Criptomonedas: guía básica para agencias de protección al consumidor

William Taborda
Oficial Asociado de Información
UNCTAD

Introducción

"Criptomoneda" es un concepto complejo. La definición exacta de cada criptomoneda está profundamente arraigada en la criptografía utilizada para su creación y autorregulación inherente. Definir y comprender cada una de las criptomonedas y los diferentes conceptos que las rodean, requiere un profundo conocimiento de varios campos, incluyendo criptografía matemática, redes distribuidas, algoritmos y economía. Aún así, los expertos en una criptomoneda pueden encontrar difícil entender otras.

Este artículo se centra principalmente en bitcoin y su tecnología *blockchain* o cadena de bloques.

El documento no tiene la intención de dar una definición exhaustiva de criptomonedas o cualquiera de ellas en especial. No está destinado a obtener una comprensión completa de su funcionamiento. En su lugar, su objetivo es dar al lector una visión general que sea suficientemente detallada para comprender las implicaciones que pueden tener estas tecnologías en nuestra vida cotidiana. El objetivo final es proporcionar al lector suficiente material para permitir un debate informado sobre sus características, reglamentación y trascendencia.

Criptomonedas: una definición simplificada

Las criptomonedas son un subconjunto de las monedas electrónicas, para las cuales no hay una entidad centralizada a cargo de controlar la emisión, transacción, propiedad o cualquier otra política monetaria. En su lugar, utilizan el protocolo de *blockchain* para auto-regularse a través de un consenso distribuido de todos los elementos que participan en la red.

La palabra criptomoneda ya nos da por sí misma una idea de su significado. "Cripto" se refiere a el uso de técnicas de cifrado criptográfico en sus diferentes componentes. "Moneda" es lo que nos lleva a la la conclusión de que podemos hacer transacciones con ella o que tiene un cierto valor. En otras palabras, que es un medio de intercambio.

Para entender cómo funcionan las criptomonedas, primero debemos analizar la invención que permite su existencia, el *blockchain* o cadena de bloques.

Blockchain

El *blockchain* es una especie de libro mayor distribuido y criptográfico que es capaz de registrar un historial de transacciones en forma segura sin una autoridad central.

Blockchain utiliza la criptografía para crear enlaces entre bloques de tal manera que cualquier manipulación no autorizada de la información almacenada en cualquier bloque rompe todos los enlaces subsiguientes, haciendo así cualquier manipulación evidente. El *blockchain* se replica en cada nodo de la red (también llamado par). La replicación entre todos los nodos en la red permite la identificación y depuración de cualquier bloque y/o cadena de bloques que no respetan las reglas del protocolo (es decir, aquellas que han sido manipuladas). Esto soluciona el problema del doble gasto.

En el caso de bitcoin, la distribución de datos también aporta cierto grado de transparencia, permitiendo a cualquiera acceder y verificar cualquiera de los registros del libro mayor.

Un bloque es un conjunto de información que detalla las transacciones ocurridas desde que el último bloque fue creado y unido a la cadena. La única excepción a esta definición es el denominado "bloque génesis" o, en otras palabras, el primer bloque jamás creado.

Los bloques también incluyen otras informaciones importantes, como la recompensa de bloque, el *hash* de bloque, el *hash* del bloque anterior (*hash* anterior), el *timestamp* o marca de tiempo y el *nonce*. Los bloques están diseñados de tal manera que, para poder fijar un bloque al final de la cadena, junto al último bloque creado, debe realizarse algún trabajo. Por cada bloque, los mineros entran en una carrera para encontrar un número, el *nonce*, para que el *hash* del bloque satisfaga ciertas condiciones. Esta prueba de trabajo y la recompensa económica que el sistema otorga es el mecanismo que crea un incentivo para que los mineros aseguren la red.

Los mineros son individuos que buscan rentabilidad a cambio del trabajo dado a la red de la criptomoneda. La dificultad es una medida de cuánto trabajo se requiere para minar o generar un bloque. Un bloque es minado al encontrar el número (*nonce*) que produce un *hash* (una cadena de caracteres alfanuméricos) que satisface la condición del *hash* de bloque.

La recompensa de bloque es la cantidad otorgada al primer minero o grupo de mineros que encuentren el *nonce* que satisface la condición del *hash* de bloque (también llamada dificultad). En el bloque genesis, la recompensa de bloque comenzó en 50 bitcoins, pero está programado para reducirse a la mitad cada 210.000 bloques. Al momento de escribir esto, estábamos en el bloque número 485,227, lo que significa que la actual recompensa de bloque está fijada en 12,5 bitcoins.

Algo de historia

Blockchain y Bitcoin fueron diseñados e implementados por primera vez por un individuo o grupo de individuos bajo el seudónimo Satoshi Nakamoto. La idea se publicó por primera vez a través de una lista de correo de criptografía el 31 de octubre de 2008 en el documento "Bitcoin: A Peer-to-Peer Electronic Cash System". La primera implementación fue publicada por Satoshi el 9 de enero de 2009.

El bloque génesis se estableció el 3 de enero de 2009 a las 18:15:05 GMT. La primera transacción fue el 12 de enero de 2009 de Satoshi a Hal Finney y se registró en el bloque 170.

El 5 de octubre de 2009, New Liberty Standard publicó un tipo de cambio que establecía el valor de bitcoin en 1 USD = 1.309,03 BTC. Para ello, utilizaron una ecuación que incluía el costo de la electricidad necesaria para ejecutar una computadora que generaba bitcoins.

El 6 de febrero de 2010, se creó la primera casa de cambio de divisas en línea que aceptaba bitcoins. Fue llamado "Bitcoin Market".

El 22 de mayo de 2010, una de las primeras y más renombradas transacciones del mundo real con bitcoins tuvo lugar cuando Laszlo Hanyecz, un programador de Jacksonville, Florida, pagó 10.000 bitcoins por una pizza. En ese momento, el tipo de cambio puso el precio de compra de la pizza en alrededor de 25 USD.

Beneficios de estas tecnologías

Muchos expertos en criptomonedas han expresado en libros y entrevistas la sensación al haber oído hablar de Bitcoin y *Blockchain* por primera vez. La mayoría de ellos comparten una primera sensación de escepticismo, un sentimiento de que tal cosa no podría existir, que es demasiado bueno para ser verdad. Es realmente difícil de creer que una moneda pueda existir sin un banco central o una entidad central que la regule y defina su validez. Aún más difícil de entender es cómo tendría algún valor si no existe físicamente y no hay nadie que asegure su valor. La verdad es que las criptomonedas como bitcoin están diseñadas como redes sin confianza donde las políticas económicas se expresan claramente en su algoritmo, son verificables y son prácticamente irrompibles. Los expertos en criptomonedas no confiaron ciegamente en estas nuevas tecnologías, no sólo aceptaron o rechazaron su concepto; en su lugar, un profundo estudio y análisis les llevó a reconocer su valor y relevancia en el actual mundo globalizado.

Los desarrolladores de estas tecnologías previeron un sistema en el que no se requeriría un órgano de gobierno centralizado. Las criptomonedas son autosostenibles precisamente porque, entre otras cosas, hay un conjunto de recompensas otorgadas a los guardianes de la red, garantizando así que haya más incentivos económicos para aquellos que deciden jugar por las reglas que apara aquellos que intentar actuar contra la red. Este concepto descentraliza los datos, el consenso, y por lo tanto su existencia, haciendo que las criptomonedas y los sistemas basados en cadenas de bloques sean autosuficientes. Dadas estas características únicas de las criptomonedas y el *blockchain* podemos empezar a entender sus beneficios para la sociedad.

En primer lugar, permiten la existencia de una red capaz de mover valor de manera rentable, oportuna y segura. Esta es una herramienta con la cual los bancos están comenzando a experimentar, ya que un día podría reemplazar la infraestructura costosa y relativamente insegura que tienen que utilizar para sus transacciones electrónicas.

La tecnología del *blockchain* también permite la existencia de un repositorio de datos seguro donde no se necesita confiar en la moralidad de su guardián o en su capacidad para mantenerlo privado y seguro. Esto crea valor al reemplazar confianza por conocimiento. Podemos ver lo importante que puede ser esta tecnología en un momento en que grandes *hacks* y fugas de datos se están convirtiendo en noticias semanales.

Esta nueva tecnología trae verdadera responsabilidad, transparencia y bajo costo a asuntos delicados tales como: gestión de identidad, votación, representación, privacidad de datos, remesas, crowdfunding, trazabilidad, propiedad intelectual, consolidación de datos sanitarios, propiedad legal, compartición de recursos y muchos otros.

Por ejemplo, el Banco Central Europeo está investigando el uso de *blockchain* para mejorar sus propios sistemas que ayudan a movilizar dinero y activos en toda Europa.

El banco suizo UBS también está experimentando con Ethereum para crear "bonos inteligentes". Como explica Claudio Lisco, Gerente de Innovación de UBS: "Uno de nuestros primeros experimentos con los contratos inteligentes resultaron en el desarrollo de un "bono inteligente". Hemos creado una aplicación en la Plataforma Ethereum que puede recrear la emisión de un bono, cálculo de intereses, pagos de cupones y procesos de maduración. En este modelo, no hay necesidad de intermediarios pre y post-transacción ya que el software en *blockchain* fue configurado específicamente para manejar automáticamente el flujo de información y dinero entre el emisor y el comprador".

Otro proyecto digno de mención es la solución de trazabilidad sobre el *blockchain* de IBM en colaboración con Walmart. Actualmente en fase piloto, el proyecto tiene como objetivo proporcionar un sistema de alimentos más seguro, más asequible y sostenible, de acuerdo con Frank Yiannas, Vicepresidente de Seguridad Alimentaria de Walmart. El Sr. Yiannas también explica que "no creemos que la trazabilidad sea la meta, creemos que la transparencia es el objetivo final, *blockchain* nos dará la capacidad no sólo de seguir de donde vienen los alimentos, sino de cómo fue su producción, si se produjo de manera segura, si se produjo de manera responsable, y si fue cultivado de manera sostenible".

Uno de los mejores ejemplos es el proyecto piloto denominado "Building Blocks" del Programa Mundial de Alimentos de las Naciones Unidas (WFP), donde se utilizó la criptomoneda Ethereum para distribuir ayudas a 10.000 refugiados sirios en el campamento Azraq de Jordania usando contratos inteligentes. Estos cupones o monedas están programados para vincularse a los datos biométricos de la retina de los usuarios con el fin de detener el fraude y la falsificación.

Según Robert Opp, Director de Innovación y Gestión del Cambio del WFP: "A través de *blockchain*, pretendemos reducir los costos de pago, proteger mejor los datos de los beneficiarios, controlar los riesgos financieros y responder más rápidamente durante las emergencias. Utilizar *blockchain* puede ser un salto cualitativo no sólo para el WFP, sino para toda la comunidad humanitaria".

Riesgo para los consumidores

A medida que los consumidores se empoderan más a través de la tecnología, la cual les permite reducir a 0 el número de intermediarios para un servicio particular, también se les transfiere a ellos toda la responsabilidad. Esto es particularmente cierto para los usuarios de criptomonedas. Para los nuevos usuarios es difícil entender que el olvido una contraseña podría significar perder completamente el acceso a sus valiosos activos.

Los usuarios que no quieran manejar la responsabilidad podrían decidir contratar los servicios de un proveedor de servicios de *fintech* para desempeñar el papel de un banco. Normalmente, este servicio tendría un precio menor porque el proveedor de servicios no tendrá que ejecutar y mantener la costosa infraestructura que tienen los bancos tradicionales.

El verdadero perjuicio para los consumidores comienza cuando tratan con proveedores abusivos que se aprovechan de la falta de conocimiento del consumidor y de una legislación a menudo inexistente o muy genérica. El abuso puede venir en formas simples como esquemas Ponzi, robo y sobrecargos, o más complejos como altcoins pre-minadas, creación de contratos inteligentes amañados o venta de acciones de empresas con un plan de negocios falso a través de ofertas iniciales de monedas (ICOs por sus siglas en inglés).

Una oferta inicial de monedas (ICO) es un mecanismo de recaudación de fondos que negocia fichas a futuro a cambio de criptomonedas de valor líquido inmediato. Las ICO permiten a su creador evitar el riguroso y regulado proceso de recaudación de capital.

Cada día, estafadores crean nuevas formas de engañar a los consumidores y no hay duda de que las criptomonedas están convirtiéndose en una nueva herramienta en su arsenal. La complejidad del tema y la presencia constante en las noticias sobre su potencial de inversión hacen que sea más fácil para los estafadores ocultar sus verdaderas intenciones.

Desde la perspectiva de una agencia de protección al consumidor, una forma de mitigar el riesgo de las criptomonedas para los usuarios/consumidores es a través de la educación. En primer lugar, las agencias deben exponer claramente cuán complejos son realmente los conceptos y los mecanismos. Segundo, deben transmitir el mensaje de que las criptomonedas y el *blockchain* son tecnologías aún en su infancia, que su valor monetario es altamente volátil y que hay muchas personas especulando. En tercer lugar, deben indicar claramente que la participación en el mundo de las criptomonedas no es recomendado sin una profunda comprensión técnica y económica. Cuarto, y lo más importante, sería deseable que los organismos de protección del consumidor se convirtieran en una fuente confiable de información sobre estas nuevas tecnologías para los consumidores que buscan comprender sus beneficios, riesgos y mecanismos en detalle. Para este propósito, las agencias necesitan fortalecer sus capacidades en el área.

Otra forma de mitigar los riesgos sería proporcionar insumos y cooperar con otras instituciones gubernamentales pertinentes en la creación de una legislación específica de criptomonedas. Esta legislación podría proporcionar las herramientas necesarias para proteger a los consumidores en situaciones complejas.

Camino a seguir: políticas para la protección del consumidor

Es difícil saber a dónde nos llevará esta nueva tecnología porque parece estar creando continuamente una infinita variedad de posibles caminos. Los gobiernos y las grandes empresas están tratando de explotar el poder del *blockchain* para poder aprovecharse de él, manteniendo, al mismo tiempo, el control. Sin embargo, esto será en sí mismo un desafío, ya que la esencia de esta tecnología reside en su transparencia y en la inherente falta de control.

No hay duda de que las criptomonedas y el *blockchain* revolucionarán la forma en que interactuaremos en el futuro, de la misma manera que lo hizo la creación de Internet y la World Wide Web. Si tenemos algo que aprender de la llegada de nuevas tecnologías disruptivas es que el proceso de adopción tiende a ser caótico, experimental y peligroso.

Aunque los Estados podrían optar por prohibir las criptomonedas o el *blockchain* en general, sería tan imposible ilegalizarlas como lo sería declarar Internet ilegal. Ya que la prohibición no es una opción práctica, los Estados deben entonces encontrar una forma de educar a sus ciudadanos y regular estas nuevas tecnologías para asegurar la protección de sus consumidores.

Las instituciones nacionales e internacionales deben crear medios de entendimiento (educación), marcos regulatorios (eficientes) y herramientas prácticas (por ejemplo, software de fuente abierta) para que la sociedad pueda beneficiarse de estos grandes inventos y para mitigar, al mismo tiempo, los posibles riesgos.

Antes o mientras se actualice o se cree e implemente una regulación, las instituciones deben poder utilizar los sistemas legales y judiciales existentes para proteger a los consumidores. Para ello, las criptomonedas deben ser reconocidas como moneda, bien o servicio. Este reconocimiento oficial es vital para que las agencias de protección al consumidor puedan actuar.

Por ahora, las regulaciones gubernamentales referentes a las criptomonedas están destinadas principalmente a evitar el blanqueo de capital y la financiación de actividades terroristas. Esto se hace principalmente exigiendo a los proveedores implementar las reglas KYC (*know-your-customer*). De hecho, es una manera eficaz de proteger los intereses del gobierno, pero deja a los consumidores parcialmente expuestos y entregando sus datos a nuevos pequeños proveedores que en algunos casos tienen prácticas de ciberseguridad laxas.

Para mitigar estos riesgos, las agencias de protección al consumidor deben establecer o continuar implementando políticas para la protección de los datos y privacidad de los consumidores (artículo 14 h de las Directrices).

Las Directrices mencionan cómo las empresas deben proteger la privacidad de los consumidores; su artículo 11(e) establece que "las empresas deben proteger la privacidad de los consumidores mediante una combinación de mecanismos adecuados de control, seguridad, transparencia y consentimiento en lo relativo a la recopilación y utilización de sus datos personales". Al mismo tiempo, las empresas deben "facilitar información completa, exacta y no capciosa sobre los bienes y servicios, términos, condiciones, cargos aplicables y costo final para que los consumidores puedan tomar decisiones bien fundadas" (artículo 11 (c)).

Por consiguiente, los consumidores tienen derecho a un trato justo y, cuando no sea así, a una compensación. Los organismos de protección al consumidor deben poder garantizar esos derechos. Algunos, como la Comisión Federal de Comercio de los Estados Unidos y la Agencia de Asuntos del Consumidor de Japón, ya han empezado a hacerlo en el contexto de las criptomonedas. Las directrices y reglamentos existentes pueden ser y han sido utilizadas en casos de abuso del consumidor a través de criptomonedas.

Las agencias de protección al consumidor pueden seguir dependiendo de las Directrices de Protección al Consumidor de las Naciones Unidas (a partir de ahora, las Directrices) como primer paso hacia la regulación del uso de estas nuevas tecnologías con el fin de proteger consumidores.

Por un lado, las políticas nacionales destinadas a proteger a los consumidores deberían ser directamente aplicables a los casos en que se utilicen nuevas tecnologías. Todas las empresas de criptomonedas deberían, por lo tanto, proveer a la agencia pertinente información clara y oportuna

sobre ellas mismas, así como sobre los bienes y servicios ofrecidos(artículos 14 (b) y (c) de las Directrices).

Al mismo tiempo, los Estados deben promover la educación de sus ciudadanos, o al menos de los posibles consumidores, sobre las criptomonedas y las tecnologías involucradas. Estos programas educativos e informativos deben tener por objetivo capacitar a los posibles consumidores para que puedan tomar decisiones siendo conscientes de sus derechos y obligaciones, así como de las posibles consecuencias (artículo 42 de las Directrices).

Sin embargo, incluso si los Estados tienen una reglamentación clara aplicable a las empresas y a los consumidores dentro de su territorio, el problema sigue existiendo para las empresas establecidas fuera de la jurisdicción de cada Estado. En un mundo cada vez más globalizado, y en particular en los casos de tecnologías en línea, los consumidores hacen cada vez más transacciones con empresas en el extranjero. ¿Cómo puede un Estado proteger a sus consumidores cuando no tienen la jurisdicción requerida? Una forma de mitigar estos riesgos es fomentar el registro o la incorporación de proveedores de servicios de *blockchain* en el país. La recomendación directa y clara del Estado de que los consumidores utilicen únicamente empresas registradas o incorporadas a nivel nacional sería un incentivo para que las empresas se inscriban a nivel local o nacional, incluso si operan en el extranjero. Además, el Estado podría optar por establecer "jurisdicciones de confianza", que también podrían recomendar a sus consumidores. Las empresas interesadas en atender a los consumidores de un determinado Estado tendrían entonces un incentivo para ser registradas en ese Estado o en cualquiera de las jurisdicciones que este considerara oficialmente "de confianza".

Por otra parte, y entendiendo que el hecho de disponer de una regulación y/o guía no implica que no habrá abusos, conflictos o disputas, los Estados deben establecer mecanismos justos, transparentes, efectivos e imparciales de solución de controversias (artículos 37-41 de las Directrices). Estos mecanismos deben estar plenamente preparados para hacer frente a los casos de abusos a los consumidores vinculados a nuevas tecnologías como las criptomonedas. También deben estar equipados con los mecanismos necesarios para permitir que los consumidores busquen y obtengan compensaciones por los abusos sufridos. Estos mecanismos podrían ser administrativos o judiciales o seguir prácticas alternativas de solución de controversias. También se podría establecer una combinación de dos o varios de estos mecanismos (por ejemplo, el primer paso podría requerir la mediación entre las partes y, en caso de no funcionar, exigir el establecimiento de un sistema alternativo de resolución de controversias o someter la jurisdicción a un tribunal o corte nacional). Al contemplar estos mecanismos, deberían considerarse no sólo las controversias nacionales sino también transfronterizas. Al hacerlo, el Estado podría optar por establecer distintos mecanismos de solución de controversias para casos nacionales o internacionales.

En general, e independientemente de qué mecanismos de solución de controversias hayan sido elegidos por el Estado, éstos deben ser imparciales, justos, transparentes y accesibles para todos sin imponer costos ni demoras excesivas.

Es de vital importancia que nos adaptemos a la evolución del mercado para que podamos seguir salvaguardando y garantizando la protección del consumidor. No evolucionar con las nuevas tecnologías dejará a millones de consumidores desprotegidos ante cualquier abuso. Si no hay un marco legal aplicable a las nuevas tecnologías que incluya los derechos y obligaciones de los consumidores, habrá un vacío legal que protegerá a los abusadores en lugar de los abusados.