mercado todavía parece bastante animado. Si bien estas transacciones pueden no ser tan importantes hoy en día, hubo un momento en que las Q-coins llenaron un vacío, actuando como un sistema de pago fácil de usar, que esencialmente reemplazó a las tarjetas de crédito. En el momento en que la mayoría de los

chinos no tenían tarjetas de crédito, los sitios de comercio electrónico que aceptaban monedas Q hacían que el comercio fuera un poco más fácil.

Con el predominio de las plataformas móviles, el negocio de Tencent desarrolló dos vías para la presencia móvil. Por un lado, Tencent ha introducido una aplicación móvil con una versión de la conocida plataforma en línea, optimizada para teléfonos inteligentes. En paralelo, Tencent también introdujo una Red social completamente nueva construida desde cero: WeChat.

WeChat ha evolucionado para convertirse en una de las redes sociales

más exitosas de la actualidad. Curiosamente, las monedas Q no se promocionan en WeChat. De hecho, ni siquiera son utilizables allí.

WeChat usa moneda emitida por el estado y funciona de manera similar a PayPal. Parece que la compañía quiere que WeChat sea un sitio de comercio electrónico completo donde los comerciantes pueden tener una página y pueden promocionar y vender directamente sus productos, de manera similar a Amazon o Alibaba.

3.2.4. Plataformas de promoción y monedas de Amazon

Las plataformas de promoción son plataformas especializadas de dos caras

que reúnen a compradores y vendedores. El rol de la plataforma es facilitar las transacciones entre estos grupos de clientes sin involucrarse realmente. Las plataformas de promoción están en algún lugar entre las tiendas tradicionales y los mercados de pleno derecho, como la Bolsa de Nueva York o la plataforma de comercio electrónico de Amazon. Estos últimos brindan oportunidades comerciales para un amplio y diverso conjunto de acciones o productos. En contraste, las plataformas de promoción son mercadas con productos que están estrechamente vinculados. Las plataformas de juegos, como Valve's Steam, albergan una multitud de juegos en su mayoría similares.

Estas plataformas a menudo ofrecen una moneda de propiedad a sus usuarios. Uno podría pensar en estos servicios de divisas como billeteras virtuales. La moneda virtual se puede comprar con la moneda emitida por el estado, pero por lo general no se puede cambiar de nuevo a la moneda emitida por el estado. Por lo general, no es transferible, aunque uno puede comprar regalos para otro usuario. En casi todos los casos, este sistema relativamente cerrado sirve a alguna forma de actividad de promoción.

Para ver esto, consideremos un ejemplo particular: Amazon Coins. Los clientes obtienen monedas de Amazon cuando

compran La tableta Kindle Fire de Amazon. De lo contrario, los clientes solo pueden obtener Amazon Coins comprando. Las monedas de Amazon no pueden ser ganadas o transferidas entre clientes.

Esta última característica a veces puede crear problemas cuando, por ejemplo, Kindle Fire se compra como un regalo. Las monedas de Amazon que vienen con la tableta no se pueden transferir posteriormente al destinatario del regalo. Los clientes tampoco pueden cambiar las monedas de Amazon por la moneda emitida por el estado. Finalmente, las monedas de Amazon solo se pueden gastar en una selección

muy limitada de productos. A menudo se dice que Amazon es el minorista con la mayor selección en la Tierra, pero las monedas de Amazon solo se pueden gastar en aplicaciones seleccionadas en Kindle Fire. Para calificar, las aplicaciones deben aprovechar las propiedades únicas de Kindle Fire (a diferencia de otras tabletas que funcionan con Android, por ejemplo).

Esas propiedades son demasiado restrictivas para que Amazon Coins gane terreno como una moneda ampliamente aceptada. ¿Por qué Amazon no aprovecharía su gran base de clientes y selección de productos introduciendo una moneda internacional, en lugar de

restringirla tanto? La respuesta es que la moneda tiene un propósito promocional particular.

Amazon era un referente relativo al mercado de las tabletas.

El mercado de tabletas es otro mercado caracterizado por efectos de red. Sin embargo, este tipo de efecto de red es algo diferente del que ocurre entre los usuarios de Facebook. Es más similar al efecto de red entre los usuarios de Facebook y los desarrolladores de aplicaciones de Facebook.

A estos efectos de red los llamamos indirectos. Cuantas más aplicaciones estén disponibles para un tipo particular de tableta, más valiosa será la tableta

para los consumidores, al menos suponiendo que la calidad de las aplicaciones en la plataforma de la competencia no sea significativamente más alta para compensar el menor número de aplicaciones. A su vez, los desarrolladores desean desarrollar aplicaciones para cualquier tableta que tenga la mayor cantidad de consumidores. Ya que tendrán una base más grande a la que se podría vender la aplicación. Por lo tanto, más aplicaciones atraen a más consumidores, que atraen más aplicaciones, que atraen a más consumidores.

Entonces, de manera indirecta, cuanto más popular es la tableta, es decir,

cuanto más la compran los consumidores, más atractiva es esta tableta para el próximo consumidor, ya que ofrece más aplicaciones. Por eso los llamamos efectos de red indirectos.

Es fácil ver cómo esta dinámica "de gran tamaño crece" da lugar a resultados que el ganador se lleva todo. Los efectos de red indirectos hacen que sea muy difícil entrar en estos mercados. Por lo general, una entrada exitosa en un mercado con efectos de red implica subsidiar o "sobornar" a una de las partes o al grupo inicial de consumidores para obtener la masa crítica necesaria.

En el caso de Amazon, bajar demasiado

el precio de Kindle Fire afectaría los ingresos de Amazon de esta categoría. En cambio, Amazon quería aumentar el valor de la tableta Kindle Fire al tener más aplicaciones disponibles para los usuarios. Sin embargo, el hecho de tener más aplicaciones para Android haría que todas las tabletas basadas en Android sean más valiosas. Amazon necesitaba adquirir aplicaciones que serían específicas para Kindle Fire. Una forma sería simplemente pagar a los desarrolladores por desarrollar tales aplicaciones. Pero eso podría ser arriesgado. Si Amazon les pagara a los desarrolladores por adelantado, ¿cómo sabrían si los desarrolladores desarrollarían aplicaciones realmente

buenas que los consumidores valorarían? Una solución es darles dinero a los desarrolladores solo después de que los consumidores "voten", es decir, que compren sus aplicaciones. De esta manera, las aplicaciones específicas de Kindle Fire más valiosas ganan más dinero, lo que da a los desarrolladores incentivos para desarrollar mejores aplicaciones.

Los clientes que compraron la segunda generación de Kindle Fire por $ 199 obtuvieron $ 50 en monedas de Amazon. Puede parecer un reembolso, pero como las monedas solo se pueden gastar en las aplicaciones aprobadas, no es lo mismo que bajar el precio. Los clientes no

pueden gastarlo libremente. Podría contar como una rebaja solo para clientes que querían gastar $ 50 en aplicaciones Kindle Fire de todos modos, lo que probablemente no sea el caso para la mayoría de los clientes. Los desarrolladores saben que para esta plataforma en particular, los usuarios tienen $ 50 en sus manos que solo pueden gastar en las aplicaciones. Estarán más dispuestos a gastar las monedas de Amazon que el efectivo normal, por lo que será más probable que compren aplicaciones aprobadas.

Para que la aplicación se apruebe para los pagos de Amazon Coins, la aplicación debe demostrar que

aprovecha las características específicas de Kindle Fire y, por lo tanto, aumenta el valor de Kindle Fire más que el valor de otras tabletas Android. El solo hecho de obtener la aprobación de la aplicación no garantiza que sus desarrolladores obtendrán Amazon Coins. Estas aplicaciones están sujetas a calificaciones y revisiones al igual que otras aplicaciones. Por lo tanto, los consumidores elegirán comprar la más valiosa de las aplicaciones aprobadas. Las monedas de Amazon que los desarrolladores recolectan se pueden canjear de Amazon, después del corte típico del 30 por ciento. A pesar de que los desarrolladores pueden canjear monedas

de Amazon, la moneda aún no es canjeable para los clientes. Por lo tanto, Amazon le está dando los $50 no al cliente que compra Kindle Fire, sino a los desarrolladores que hacen que Kindle Fire sea más valioso.

Aliviar cualquiera de las restricciones estaría en desacuerdo con este objetivo. Permitir que los consumidores cambien las monedas de Amazon por una moneda emitida por el estado eliminaría el incentivo para los desarrolladores, porque la mayoría de las personas tomaría el dinero o gastaría las monedas en otros artículos en Amazon.com, que quisieran comprar. Aceptar las monedas de Amazon en otras áreas del negocio de

Amazon tendría el mismo efecto. No ayudaría a aumentar los efectos de red para Kindle Fire. ¿Y qué tal la transferibilidad? Si Amazon Coins pudiera ser transferido entre clientes, esto podría resultar en una distribución sesgada de Amazon Coins.

Esas pocas personas que usan una gran cantidad de aplicaciones Kindle Fire Obtienen monedas de personas que prefieren gastar esta moneda en otros productos. Esos usuarios de aplicaciones intensivas tendrían muchas monedas de Amazon, pero no comprarían varias copias de la misma aplicación. Esto daría como resultado un mayor número de aplicaciones

distintivas compradas con Amazon Coins, pero menos copias por aplicación. Las mejores aplicaciones podrían ver su cuota de mercado reduciéndose, mientras que otras no tan geniales serían compradas por los usuarios de la aplicación. Esto haría que todo el esquema sea menos atractivo para los desarrolladores de las mejores aplicaciones. Y, lo más importante, no proporcionaría incentivos tan fuertes para producir las mejores aplicaciones.

Por lo tanto, nuevamente, vemos que Amazon Coins es una moneda diseñada de manera óptima para el propósito que se supone debe servir.

Dólares de billetera

Las plataformas de videojuegos son otro tipo de plataforma de promoción. Estas plataformas ofrecen una colección de videojuegos que reúne a jugadores y desarrolladores de juegos. Para los jugadores, brindan un conveniente escaparate con capacidades de búsqueda y una billetera digital que puede ayudarlos a asignar sus recompensas y fondos a través de varios juegos.

Para los desarrolladores de juegos, brindan una plataforma de publicidad y promoción con una oportunidad para generar lealtad con sus clientes. Al igual que con Amazon Coins, tiene sentido

que la plataforma ofrezca una moneda que se pueda gastar en todos los juegos, manteniendo a las personas dentro del ecosistema de la plataforma de juegos. Si bien las personas pueden aburrirse con un juego en particular, la plataforma les brinda la oportunidad de gastar lo que tienen en otros juegos de la plataforma.

Steam es un ejemplo de tal plataforma. Originalmente, fue desarrollado por Valve, un desarrollador de juegos en línea, para proporcionar un sitio desde el cual los jugadores podían descargar las versiones actualizadas de los juegos lanzados anteriormente. Rápidamente quedó claro que el sitio también podría

servir como una plataforma de distribución para nuevos juegos. Una vez que los jugadores de Valve se convirtieron en visitantes regulares en Steam para sus actualizaciones y compras, la compañía se dio cuenta de que podía abrir la plataforma para que otros desarrolladores vendieran y actualizaran sus juegos.

Como primer motor, Steam se benefició de los efectos indirectos de la red: a los jugadores les gustaba Steam porque tenía la mayor variedad de juegos y, de manera similar, los desarrolladores de juegos se sintieron atraídos por Steam debido a la visita de todos los jugadores. A principios de la década de

2000, Steam se ha convertido en una de las principales plataformas de distribución en línea. Sin embargo, no importa cuán grande sea, tal plataforma de distribución no necesita una moneda virtual. ¿Qué llevó entonces a la introducción de Steam Wallet?

La respuesta es el contenido generado por el usuario en los juegos. En muchos juegos en línea, los usuarios pueden crear pequeñas modificaciones, equipos digitales o nuevas reglas dentro del juego que pueden compartirse con otros usuarios. Sims, por ejemplo, es uno de esos juegos que ganó mucha más popularidad cuando se hizo posible compartir. Desde una perspectiva

técnica, la plataforma Steam ya estaba bien adaptada para servir este intercambio entre usuarios. Sin embargo, podría mejorar aún más proporcionando un incentivo para el desarrollo de contenido generado por el usuario a través de la facilitación del comercio. En el camino, la plataforma puede generar ingresos adicionales. Steam presentó una billetera que los usuarios pueden cargar con sus tarjetas de crédito o tarjetas de regalo compradas en las tiendas de juegos. Los jugadores pueden buscar y adquirir una gran variedad de contenido generado por el usuario a través de los juegos disponibles en la plataforma. Las modificaciones populares se recompensan pagando a sus

creadores, es decir, acreditando su Steam Wallet. Steam mantiene una parte de la transacción como ingresos.

Los dólares de Steam Wallet no son canjeables por moneda emitida por el estado. Al igual que con las monedas de Amazon, deben gastarse dentro del ecosistema Steam. Como este ecosistema crece, Steam tiene un fuerte incentivo para mantener a sus miembros gastando dinero en la plataforma.

3.3. El futuro de las monedas basadas en plataforma

Los ejemplos anteriores ilustran cómo los diferentes atributos de las monedas inducen diferentes usos y comportamientos de los usuarios.

Por lo tanto, el conjunto óptimo de atributos depende del modelo de negocio de la plataforma.

Una característica de diseño general de las monedas basadas en la plataforma no es permitir el retiro. Esto está directamente relacionado con el esfuerzo de las plataformas para aumentar la lealtad y el bloqueo de sus miembros. Esto es particularmente importante para las empresas de plataforma porque existen fuertes externalidades de consumo que conducen a efectos de red. Un miembro que pasa tiempo en la plataforma hará que la plataforma sea más atractiva para los demás.

Esto explica en gran parte por qué la mayoría de las monedas basadas en plataformas no tienen opciones de retiro. Una excepción notable es la categoría de mundos virtuales. Como vimos, en este caso, proporcionar fuertes incentivos para que las personas inviertan en el contenido de la plataforma requiere la posibilidad de que los miembros recuperen su efectivo.

Los fuertes efectos de red también favorecen la idea de que los usuarios pueden comprar la moneda de la plataforma con la moneda emitida por el estado.

Nuevamente, esto solo puede aumentar la actividad total en la plataforma y, en

presencia de externalidades de consumo, puede hacer que la plataforma sea más atractiva para los usuarios existentes y nuevos. Este argumento tiene un límite en un caso particular: cuando alguna meritocracia específica de la plataforma es una parte clave de la propuesta de valor de la plataforma. Permitir la compra puede perturbar esta meritocracia y tener una externalidad negativa en los usuarios. De hecho, si algún tipo de meritocracia en el juego es importante para el funcionamiento de la plataforma. Entonces la plataforma debe abstenerse de permitir la compra para sus miembros. Esto fue más visible para el caso de los MMORPG, donde la habilidad era importante para que todos

los jugadores disfrutaran del juego, y uno podía fingir habilidades al comprar ciertos artículos. Además, como hemos visto, un sistema de doble moneda permite que la meritocracia coexista con éxito con el intercambio económico.

La transferibilidad es probablemente la característica de diseño más importante de una moneda y la más matizada. En la práctica, es la única característica que es necesaria, pero no suficiente, para que la moneda tenga un impacto fuera de la plataforma. La transferibilidad es necesaria si la plataforma necesita promover actividades económicas para su propuesta de valor, como es el caso de muchos de los modelos de negocios

interactivos. Sin embargo, una vez que se permite la transferibilidad, se abre una puerta trasera para que los usuarios compren y cobren, incluso si la política de la plataforma pretende evitar eso.

¿Las monedas restringidas son realmente monedas?

La mayoría de las monedas digitales basadas en plataformas están restringidas en al menos algunos de sus atributos. Algunos, como los créditos de Facebook y las monedas de Amazon, incluso tienen una capacidad de transferencia restringida, posiblemente el atributo más importante de una moneda. Uno puede preguntarse legítimamente si las monedas

restringidas son todavía dinero.

En el capítulo anterior, discutimos la definición económica del dinero y sus limitaciones. El dinero se define como (1) unidad de cuenta, (2) almacenamiento de valor y (3) medio de intercambio. Entonces, ¿son los créditos de Facebook, las monedas de Amazon o el dinero de oro de WoW? Algunos argumentan que no lo son. Ellos tienen su propia unidad de cuenta, incluso si están vinculados a una moneda emitida por el estado, pero son un depósito de valor pobre, y casi no se puede usar como un medio de intercambio ampliamente aceptado en las transacciones. Sin embargo, el oro de

WoW es definitivamente una moneda, es la moneda del mundo de World of Warcraft. No puedes usar dólares estadounidenses en World of Warcraft. El problema con los créditos de Facebook y las monedas de Amazon es más complicado. Su transferencia y, por lo tanto, su papel como medio de intercambio es limitada. Los créditos de Facebook solo pueden ser pagados a Facebook.

Pero, de nuevo, uno podría comprar artículos de Facebook solo con los Créditos de Facebook, por lo que el Crédito de Facebook es un medio de intercambio para tal transacción en particular. Al final del día, la moneda

debe facilitar el comercio. Se podría argumentar que WoW Gold o Amazon Coins solo se pueden utilizar para operaciones específicas. Pero, en cierto sentido, también lo hace el dólar estadounidense y la corona sueca. Una moneda puede facilitar el comercio en un área geográfica específica o solo para un tipo específico de comercio. Cuanto más limitado sea el comercio que puede facilitar, más limitada será la moneda. Tradicionalmente, las monedas muy limitadas no serían viables. Hoy en día, sin embargo, las posibilidades de diseño asociadas con las monedas digitales permiten la creación de monedas personalizadas que están optimizadas para su uso restringido.

¿Se convertirán las monedas basadas en plataforma a una moneda única?

Las monedas digitales basadas en plataforma se limitan principalmente al uso en una plataforma determinada. No hay ninguna razón para esperar la convergencia hacia una moneda en todas las plataformas, ya que los efectos de la red generalmente se limitan a una sola plataforma y rara vez hay efectos de red en las plataformas.

Además, usar la misma moneda para múltiples plataformas requiere un grado razonable de coordinación. Esto es posible cuando esas plataformas pertenecen a la misma familia, por ejemplo, diferentes juegos de Zynga, o si

se coordina el uso de la moneda, como en la plataforma Steam o como intenta Facebook con los créditos de Facebook. Sin embargo, en la mayoría en los casos, habrá una moneda distinta en cada plataforma que considere beneficioso tener una moneda privada. En algunos casos especiales, una plataforma puede tener más de una, como vimos con Guild Wars 2 o World of Warcraft después de la adopción del sistema dual. Esto solo puede suceder si cada una de esas monedas tiene un propósito diferente. En el caso de estos MMORPG, la multiplicidad proviene de la necesidad de separar la señalización de habilidades de la actividad económica en el juego.

Capítulo 4
Criptomonedas

Hasta ahora, en este libro, vimos monedas digitales emitidas por plataformas digitales. Estas innovaciones son un buen objeto para comenzar cuando se analiza la economía de las monedas digitales. Sin embargo, cuando la gente escucha "moneda digital" sus primeros pensamientos probablemente serán "criptomonedas" y "Bitcoin".

Esto no es sorprendente: en los últimos años, estos términos han aparecido con frecuencia en los medios de

comunicación populares, en discusiones técnicas e incluso en debates sobre políticas y legislación. Ahora pasamos a este segundo tipo de monedas digitales, especificamos las principales diferencias con las monedas digitales basadas en plataformas y discutimos qué implicaciones tienen tales diferencias.

Antes de hacer esto, sin embargo, no deberíamos discutir el desencadenante (o, si lo prefiere, el culpable) de la conmoción en los medios: el Bitcoin. Como veremos, Bitcoin es una moneda digital descentralizada inventada en 2008. Por alguien escondido detrás del seudónimo de Satoshi Nakamoto. Nakamoto propuso Bitcoin para abordar

un problema económico inherente al comercio electrónico: las fricciones y los altos costos de transacción de la negociación a través del Internet, especialmente relevante para transacciones de pequeño valor.

De hecho, si bien la innovación clave en el artículo de Nakamoto es la criptografía y la informática, quienes lo leen a menudo comentan cuánto espacio le dedica a la economía y una teoría del dinero del tipo que analizamos en los primeros capítulos de este libro.

En sus primeros años, Bitcoin ha sido conocido por una comunidad relativamente estrecha de entusiastas de la criptografía.

La primera vez que la moneda llegó a los medios de comunicación principales fue probablemente en junio de 2011, durante el caso WikiLeaks. WikiLeaks es un sitio web que publica información, especialmente filtraciones de noticias e información secreta de fuentes clasificadas. En 2010, WikiLeaks publicó una serie de documentos clasificados relacionados con la guerra en Afganistán, lo que atrajo la atención de los medios de comunicación principales al sitio y puso a WikiLeaks en desacuerdo con el gobierno de los Estados Unidos.

En diciembre de 2010, varios bancos y proveedores de servicios de pago (por

ejemplo, Bank of America, PayPal y Visa) se negaron a proporcionar sus servicios a WikiLeaks, lo que dificulta, si no imposible, que el sitio web reciba donaciones de sus partidarios. El fundador de WikiLeaks, Julian Assange, decidió en junio de 2011 comenzar a aceptar donaciones en Bitcoin, destacando la flexibilidad de la moneda, su anonimato y su independencia de los proveedores financieros tradicionales.

Bitcoin volvió a hacerse con los titulares, de una manera aún más espectacular, a fines de 2013, cuando parecía ser una oportunidad de inversión especulativa cada vez más interesante. Su precio (es decir, su tasa de cambio al

dólar estadounidense) se disparó desde menos de $ 15 a principios de 2013 a más de $ 1,200 a fines de noviembre de 2013. Al mismo tiempo, Bitcoin estaba ganando terreno en el comercio electrónico. Por ejemplo, Baidu, un motor de búsqueda chino y El quinto sitio más visitado del mundo, decidió en octubre de 2013 comenzar a aceptar Bitcoin para Jiasule, su servicio comercial para mejorar la seguridad y el rendimiento de los sitios web.

Al mismo tiempo, otra gran razón para la presencia de Bitcoin en los medios de comunicación fue su notoriedad. La moneda estaba en el centro de varios eventos y escándalos. El mayor de ellos

fue el asalto a la Ruta de la Seda por la Oficina Federal de Investigaciones (FBI). Silk Road era un sitio web que combinaba a compradores y vendedores de sustancias y servicios ilegales, por ejemplo, drogas. El FBI estimó que los ingresos de las operaciones en Silk Road durante los 2.5 años de operación del sitio fueron del orden de $ 1.2 mil millones. Bitcoin se convirtió en la moneda de elección para las partes en estas transacciones ilícitas, atrayéndolos con su percepción de anonimato y operaciones fuera del sistema legal. El 2 de octubre de 2013, la policía estadounidense cerró Silk Road y arrestó a Ross William Ulbricht, quien en 2015 fue declarado culpable de

dirigir el sitio.

En el proceso, el FBI incautó alrededor de 26,000 Bitcoin, luego de aproximadamente $ 3.5 millones.

Todos estos eventos atrajeron inevitablemente la atención de los reguladores y formuladores de políticas a Bitcoin. En los Estados Unidos, las audiencias del Senado se llevaron a cabo en Bitcoin del 18 al 19 de noviembre de 2013.

La moneda digital causó una impresión generalmente positiva, y aunque los responsables políticos hicieron hincapié en sus riesgos potenciales, no se recomendó una regulación inmediata. En algunos otros países, la reacción fue más

dura. El banco central de China, que probablemente aún recuerda el episodio de la moneda Q que describimos en el capítulo anterior, prohibió a las instituciones financieras manejar la moneda digital. En consecuencia, el sitio web de Baidu dejó de aceptar Bitcoin en diciembre.

Del mismo modo, las autoridades financieras de Vietnam hicieron que la moneda fuera totalmente ilegal en ese país, en presencia de estas y otras historias similares, Bitcoin llegó a las noticias principales. A pesar de que carecía de detalles, el público en general escuchó sobre este "Bitcoin": una moneda digital emergente, sin banco

central, que desafía las fronteras nacionales, que estaba ganando valor y popularidad. Bitcoin ha sido promocionado como una forma instantánea, anónima y gratuita de realizar transacciones. Se estaba empezando a percibir como una alternativa más rápida y económica al dinero existente, para ser utilizado en transacciones de igual a igual, transferencias internacionales, etc. Como veremos, al menos parte de este entusiasmo se perdió. Resulta que pagar con Bitcoin no es completamente anónimo, y no siempre es gratis o instantáneo. No obstante, Bitcoin es un ingenioso desarrollo en informática. Su principal contribución que va más allá

de su uso potencial como moneda es que resuelve el problema del doble gasto en una red descentralizada.

4.1. El problema del doble gasto

El problema del doble gasto fue el principal escollo; Durante mucho tiempo, se percibió como un obstáculo insuperable en el desarrollo de monedas digitales descentralizadas. Para ilustrar su naturaleza, comenzaremos con un simple experimento mental.

Supongamos que tiene una tecnología que le permitiría copiar dinero perfectamente, digamos una ingeniosa máquina fotocopiadora que podría

duplicar billetes rápidos y fácilmente.

En el Capítulo 2, mencionamos la falsificación del dinero tradicional; aquí estamos hablando de crear copias que serían absolutamente indistinguibles de los originales.

Si fuera la única persona con acceso a dicha tecnología, podría disfrutarla por un tiempo (notamos que su uso sería, por supuesto, ilegal, por lo que mantenemos Esta discusión se limita a un experimento de pensamiento. Si, por el contrario, esta tecnología de copia fuera generalizada, a nadie le importaría trabajar para ganar dinero. ¿Por qué molestarse con un trabajo si simplemente pudiera copiar el dinero

que necesita? Siempre que tenga una unidad de dinero, puede duplicar y triplicar su dinero y demás, simplemente copiándolo y multiplicando el original tanto como desee. Al mismo tiempo, nadie querría venderle nada a otra persona. ¿Por qué separarse de un objeto o un servicio si lo que recibe a cambio es algo que podría haberse replicado en primer lugar?

En otras palabras, el dinero dejaría de funcionar y la economía se paralizaría, a menos que hubiera una diferencia.

Todo esto nos lleva a la moneda digital. La moneda digital es esencialmente una cadena de ceros y unos, quizás codificada en una banda magnética, en

un chip, o almacenada en algún lugar de la nube. Independientemente de dónde se encuentre, esta pieza de datos se puede copiar inminentemente. Podemos reproducirlo exactamente, en tantas copias como deseemos, sin dañar el original. Si el dinero fuera simplemente impulsos electrónicos, parece que estaríamos peligrosamente cerca del experimento mental anterior.

Para que una moneda digital sirva de dinero, debe resolver este problema de doble gasto. Quizás la solución más fácil es mantener un libro mayor, una cuenta que incluya cada unidad de la moneda digital (quizás por su número de serie) y hacer un seguimiento de quién

posee esa unidad en un momento dado. Después de una transacción, el libro mayor se actualizaría cambiando la propiedad de la unidad monetaria del comprador al vendedor.

Mantener ese libro de contabilidad es una buena idea, pero aún no hemos resuelto el problema por completo. Después de todo, un libro de contabilidad en el mundo digital es solo un dato, y uno puede copiarlo tan fácilmente como antes. Por ejemplo, un comprador deshonesto puede copiar el libro mayor antes de una transacción. Si bien el libro de contabilidad se actualizaría en cualquier transacción, el comprador deshonesto intentaría volver

a su versión anterior que aún lo enumera como el propietario de una unidad de moneda que acaba de gastar. Entonces, parece que simplemente hemos reemplazado el problema de copiar la moneda digital con el problema de mantener la integridad del libro mayor.

Las cosas serían diferentes si pudiéramos designar un tercero de confianza que estaría a cargo del libro mayor. La moneda digital se centralizaría en el sentido de que la parte de confianza sería la única entidad con derecho a modificar el libro de contabilidad, y el tercero registraría todas las transacciones en el libro de contabilidad de manera diligente y

veraz. Todas las transacciones deberían ser informadas a esa parte de confianza, y los vendedores lo consultarían para verificar que un posible comprador tenga fondos suficientes para completar una transacción.

Las monedas digitales gestionadas de forma tan centralizada funcionarán y, de hecho, funcionarán. Esto es lo que hacen los bancos cuando mantienen nuestras cuentas de depósito o de tarjeta de crédito.

Todas las monedas basadas en plataformas que analizamos en el capítulo anterior también se organizan de esta manera. Ya sea que hablemos de Amazon Coins o de Facebook Créditos,

siempre hay una institución en segundo plano que realiza un seguimiento de todas las cuentas y que está lista para actualizar los registros cuando se produce una transacción. Esta institución tiene información sobre las participaciones de todos y sobre todas las transacciones que tienen lugar. Esto es muy diferente del anonimato de las transacciones en efectivo.

¿Es posible diseñar una moneda digital descentralizada?

¿Una que podría operar como dinero sin una entidad centralizada para realizar un seguimiento de las transacciones? Inicialmente, el consenso entre los informáticos fue que esto sería difícil o

tal vez simplemente imposible: de hecho, el problema del efectivo electrónico fue un desafío de larga data en la informática desde principios de los años ochenta. La solución a este enigma finalmente se propuso en 2008 en un artículo publicado por Satoshi Nakamoto, "Bitcoin: Un sistema de efectivo electrónico punto a punto".

El impacto del artículo de Nakamoto ha sido inmenso.

La solución que él (o ella, o ellos, no sabemos quién está detrás del seudónimo) propuesta, conocido como el protocolo de Bitcoin, fue la primera solución que funcionó bien al problema de la moneda digital descentralizada.

Más precisamente, fue la primera solución descentralizada completamente funcional para el problema del doble gasto discutido anteriormente. Como tal, es una contribución importante a la criptografía y a la informática en general. Además, como veremos más adelante en este capítulo, se han propuesto varios cientos de monedas digitales descentralizadas. Si bien difieren en una serie de dimensiones, muchos de ellos comparten la confianza en la misma tecnología general que Bitcoin. Todas estas monedas, incluida Bitcoin, se denominan comúnmente criptomonedas, para reflejar la idea de que la solidez del sistema depende solo del algoritmo y las herramientas

criptográficas que utiliza.

4.2. Como hace Bitcoin

¿Trabajo? Breve descripción

Limitaremos nuestra discusión de cómo funciona Bitcoin a una visión general de alto nivel que evita algunas de las complejidades técnicas y la innovación informática por la cual el Bitcoin es justamente famoso. Nuestra intención no es dar una descripción detallada del funcionamiento interno de Bitcoin, sino más bien para ilustrar el mecanismo y, especialmente, los incentivos que el mecanismo proporciona para que el sistema funcione.

Intentaremos ser técnicos solo en la

medida en que contribuya. A una mejor apreciación de las fuerzas económicas que afectan a la moneda.

Lo más importante, como señalamos anteriormente, todas las transacciones que involucran Bitcoin se escriben en un libro público. Ese libro mayor está disponible para cualquier persona y es transparente: en cualquier momento, puede rastrear la ruta de todas las transacciones en las que ha estado involucrado un Bitcoin determinado (o parte de un Bitcoin). Al mismo tiempo, se identifican las partes en las transacciones. No por nombre sino por una cadena de letras y números. La contabilidad general es actualizada por

la comunidad de Bitcoin: es el "público" el que escribe las transacciones en el libro mayor y con eso se valida. Esta comunidad se conoce comúnmente como la red Bitcoin, o sistema Bitcoin, con el capital "B".

El "Bitcoin" en minúscula se utiliza para las unidades monetarias, también abreviadas BTC. La convención de ortografía, sin embargo, a veces es diferente para otras criptomonedas.

Cuando se realiza una transacción, el libro mayor se anexa con la información sobre el número de monedas movidas y la dirección de Bitcoin a la que se mueven. La dirección es una cadena de 26 a 35 caracteres alfanuméricos y está

destinada a ser compartida. Esta es la razón por la que a menudo se la conoce como dirección de Bitcoin "pública". Cuando una persona quiere pagar con Bitcoin, la transacción se transmite a la red, junto con una firma, basada en la clave privada del remitente y la dirección del receptor. La clave privada también es una cadena de caracteres alfanuméricos de longitud variable. Debido a que está matemáticamente relacionado con la dirección a la que se envió el Bitcoin por última vez, esto prueba que el remitente tiene el derecho de gastar este Bitcoin. Todo esto significa que la transacción propuesta tiene información incrustada sobre transacciones pasadas. Dado que la

clave del remitente es lo único que se necesita para crear una firma válida, además de la dirección del destinatario, se recomienda a los propietarios de Bitcoin que mantengan su clave privada secreto. De lo contrario, cualquiera que conozca la clave privada puede enviar los Bitcoin relacionados con la clave a la dirección que controla. Este sistema se denomina criptografía de clave pública y se aplica comúnmente en muchos sistemas de Internet, como contraseñas de correo electrónico o de inicio de sesión.

El procedimiento de transmisión de transacciones es en realidad bastante similar a lo que ocurre en una red

centralizada, por ejemplo, cuando uno paga con monedas Q o monedas Amazon o paga desde una cuenta bancaria. También debe demostrar que tiene derecho a gastar una moneda determinada, aunque lo haga de una manera diferente. Cuando se trata de monedas basadas en plataforma o de un banco, se identifica al iniciar sesión en la plataforma, que realiza un seguimiento de todas las tenencias de moneda digital en su cuenta. Cuando realiza transacciones con alguien, la plataforma verifica que los fondos estén efectivamente disponibles en la cuenta y ajusta el saldo de su cuenta y la cuenta con la que está realizando transacciones. También emite una confirmación de que

los fondos fueron transferidos.

La innovación clave en Bitcoin es que un tercero tan confiable ya no es necesario. En primer lugar, el libro de contabilidad está disponible públicamente en la forma llamada blockchain. El blockchain es simplemente el registro de todas las transacciones de Bitcoin que se hayan completado. Eso incluye los registros de la acuñación de nuevos Bitcoin y la parte a la que se asignó este bit recién emitido de la moneda. Cuando esa persona gasta sus Bitcoin, la nueva transacción se envía a la red de Bitcoin para que se agregue al final de la cadena de bloques, lo que permite a todos

rastrear el movimiento de Bitcoin de una dirección a otra.

Es importante destacar que el envío de esta información aún no concluye la transacción. En un sentido muy directo, el trabajo duro solo comienza en esa etapa. Las nuevas transacciones se recopilan en un bloque que debe agregarse a la cadena de bloques Las transacciones se verifican al verificar en la cadena de bloques que los Bitcoin son enviados por alguien que los recibió antes y que no se han gastado antes. Esta verificación es computacionalmente fácil. Sin embargo, para que se reconozca la adición a la cadena de bloques, un participante de la red

Bitcoin debe completar la prueba de trabajo, que consiste en resolver un rompecabezas complicado y muy computacionalmente intenso publicado por el sistema.

Los participantes de la red que se acercan a este desafío se denominan mineros. El rompecabezas se resuelve mediante la fuerza de cálculo bruta, es decir, por prueba y error. Por lo tanto, cuanto más poder de cómputo tenga, más rápido podrá proponer y verificar posibles respuestas y más rápido esperará encontrar una solución.

El rompecabezas es un rompecabezas de una sola vía, basado en un algoritmo de función de hash. "De un solo sentido"

significa que, si bien es difícil encontrar una solución válida al problema, es fácil y rápida de verificar por otros en la red de Bitcoin.

La función principal de la prueba de trabajo es garantizar la inmovilidad del libro mayor. La solución al rompecabezas se convierte en parte del bloque que se agrega a la cadena de bloques. Es importante destacar que la solución depende de los bloques que la preceden en la cadena de bloques. Supongamos que desea volver y cambiar una transacción, por ejemplo, reemplazar el recibo de los Bitcoin que se envían con usted. Esto cambiaría uno de los bloques anteriores, lo que

significa que necesitaría rehacer la prueba de trabajo de ese bloque para que sea una adición válida a la cadena de bloques.

Aún más importante, también necesitaría rehacer la prueba de trabajo para todos los bloques que la siguen. Necesitaría el 51 por ciento del poder de cómputo de toda la red para superar a otros mineros con el fin de poner con éxito bloques fraudulentos en la cadena de bloques. Ganar tal potencia computacional es muy costoso, como lo fue la intención en el diseño de la red Bitcoin. La prueba de trabajo también formaliza los incentivos para que los mineros participen en la red de Bitcoin,

mantengan sus máquinas en funcionamiento y ayuden a garantizar que se procesen nuevas transacciones. La participación es costosa, y el sistema debe prometer una recompensa, o al menos una posibilidad de recompensa, para que la gente haga eso. La prueba de trabajo es una forma de formalizar esa promesa.

El primer minero en llegar a una solución válida consigue adjuntar el bloque a la cadena de bloques y recibe un lote de Bitcoin recién acuñados como recompensa. La cadena de bloques adjunta se envía al resto de la red de Bitcoin. Todos los mineros que también trabajan en esta transacción (más

precisamente, en un bloque de transacciones, incluido el actual) pierden la carrera, aceptan el bloque y necesitan pasar a otras transacciones. El rompecabezas depende tanto del bloque de transacciones que se agrega como de la cadena de bloques en general, por lo que cualquier minero que trabaje en transacciones diferentes y use una versión anterior de la cadena de bloques también debe reiniciar su trabajo.

Esto crea una estructura de torneo para los mineros. Compiten entre sí (a veces, los mineros individuales combinan su poder de cómputo para competir como grupo de minería), y la recompensa que ganan es todo o nada: o son los primeros

en resolver el rompecabezas y obtener la recompensa o su inversión en él se pierde. Inicialmente, los Bitcoin se extraían en computadoras normales. Pero hoy en día, la inversión en resolver el rompecabezas no es intrascendente.

Convertirse en un minero significativo en la red de Bitcoin requiere una inversión fija en el hardware, por ejemplo, máquinas de circuitos integrados de aplicaciones específicas (ASIC) diseñadas para enfocarse en resolver un problema particular, en este caso, un rompecabezas de Bitcoin. También requiere tiempo durante el cual esa potencia de computación podría gastarse en otra cosa, y cantidades

considerables de electricidad. Ese último elemento Es lo suficientemente importante como para que los mineros serios se ubiquen en lugares donde el costo de la electricidad y el enfriamiento de sus máquinas sea de bajo costo, por ejemplo, en Islandia.

El algoritmo de Bitcoin permite agregar un bloque a la cadena de bloques cada 10 minutos aproximadamente. Este ritmo se asegura ajustando automáticamente la dificultad del "Puzzle" para que la red tarde unos 10 minutos en resolverlo. Y así, cada 10 minutos, un minero obtiene nuevas monedas. El número de monedas otorgadas para agregar un bloque, inicialmente establecido en 50 Bitcoin,

se reduce a la mitad cada 210,000

Bloques, por lo que aproximadamente cada 4 años. Desde el 28 de noviembre de 2013, agregar un nuevo bloque recompensa a 25 Bitcoin. Eventualmente, este proceso de reducción a la mitad resultará en un solo Satoshi (0.00000001 de Bitcoin) como recompensa del minero, y después de cuatro años, aproximadamente en 2140, no habrá recompensa.

Para entonces, la cantidad total de todos los Bitcoin acuñados se fijará en poco menos de 21 millones. Esta decisión de diseño fue motivada por el deseo de asegurar la escasez de Bitcoin, de una manera que los haga similares al oro.

Pero, como veremos más adelante, esto puede tener consecuencias deflacionarias para la economía de Bitcoin.

Una vez que Bitcoin alcance su suministro fijo, no habrá nuevos Bitcoin para proporcionar el incentivo para participar.

En su lugar, los mineros serán compensados con las tarifas pagadas por las partes en cada transacción. Curiosamente, el algoritmo de Bitcoin permite tarifas incluso hoy, y muchas transacciones ya involucran dichas tarifas. Las tarifas son voluntariamente agregadas por el remitente de Bitcoin. La tarifa la cobra el minero que agrega

esta transacción en particular a la cadena de bloques.

Por lo tanto, agregar tarifas aumenta la probabilidad de que la transacción se verifique y se agregue a la cadena de bloques antes, ya que los mineros prestan atención para incluir transacciones de pago en sus bloques. En la actualidad, las tarifas son relativamente pequeñas (del orden de 0.0001 de Bitcoin), con las principales recompensa para la minería siendo los Bitcoin recién emitidos. Uno podría imaginar que en el futuro dichas tarifas serán fijadas por fuerzas competitivas: el suministro del poder de cómputo por parte de los mineros y la demanda de

verificación de transacción por parte de los compradores y vendedores de Bitcoin.

La innovación técnica clave, la ausencia de un tercero de confianza centralizado, hace que Bitcoin sea muy diferente de las monedas basadas en plataformas y tiene implicaciones importantes para la economía de la moneda. Al mismo tiempo, Bitcoin es, en muchas dimensiones, más similar a las monedas digitales centralizadas de lo que la mayoría de la gente espera.

Por ejemplo, a menudo se piensa que Bitcoin es el equivalente digital de efectivo: anónimo y casi imposible de rastrear una vez gastado. Esto es, en el

mejor de los casos, una simplificación. El blockchain es un registro exacto de la ruta de todas las direcciones a las que se envió un Bitcoin, lo que significa que Bitcoin se describe más correctamente como una moneda "seudónima" que como una moneda “anónima”. Además, el registro de todas las transacciones anteriores se almacena en el libro mayor abiertamente y es transparente para todos los usuarios de Bitcoin. En la práctica, pocos usuarios serían lo suficientemente determinados, o tendrían recursos suficientes, para poder rastrear las transacciones y las tenencias de Bitcoin directamente a las personas de la vida real involucradas. Esto hace que la moneda sea lo suficientemente opaca

y lo suficientemente anónima para algunos propósitos nefarios. No obstante, las instituciones con amplios recursos pueden seguir el movimiento de los Bitcoin lo suficientemente cerca como para poder identificar la identidad de la vida real de los usuarios de la moneda. Por ejemplo, cuando el FBI investigó el sitio web de Silk Road descrito anteriormente, pudieron identificar a la persona responsable del sitio web y rastrear los fondos que ingresan a su cuenta.

Del mismo modo, a veces se cree que un Bitcoin es fácil de perder. Sin embargo, esto es al menos conceptualmente similar a las monedas centralizadas o

basadas en plataforma. Puedes perder sus Bitcoin si pierde su clave privada, el dato que lo identifica como la parte propietaria de los Bitcoin.

Esto es similar a perder su contraseña a un sitio web que le emitió una moneda basada en plataforma. Es posible que pueda recuperar su acceso y sus existencias si puede demostrar a la plataforma que usted es quien dice ser, tal vez respondiendo una pregunta secreta o comprobando que tiene acceso a la cuenta de correo electrónico asociada con esta cuenta.

Si no puede demostrar quién es, no podrá recuperar sus existencias y se perderán para usted. En la red de

Bitcoin, la única manera de identificarse es proporcionando su clave privada.

Además, suponga que sus tenencias de Bitcoin son pirateadas (quizás porque usó una billetera electrónica, una pieza de software responsable de administrar su Bitcoin, de una fuente dudosa). Si el hacker gasta tus Bitcoin, tienes pocas esperanzas de recuperarlos. En principio, podría tener problemas similares si alguien roba la contraseña de su cuenta en una plataforma de emisión de moneda digital. Esa persona tendría el poder de gastar la moneda, aunque el gasto podría limitarse a artículos menos atractivos para ellos, como las aplicaciones que solo se

pueden cargar en su propia cuenta. Una diferencia específica de las plataformas basadas en la plataforma y otras monedas centralizadas es que el emisor, en principio, puede estar listo para revertir transacciones fraudulentas o fraudulentas y deshacer el daño que el ataque pudo haber causado.

Finalmente, las personas a menudo afirman que Bitcoin es una forma sin costo para realizar transacciones. Esta es una percepción errónea. Como vimos, muchas transacciones aún hoy involucran tarifas, aunque actualmente son muy pequeñas.

Además, el costo de la minería el equipo y la electricidad son muy

grandes. Este costo se difunde actualmente en toda la red Bitcoin y por lo tanto, puede parecer invisible para muchos participantes. Podría decirse que esto es similar a una moneda digital basada en plataforma que parece libre de usar, a pesar de que es costoso para la plataforma mantener la infraestructura necesaria para hacerlo.

4.3. Predecesores de Bitcoin

Nuestra descripción de cómo funciona Bitcoin se simplifica intencionalmente, por lo que podemos enfocarnos en las fuerzas económicas y la competencia más adelante en este capítulo. Pero incluso a partir de esta descripción simplificada, se puede ver que es muy

exigente construir un sistema de moneda descentralizado que resuelva el problema del doble gasto. De hecho, tomó muchos intentos para hacerlo. Bitcoin no fue la primera moneda digital descentralizada. Sin embargo, fue el primero que funcionó lo suficientemente bien como para obtener cierta aceptación por parte del público en general. Y en su sistema, Bitcoin incorporó muchas de las soluciones anteriores. La comunidad de criptografía estaba interesada en desarrollar un sistema de moneda descentralizado desde el surgimiento de Internet.

La primera pieza de tecnología similar a Bitcoin fue el hashcash, un sistema

basado en la prueba de trabajo presentado en 1997 por Adam Beck. El propósito de Beck era prevenir el spam de correo electrónico al exigir que la computadora del remitente realice un trabajo informático antes de enviar el correo electrónico. Dicho trabajo sería relativamente trivial para un correo electrónico individual y no afectaría el rendimiento del equipo. Sin embargo, haría que el envío de miles o millones de correos electrónicos sea prohibitivamente costoso en términos de poder de cómputo, lo que hace que el envío de correos electrónicos masivos no rentables sea económico.

El ingenio del hashcash es que logró

este objetivo sin cobrar dinero por los correos electrónicos. Como vimos, Satoshi Nakamoto incorporó este elemento en Bitcoin para que sea costoso crear una cadena de bloques falsa En 1998, Wei Dai diseñó una moneda digital descentralizada, llamada b-moneyy, que permitiría transacciones anónimas entre pares. Las transacciones serían registradas por los miembros de la red en un libro mayor.

Cada participante tendría una copia del libro mayor. Para combatir la mala conducta, por ejemplo, para evitar que los participantes registren transacciones que no ocurrieron, los nodos del sistema tenían que depositar dinero en un grupo

común. El dinero depositado se utilizó para multas por mala conducta y recompensas por prueba de mala conducta. Sin embargo, tal sistema de multas y recompensas es difícil de hacer cumplir sin una autoridad central para decidir y resolver desacuerdos.

En 2005, Nick Szabo propuso bit-gold, que también usaba la prueba de trabajo y un registro de títulos de propiedad distribuidos, similar al libro de contabilidad posterior de Bitcoin. El trabajo de resolver un rompecabezas unidireccional se usó para crear nuevas piezas de bit-gold, pero no hubo un control claro sobre la cantidad de bit-gold que se puede crear y con qué

rapidez. El propio Szabo expresó la preocupación de que una computadora poderosa podría "inundar el mercado con poco oro", reduciendo su valor porque el mercado se ajustará.

B-money y bit-gold fueron ideas, consideraciones teóricas, que nunca se implementaron realmente, lo que dificulta saber qué tan bien funcionarán. Nunca habían captado suficiente interés de personas ajenas al pequeño grupo de entusiastas de la criptografía.

B-money, bit-gold y, más tarde, Bitcoin fueron desarrollados por entusiastas para satisfacer la necesidad de anonimato en las transacciones digitales. También hubo esfuerzos comerciales

para crear sistemas anónimos de moneda digital. Similar a Bitcoin, estos sistemas comprendían unidades monetarias independientes, permitían una mayor divisibilidad e incluían un libro de contabilidad universal permanente. Sin embargo, Esos sistemas estaban centralizados. Dos de los ejemplos más conocidos son DigiCash y el efectivo electrónico de Citibank llamado Sistema Monetario Electrónico.

DigiCash

Fue una empresa comercial, creada en 1989. Por David Chaum, y propuso construir un sistema de efectivo electrónico anónimo para gobiernos y bancos.

El sistema DigiCash tenía un anonimato asimétrico: el pagador era anónimo, mientras que el beneficiario podía ser "identificado de manera irrefutable si fuera necesario". Esta característica fue motivada por el deseo de acabar con la corrupción y el crimen organizado.

La innovación del sistema era la capacidad de transportar información de forma inalámbrica, y por lo tanto, estaba bien adaptada para pagar los peajes, que se suponía que era su primer uso.

David Chaum incluso había firmado un contrato con el gobierno holandés para este propósito. La idea del sistema DigiCash también atrajo algo de atención más allá de la aplicación de

peaje. Hubo interés de los bancos (como Deutsche Bank y Credit Suisse), Visa y Microsoft. A fines de la década de 1990, sin embargo, todo se derrumbó, incluida la propia empresa. Durante algunos años, un banco en los Estados Unidos, The Mark Twain Bank de St. Louis, Missouri, estaba usando DigiCash. La iniciativa, sin embargo, terminó en 1997.

El segundo ejemplo de desarrollo comercial de una moneda digital descentralizada fue el efectivo electrónico de Citibank. En la década de 1990, Citibank estaba desarrollando un sistema de dinero electrónico interno. El dinero tenía la característica interesante

de que expiró después de un tiempo, y el titular necesitaba contactar al banco para reemplazarlo. Esta característica estaba destinada a prevenir el lavado de dinero. Se realizaron pruebas y programas piloto en 1997 y 2001. En 2001, la nueva administración de Citigroup cerró el proyecto.

Bitcoin tomó algunos elementos de estos sistemas anteriores y los combinó en una nueva innovación que tenía algunos elementos que habían sido comunes y esperados para entonces, por ejemplo, su naturaleza de igual a igual (cualquier persona con una computadora podría convertirse en parte de la red) o su uso del cifrado de clave pública con clave

privada. Su novedad e importancia provino de la combinación de la idea de una cadena de bloques (un libro de contabilidad público que sería prohibitivamente costoso forjar debido a la prueba de trabajo) y el sistema de incentivos monetarios para alentar a los nodos a mantener el libro de contabilidad actualizado. Estas dos características permiten a los usuarios mantener el sistema honesto mientras luchan contra los piratas informáticos.

4.4. Nuevos desafíos

Por todo su ingenio, Bitcoin no está exento de defectos. Ya hemos visto uno de ellos: el costo sustancial y en

aumento de la extracción de nuevos Bitcoin. La parte más obvia del costo es la electricidad. Además, uno necesita una inversión sustancial para ser competitivo en el negocio minero. Ya no es suficiente tener un grupo de computadoras, uno necesita plataformas de minería especializadas diseñadas para resolver el rompecabezas de prueba de trabajo de la manera más eficiente posible.

Vemos una carrera de armamentos en el negocio de la minería, donde los mineros invierten continuamente en nuevo hardware para crear una ventaja competitiva y empujar a sus competidores a hacer lo mismo.

Inicialmente, los Bitcoin se extraían con computadoras normales.

Finalmente, uno de los primeros mineros notó que se podía aprovechar la tarjeta gráfica para obtener una ventaja computacional en la minería. Esto dio lugar al diseño de dispositivos que serían cada vez más eficientes para resolver el rompecabezas de Bitcoin.

Esta carrera despiadada hacia una tecnología nueva y más poderosa surge debido a la estructura del torneo del algoritmo de Bitcoin. Desde el ganador del rompecabezas minero, toma toda la recompensa, incluso leves mejoras que ponen a un minero un poco por delante de todos los demás, dándole al minero

una gran recompensa esperada. En cualquier momento dado, la inversión incremental puede parecer pequeña y valer la pena, pero cuando en respuesta todos los demás también invierten y se ponen al día, la inversión total de la industria minera en general puede valer más que el valor que los mineros pueden ganar.

La carrera se acelera por una característica particular del sistema Bitcoin: la dificultad de los enigmas criptográficos se ajusta para mantener la expansión de la cadena de bloques a un ritmo constante de un bloque que se agrega cada 10 minutos.

La introducción de plataformas de

minería más potentes aumenta efectivamente la dificultad del rompecabezas. Como los mineros tienen más poder de cómputo a su disposición, resuelven cualquier rompecabezas en menos tiempo; para frenarlos, el rompecabezas debe hacerse más complejo al requerir que se realicen más operaciones criptográficas. Esto a su vez conduce a un mayor uso de la energía: aunque las nuevas plataformas de minería están diseñadas para funcionar de manera más eficiente, la ejecución de más cálculos generalmente requiere más electricidad.

Una consecuencia interesante de la estructura del torneo de Bitcoin es la

aparición de grupos mineros. Los grupos de minería son cooperativas de mineros que dividen las tareas de minería entre sí y comparten cualquier recompensa, normalmente proporcionalmente a la potencia de cálculo que aportan al grupo. Para los mineros individuales, el incentivo para entrar en la piscina es disminuir la incertidumbre de ir solo. Ganar el rompecabezas es rentable pero muy improbable para un minero individual. En cambio, participar en un grupo permite a los usuarios compartir el riesgo y esencialmente asegurarse entre sí.

El grupo gana con más frecuencia que cualquier individuo. Aunque, por

supuesto, trae una recompensa más baja al ganar, como los Bitcoin recién extraídos y las tarifas ganadas deben distribuirse por toda la piscina. Para muchos mineros, esta compensación es atractiva. Prefieren renunciar a la posibilidad de premios grandes pero poco frecuentes por la posibilidad de una acumulación constante de premios más pequeños.

En general, este tipo de minería conduce a tres grandes categorías de costos:

Primero, están los costos impulsados por el uso de energía por las máquinas mineras especializadas. En segundo lugar, el sistema induce una participación desigual en la red: los

mineros de élite, que invierten en plataformas de minería, pueden terminar controlando el libro de contabilidad mientras recolectan nuevos Bitcoin, lo que les permite adquirir maquinaria de minería actualizada. Tercero, y como consecuencia de lo anterior, podemos observar la sobreinversión en equipos de minería.

En el momento de redactar este documento, una consecuencia importante del aumento de los costos de la energía es la externalidad que impone al medio ambiente y a la economía en general. Esta externalidad se amplifica porque muchos de los cálculos subyacentes de Bitcoin terminan siendo en última

instancia inútiles. Debido a la estructura del torneo del ganador se lleva todo, solo los cálculos del minero que gana la carrera son importantes en el sentido de que su resultado se incorpora a el blockchain. Todos los demás mineros que trabajaban al mismo tiempo pierden la competencia, y todos los cálculos en los que estaban trabajando deben ser descartados, ya que el problema de hashing se resuelve esencialmente mediante prueba y error, esos cálculos no son útiles para los bloques subsiguientes que los mineros puedan estar trabajando desde este punto de vista, la energía gastada en los cálculos descartados es una pérdida para el sistema.

Sin embargo, hasta ahora los ingresos de Bitcoin extraídos compensan los costos de energía y hacen que la extracción sea económicamente viable para los mineros individuales, al menos aquellos que invirtieron en equipos de extracción de mayor calidad y eficiencia. Sin embargo esta situación eventualmente cambiará como describimos anteriormente, la velocidad a la que el algoritmo de Bitcoin genera nuevos Bitcoin está disminuyendo con el tiempo. Es poco probable que el precio de Bitcoin aumente al mismo ritmo, lo que significa que la recompensa por extraer nuevas monedas disminuirá gradualmente.

Eventualmente, los altos costos de la

energía se pondrán al día con la disminución de las ganancias. Es poco probable que esto solo apague el sistema, pero hará que las tarifas sean cruciales. En este momento, muchas transacciones de Bitcoin se realizan con tarifas mínimas (una pequeña fracción en una Bitcoin, opcional pero generalmente impuesta por las billeteras digitales que usa la gente) o incluso sin tarifas. Eventualmente, estas tarifas deberán incrementarse para compensar la caída en los nuevos Bitcoin creados y en los costos de energía, que probablemente no caigan a una tasa similar.

De los tres inconvenientes que

discutimos aquí, el aumento de los mineros de élite puede convertirse en un desafío aún más serio para Bitcoin debido a su potencial para conducir al "ataque del 51 por ciento". El sistema de Bitcoin mantiene la integridad de la cadena de bloques al confiar en un difuso Red de mineros que efectivamente se mantienen unos a otros honestos. Este sistema de controles distribuidos falla cuando un minero, o un grupo coordinado de mineros, obtienen el control de más de la mitad de la potencia de cómputo subyacente en la red. En tal caso, el súper-minero sería capaz de tomar el control del libro mayor, con poderes que van desde evitar que se agreguen nuevas transacciones a

la cadena de bloques hasta un gasto doble potencial.

La carrera de armamentos en la minería hace que sea más probable que aparezca un súper-minero. Primero, la carrera de armamentos obliga a los mineros menos eficientes, o mineros que no pueden costear mejoras a su plataforma de minería, a salir del sistema. Incluso si esos mineros permanecen en la red, tendrán una proporción relativamente menor del poder de cómputo total. Con Menos participantes de alta potencia, es más probable que uno de ellos domine la red. Las reservas mineras también aumentan la amenaza del ataque del 51 por ciento. Como explicamos

anteriormente, la carrera de armamentos ofrece incentivos a los mineros para que combinen sus recursos en grupos mineros. Dichos grupos combinan la potencia de cálculo de los mineros individuales, lo que facilita que el conjunto total supere el 50 por ciento del poder de cálculo de la red. Una de las principales innovaciones en Bitcoin fue la eliminación de la necesidad de un tercero de confianza que supervisara y gestionara la red. Un minero o un grupo minero que controla más de la mitad de la red se convertirá esencialmente en un tercero que domine la red. Irónicamente, ni siquiera estaría claro si tal entidad puede o no ser un Tercero "de confianza".

La amenaza de un ataque del 51 por ciento no es puramente académica.

A mediados de 2014, se informó de que Ghash.io, uno de los grupos de minería de Bitcoin más grandes, ha alcanzado brevemente el 50 por ciento de la potencia informática de la red Bitcoin en general.

No hubo daños en el sistema porque, como explicó la piscina, no hubo ninguna intención nefasta.

Otra debilidad de Bitcoin es la presión deflacionaria potencial incorporada en su algoritmo. Como vimos anteriormente, el suministro de Bitcoin, es decir, el número de Bitcoin en

existencia, está aumentando, pero lo está haciendo a un ritmo decreciente y, en algún momento, el suministro se fijará.

Esta característica fue incorporada conscientemente en el diseño, pero puede tener consecuencias no deseadas. La escasez puede traducirse en una presión a la baja sobre los precios denominados en Bitcoin: con menos monedas, los consumidores pueden no querer gastar demasiadas monedas en un bien determinado.

¿Por qué el suministro limitado de Bitcoin se traduce en precios decrecientes? Para explicar este fenómeno, podemos utilizar una teoría económica llamada "teoría cuantitativa

del dinero". La teoría vincula cuatro cantidades económicas: la oferta de dinero, M; la velocidad del dinero m, V (es decir, con qué rapidez V el dinero circula en la economía); los bienes y servicios que produce la economía, Y; y el precio de estos productos, p.

PAG

Estas cantidades están vinculadas a través de una identidad, MV

$V = PY$

Esa identidad es ampliamente aceptada entre los economistas (después de todo, es una identidad) y tiene una interpretación atractiva. El tamaño de la economía (piense en el PIB) se basa en la cantidad de bienes y servicios que se

comercializan (Y) y en sus precios (P). La suma total de estas transacciones P

Necesita ser apoyado por el dinero que circula en la economía. Si el dinero circula muy lentamente (baja velocidad V), necesita más para respaldar la economía. Por ejemplo, suponga que cada unidad de la moneda, por ejemplo, cada dólar por separado, solo puede usarse una vez al año (V = 1). Esto significa V que para soportar el PIB de $ 100 (el valor de todos los bienes y servicios igual a $ 100), necesitamos 100 dólares separados (o una combinación de billetes y monedas separados que suman hasta $ 100).

La identidad anterior nos ayuda a

comprender qué sucede cuando se producen más bienes en la economía; es decir, cuando Y aumenta. Si la oferta de dinero, M, es constante, M y si la velocidad del dinero, V, no cambia, hay V.

Una sola posibilidad: los precios deben bajar. Si no lo hicieran, no tendríamos suficiente dinero en la economía para respaldar todas las transacciones que subyacen a la producción total.

¿Qué predice esta teoría para Bitcoin? En primer lugar, tenga en cuenta que tan pronto como se fije el suministro de Bitcoin, el suministro de dinero, M, será constante, o incluso disminuirá, ya que algunos de los Bitcoin pueden perderse,

si sus propietarios pierden sus claves privadas. Si Bitcoin gana popularidad y más gente decida utilizarlo, habrá más productos ofrecidos y comprados en la economía de Bitcoin; es decir, Y aumentará.

La teoría cuantitativa del dinero nos dice que, en respuesta, el nivel de precios, P, debería disminuir proporcionalmente. En pocas palabras, no habrá suficientes Bitcoin para apoyar el aumento del gasto, y en respuesta, los precios deberán ajustarse.

Por supuesto, una caída en los precios no es inevitable. Puede ser que el cuarto término de nuestra ecuación, la velocidad del dinero, V, se ajuste en su

lugar. Si cada Bitcoin circula en la economía más rápido que antes, entonces el mismo suministro de Bitcoin podrá soportar un mayor volumen de gasto. Puede que no esté claro cómo exactamente puede aumentar la velocidad de Bitcoin, pero es una posibilidad teórica. Un resultado quizás menos atractivo sería un límite al crecimiento de la economía de Bitcoin.

Si el uso de Bitcoin se limita a un volumen relativamente estable de bienes y servicios (es decir, cuando Y sobre Y es fijo), entonces los precios pueden no cambiar aunque la oferta de dinero sea constante. De cualquier manera, la identidad anterior nos dice que algo

debe ceder: sería miope pensar que el tamaño de la economía de Bitcoin puede cambiar sin tener un impacto en el nivel de precios.

Si bien la caída de los precios puede parecer algo bueno, tienden a tener un efecto adverso en la economía. Por ejemplo, las personas que anticipan precios más bajos en el futuro pospondrán su consumo e inversiones, lo que reduce el tamaño actual de la economía.

Dado el razonamiento anterior, ¿por qué se decidió que el suministro total de Bitcoin sería constante? La razón más probable es que se incorpore un elemento de escasez en el diseño de la

criptomonedas para garantizar que no se pueda inflar. En el contexto de las monedas tradicionales, la inflación a menudo se desencadena por un aumento en la oferta de dinero. Sin embargo, la protección contra fallas integrada en Bitcoin funciona tan bien como para inclinar el balance en la dirección opuesta y errar en el lado de la deflación. Para compensar la tendencia deflacionaria, uno puede imaginar la introducción de un aumento gradual de la oferta monetaria en el algoritmo de Bitcoin. El problema se convierte entonces en obtener la tasa de aumento exactamente correcta, para garantizar que los precios se mantengan relativamente constantes. Es dudoso (en

el mejor de los casos, discutible) si existe una fórmula pre-especificada que pueda lograr este objetivo; en cambio, en la mayoría de los países, se dejan ajustes similares a los bancos centrales. A juzgar por la narrativa que acompaña a Bitcoin, al menos algunos de sus usuarios están dispuestos a aceptar la inestabilidad potencial de los precios a cambio de ser independientes de una institución como un banco central.

Para tales usuarios de Bitcoin, esta característica en el diseño de Bitcoin se percibe como positiva, y contribuiría a una mayor adopción de Bitcoin por parte de dichos usuarios.

4.5. Competencia contra Otras criptomonedas

Vimos que el algoritmo original de Bitcoin tiene algunas externalidades desagradables (por ejemplo, el alto consumo de electricidad) e inconvenientes que pueden afectar su viabilidad económica (por ejemplo, la presión deflacionaria). Debido a que el algoritmo de Bitcoin está disponible públicamente y es gratuito para que las personas lo copien y lo mejoren, han aparecido varias criptomonedas alternativas, a menudo denominadas "altcoins", que corrigen las debilidades reales, y en ocasiones solo las

percibidas, en el diseño de Bitcoin. . En muchos casos, estas nuevas criptomonedas funcionan de una manera muy similar a la del Bitcoin original. Al igual que Bitcoin, no tienen una autoridad centralizada (un tercero de confianza) que supervise las transacciones y las registre en las cuentas de los usuarios. En cambio, estas monedas se basan en la criptografía para mantener y distribuir un libro de contabilidad (blockchain) que refleja todas las transacciones en una moneda determinada. La ecología de tales criptomonedas. También es similar a la de Bitcoin. Los participantes en el sistema verifican las transacciones propuestas; por lo general, un grupo de

participantes (mineros) necesita resolver complicados "rompecabezas" matemáticos para ingresar las nuevas transacciones en el libro mayor.

Crear un nuevo altcoin es un negocio con barreras de entrada relativamente bajas. Cuando Bitcoin atrajo la atención fuera de la comunidad de criptografía a fines de 2013, la cantidad de criptomonedas basadas en el protocolo de Bitcoin se disparó. Algunas de estas nuevas criptomonedas son poco más que una copia de Bitcoin (por ejemplo, Terracoin). Otros difieren en un detalle técnico; por ejemplo, Litecoin usa un Algoritmo de hashing diferente que Bitcoin, pero es muy similar.

Sin embargo, otros proponen un cambio más extenso del algoritmo, con el potencial de cambiar significativamente las fuerzas económicas detrás de la criptomonedas.

Ahora hacemos un resumen de algunos de los altcoins, centrándonos en los que ganaron más popularidad o aquellos que mejoraron las debilidades de Bitcoin que analizamos anteriormente en este capítulo. Luego, discutiremos las consecuencias de la competencia en estas diversas criptomonedas.

Litecoin

Una de las primeras altcoins que siguieron a Bitcoin fue Litecoin.

Litecoin fue creada en octubre de 2011 por Charles Lee. La principal fuerza impulsora detrás de su introducción fue la frustración con la complejidad de las herramientas criptográficas utilizadas en Bitcoin, en particular el algoritmo de hash que utiliza Bitcoin, SHA-256. El algoritmo impone una carga computacional sustancial a los mineros de Bitcoin y los obliga a invertir mucho en su hardware si quieren seguir siendo competitivos. En consecuencia, los mineros de Bitcoin que pudieron actualizarse para usar tarjetas de video y equipos ASIC, el hardware más moderno para la minería de Bitcoin:

Dominó el negocio minero.

Litecoin se propuso resolver el problema del uso excesivo de energía y la "carrera armamentista" entre los mineros. Para hacerlo, Litecoin propuso usar un algoritmo de hashing diferente para la prueba de trabajo que Bitcoin: scryptt en lugar de SHA-256. Scrypt requiere relativamente menos potencia de computación, reduciendo la cantidad de energía eléctrica que necesita la minería y haciendo posible la extracción de litecillas utilizando PC estándar en un momento en que la extracción de Bitcoin ya requería equipos especializados.

Resolver este problema es importante por varias razones. Primero, ciertamente vale la pena intentar economizar el uso

de la energía eléctrica necesaria para resolver el enigma criptográfico que subyace en un algoritmo de criptomonedas determinado. Las personas que usan la criptomonedas se preocupan por esto no solo porque son conscientes del medio ambiente (aunque algunos de ellos sí lo son). También hay una razón más prosaica: los costos de ejecutar una criptomonedas son, en esencia, nacidos por todos los que usan esa criptomonedas. Si los costos son demasiado altos (por ejemplo, más altos que la recompensa esperada ganada por los mineros), la moneda no será sostenible en primer lugar; y sería incluso menos probable que se convierta en un potencial retador de otras

criptomonedas o de monedas emitidas por el estado. Volveremos sobre estos temas más adelante en este capítulo.

La segunda razón por la cual era importante frenar o incluso detener la carrera de armamentos entre los mineros es el riesgo de que la minería se concentre en los pocos jugadores que pueden pagar las plataformas mineras más grandes y más rápidas. El problema aquí es el "ataque del 51 por ciento" que describimos anteriormente. A medida que los mineros intentan superarse entre sí para mantenerse al día en la carrera de armamentos, los mineros con menos recursos pueden quedarse atrás rápidamente, y pueden decidir

abandonar la reserva minera. Con menos participantes, la importancia de aquellos mineros que invierten continuamente en la mejor tecnología aumentará, por lo que es probable que uno de ellos, o un grupo organizado de tales mineros que actúen juntos, eventualmente tengan más de la mitad del poder de cómputo en el sistema de la criptomonedas. Tal grupo puede o no ser benevolente hacia el resto del ecosistema de criptomonedas, pero crea un riesgo de colapso del sistema.

Todo esto significa que la innovación de Litecoin fue bien intencionada y estaba dirigida a abordar un riesgo importante en el diseño de Bitcoin. Sin embargo, la

forma en que Litecoin abordó este problema no ha cambiado los incentivos de los participantes en el ecosistema de la criptomonedas y, en última instancia, no ha logrado resolver el problema de la carrera de armamentos en la minería. El algoritmo subyacente aún tiene la estructura del torneo que recompensa al minero con la máquina más poderosa, al menos en promedio. Esto significa que a medida que Litecoin se hacía más popular, los mineros tenían un incentivo cada vez más fuerte para invertir en máquinas más poderosas para hacer más probable que compitieran con otros mineros.

El algoritmo en sí magnificó este efecto:

a medida que aparecían computadoras más rápidas, la red Litecoin aumentaba la diferencia.

La complejidad de la tarea de minería, que por sí misma empujó a los mineros a actualizar sus equipos.

El equipo ASIC que se había desarrollado para Bitcoin estaba especializado para la función de hash SHA-256 y no podía adaptarse para el scrypt de Litecoin. Sin embargo, a medida que Litecoin se hizo más popular, la demanda creció para plataformas de minería personalizadas para scrypt. Con el tiempo, los fabricantes de ASIC resultaron económicos para diseñar equipos

especializados para scrypt. Hoy en día, es virtualmente imposible minar Litecoin con una PC, ya que está minada principalmente por mineros de ASIC. Esto ha llevado a la situación que Charles Lee trató de evitar al diseñar Litecoin. La segunda diferencia principal entre Bitcoin y Litecoin está en el suministro total de las monedas. Si bien el suministro de Bitcoin se limita a 21 millones, se crearán muchos más litecoins, un total de 84 millones. Este cambio se propuso para abordar una inquietud que se plantea comúnmente para Bitcoin: el potencial de deflación causado por el suministro fijo de la moneda. Desafortunadamente, aumentar la cantidad total de monedas cuatro

veces en relación con Bitcoin hace poco para cambiar los incentivos deflacionarios. Esto se debe a que los usuarios de Litecoin son conscientes de que el suministro es finito y que dejará de crecer en una fecha conocida. Esto nos lleva al mismo problema que el que describimos para Bitcoin: el número finito de monedas es cada vez más ineficaz en el servicio de un número potencialmente creciente de transacciones, lo que hace que las monedas sean relativamente más escasas y, por lo tanto, más valiosas.

En consecuencia, los precios bajan: con el tiempo, se necesitarán menos litecillas para comprar un bien o

servicio determinado. Cuadruplicar el número de monedas cambia la estética del problema pero no lo resuelve. Quizás la forma más fácil de verlo es imaginar que las tenencias de una moneda de las personas de repente multiplicar por cuatro. La consecuencia más obvia de esto.

La "devaluación" sería que todos los precios también se cuadruplicarían, haciendo a todos tan ricos o pobres como lo eran antes.

Finalmente, otro intento significativo de mejorar Litecoin en comparación con Bitcoin fue permitir una validación más rápida de las transacciones. Mientras que Bitcoin procesa cada bloque de

transacciones cada 10 minutos, Litecoin está diseñado para procesar un bloque cuatro veces más rápido, cada 2.5 minutos. Esta característica realmente hace una diferencia:

Litecoin es más rápido para validar transacciones que Bitcoin. Sin embargo, argumentaríamos que esta mejora hace relativamente poco para alterar los incentivos en el ecosistema de Litecoin.

En general, aunque Litecoin reconoció una serie de fallas importantes en el diseño de Bitcoin, la forma en que se propuso evitar esas fallas no fue necesariamente exitosa.

Feathercoin

Otro intento de mejora en el diseño de

Bitcoin y el de Litecoin fue Feathercoin, una criptomonedas introducida por Peter Bushnell en abril de 2013. Tiene un diseño muy similar al de Litecoin. Por ejemplo, al igual que Litecoin especifica que el suministro total de monedas será cuatro veces el límite de Bitcoin, Feathercoin pretende tener una circulación total cuatro veces mayor que la de Litecoin. Desafortunadamente, como vimos, esta no es una buena manera de deshacer los incentivos deflacionarios inherentes al diseño de la moneda.

Una diferencia mayor y posiblemente una mejora en el diseño de Feathercoin es el algoritmo de hash utilizado para la

prueba de trabajo. Feathercoin utiliza el nuevo desarrollo NeoScrypt, una versión de scrypt que se modificó especialmente para proteger contra plataformas de minería de estilo ASIC. Este cambio tiene como objetivo "democratizar" la minería y ahorrar energía en general y los costes asociados a la criptomonedas. La consecuencia deseada es atraer a los mineros que no pueden darse el lujo de explotar con éxito en entornos dominados por ASIC, que, para 2013, incluían tanto Bitcoin como Litecoin. No obstante, incluso en la introducción de NeoScrypt, se admitió que no resolvería completamente el problema de ASIC; podría simplemente posponerlo en el

futuro. Esto no debería ser demasiado sorprendente. Cualquier algoritmo de prueba de trabajo favorecerá una mayor potencia de cómputo y dará una ventaja a quien la ejerza, sin importar cuán pequeña sea la diferencia entre ese minero y el siguiente minero más poderoso. Esto brinda a los mineros incentivos para participar en una carrera de armamentos, lo que a su vez puede incentivar a los productores de hardware a desarrollar plataformas de minería especializadas para NeoScrypt tan pronto como vean suficiente demanda. En otras palabras, terminamos con la dinámica que conocemos tanto de Bitcoin como de Litecoin. Por supuesto,

es posible que en esta etapa se proponga una nueva criptomonedas con un algoritmo de hashing ligeramente diferente, que permitirá a los mineros mantenerse un paso por delante de los diseñadores de hardware.

Claramente, sin embargo, esto es simplemente posponer el resultado no deseado, no eliminarlo por completo.

Peercoin

Como vimos, los problemas de la carrera de armamentos y del consumo excesivo de energía surgen debido a la naturaleza de torneo del sistema de prueba de trabajo en las primeras criptomonedas. Una vez que quedó claro que ni Litecoin ni Feathercoin podían

resolver este problema, algunas criptomonedas subsiguientes experimentaron alejándose del sistema de prueba de trabajo. Para hacerlo con éxito, tenían que crear una configuración que, según la información de las transacciones anteriores, verificara automáticamente que las transacciones propuestas fueran válidas y las agregara a la libro mayor. Una de las innovaciones que se propuso para lograrlo fue el plan de prueba de estaca, destinado a complementar o incluso reemplazar el plan de prueba de trabajo. Si bien la prueba de trabajo premia a la primera parte para encontrar una solución al problema del hash, la prueba de juego distribuye la recompensa a

todos los poseedores de una criptomonedas, con personas que tienen más monedas (es decir, quienes tienen más participación en el sistema) que recibe un mayor "dividendo". Similar a la prueba de trabajo, la prueba de participación proporciona una medida de seguridad para el sistema porque no se puede falsificar fácilmente. Mientras que el primero requiere cálculos sustanciales que serían difíciles de reproducir para un atacante, el segundo requiere establecer grandes cantidades de una criptomonedas, que no solo sería costosa para un atacante sino que también alinearía los incentivos con el resto del sistema. La pérdida de moneda

es menos atractiva cuando uno tiene una gran participación en esa moneda.

La primera criptomoneda basada en esta idea fue Peercoin, establecida en agosto de 2012. Peercoin utiliza una mezcla de prueba de trabajo, que le permite extraer monedas de la misma manera que lo hace Bitcoin, y prueba de juego, que eventualmente reemplazaría a la prueba de trabajo cuando la criptomoneda se establece más. La prueba de juego de Peercoin se basa en el concepto de la edad de la moneda, que no solo explica cuántas monedas tienen los participantes de la red, sino también el tiempo que han tenido estas monedas sin obtener el dividendo de la prueba de juego de sus

tenencias. .

El algoritmo de prueba de juego de Peercoin selecciona al azar al titular de Peercoin que explotará el siguiente bloque en la cadena de bloques, con la probabilidad de ser elegido de acuerdo con la edad de las monedas que la persona posee. Esa persona podrá entonces para crear el siguiente bloque en la cadena de bloques de Peercoin y obtener la recompensa por hacerlo. Es importante destacar que el ganador debe estar activo en la red para hacerlo, es decir, Peercoin otorga a los titulares de su criptomoneda, pero solo si dichos titulares mantienen su computadora en línea, listos para participar en la red y

para ayudar a validar las transacciones de Peercoin.

A medida que Peercoin gana popularidad, sus creadores planean que dependa exclusivamente de la prueba de juego, eliminando la necesidad de la prueba de trabajo y sus posibles efectos negativos. Para que el sistema siga siendo atractivo, se permitirá que el número total de peercoins aumente constantemente (en contraste con el número limitado de Bitcoin), proporcionando un incentivo continúo para que los usuarios de Peercoin participen en la red y obtengan sus recompensas de prueba de juego. Los diseñadores de Peercoin acumularon el

constante aumento del 1% anual en el suministro de peercoins en el algoritmo de criptomonedas.

Nxt

Una criptomoneda más reciente que utiliza el esquema de prueba de estaca es Nxt, establecida en noviembre de 2013. Su innovación es que la criptomoneda se basa únicamente en la prueba de estaca y que descarta la prueba de trabajo por completo.

Otra innovación interesante en Nxt es que mantiene la oferta de dinero estática, ya que todas las monedas se premian y asignan a los usuarios iniciales del sistema. Esto significa que todas las transacciones de Nxt deben ir

acompañadas de tarifas, que luego se obtienen por los nodos de la red que validan estas transacciones en función de su prueba de estaca.

Los métodos de prueba de estaca utilizados en Peercoin y Nxt ayudan mucho a resolver los efectos secundarios negativos de los sistemas de prueba de trabajo: el consumo excesivo de energía y la carrera armamentista en la minería. La razón de esto se remonta a la economía de estos sistemas y los incentivos que crean.

Como vimos anteriormente, las externalidades de prueba de trabajo tienen que ver con la estructura del torneo de ese sistema. En contraste, la

prueba de la apuesta elimina el torneo y simplemente selecciona al ganador de forma aleatoria en función del número de monedas que tienen. Luego, el ganador deberá participar en la resolución de un enigma criptográfico, pero el enigma es mucho más fácil que los que se están resolviendo actualmente para Bitcoin y otras criptomonedas basadas en pruebas de trabajo.

Esto significa que el ganador tiene pocos incentivos para invertir en sistemas informáticos de vanguardia. Además, no hay ningún incentivo para que otros intenten involucrarse en ningún cálculo: el autor del siguiente bloque se asigna al azar, y no puede mejorar su

probabilidad invirtiendo en una plataforma de minería más nueva o haciendo algunos cálculos de manera proactiva.

La probabilidad de ser elegido puede verse influida por la adquisición de más monedas. Esto ilustra un posible inconveniente de los sistemas de prueba de estaca: una entidad que controla la mayoría de la moneda se seleccionará con más frecuencia que cualquier otra persona, y por lo tanto la entidad puede adquirir el poder para tomar el control y posiblemente reescribir la cadena de bloques.

Algunos de los defensores de estos sistemas argumentarían que difieren la

fusión de la moneda en un gran número de usuarios haría que estos resultados sean menos probables, lo que sin duda es cierto. Sin embargo, también hay dispositivos de seguridad adicionales integrados en los algoritmos. Por ejemplo, Nxt utiliza la "forja transparente", que permite a los participantes de la red monitorear los nodos dibujados al azar que pueden extraer nuevos bloques en la cadena de bloques.

Novacoin

En general, parece que la innovación de prueba de juego es una solución inteligente y exitosa para el consumo excesivo de energía y la carrera de

armamentos minera experimentada por Bitcoin y criptomonedas similares. Mientras tanto, sin embargo, Peercoin al menos depende en gran medida de la prueba de trabajo (en el momento de redactar este informe, el 90 por ciento de las recompensas se basan en la prueba de trabajo en lugar de la prueba de estaca) y tiene inconvenientes similares a los de las criptomonedas anteriores.

Por ejemplo, vemos que las máquinas ASIC que dominan la minería de Bitcoin y Litecoin también se utilizan cada vez más en Peercoin. La comunidad de criptomonedas respondió de manera similar a este desarrollo que a Bitcoin:

creó un nuevo altcoin. Esa nueva moneda, Novacoin, se introdujo en febrero de 2013. Está estrechamente relacionada con Peercoin en su diseño, pero Novacoin utiliza scrypt, un algoritmo de hash que en ese momento aún no ha sido dominado por la minería a gran escala basada en máquinas ASIC. Nuestra revisión de varios altcoins ha destacado cómo sus diseñadores abordaron las fallas que vieron en el diseño de Bitcoin.

Litecoin y Feathercoin se enfocaron en cambiar el algoritmo de hashing para mejorar el consumo de energía. Peercoin y Novacoin adoptaron un enfoque diferente del problema de la energía al

adoptar la prueba de la participación. Además del consumo de energía, Peercoin y Novacoin abordaron la oferta limitada de divisas. En general, Litecoin, Feathercoin, Peercoin y Novacoin mejoran en Bitcoin y entre sí al aliviar los problemas de consumo de energía, ataque del 51 por ciento e incentivos deflacionarios. Fuera de este grupo, Novacoin tiene posiblemente los atributos más atractivos, y puede ser considerado como la más alta promesa de entre los criptocurrenos.

No obstante, Bitcoin es el más popular. Litecoin sigue siendo bastante activo, pero otras criptomonedas, especialmente Novacoin, apenas se negocian. La razón

principal de esta dinámica es probablemente los efectos de la red y la inercia excesiva resultante. Como hemos visto en la historia de las monedas, a veces las personas son reacias a adoptar una nueva moneda, incluso una con atributos más atractivos, si les preocupa que otras personas no puedan adoptarlo también. Entonces, a veces, las expectativas de si otras personas lo usarán pueden ser más importantes que los atributos de la moneda. De hecho, entre el grupo considerado, la popularidad y la actividad de una moneda están más estrechamente relacionadas con la edad de la moneda, es decir, la fecha en que se inició, que con los detalles de su diseño.

Monedas de anonimato

Otros altcoins intentaron mejorar el diseño de Bitcoin en una dimensión diferente: el anonimato. Como hemos comentado anteriormente, Bitcoin se caracteriza mejor como una moneda seudónima que como una moneda anónima. Con suficientes recursos, la identidad de la vida real de los usuarios de Bitcoin se puede desenmascarar, como en el caso de Silk Road. En consecuencia, algunos altcoins intentaron mejorar la protección de la privacidad de los usuarios y aumentar el anonimato de las transacciones. De estos, Dash y Cloakcoin son quizás los más conocidos.

Dash se presentó como XCoin en enero de 2014. En febrero de 2014, el nombre fue cambiado a Darkcoin y en marzo de 2015, se cambió a Dash. Aumenta el anonimato al agrupar las transacciones a través de un proceso llamado mezcla de monedas. Por ejemplo, en lugar de dos Transacciones separadas, de A a B y de X a Y, el libro de contabilidad refleja solo una transacción, de A y X a B e Y, ocultando los enlaces de transacciones individuales. El problema con la mezcla directa de monedas es que las entradas y salidas de la transacción se pueden ajustar por tamaño. Si A envía 2 Dash y X envía 5 Dash mientras que B recibe 2 Dash y Y recibe 5 Dash, las

transacciones se pueden hacer coincidir, incluso con la mezcla de monedas. Darkcoin lo contrarrestó con denominaciones de premezcla ya en la billetera y combinando entradas idénticas, de modo que las entradas no pueden coincidir con las salidas. Por ejemplo, la billetera de A puede enviar dos transacciones independientes (y por lo tanto no se puede conectar al mismo remitente), y la billetera de X puede enviar cinco transacciones independientes, 1 Dash cada una. Con siete transacciones 1 Dash independientes, cada una recibida en una dirección separada, no se puede ver directamente que B recibió 2 Dash y X recibió 5 Dash.

Aunque a algunas personas les preocupa que la mezcla de monedas no sea una garantía suficiente de anonimato o que la combinación de monedas aún permita el rastreo de transacciones. Esto puede deberse a que no creen que la combinación de entradas idénticas sea suficiente para evitar la identificación mediante la comparación de entradas y salidas, o que les preocupa que, a pesar del costo, alguna entidad: digamos, un gobierno — podría tomar el control de una gran cantidad de masternodes y ser capaz de rastrear las transacciones.

El atributo de anonimato parece ser lo suficientemente importante como para que la comunidad continúe los nuevos

desarrollos en esta dirección.

El Cloakcoin, presentado en mayo de 2014, mejora aún más el anonimato con un sistema diferente, un anonimato de prueba de juego, a menudo denominado PoSA. En lugar de la prueba de trabajo más común, utiliza un sistema modificado de prueba de juego, que promete un rendimiento del 6 por ciento para aquellos que mantienen sus billeteras digitales activas en línea, listas para realizar la verificación de las transacciones. Para garantizar el anonimato, cada transacción utiliza una dirección oculta única.

Los diseñadores de Cloakcoin se dan cuenta de que para lograr el anonimato

en una transacción, no es suficiente asegurar el anonimato del libro mayor, sino que también se necesita el anonimato para otros elementos del ecosistema. Por lo tanto, la billetera digital de Cloakcoin está vinculada a un intercambio de propiedad que cotiza a Cloakcoins, llamado CloakTrade. El intercambio está descentralizado y funciona de manera puramente entre pares.

Sin embargo, a pesar de las mejoras, ninguno de estos altcoins se ha vuelto más popular que Bitcoin. Nuevamente puede ser debido a un exceso de inercia, o en este caso, puede haber También otra razón: un número insuficiente de

personas se preocupa por este atributo en particular.

Monedas de propina

Las criptomonedas que discutimos anteriormente se basaron en innovaciones anteriores y, directas o indirectamente, en Bitcoin.

Pero en cada caso, las monedas introdujeron un nuevo elemento al diseño. Discutimos cómo estos nuevos elementos influyen en la economía de estas monedas.

Al mismo tiempo, dado que el algoritmo de criptomonedas básico está en el dominio público, es fácil crear un nuevo altcoin con exactamente el mismo diseño (y, por lo tanto, la misma economía)

pero con una marca diferente. Discutimos tres ejemplos de tales criptomonedas: Dogecoin, Karmacoin y Reddcoin.

Dogecoin fue creada por Billy Markus y Jackson Palmer en diciembre de 2013. En ese momento, Bitcoin había ganado gran popularidad y presencia en los medios de comunicación.

El interés se debió en parte a la innovación de Bitcoin y al posible desafío al dinero emitido por el estado, pero algunos tuvieron orígenes más sensacionales, por ejemplo, las investigaciones de quién fue realmente Satoshi Nakamoto o el busto de la Ruta de la Seda en el otoño de 2013. La

notoriedad recién adquirida hizo de Bitcoin un concepto interesante para leer o escuchar, pero posiblemente no sea una innovación de la que te gustaría formar parte. Markus y Palmer querían cambiar eso, y pensaron en un diseño de criptomoneda que sería más "divertido de usar". Para hacer más divertido su altcoin, lo asociaron con la imagen de un perro Shiba Inu. El nombre de la moneda también se deriva de una palabra mal escrita, o tal vez deletreada de una manera más fresca, palabra: "perro".

La criptomoneda se propuso como una "moneda de vuelco": disponible en grandes cantidades, con un precio por

unidad relativamente bajo. El objetivo era hacerlo adecuado para la filantropía. Caridad y propinas: en esencia, el equivalente a un Botón "Me gusta" o "+1" que transmite una pequeña recompensa monetaria.

Por supuesto, un método de inclinación similar podría diseñarse utilizando una de las criptomonedas anteriores, por ejemplo Bitcoin.

Sin embargo, la preocupación habría sido que los aspectos negativos de la reputación de Bitcoin harían menos probable que las personas usen la moneda de esta manera. Para estar a la altura de su línea "hacer el bien y sentirse bien", Dogecoin necesitaba

proyectar una imagen diferente. Lo hizo, literalmente. Además, la denominación importa psicológicamente: enviar o recibir 100 dogecoins puede sentirse mejor que, digamos, enviar o recibir 0.00006 Bitcoin, incluso si el valor del regalo es el mismo en las unidades de la moneda emitida por el estado, por ejemplo, un dólar.

Dogecoin fue diseñado con su uso previsto en mente.

Su algoritmo original fue tomado de la "luckycoin", una "moneda de casino" que hizo aleatorio las recompensas de la minería, probablemente para hacer que la moneda sea más emocionante para sus usuarios. Sin embargo, debido a que esta

característica creó incertidumbre sobre el costo y los beneficios de la minería. En consecuencia, en febrero de 2014, las recompensas por la minería se fijaron en un monto fijo de 250,000.

Inicialmente, se pensó que el número total de dogecoins que se crearía se fijaría en un número relativamente grande (100 mil millones), prometiendo suficientes unidades de la moneda para apoyar la propina. Sin embargo, debido a una peculiaridad (probablemente un error) en la programación de Dogecoin, el algoritmo se estableció para otorgar un número fijo de Dogecoin por bloque de forma indefinida, haciendo que el suministro de la moneda aumente con el

tiempo y sea potencialmente ilimitado. La comunidad Dogecoin ha decidido no eliminar esta característica. Una consecuencia de la mayor oferta total de La Dogecoin y de su premio más alto por bloque es que su valor por moneda es menor que el del Bitcoin. Esto encaja bien con el uso previsto de la criptomonedas, por ejemplo, inclinando pequeños valores monetarios en unidades redondas de la moneda.

Dogecoin parece haber encontrado un nicho en la economía de Internet. Para sorpresa de sus primeros críticos, ha ganado un número considerable de seguidores y se ha incorporado a varios sitios web. Por ejemplo, en junio de

2014, Facebook aprobó la inclusión de Dogecoin en su plataforma.

Dogecoin no es la única moneda que tiene como objetivo promover la filantropía. Karmacoin (que luego se renombró simplemente Karma) comenzó en febrero de 2014. Al igual que la Dogecoin, es una "moneda de inflexión" diseñada para permitir a sus usuarios enviar pequeños valores monetarios como muestra de su aprecio y para "difundir el karma". Su diseño era inicialmente muy similar a Dogecoin, que en ese momento ya había adoptado recompensas deterministas para la minería.

En junio de 2014, Karma experimentó un

rediseño sustancial, cambiando su algoritmo de hashing de scrypt (el mismo algoritmo que adoptó Litecoin) a X y agregando un elemento de prueba de juego a su sistema de recompensa. Estos cambios probablemente fueron motivados económicamente y sirvieron para diferenciar Karma de sus dos competidores directos, Dogecoin y Reddcoin.

Reddcoin, la "moneda de inflexión" final que describimos aquí, ha sido calificada como "moneda social": se utiliza con las redes sociales para transferir dinero de manera instantánea y sin cargos por transacción. Al igual que Dogecoin y Karma, Reddcoin estaba destinado a ser

utilizado para expresar aprecio con dinero, en otras palabras, para dar propina. Reddcoin también comenzó con un diseño similar al de Dogecoin, utilizando el mismo sistema de prueba de trabajo que Dogecoin y el mismo algoritmo de hashing. Si bien el algoritmo básico adoptado en Reddcoin es relativamente común, su diseño incluyó algunas características que estaban orientadas a la interacción social, por ejemplo, la billetera digital de Reddcoin incluía la opción de publicar feeds de Twitter.

En agosto de 2014, Reddcoin experimentó un importante cambio en su diseño, al cambiar su enfoque de prueba

de trabajo a la velocidad de prueba de estaca (PoSV) recientemente desarrollada.

PoSV se basa en la misma idea que la prueba de juego, utilizada en Peercoin. Como innovación, PoSV recompensa a los participantes en el ecosistema de Reddcoin con monedas recién emitidas. El sistema original de prueba de juego otorga las nuevas monedas en función de las tenencias de la criptomoneda, en esencia, paga un dividendo, independientemente de la forma en que una está utilizando la moneda. En contraste, PoSV recompensa a los usuarios no solo por tener las monedas sino también por gastarlas y recibirlas.

Esta ingeniosa innovación no solo fomenta la propiedad (estaca) sino que también promueve la actividad (velocidad).

Esto ayuda a alinear los incentivos de los usuarios de la criptomoneda con la utilidad y el potencial del esquema general. PoSV lo hace relativamente más atractivo para gastar y ganar reddcoins. Esto, a su vez, hace que sea más probable que las personas estén activas en el ecosistema de Reddcoin, lo que lleva a mayores efectos de red. Por ejemplo, alguien que piense en adoptar una moneda evaluará qué tan fácil será encontrar a otras personas que estén dispuestas a usar esa moneda mientras

realizan transacciones con él. Todo lo demás igual, será más fácil encontrar compradores y vendedores dispuestos en un ecosistema con PoSV.

En general, incluso en la categoría relativamente estrecha de "monedas de vuelco" encontramos una cantidad de monedas diferentes que comenzaron con un diseño muy similar y apuntaron a un propósito similar. Al igual que con las otras criptomonedas, aquí también vemos una rápida innovación y mejoras en el algoritmo inicial, lo que lleva a un aumento de las diferencias a través del monedas De estos, PoSV, adoptado por primera vez en Reddcoin, parece ser la forma más creativa de mejorar las

perspectivas económicas de la criptomoneda.

A pesar de la innovación en curso, la primera moneda de vuelco, Dogecoin, sigue siendo la más significativa, por ejemplo, en términos de su presencia en los intercambios de criptomonedas, el volumen de comercio, etc. Esto es probable porque Dogecoin es la moneda de vuelco más antigua, y quizás haya tenido más tracción al principio y haya tenido la oportunidad de ganar un número de seguidores relativamente mayor que las monedas de vuelco más jóvenes. Nuevamente, el tamaño de la red y los efectos de red correspondientes y el exceso de inercia

determinan la popularidad de la criptomoneda, aunque algunos argumentarán que otras innovaciones más recientes ofrecen un diseño y una funcionalidad relativamente mejores.

Criptomonedas Copycat

En nuestra breve revisión, describimos a varios primos de Bitcoin, centrándonos en aquellos que introdujeron una innovación particularmente interesante y aquellos que pueden ser los competidores más fuertes para Bitcoin y posiblemente para las monedas emitidas por el estado.

Esto, sin embargo, simplemente rasca la superficie. Actualmente hay muchos

cientos de criptomonedas que son básicamente copias o clones de Bitcoin, Litecoin o Peercoin. Por ejemplo, Zetacoin y Monacoin se basan en Bitcoin; Infinitecoin, Goldcoin y Ekrona utilizan el diseño de Litecoin, y así sucesivamente. Estas criptomonedas pueden diferir de sus predecesoras en ciertas características de su diseño técnico; por ejemplo, qué algoritmo de hash se usa, con qué frecuencia se agregan nuevos bloques a la cadena de bloques, cuántas monedas se recompensan por bloque, o si solo usan prueba de trabajo o alguna combinación de prueba de trabajo y prueba de trabajo -estaca. Como dijimos las

características tienen relativamente poco impacto en la economía de estas monedas, en términos de la estructura de incentivos que las características imponen a los usuarios y cómo afectan al sistema. Desde este punto de vista, podríamos llamar a estas monedas, tal vez un poco ásperamente, monedas copiadas.

El número de monedas de imitación que se han multiplicado en los últimos años es sorprendente. Estos altcoins utilizan la misma tecnología y no ofrecen a sus usuarios ninguna mejora significativa sobre las anteriores. Además, el hecho de que los copycats sean más recientes significa que generalmente tienen una

red de usuarios más pequeña que las antiguas criptomonedas, y por lo tanto su uso se basa en efectos de red relativamente más débiles. En general, esto significa que las monedas de imitación tienen menos probabilidades de ser ampliamente adoptadas que sus predecesoras. ¿Por qué, entonces, se crean esas criptomonedas de imitación y cuáles son los incentivos de las personas que las explotan?

Primero, los costos de crear un nuevo altcoin son muy bajos.

Dado que Bitcoin es de código abierto, cualquiera puede reutilizar el mismo algoritmo y código para crear una criptomoneda similar. De hecho, dado

que cambiar el código subyacente requiere más experiencia que simplemente copiarlo, es más fácil y, por lo tanto, más barato producir una moneda de imitación que crear una criptomoneda significativamente diferente de sus predecesores. Una ilustración reveladora de la facilidad de crear un nuevo altcoin es un sitio web ya desaparecido, Coingen.io, que permitió a los usuarios generar un altcoin automáticamente al elegir las configuraciones deseadas para diferentes atributos (por ejemplo, con qué frecuencia se agrega un bloque a la cadena de bloques, cómo muchas monedas que obtienen los mineros exitosos, qué tan rápido disminuye la

recompensa por la minería

Si los costos son tan bajos, ¿cuáles son los incentivos y los beneficios potenciales para las personas que comienzan una nueva criptomoneda o que ayudan a explotar a un imitador? Se ha sugerido que algunas de estas criptomonedas pueden realmente caracterizarse como esquemas de bombeo y descarga. Las criptomonedas suelen comenzar con una cantidad de monedas que ya están preminadas. Es decir, estas monedas se crean antes del primer bloque en la cadena de bloques y antes de que la criptomoneda se introduzca en la comunidad minera. Más tarde, a medida que los mineros extraen

nuevas monedas y las venden en el mercado, el propietario de las monedas preminadas las compra para aumentar el precio.

Esa es la "bomba". Con el aumento del precio, el altcoin atrae la atención. A medida que más personas lo vean como un éxito potencial, es posible que quieran participar o incluso comenzar a verlo como una inversión. Cuando compran algunas unidades de la criptomoneda, normalmente las compran a los creadores del esquema, que eligen esta oportunidad para cobrar, mediante la venta de sus acciones del altcoin.

Eso es "Volcado". Después, el precio generalmente baja y nunca se recupera.

Otra razón, y tal vez menos controvertida, por la cual se inician las monedas de imitación, son los mineros que buscan alternativas. Se les puede desalentar a participar en los esquemas anteriores porque carecen del ASIC especializado

Máquinas necesarias para tener la oportunidad de tener éxito al extraer bitcoins o litecoins. En su lugar, estos mineros pueden estar buscando alternativas más nuevas y menos concurridas, ya que tienen una mayor probabilidad de ganar con éxito esas monedas. Entonces podrían esperar vender esas criptomonedas en intercambios digitales.

Por supuesto, el argumento anterior solo plantea la pregunta de por qué alguien compraría los fondos de imitación a tales mineros. Es posible que algunas personas los intercambien como un experimento, quizás para conocer la industria, y perciban que esas criptomonedas son más accesibles que, por ejemplo, Bitcoin. De hecho, a menudo vemos que aparecen monedas tan nuevas en los intercambios de criptomonedas, e incluso aunque típicamente no logran atraer grandes volúmenes de comercio, ocasionalmente realizan transacciones.

En general, aunque ha habido una proliferación de criptomonedas con una

amplia gama de atributos, generalmente vemos que las monedas más antiguas tienen una ventaja sobre las más jóvenes. Bitcoin, el más antiguo de todos, sigue siendo el más exitoso entre las criptomonedas. Podemos ver esto, por ejemplo, comparando la capitalización de mercado de las distintas monedas, es decir, el número de monedas en circulación multiplicado por el precio por moneda. Según esa medida, la capitalización de mercado total de Bitcoin a partir de mayo de 2015, alrededor de $ 3 mil millones de dólares estadounidenses, fue muchas veces mayor que la capitalización de mercado de Litecoin, el segundo altcoin más popular.

El éxito de Bitcoin probablemente esté vinculado a su ventaja en primer movimiento. Como la primera criptomoneda, ha tenido el mayor tiempo para atraer a un mayor número de seguidores. Aparece más en los medios de comunicación.

En términos de nuestros análisis anteriores, el dominio de Bitcoin puede reflejar una inercia excesiva.

Al mismo tiempo, una nueva criptomoneda puede superar esta desventaja inicial si atrae a una audiencia suficientemente grande. Puede ser capaz de atraer a esa audiencia ya sea porque es tecnológicamente superior en general o porque es superior para un

propósito particular. Esto significa que las monedas de imitación que discutimos anteriormente parecen tener pocas posibilidades de ser más ampliamente aceptadas. Además, en línea con estos argumentos, observamos mejoras en la calidad, o al menos intentos de tales mejoras, que pueden hacer que una criptomoneda sea más atractiva para la audiencia general. Discutimos tales mejoras en el contexto de Litecoin, Feathercoin, Peercoin y Novacoin, aunque hasta ahora ninguna de estas monedas logró desafiar a Bitcoin de manera significativa.

En paralelo, vemos el desarrollo de altcoins optimizados para un propósito

particular. Por ejemplo, vimos monedas como Dash o Cloakcoin, diseñadas para mejorar la protección de la privacidad de sus usuarios o las monedas diseñadas para propinas y transferencias de caridad de bajo valor, por ejemplo, Dogecoin, Karma o Reddcoin. Estos sistemas de criptomoneda pueden atraer a sus seguidores al enfocarse en un nicho tan estrecho y darles un buen servicio.

4.6. Más que solo una moneda

Hasta ahora, nos hemos centrado en las criptomonedas que están diseñadas para servir como un equivalente de efectivo en el universo digital. Estas

criptomonedas se basan en última instancia en Bitcoin y su ingeniosa forma de resolver el problema del doble gasto. Sin embargo, resulta que la solución propuesta por Satoshi Nakamoto no se limita a las monedas digitales. El concepto de blockchain se puede generalizar para una amplia gama de otras aplicaciones.

Namecoin se introdujo en 2010 con el objetivo de mejorar el anonimato de la actividad de Internet, por ejemplo, para proteger las voces de los disidentes. El sistema Namecoin es un alojamiento descentralizado del dominio web ".bit", de modo que ninguna entidad puede tomar el control y cerrar un sitio web, a

diferencia de los dominios regulares, facilitado por la ICANN: Corporación de Internet para Nombres y Números Asignados.

El sistema Namecoin usa moneda nativa, denominada en namecoins, para los pagos para obtener o renovar un sitio web en el dominio .bit a través de la cadena de bloques de Namecoin. Sin embargo, en términos de diseño de moneda, no difieren de bitcoins. De hecho, se pueden extraer simultáneamente en el mismo proceso.

Otra innovación de blockchain es Ethereum, un sistema que fue diseñado en 2011 y lanzado en 2015. Sus desarrolladores describen a Ethereum

como "una plataforma para aplicaciones descentralizadas". Utiliza una tecnología similar a otras criptomonedas, pero en lugar de crear una plataforma descentralizada, para enviar transacciones, apunta a construir una red que apoye los contratos de Ethereum. Estos contratos proporcionarían servicios tales como publicación de contenido, mensajería dinámica y transacciones, pero de forma totalmente descentralizada y seudónima.

Ethereum se puede considerar como un marco o un lenguaje en el que se pueden escribir contratos inteligentes. Estos contratos son aplicaciones que tienen sus propias reglas de propiedad,

transacciones, etc. Estos contratos inteligentes pueden encontrar aplicaciones en varios entornos, desde sistemas de votación hasta propiedad intelectual e intercambios financieros.

Los conceptos de blockchain y ledger descentralizado también se pueden usar con protocolos distintos a los de Bitcoin.

El sistema alternativo más conocido es Ripple. Ripple es una red de pago desarrollada por Ripple Labs, una empresa de Vancouver conocida anteriormente como OpenCoin, que ahora se encuentra en San Francisco. La compañía desarrolló el Ripple para facilitar el comercio en varias monedas

(criptográficas y emitidas por el estado); por ejemplo, para permitir remesas transfronterizas que serían más baratas que las disponibles de proveedores tradicionales como bancos o Western Union. El sistema de pago Ripple fue lanzado en 2011.

La red Ripple presenta un libro mayor descentralizado y abierto que registra las ofertas de los participantes para comerciar en varias monedas. Para ejecutar el comercio, el sistema utiliza una criptomoneda intermedia, XRP, también llamada "rizo". A diferencia de la mayoría de las criptomonedas, el conjunto de rizos ya está preminado: la moneda está disponible para la venta en

Ripple Labs o en fiestas privadas, pero no se pueden hacer nuevos rizos. Ser generados por el equivalente de la minería de Bitcoin. La forma en que funciona esta moneda intermedia se remonta al sistema medieval de transferencia de dinero. A través de pagarés emitidos por intermediarios financieros. En esos días, depositaría su dinero en efectivo con un intermediario y cobraría su IOU. Luego puede entregar el IOU a otro intermediario, tal vez en una región geográfica diferente, y cobrar su dinero en efectivo. Los cheques de viajero son un invento más moderno que funciona de manera muy similar.

Cuando desea utilizar Ripple para

transferir moneda, se aproxima a un nodo en la red Ripple con su solicitud.

Ese nodo encuentra un nodo en su destino deseado. En la práctica, puede haber una cadena de nodos intermedios entre los dos. En lugar de enviarles su efectivo, lo que llevaría mucho tiempo y necesitaría utilizar la infraestructura de las instituciones financieras tradicionales, el nodo de origen envía el equivalente de XRP de su efectivo al nodo de destino. El nodo de destino puede intercambiar las ondas en la moneda deseada en ese extremo de la transacción. Al pasar por alto gran parte de la infraestructura financiera tradicional, Ripple promete que dichas

transferencias o intercambios serían de bajo costo en relación con los servicios tradicionales.

Por su diseño, la red Ripple puede ser más atractiva para las instituciones financieras que para los consumidores individuales.

Dado que un consumidor necesitaría encontrar un nodo Ripple para poder usar el sistema, podría ser más fácil si dichos nodos estuvieran ubicados en el banco de la elección del consumidor. El beneficio para el banco es que la red Ripple le brindaría una cobertura global y la capacidad de enviar pagos en tiempo real. Por lo tanto, Ripple no se posiciona como competidor de Bitcoin u

otras criptomonedas, o de las monedas emitidas por el estado.

Ripple ha ganado gran popularidad en los últimos años. Su moneda, XRP, ha ganado una sustancial capitalización de mercado. A partir de mayo de 2015, fue de alrededor de $ 200 millones de dólares estadounidenses, aproximadamente tres veces más que Litecoin, pero aun sustancialmente inferior a los $ 3 mil millones de Bitcoin. Quizás un testimonio más persuasivo de la popularidad de Ripple es que está siendo adoptado por instituciones en el sistema financiero tradicional interesado en modernizar sus redes de pago. La primera institución en

integrar el protocolo Ripple fue Fidor, un banco alemán, que lo hizo en 2011. Unos meses más tarde, dos bancos estadounidenses, CBW Bank y Cross River Bank, siguieron su ejemplo.

4.7. Criptomonedas de comercio

Hasta ahora, hemos discutido cómo el dinero facilita el intercambio, asumiendo implícitamente que las personas que quieren usarlo ya tienen la moneda de alguna fuente. También cubrimos una de esas fuentes de criptomonedas: la minería. Sin embargo, pocos usuarios potenciales de, digamos, Bitcoin, pueden obtener de manera confiable esa moneda de la minería. Como explicamos, la minería se ha

vuelto ultra competitiva y requiere recursos y experiencia sustanciales por parte de cualquiera que quiera hacerlo con éxito.

Del mismo modo, puede ganar bitcoins si es un comerciante y acepta el pago de su producto en esa moneda.

Sin embargo, pocas personas desearían iniciar un negocio únicamente para adquirir bitcoins para luego gastarlos en un bien diferente.

Afortunadamente, hay formas más fáciles de adquirir criptomonedas como Bitcoin: puedes comprarlas a otras personas. "Comprar" las criptomonedas es conceptualmente similar al intercambio de unidades de una moneda

emitida por el estado (por ejemplo, el dólar) por otra (por ejemplo, la libra). En este capítulo, presentamos una descripción general de varias formas de realizar dichas transacciones, con especial atención a los intercambios en línea que permiten dichas transacciones.

Si las criptomonedas se adoptaran ampliamente, los intercambios como estos se convertirían en características importantes del sistema financiero. Sin ellos, los flujos a gran escala entre criptomonedas como Bitcoin y otras monedas (tanto las criptográficas como las emitidas por el estado) serían difíciles, lo cual sería un impedimento importante para que las criptomonedas

desempeñen un papel en la economía.

Antes de pasar a los intercambios, una forma sencilla para que una persona promedio adquiera una criptomoneda es encontrar un vendedor directamente. Esos encuentros eran la forma más antigua para que las personas adquirieran bitcoins sin tener que convertirse en mineros. Por lo general, las personas interesadas en el comercio se coordinan a través de Internet, mediante tableros de mensajes y correo electrónico. Luego se encontrarían "en el mundo real" y realizarían las transacciones. El comprador proporcionaría la moneda emitida por el estado y el vendedor iniciaría la

transferencia de Bitcoin.

La descripción anterior probablemente le recuerda una forma temprana de intercambio: el trueque. El problema asociado con el trueque, la coincidencia de deseos, surge aquí también. Si desea comprar bitcoins, primero debe encontrar a alguien dispuesto a participar con ellos por la cantidad de moneda emitida por el estado que ambos consideren aceptable. Por supuesto, la tecnología moderna hace que este problema sea mucho más fácil de resolver de lo que ha sido históricamente, pero no obstante, es una fricción. Uno de los temas de nuestro libro es que tales fricciones estimulan la

innovación y catalizan diseños nuevos y mejorados. Esta vez no es diferente: los cajeros automáticos de Bitcoin han aparecido en algunos países, lo que permite un fácil intercambio de la moneda emitida por el estado por bitcoins.

Los cajeros automáticos de Bitcoin (a menudo denominados BTM) permiten a los usuarios intercambiar efectivo emitido por el estado por bitcoins sin tener que encontrar un vendedor dispuesto y concertar una reunión con él o ella. La primera máquina de este tipo se introdujo en octubre de 2013 en Vancouver, Canadá. En los últimos años, los BTM se han introducido en

países que van desde Argentina a los Estados Unidos, lo que los convierte en un lugar cada vez más popular, pero quizás todavía algo exótico. Inicialmente, estos BTM permitían a los usuarios comprar solo bitcoins, y los BTM no estaban diseñados para permitir usuarios para vender sus bitcoins para monedas emitidas por el estado. La mayoría de BTM todavía tiene esta limitación. Recientemente, sin embargo, también aparecieron algunos BTM de dos vías, donde uno puede comprar y vender bitcoins.

Tanto las reuniones personales como las BTM pueden satisfacer la demanda de una criptomoneda de una persona

promedio, pero difícilmente pueden servir a la economía en general. Por ejemplo, no sería económico que los comerciantes más grandes traten de identificar las partes privadas listas para intercambiar sus ingresos desde y hacia bitcoins o para que dichos comerciantes hagan viajes frecuentes a un BTM. Para que la economía funcione sin problemas, necesitamos una forma de realizar más transacciones mayoristas. Los intercambios de criptomonedas en línea proporcionan una de esas formas.

Un intercambio de criptomonedas en línea es una plataforma de dos caras que conecta a compradores y vendedores y

les permite comerciar con sus tenencias de criptomonedas. Conceptualmente, es similar a un intercambio financiero tradicional, y brinda a los usuarios la oportunidad de implementar estrategias similares a las que uno implementaría, por ejemplo, en un mercado de valores. Por ejemplo, usted podría tramitar su criptomoneda al precio vigente en un momento dado, pero también puede publicar órdenes de límite, es decir, indique el cambio para comprar o vender en su nombre en el futuro, siempre que el precio sea lo suficientemente barato o costoso.

Los intercambios también están comúnmente vinculados al sistema

financiero tradicional, lo que permite a los usuarios financiar sus cuentas con monedas emitidas por el estado para luego adquirir criptomonedas o, a la inversa, vender sus criptomonedas y luego retirar la moneda emitida por el estado del intercambio. Es importante destacar que los intercambios generalmente no compran ni venden criptomonedas en su propia cuenta; sólo coinciden con los compradores y vendedores. Los intercambios son simplemente intermediarios que brindan el servicio de compradores y vendedores que están dispuestos a realizar transacciones a un precio determinado. El paisaje de los intercambios de criptomonedas es

todavía joven y muy dinámico. Vemos nuevos participantes compitiendo con intercambios establecidos más largos, a menudo con éxito, lo que lleva a frecuentes cambios en el ranking de los intercambios más activos. A continuación le damos un rápido historial histórico en el Monte Gox: probablemente el intercambio más conocido por el público y también uno de los más importantes para el desarrollo del comercio de Bitcoin. Monte Gox era un intercambio con sede en Tokio que había sido el intercambio de Bitcoin más importante en los primeros años de la existencia de Bitcoin. Según algunas estimaciones, el

monte. Gox fue responsable de manejar el 90 por ciento de las operaciones de Bitcoin, dominando claramente este mercado. Su tamaño e importancia atrajeron no solo a usuarios dispuestos a intercambiar bitcoins sino también a atacantes.

En 2011, el intercambio se vio comprometido por un pirata informático que logró manipular el sitio y el precio de Bitcoin que figuraba en la lista y logró enviar a sí mismo una gran cantidad de bitcoins obtenidos al precio artificialmente bajo. Monte Gox se recuperó del ataque, pero su debilidad temporal hizo que perdiera cuota de mercado frente a sus competidores.

A pesar de sus problemas, el Monte Gox siguió siendo el intercambio de Bitcoin dominante hasta mediados de 2013. A principios de 2013, se hizo difícil para los clientes de EE.UU. Acceder a Mt.Gox históricamente, los clientes de los EE. UU. Recibieron servicios con una cuenta bancaria que pertenecía a un Mt. Filial de Gox, pero en mayo de 2013, esa cuenta fue congelada por el FBI.

Durante los próximos meses, el saldo se inclinó, y mientras el Monte Gox, siguió siendo un importante intercambio, perdió su posición dominante ya solo controlaba alrededor del 27 por ciento del mercado. Su cuota de mercado

restante se dividió entre la bolsa china BTC China (35 por ciento de las operaciones con Bitcoin), Bitstamp (24 por ciento) y BTC-e (14 por ciento). Cada uno de estos intercambios tenía sus propias reglas específicas, por ejemplo, BTC China solo permitió transacciones de Bitcoin contra el yuan chino, mientras que los intercambios restantes permitieron la negociación de Bitcoin frente al dólar estadounidense.

Durante los siguientes meses, aparecieron nuevos intercambios (por ejemplo, OKCoin de China, que se convirtió en uno de los intercambios más grandes en el momento de la escritura); Otros desaparecieron del

mercado, sobre todo, el MonteGox en sí. En febrero de 2014, el intercambio fue nuevamente atacado por hackers, y esta vez el ataque ha demostrado ser inestable. Según las estimaciones, se perdieron $ 350 millones en bitcoins (posiblemente robados), lo que llevó al cierre del intercambio.

Después del cierre de Monte Gox, el mercado de Bitcoin estaba en crisis; previsiblemente, el tipo de cambio de la criptomoneda frente a las monedas emitidas por el estado cayó. No obstante, el mercado demostró ser notablemente resistente y los nuevos intercambios parecieron llenar el vacío dejado por la desaparición del Monte

Gox A partir de la redacción de este libro, Bitcoin puede intercambiarse en aproximadamente 100 intercambios en línea diferentes, muchos de los cuales también permiten comerciar una serie de otras criptomonedas.

Gandal y Halaburda (2014) ofrecen una visión general de la economía de los intercambios de criptomonedas en línea. El documento se centra en BTC-e, uno de los intercambios más grandes en el momento que permitía realizar transacciones en varias criptomonedas, incluidas siete particularmente populares que conocemos de los capítulos anteriores: Bitcoin, Litecoin, Peercoin, Namecoin, Feathercoin,

Novacoin, y Terracoin. Para verificar la robustez de sus hallazgos, los investigadores también analizaron Cryptsy, otro intercambio popular.

Un análisis económico de los intercambios no solo nos ayuda a comprender qué tan bien funcionan las criptomonedas como parte de economía global en términos de la calidad de la infraestructura financiera, por ejemplo, los intercambios en sí mismos pero también nos ayuda a evaluar cuánta atención prestan las personas a las distintas criptomonedas. Por ejemplo, en un mercado que funciona bien, los precios en el intercambio deben reflejar toda la información disponible sobre

cada criptomoneda. En realidad, es bastante difícil probar qué tan eficientes son los mercados desde esa perspectiva. De hecho, la gente todavía discute sobre la eficiencia de los mercados en el sistema financiero tradicional.

Sin embargo, ya sea que el mercado sea más o menos eficiente, generalmente se acepta que un mercado no debe permitir lo que los economistas denominan "oportunidades de arbitraje". El arbitraje es un tipo de comercio que garantiza a los inversores un beneficio instantáneo, sin que el inversor asuma ninguna responsabilidad, o riesgo. En mercados que funcionan bien, las oportunidades de arbitraje deberían

surgir solo accidentalmente. En la medida en que surgen en la práctica, generalmente son causados por la fragmentación del mercado, una fricción particular en la forma en que las personas comercian, o tal vez son solo un testimonio de que el mercado es relativamente pequeño y que sus participantes no prestan suficiente atención a lo que está pasando.

Podemos ilustrar una oportunidad de arbitraje con un ejemplo simple. Supongamos que inicia sesión en un intercambio de criptomonedas en línea que le permite comprar o vender un Bitcoin por $ 250. Si en su lugar desea intercambiar litecoins, puede comprar o

vender una litecoin por $ 2 cada uno. Por último, puede decidir intercambiar las dos criptomonedas directamente una contra otra, sin recurrir a los dólares estadounidenses. Para tal comercio, suponga que el tipo de cambio cotizado es de 100 litecoins por Bitcoin.

Resulta que los precios en nuestro ejemplo no son consistentes internamente, y esto presenta una oportunidad de arbitraje para un comerciante inteligente. Aquí es cómo puedes aprovechar esta oportunidad. Supongamos que compra 100 litecoins por $ 200, utilizando el segundo tipo de cambio en el párrafo anterior.

Tan pronto como se realice la

transacción, puede comprar un Bitcoin por sus 100 litecoins recién ganados, según el tercer tipo de cambio anterior. Finalmente, puede vender su Bitcoin por $ 250 usando el primer tipo de cambio. Su ganancia total de la transacción es de $ 50, la diferencia entre su inversión inicial de $ 200 y el pago total de la venta de Bitcoin a $ 250. Este tipo de arbitraje, popular en las inversiones en divisas, a menudo se denomina "arbitraje triangular", ya que se necesitan tres tipos de cambio para ejecutarlo.

Podrías considerar $ 50 como un pago decente por un momento de trabajo. (Recuerde, está tratando de ejecutar

estas operaciones lo más rápido que pueda; si espera demasiado tiempo, corre el riesgo de que los precios cambien y la oportunidad desaparezca). Sin embargo, este principio, la oportunidad de arbitraje puede llevar a ganancias sustancialmente mayores. Para maximizar sus ganancias, un comerciante intentaría comprar la mayor cantidad posible de litecoins, canjearlos por bitcoins y finalmente canjear todos los bitcoins por dólares. A medida que los participantes en el mercado aprovechan la oportunidad, comienzan a negociar de esta manera, presionando los precios hasta que se ajustan a los niveles que eliminarán la oportunidad de arbitraje (por ejemplo, hasta que la litecoin se

vuelva más cara o la Bitcoin se haga más barata).

La estrategia que describimos anteriormente es relativamente simple, entonces, ¿deberíamos esperar ver esto en realidad? Este tipo de arbitraje triangular es extremadamente raro en los mercados de divisas tradicionales, donde una multitud de comerciantes, tanto humanos como informáticos, prestan mucha atención a los precios y actúan tan pronto como los precios se desvían de los niveles de no arbitraje. Sin embargo, Gandal y Halaburda (2014) mostraron que sí vemos tales oportunidades de arbitraje en los mercados de criptomonedas, lo que

sugiere que no están tan desarrollados como podríamos esperar. Gandal y Halaburda analizaron unas cuantas monedas triples diferentes. Su primera prueba se ocupó de los tipos de cambio que vinculaban las monedas más populares: el dólar estadounidense, Bitcoin y Litecoin. No encuentran evidencia de arbitraje en promedio, lo que sugiere que el intercambio funciona bien la mayor parte del tiempo.

Sin embargo, a veces todavía no funciona de manera eficiente. Resulta que aproximadamente el 2% del tiempo que estos tipos de cambio permitieron una oportunidad de arbitraje triangular, arrojando rendimientos superiores al

1,4%. Si bien la magnitud de los rendimientos puede parecer baja, tenga en cuenta que este es un rendimiento potencialmente sin riesgo que un comerciante puede obtener en un período de tiempo muy corto. Incluso si la oportunidad de arbitraje se elimina relativamente rápido, la tasa de rendimiento es mucho más atractiva en comparación con la mayoría de las otras inversiones.

La evidencia de oportunidades de arbitraje rentables resultó ser más fuerte para las criptomonedas que son menos populares que las de Bitcoin: Peercoin y Namecoin. Para estas monedas, aproximadamente el 2% del tiempo las

ganancias potenciales excedieron el 2% del capital invertido, lo que indica que las oportunidades comerciales entre Peercoin y Namecoin fueron más atractivas que las entre Bitcoin y Litecoin. Esto probablemente refleja las diferencias en el interés que generan estas criptomonedas y la liquidez relativa de su mercado que es la consecuencia de este interés: En general, esperamos que los mercados más líquidos proporcionen menos oportunidades comerciales triangulares.

Otro tipo de arbitraje que es posible con múltiples intercambios es el arbitraje de intercambio cruzado. Es decir, supongamos que los bitcoins están

disponibles al tipo de cambio de $ 240 por bitcoin en un intercambio pero a $ 250 por bitcoin en otro. Esto nuevamente brinda oportunidades para obtener ganancias sin riesgo: un operador podría comprar bitcoins al precio más bajo en el primer intercambio, y luego venderlos al precio más alto en el segundo, quedándose con la diferencia. Una vez más, los comerciantes tendrían incentivo para seguir haciendo eso hasta que su presión de compra y venta iguale los precios en las dos bolsas.

Gandal y Halaburda (2014) investigan la ocurrencia de tal arbitraje entre los intercambios BTC-e y Bitstamp. Como

antes, hay poca evidencia de oportunidades de arbitraje sistemático; en otras palabras, si hay diferencias en las tasas cotizadas en los distintos intercambios, estas diferencias no surgen todo el tiempo. Una vez más, sin embargo, los investigadores encontraron evidencia de desviaciones significativas en algunas ocasiones. Por ejemplo, encontraron que en la mitad de los días de negociación que analizaron, la diferencia en los tipos de cambio Bitcoin-dólar difería en más del 2% en los dos intercambios. El potencial para el comercio oportunista fue incluso mayor cuando los investigadores analizaron Litecoin, una criptomoneda ampliamente comercializada pero menos

conocida que Bitcoin.

Gandal y Halaburda utilizaron datos sobre los precios de criptomoneda registrados a la medianoche, hora de Greenwich, y trabajaron efectivamente solo con una instantánea de datos por día.

Sus datos también cubrieron sólo dos grandes intercambios. Esto significa que su análisis probablemente subestima la posibilidad de arbitraje: puede haber habido oportunidades más atractivas en diferentes momentos del día o entre otros intercambios que los que ellos han analizado.

La existencia de intercambios de criptomonedas también es importante

para la competencia entre las distintas criptomonedas. Los precios a los que cotizan en las bolsas pueden interpretarse como la evaluación del mercado de la importancia relativa y el valor de cada criptomoneda. Dada la importancia de los efectos de la red, este valor depende de la evaluación de qué moneda tiene más probabilidades de obtener una adopción generalizada no solo en el mercado de la criptomoneda sino también en el segmento tradicional de la economía. En el documento mencionado anteriormente, Gandal y Halaburda investigan esta pregunta utilizando datos de precios de los intercambios. Sus resultados ilustran dinámicas interesantes en la visión del

mercado de las diferentes criptomonedas. En la parte anterior de su muestra, los investigadores encontraron evidencia de los efectos del ganador para llevar todo lo que discutimos anteriormente en el libro. Durante ese período, a medida que Bitcoin se hizo más valioso frente al dólar estadounidense, al mismo tiempo se hizo más valioso frente a otras criptomonedas.

Una interpretación de este patrón es que refleja la evaluación de los participantes del mercado sobre si el mercado podría eventualmente inclinarse a favor de Bitcoin. A medida que aumenta la probabilidad de ese evento, Bitcoin se

vuelve más valioso en comparación con la moneda emitida por el estado (es decir, sus aumentos de precios), pero también en comparación con las otras criptomonedas que podría reemplazar en el futuro.

Curiosamente, en la parte más reciente de la muestra en Gandal y Halaburda (2014), este patrón se invierte. A medida que Bitcoin se vuelve más caro en términos de dólares estadounidenses, en realidad se vuelve más barato cuando se mide en unidades de otras criptomonedas. Al final del período de muestra (febrero de 2014), Bitcoin es más fuerte frente al dólar estadounidense y más débil frente a otras criptomonedas

principales de lo que era al comienzo del período. Por lo tanto, ya no vemos la dinámica del ganador se lo lleva todo. Puede ser que en ese momento el interés en las criptomonedas creciera tan fuertemente que el aumento de la demanda elevara todos sus precios, y el precio de Bitcoin, la criptomoneda más conocida, subiera lo mínimo. Los impulsores de este aumento de la demanda probablemente sean variados. Pueden incluir tanto la creciente aceptación de las criptomonedas como la mayor confianza de que uno de ellos será más ampliamente adoptado en la economía. Otro impulsor de la demanda puede ser la especulación: la esperanza de descubrir "el próximo Bitcoin" puede

tener incentivó a la gente a invertir más en criptomonedas alternativas, lo que elevó sus precios más que los de Bitcoin. No tenemos evidencia adicional que corrobore ninguno de estos canales, pero el tono de los artículos de los medios de ese tiempo sugiere que ambos pueden haber estado operando al mismo tiempo.

4.8. ¿Cómo hacer criptomonedas?

Dado que el diseño de Bitcoin tiene como objetivo crear una versión digital de efectivo, es natural preguntarse cómo se compara con las monedas tradicionales en sus características más importantes, que revisamos en el Capítulo 2. Esto es particularmente

relevante para cualquier discusión de la competencia entre Bitcoin y otras monedas, no solo para responder a la pregunta de si es "mejor" sino también para debatir si es "Lo suficientemente bueno" para cumplir algunas o todas las funciones que el dinero tradicional cumple hoy. Si bien consideramos estas preguntas desde el punto de vista de Bitcoin, la discusión en este capítulo también se aplica a otras criptomonedas, incluidas aquellas que intentaron solucionar algunas de las deficiencias de Bitcoin.

Vimos que una de las características relevantes del dinero es la divisibilidad. Aquí, Bitcoin se compara muy

favorablemente con las monedas emitidas por el estado, que normalmente funcionan con el sistema métrico y son divisibles hasta la centésima parte de una unidad.

En contraste, Bitcoin permite la precisión hasta el octavo lugar decimal, con su unidad más pequeña llamada "Satoshi". Esto proporciona más divisibilidad y una mayor precisión no solo que las monedas emitidas por el estado sino también que la medición de cebada o metal mediante peso. Esta mayor divisibilidad puede ser particularmente útil para micropagos.

Otra característica es la durabilidad, es decir, cuánto puede durar una moneda.

Una vez más, la ventaja aquí es para Bitcoin. Los bitcoins no se desgastan ni se deterioran. Por supuesto, uno puede perder bitcoins. Los medios de comunicación informaron sobre una serie de historias de personas que tiraron discos duros o que eliminaron billeteras y, por lo tanto, perdieron claves privadas que les dan acceso a sus bitcoins. Los bitcoins, sin embargo, todavía están en la cadena de bloques, y estarán allí mientras la red de Bitcoin funcione. Desde el punto de vista de la red, es imposible distinguir entre un bitcoin que se ha perdido y un bitcoin cuyo propietario aún no ha decidido gastarlo. Por el contrario, puede perder un billete (o incluso una moneda) de

forma permanente destruyéndolos o dañándolos hasta el punto de que ya no sean reconocibles.

Los bitcoins, al ser digitales, también son fáciles de transportar. Por supuesto, existe la necesidad del software/hardware que los administre, por ejemplo, una billetera digital en su teléfono inteligente. ¿Es esto más fácil o más difícil, que llevar efectivo o una tarjeta de crédito? Eso puede depender de la persona.

El almacenamiento de bitcoins no necesita involucrar cajas fuertes físicas y seguridad, pero uno necesita almacenamiento digital cifrado para mantener a salvo a los bitcoins. Esto se

ilustra mediante la implosión de una serie de servicios que ofrecen almacenamiento de bitcoins. El más espectacular de esos fue probablemente el MonteGox, mencionado anteriormente. Almacenar bitcoins de manera segura puede ser más fácil o más económico que mantener el efectivo en casa, pero es probablemente más complejo que usar tarjetas de crédito y depósitos bancarios.

Los bancos o proveedores de servicios de pago tienden a ser más confiables que almacenar bitcoins, debido a su experiencia, a los sistemas bien desarrollados y la seguridad que ofrecen directa o indirectamente. Por supuesto,

a medida que el sistema Bitcoin madura, uno puede imaginar el desarrollo de opciones y servicios de almacenamiento más seguros.

Bitcoin es todavía una moneda joven, y se podría argumentar que los bancos no estaban particularmente seguros al principio de su historia debido al robo desde el exterior y el fraude desde el interior.

En cuanto a la facilidad de transferencia, depende tanto de la tecnología disponible (por ejemplo, el acceso a computadoras o teléfonos inteligentes) como del ecosistema (por ejemplo, la interfaz). Cuando se confía directamente en el sistema básico de Bitcoin, las

transferencias son engorrosas. Son más difíciles que manejar efectivo para transacciones de persona a persona, o usar tarjetas de crédito para transacciones de larga distancia. Puede comparar el uso de la red Bitcoin directamente con el peso del metal para liquidar las transacciones. Este sistema histórico de metal sin repintar era engorroso y requería sofisticación adicional, lo que generaba costos de transacción adicionales y, finalmente, se eliminaba con la introducción de monedas. De manera similar, el ecosistema de Bitcoin se está desarrollando y ha aparecido una variedad de billeteras digitales, lo que facilita la transacción de los usuarios de

Bitcoin.

Finalmente, a diferencia del dinero en efectivo, Bitcoin no puede ser falsificado, así que si lo obtiene en una transacción, puede estar tranquilo de que es genuino. Los Bitcoin pueden ser robados, pero las transacciones no son reversibles (a diferencia de las tarjetas de crédito), por lo que es una preocupación para el vendedor. Además, ninguna persona o institución puede manipular el suministro de bitcoins, ya que es administrado por un algoritmo.

Por lo tanto, en algunas dimensiones no está claro si las criptomonedas tienen atributos más convenientes que las

monedas tradicionales. Si es más fácil de transportar y transferir o más seguro de almacenar puede depender de las preferencias de los usuarios. Pero en otras dimensiones, proporcionan una mejora clara, como divisibilidad, durabilidad o riesgo o fraude y falsificación. Esos atributos podrían hacer que las criptomonedas sean más útiles para algunos usos, como los micropagos o los pagos internacionales remotos, que las alternativas anteriores. Pero el beneficio debe ser lo suficientemente grande como para que las personas lo adopten y lo usen junto con (o en lugar de) el sistema bancario tradicional y el sistema de tarjetas de crédito.

4.9. Competencia contra el Estado

La ráfaga de nuevas criptomonedas que describimos anteriormente ilustra cuán intensa es la competencia entre estas nuevas monedas. Al mismo tiempo, una pregunta igualmente interesante y quizás más importante es la competencia entre las criptomonedas (o una única criptomonedas que podría ganar la lucha discutida anteriormente) y las monedas fiduciarias emitidas por el estado. Las herramientas que hemos desarrollado hasta ahora en este libro nos permitirán analizar esta pregunta.

Las cuestiones clave relacionadas con la

posible adopción generalizada de criptomonedas (o una criptomonedas particular) son los efectos de red y la superación de la inercia excesiva que actualmente beneficia a las monedas emitidas por el estado. Desde este punto de vista, la plétora de criptomonedas puede ser un problema. Como vimos, las criptomonedas individuales tienen sus ventajas y es probable que los proponentes prefieran esas monedas frente a otras criptomonedas. Si bien esto bien puede mejorar la calidad de toda la categoría y llevar a nuevas innovaciones, tal división del mercado limita los efectos de red que disfruta cualquier criptomonedas.

Hay dos razones generales por las que esto es perjudicial para las criptomonedas que compiten con las monedas emitidas por el estado.

Primero, y más directamente, las criptomonedas más diferentes monedas para la criptomoneda, y así sucesivamente. Los vendedores también necesitarían encontrar una manera de incorporar la criptomoneda en sus sistemas contables, poner precio a sus bienes en las unidades de la criptomoneda, posiblemente permitir la transmisión sin interrupciones de las monedas emitidas por el estado y la criptografía entre proveedores y otros socios comerciales, y pronto. Además,

los nuevos usuarios necesitan aprender a usar la nueva criptomoneda. Es posible que no estén interesados en los detalles de cómo funciona, pero necesitan entender cómo usar el software que les permite gastarlos, cómo pensar en su billetera que ahora combina varios tipos de monedas, etc.

Estos costos aumentan cuando hay varias criptomonedas que pueden usarse en el mercado. Si bien el costo de adquirir una segunda o tercera criptomoneda, o vincularlas a su billetera digital, es relativamente más bajo que el costo de la primera, sin embargo estos costos existen y hacen que sea más difícil persuadir a las personas para que usen

la moneda. Los usuarios que solo optan por una moneda no pueden realizar transacciones con comerciantes que pueden no permitir está en particular. Si bien puede haber intermediarios que traducirán sin problemas una criptomoneda a otra para los fines de una transacción, tal servicio requeriría esfuerzo o quizás una tarifa del usuario, lo que aumentará aún más los costos de uso de la criptomoneda.

El segundo problema general es que la multiplicidad de criptomonedas crea incertidumbre que puede retrasar el desarrollo de ese mercado o impedir que la gente se una a él.

Por ejemplo, los usuarios que puedan

estar interesados en usar criptomonedas pueden preferir esperar a que el mercado se incline hacia uno de ellos antes de adoptar una criptomoneda y arriesgarse a que falle. Una analogía que es útil aquí es la batalla entre los dos formatos de DVD de alta definición, HD DVD y Blu-ray, que posiblemente sostuvieron toda la categoría.

Por supuesto, la competencia entre una criptomoneda y la moneda emitida por el estado también depende del atractivo relativo de los dos, es decir, de su eficiencia para facilitar las transacciones y actuar como dinero. Ya hemos discutido cómo se comparan los atributos básicos de las criptomonedas

con los atributos tradicionales del dinero, en las dimensiones consideradas en el Capítulo 2. Pero lo que importa al final es si estos atributos hacen que la moneda sufra.

Fiable deseable para un grupo suficientemente grande de personas.

Eso significa que la nueva moneda debe ser significativamente mejor que las alternativas existentes para algún propósito en particular.

Las criptomonedas tienen algunas ventajas sobre el dinero emitido por el estado. Los más obvios son los que se exponen en el documento de Satoshi Nakamoto que dio origen a Bitcoin: la capacidad de realizar pagos en línea de

forma económica, permitiendo micropagos debido a su divisibilidad y dando a los usuarios una medida de anonimato. Algunos de estos atributos pueden tener un impacto positivo y negativo. Por ejemplo, el anonimato puede verse como un beneficio sobre el las tarjetas de crédito y los cajeros automáticos, protege tu privacidad y puede ayudarte a evitar fraude, no está enviando el número de su tarjeta, su dirección o incluso su nombre a un comerciante que podría resultar deshonesto. Esto puede ser particularmente relevante cuando realiza transacciones con vendedores en otros países, tal vez aquellos que no le brindan la misma protección que su país

de origen. En esos casos, puede decidir no realizar transacciones si solo tiene una tarjeta de crédito a su disposición, pero puede estar más inclinado a utilizar las criptomonedas para comerciar. El anonimato también puede ser importante para los disidentes en regímenes autoritarios o, por ejemplo, para las mujeres en países como Afganistán, donde legalmente no se les permite tener una cuenta bancaria separada. Por otro lado, el anonimato también puede estimular usos infames, como en el ejemplo de la Ruta de la Seda que se mencionó anteriormente.

Existen otros atributos de las criptomonedas que a veces se

mencionan como ventajas sobre el efectivo, pero que no son tan claras como las anteriores. Por ejemplo, a menudo se ha señalado que las transacciones de Bitcoin son más rápidas y más baratas. Pero esta descripción puede ser engañosa. Las transacciones de Bitcoin suelen tardar entre 10 minutos y una hora en verificarse y liquidarse, ya que se agrega un bloque cada 10 minutos. Además, las transacciones pueden requerir una tarifa de una pequeña fracción de un bitcoin; de lo contrario, la verificación de la transacción puede llevar más tiempo.

Entonces, si es más rápido y más barato

depende de con qué lo comparamos. Sus atributos hacen que Bitcoin sea más rápido y más barato para los comerciantes que las tarjetas de crédito, pero esto no es necesariamente así para los clientes. Y es difícil argumentar en qué medida las transacciones de Bitcoin son más rápidas que las transacciones en efectivo. Las transacciones en efectivo se liquidan en el momento en que se entrega el efectivo. Es difícil imaginar a alguien revolviendo su billetera durante más de 10 minutos. Es posible, sin embargo, que las transacciones de Bitcoin sean más baratas que las transacciones en efectivo si una considera el costo de ir al banco con dinero en efectivo para depositarlo y el

riesgo de que pueda ser robado en el camino.

En general, Bitcoin y otras criptomonedas ofrecen una serie de atributos novedosos y atractivos. La gran pregunta, sin embargo, es si a la gente le importaría lo suficiente como para cambiar.

Incluso si lo hacen, la pregunta entonces es si suficientes personas se preocuparían por crear una masa crítica de adoptantes para convertirla en una moneda viable.

Capítulo 5
El camino por delante

La tecnología de la información del siglo XXI ha creado un nuevo contexto para la creación de dinero (digital).

Este nuevo entorno proporciona una flexibilidad nunca antes vista para el diseño de monedas, así como una escala sin precedentes para su introducción. No es sorprendente, por lo tanto, que el comienzo del siglo haya estado marcado por una experimentación sin precedentes con las monedas digitales, ya sea llevada a cabo por individuos, pequeñas empresas o grandes empresas de Internet. Los objetivos de estos

experimentos han sido tan diversos como sus enfoques para resolver la multitud de desafíos que presenta cualquier sistema de pago a gran escala.

De hecho, uno de nuestros objetivos era revisar estas diversas motivaciones y la multitud de soluciones propuestas para abordarlas. ¿Qué patrones emergen de esta imagen dinámica?

Primero, la experimentación está lejos de terminar por una variedad de razones, que van desde desafíos puramente tecnológicos (por ejemplo, ¿cómo hacer que la "minería" sea eficiente y rentable para las criptomonedas descentralizadas?) A las normativas (por ejemplo, ¿los gobiernos

restringirán el uso de las monedas digitales?), son muchos desafíos adicionales en el medio. Segundo, y más importante, los consumidores continuarán se acostumbraran a estas innovaciones y puede que eventualmente comience a tratarlas como herramientas de pago viables en lugar de algo que acaba de leer en los medios. Como nos han enseñado cientos de años de historia monetaria, el uso de cualquier moneda se basa en la confianza y, a partir de hoy, simplemente hay muy poca experiencia con cualquiera de las monedas digitales para que puedan construir la confianza universal. Esto no quiere decir que algunas de estas monedas no sean de confianza para las

comunidades pequeñas (por ejemplo, los usuarios de Bitcoin en Darknet) o para grupos muy grandes de personas en dominios restringidos (por ejemplo, millones de personas potenciales que usan Amazon Coins). Pero ninguna de estas monedas digitales rivaliza con la confianza en las principales monedas emitidas por el estado. En este sentido, un tema clave es que la flexibilidad y la escala que prometen las monedas digitales también conllevan un mayor riesgo para los usuarios, especialmente si se usan ampliamente.

Sin embargo, dando un paso atrás, podría ser irrazonable poner las monedas digitales a un nivel tan alto.

Otra lección que nos enseña la historia es que las monedas siempre han coexistido, y generalmente no solo unas pocas. En la mayoría de las economías desarrolladas, hay multitud de sistemas de pago restringidos, todos conectados en una red compleja, por ejemplo, cupones de alimentos o BerkShares en los Estados Unidos.

Esto también es cierto si uno toma una perspectiva global. A nivel internacional, la multitud de monedas emitidas por el estado se ve superada por unas pocas monedas particularmente fuertes, generalmente llamadas monedas de reserva porque los bancos centrales pueden mantener sus reservas de divisas

en ellas. De manera similar, ¿por qué no esperar que las monedas digitales proliferen y coexistan en múltiples formas junto con las monedas emitidas por el estado que seguiremos usando?

Desde esta perspectiva, es probable que veamos muchas formas de monedas centralizadas en uso. A medida que se desarrollen las plataformas digitales, continuarán experimentando con las monedas digitales para servir mejor a sus modelos de negocios. Estos experimentos pueden Estar limitado en el tiempo, solo cumpliendo un objetivo temporal, como es el caso de Amazon Coin, que se puede considerar como una herramienta de promoción para construir

el ecosistema de lectores electrónicos de la empresa frente a una competencia agresiva. Algunas de estas monedas pueden interrumpirse debido a que la plataforma ha crecido en sus actividades, cubriendo el comercio de un espectro mucho mayor de productos y servicios, lo que a su vez justifica el uso de la moneda emitida por el estado. Este parece ser el caso de Tencent de China, cuyo negocio ha pasado de ser una red social basada en PC a convertirse en una plataforma de comercio electrónico social de uso general en tecnología móvil, llamada WeChat. Una evolución similar parece estar en marcha en Facebook, la red social más grande del mundo hoy en día.

En resumen, no esperamos mucha desaceleración en la introducción de varias monedas basadas en plataformas centralizadas.

Es probable que ocurra más convergencia en el mundo de las criptomonedas. Como estas se esfuerzan por ser monedas globales de propósito general, pueden tener más dificultades para encontrar un nicho en el que tendrían una clara ventaja sobre las alternativas existentes para un número suficiente de personas. Sin embargo, puede ser posible que coexistan algunas monedas exitosas, cada una con una masa crítica de usuarios.

Para estas monedas descentralizadas,

los efectos de red discutidos anteriormente son de mucha más importancia.

Una pregunta importante es si las criptomonedas llevarán a las monedas emitidas por el estado fuera del negocio. Pueden tener el potencial para hacerlo, especialmente para las monedas emitidas por el estado que han perdido credibilidad con sus ciudadanos. Una vez más, para la mayoría de las monedas emitidas por el estado, es poco probable que esto suceda. En pocas palabras, los gobiernos tienen mucho poder para hacer que la moneda emitida por el estado sea atractiva para sus ciudadanos:

Siempre y cuando esté respaldado por una política monetaria sólida.

Finalmente, ¿los gobiernos prohibirán las monedas digitales?

Ciertamente son capaces de hacerlo en el caso de plataformas basadas en monedas De hecho, pueden prohibir toda la plataforma, como hizo China con Facebook, por ejemplo. Sin embargo, no está claro para qué sirve esto, dado el hecho de que las monedas basadas en plataformas suelen estar limitadas en algunas de sus funcionalidades, por lo que representan una amenaza limitada para la moneda estatal totalmente equipada. ¿Qué hay de las criptomonedas? De nuevo, en teoría, los

gobiernos pueden prohibirlos, pero la naturaleza descentralizada de las criptomonedas hace que esto sea prácticamente difícil o incluso imposible de hacer cumplir. Por lo tanto, la pregunta relevante es si las personas verán la utilidad en el uso de una criptomoneda en paralelo con la moneda emitida por el estado.

¿A dónde nos lleva todo esto? Hicimos un recorrido por el emocionante y dinámico desarrollo del panorama de la moneda digital. Nos acercamos a estas innovaciones como lo haría un economista: estudiando los roles que desempeñan en el mercado, los incentivos que ofrecen a sus usuarios y

la competencia entre varias monedas digitales y emitidas por el estado. Este marco nos ayuda a analizar lo que ha sucedido en este espacio hasta ahora y nos da una idea de lo que está por venir. La pregunta más importante de todas, por supuesto, es si el mundo se inclinará hacia una moneda puramente digital en el futuro. Esto no ha sucedido todavía, y nuestro análisis sugiere por qué. Los fuertes efectos de red y el exceso de inercia favorecen fuertemente los instrumentos tradicionales, que también satisfacen bastante bien la mayoría de las necesidades económicas. La mayoría, pero no todas las necesidades económicas: destacamos algunos usos donde las monedas digitales pueden

encontrar un nicho; Por ejemplo, micropagos o remesas transfronterizas. Hay una competencia continua para estos segmentos del mercado, y promete ser un espectáculo fascinante.

Referencias

Alden, William (2013), "The Bitcoin Mines of Iceland"

New York Times, 23 de diciembre, http://dealbook.nytimes.com/ 2013/12/23/morning-agenda-the-bitcoin-mines-of-iceland /? _ r = 0.

Antonopoulos, Andreas (2014), Mastering Bitcoin, O'Reilly Media.

Caillaud, Bernard y Bruno Jullien (2001), “Competing Cybermediaries”, European Economic Review, 45: 797–808.

Caillaud, Bernard y Bruno Jullien (2003), “Pollo y huevo: competencia

entre los proveedores de servicios de intermediación”

RAND Journal of Economics, 34: 309–328.

Casadesus-Masanell, Ramon y Feng Zhu (2010), “Estrategias para luchar contra los rivales patrocinados por la publicidad”, Management Science, 56: 1484–1499.

Castronova, Edward (2014), Wildcat Currency, Yale University Press.

CryptoCoinsNews (2014), "Facebook aprueba la aplicación de propinas Dogecoin", https://www.cryptocoinsnews.com/facebaprobaciones dogecoin-tipping-app /.

Clenfield, Jason y Pavel Alpeyev (2014), "The Other Bitcoin Power Struggle", BusinessWeek, 24 de Abril.
Coindesk (2014a), "¿Son los ataques del 51% una amenaza real para Bitcoin?" http://www.coindesk.com/51-attacks-real-threat-bitcoin/.

Coindesk (2014b), “BitOcean lanza un cajero automático de Bitcoin bidireccional para competir con los líderes del mercado”, http://www.coindesk.com/bitocean-releases-two-way kioskscompetencia-bitcoin-atm-líderes del mercado/.

Comparette, T. Louis (1914), "Disminución de la moneda de plata bajo el emperador Nerón", The

American Journal of Numismaticss, 47: 111.