BANCO DE ESPAÑA
Eurosistema

Dirección General de Operaciones, Mercados y Sistemas de Pago

Enero 2014

Divisas o Monedas Virtual: *El caso de Bitcoin*

Sergio Gorjón

1. Introducción

Las divisas o monedas virtuales constituyen un conjunto heterogéneo de instrumentos de pago innovadores que, por definición, carecen de un soporte físico que los respalde.

Estas han adquirido un auge creciente a medida que se han ido popularizando los juegos en línea y las redes sociales ofreciendo lo que, aparentemente, resulta ser una solución de pago alternativa y mejor adaptada a las necesidades particulares del intercambio de bienes o servicios virtuales. Aspiran a ocupar en el ciberespacio un papel equivalente al que actualmente juega el efectivo en el mundo real.

A pesar de su proliferación, la atención del mercado se concentra en unas pocas iniciativas de gran éxito a escala mundial, entre las que destaca, por su presencia en los medios de comunicación, el caso de *Bitcoin*. La sección 2 de esta nota presenta las características básicas del *Bitcoin* y la sección 3 los principales riesgos asociados a su uso. Por su parte, el anejo I describe el proceso técnico de generación de *Bitcoin* y el segundo anejo ofrece algunas estadísticas gráficas.

2. Características básicas del Bitcoin

Bitcoin nace en 2009 con ambiciones elevadas: proporcionar a los ciudadanos un medio de pago que posibilite la ejecución de transferencias de valor rápidas, a bajo coste y que, además, no pueda ser controlado ni manipulado por gobiernos, bancos centrales o entidades financieras.

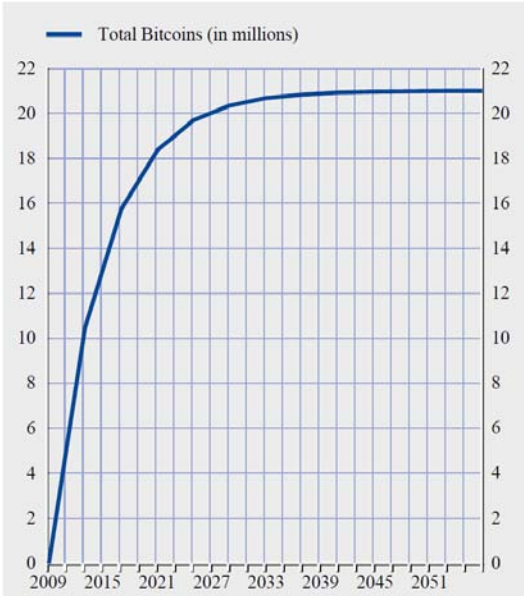
Bitcoin se basa en un modelo operativo descentralizado. Ello implica que no existe una autoridad que asuma la responsabilidad ni de su emisión ni del registro de los movimientos que se produzcan con la misma. En su lugar, se apoya en una red de distribución *Persona-a-Persona*, a través de nodos interconectados (ordenadores) que representan al colectivo de usuarios de esta moneda (se asemeja al intercambio descentralizado de archivos digitales, como música o películas, mediante *Bitorrent*).

Bitcoin puede considerarse, de facto, como una moneda internacional no anclada a ningún país en particular. En este sentido no estaría sometida en los pagos internacionales a las fluctuaciones de los tipos de cambio. Además, el *Bitcoin* proporciona a los comercios una garantía de cobro plena ya que cualquier operación, una vez ésta se haya validado, es irreversible.

La emisión de *Bitcoins*:

De forma simplificada, la emisión de *Bitcoins* no es el resultado de la decisión de una autoridad monetaria, o fruto de la concesión de préstamos. En su lugar, viene determinada por una rutina matemática preestablecida, con un calendario prefijado. En virtud de esta, se generan y distribuyen de forma aleatoria, a razón de unas 6 veces por hora, lo que se denomina lotes de *Bitcoins*. Cada lote acumula una cantidad no superior a las 50 *Bitcoins* y el tamaño del lote disminuye progresivamente, según una regla predeterminada, hasta alcanzar un monto total de las monedas en circulación que no llegue a exceder los 21 millones de "unidades".

Gráfico 1 – Calendario de emisión de *Bitcoins*



Fuente: Bitcoin (2011)

La incorporación efectiva de las “nuevas unidades monetarias” al sistema, con el objeto de que puedan ser utilizadas en transacciones posteriores, sigue un proceso cuya complejidad no es despreciable y debe ser conocida - y tenida en cuenta - por los potenciales usuarios de *Bitcoins*.

El método de incorporación se describe en el anejo I. Básicamente implica encontrar solución a un problema de cálculo no trivial. Cualquiera puede participar de este reto, descargándose un software cliente gratuito. Cuando uno de esos nodos (ordenadores) resuelve con éxito el problema lo comunica públicamente. Sólo cuando el resto de usuarios da por válida la solución tiene lugar la incorporación de las nuevas “monedas” a la cadena de operaciones históricas que figuran en un registro maestro o libro mayor del sistema. La tenencia de “unidades monetarias” de *Bitcoin* no figura bajo un nombre concreto, sino bajo una secuencia de números que constituyen la clave pública del usuario en cuestión.

La dificultad a la que se enfrenta cada ordenador se incrementa a medida que un mayor número de nodos compite entre sí por encontrar dicha solución, lo que sirve para controlar el patrón de crecimiento de la “masa de *Bitcoins*” resultante.

La transferencia de *Bitcoins:*

A la hora de transferir *Bitcoins* hace falta que el ordenante firme la transacción con su clave privada y que añada, además, la clave pública del beneficiario. Este sistema permite al receptor de los fondos verificar la legitimidad de la cadena de propiedad de la divisa. Sin embargo, por sí sólo, esto no garantiza que el ordenante no haya utilizado las mismas monedas múltiples veces en transacciones anteriores.

Con el fin de evitar esta situación, y teniendo en cuenta la naturaleza descentralizada del sistema, se ha arbitrado un procedimiento de carácter colectivo idéntico al descrito para la creación de las monedas. Cada cesión de *Bitcoins* será objeto de publicación en la red dejando que, de nuevo, sean los nodos que así lo deseen los que traten de hallar la solución a un sistema de ecuaciones complejo. Cuando un cliente verifica una transacción, lo pone en conocimiento de los demás para que, en su caso, puedan validarla.

Adquisición de *Bitcoins*:

Al margen del procedimiento descrito anteriormente (emisión de *Bitcoins*), se adquieren principalmente a través de un incipiente mercado secundario que se asemeja, operativamente, a los de negociación de divisas si bien, como es lógico, con un volumen diario de transacciones sensiblemente inferior[1].

En la práctica se trata de un mercado descentralizado OTC en el que las "unidades monetarias" de *Bitcoins* cotizan contra otras divisas, e incluso contra metales preciosos[2]. Dependiendo de los diferentes agentes que concurran a estas plataformas de negociación en cada momento, así tendrá lugar la formación de múltiples precios lo que los convierte en mercados altamente especulativos.

No obstante, este hecho constituye en sí mismo uno de los principales focos de interés para los tenedores de *Bitcoins.* Estos, en gran medida, más que por su condición como medio de pago, apuestan por la moneda virtual en razón a las oportunidades de rentabilidad a corto plazo que puedan derivarse de la volatilidad de los valores de canje.

3. Principales focos de preocupación

Sin menoscabo de sus potenciales beneficios, al igual que ocurre con otras divisas virtuales, *Bitcoin* presenta una serie de riesgos potenciales que, recientemente, han sido objeto de particular atención por parte de autoridades públicas de distintos países. Entre otras, las principales amenazas detectadas se podrían sintetizar de la siguiente manera:

a) Financiación de actividades ilícitas y/o blanqueo de capitales

Debido al carácter descentralizado del esquema, la transmisión del valor monetario se produce directamente entre las partes últimas de la operación (ordenante y beneficiario). No es necesario, por tanto, el concurso de un intermediario, administrador o repositorio central, lo que implica que no hay un único punto de contacto capaz de monitorizar el origen y destino de los saldos

[1] Otra posibilidad consiste en ser el beneficiario de donaciones o regalos fruto bien de campañas promocionales, bien de la cesión altruista de otros usuarios. Se trata de una fórmula mucho menos extendida que, en general, sólo permite obtener cantidades limitadas de la moneda.

[2] Entre las plataformas más activas se encuentran *Mt Gox*, *Gox*, *bitomatPLN*, *virwoxSLL*, *bitcoinGBP*, *bitmarketEUR*, *bcmPPUSD*, y *thUSD* (en conjunto, absorben más del 90% de todos los intercambios). También es posible la negociación bilateral entre particulares, existiendo para ello una red de contactos on-line propia de *Bitcoin*, a modo de tablón de anuncios virtual, con la relación de usuarios que manifiesta interés en intercambiar la divisa virtual (http://www.tradebitcoin.com/).

que se movilizan. Ello dificulta la identificación y alerta temprana ante posibles comportamientos sospechosos de actividades ilícitas[3].

Adicionalmente, la identidad de los tenedores goza de un elevado anonimato ya que las unidades de *Bitcoin* se almacenan en una "cartera virtual". Por simplicidad, el mantenimiento de estas "cuentas de depósito" suele externalizarse sobre proveedores terceros y la identidad de sus titulares se corresponde con una clave pública criptográfica equivalente a una larga secuencia de letras y números.

Estos dos factores unidos a la agilidad y sencillez con la que se pueden transferir los fondos entre dos puntos geográficos distantes han propiciado la aceptación de *Bitcoin* como medio de pago en páginas web que desarrollan actividades ilícitas como, por ejemplo, la venta de drogas, el fomento de la explotación sexual o la comercialización de pornografía infantil[4].

Además, se han observado igualmente indicios del uso de *Bitcoins* como vehículo para el fraccionamiento de operaciones de mayor importe en evitación de las obligaciones de reporte y mantenimiento de registro correspondientes a legislación internacional en materia de blanqueo de capitales y financiación del terrorismo.

Finalmente, en los casos en que proceda emprender acciones confiscatorias sobre los activos, una complejidad adicional reside en la dificultad para poder completar con éxito dichas actuaciones por encontrarse el correspondiente valor monetario codificado a través de claves asimétricas.

b) Efectos reputacionales negativos sobre los medios de pago digitales

El impulso al comercio electrónico mediante el desarrollo de soluciones de pago adaptadas a las especificidades del entorno on-line constituye una prioridad estratégica en la Agenda Digital Europea y en la de otras jurisdicciones. En esta coyuntura, el empleo generalizado de sistemas de pago electrónicos emergentes por parte de redes de crimen organizado puede

[3] Conviene señalar, no obstante, que por medio de una Orientación de marzo de 2013 emitida por el *Financial Crimes Enforcement Network* (FinCEN) del Departamento de Estado Norteamericano tanto las casas de cambio que efectúen operaciones de compra/venta de las divisas virtuales por dinero de curso legal como quienes actúen como "acuñadores" de *Bitcoins* tienen la obligación de registrarse como empresas prestatarias de servicios monetarios y cumplir con la normativa de blanqueo de capitales y financiación del terrorismo. Los usuarios que empleen *Bitcoins* exclusivamente como un medio de pago de bienes o servicios no se verán afectados por esta medida.

[4] Casos recientes en los EEUU son el cierre de *Silkroad* o *Freemdom Hosting*.

deteriorar la confianza del público en otras iniciativas, impidiendo así la consolidación de herramientas de pago con marcado potencial para dinamizar el crecimiento de la actividad en un mercado que, con tasas sostenidas de crecimiento de dos dígitos, observa aún importante oportunidades de expansión.

c) Tendencias oligopolísticas en la creación de la moneda virtual

A pesar de que, en principio, la filosofía de la red distribuida ofrece la posibilidad de que cualquier ordenador pueda participar activamente del proceso de creación de nuevas unidades de *Bitcoins*, la elevada capacidad computacional requerida implica que, en la práctica, esta actividad esté dominada por un reducido grupo de actores. Este escenario resulta propenso a la asignación asimétrica de unos recursos monetarios escasos que, en lugar de responder a los mecanismos de mercado (precio), favorece a aquellos con mejores conocimientos técnicos y mayor inversión en recursos informáticos.

d) Posibles transacciones fraudulentas

En la medida en que los protocolos sobre los que se asienta *Bitcoin* son desarrollos de software abierto, la implementación de sus diferentes versiones no tiene por qué producirse de manera uniforme entre todos los usuarios. Tampoco existen garantías de que éstas hayan sido suficientemente testadas antes de su puesta en producción. En consecuencia, desajustes en el ritmo de actualización de los paquetes informáticos al nivel de los distintos nodos de la red han ocasionado que, puntualmente, transacciones duplicadas hayan sido dadas por buenas en partes de la misma siendo, a posteriori, rechazadas en otros puntos de validación.

Adicionalmente, y a pesar de las mejoras anunciadas en materia de seguridad, el robo de unidades monetarias ha sido recurrente en diferentes plataformas de negociación de *Bitcoin,* así como la pérdida del valor monetario almacenado en los monederos fruto de circunstancias fortuitas como, por ejemplo, un borrado accidental de ficheros, la corrupción de los archivos o, simplemente, fallos aleatorios en un disco duro.

e) Impacto sobre la estabilidad de los precios

En teoría, el uso de *Bitcoin* podría llegar a afectar a la demanda del público respecto de los pasivos de un banco central[5] y acabar teniendo un impacto sobre el nivel general de precios de la economía y la efectividad de las medidas de política monetaria. No obstante hay dos factores que permiten matizar su incidencia y moderar la preocupación a este respecto:

- Por un lado, el canje de unidades de *Bitcoin* por moneda de curso legal debería tener un efecto de carácter nulo sobre el tamaño de los agregados monetarios en la medida en que responde a un proceso de sustitución de un medio de pago por otro alternativo.
- Por otro lado, de mantenerse realmente un patrón de crecimiento constante como el previsto, debería ser posible realizar previsiones razonablemente objetivas acerca de su evolución.

Aún así, conviene recordar que la volatilidad de la tasa de intercambio de *Bitcoins* respecto a divisas o metales preciosos aporta un considerable elemento de incertidumbre y que el nivel de aceptación y uso de estas unidades monetarias es difícil de anticipar, a priori, por encontrarse éstas aún en una fase de implantación temprana[6].

f) Impacto sobre la estabilidad financiera

Las plataformas de negociación privadas en las que resulta posible canjear *Bitcoins* por monedas de curso legal están marcadas por la elevada volatilidad de las cotizaciones debido a movimientos especulativos[7]. Esto menoscaba, obviamente, su condición como reserva de valor y perjudica su función como posible unidad de cuenta en las transacciones comerciales.

Asimismo, la transparencia, amplitud y profundidad efectiva de estos mercados resulta cuestionable por el escaso volumen de transacciones[8] así

[5] V.g cambios a la velocidad de circulación del dinero o impacto sobre los agregados monetarios (cantidad y precisión de las métricas).
[6] El desarrollo de soluciones innovadoras alrededor de los *Bitcoin* que faciliten su empleo, por ejemplo, en transacciones de compra presenciales podría, en teoría, llegar a producir efectos "*crowding-out*" sobre uso del efectivo.
[7] En el ejercicio 2013, *Bitcoin* ha llegado a experimentar variaciones del 70% de su valor de un mes a otro, llegando a superar los USD1.000 en su principal plataforma de negociación. Además, en el pasado, se han registrado episodios puntuales de hackers que, accediendo a estas plataformas han sido capaces de alterar artificialmente los precios.
[8] A modo de ejemplo, según datos de las principales plataformas de negociación, el tiempo medio observado en diciembre para completar el case de oferta y demanda se sitúa en torno a los 40 minutos.

como por las condiciones en que se ejerce su gestión: éstos no tienen un carácter regulado ni están, por el momento, sujetos a algún tipo de control por parte de las autoridades públicas.

Además, al no garantizarse legalmente la convertibilidad de estas unidades monetarias, la confianza de los usuarios en el valor de la moneda depende, fundamentalmente, de sus expectativas futuras así como de la credibilidad en la solvencia técnica del esquema. Una vez más, ésta aparece condicionada por la efectividad los mecanismos privados que se estén utilizando para prevenir la aparición de fraudes o errores.

Los usuarios de *Bitcoin* están, por tanto, expuestos a significativos riesgos operacionales y financieros (tanto de crédito como de liquidez), no existiendo tampoco claridad suficiente acerca del marco jurídico aplicable en caso de incidencias. A esto habría que sumar el tamaño de las consecuencias patrimoniales de materializarse alguno de estos riesgos ya que los saldos que se almacenan en el monedero no están cubiertos por el Fondo de Garantía de Depósitos o institución equivalente.

En todo caso, por el momento, el potencial impacto material de los aludidos factores sobre la economía en general podría calificarse de reducido habida cuenta del escaso número de usuarios implicados y la poca granularidad existente en cuanto a los puntos de aceptación de las monedas virtuales.

g) Otros inconvenientes

Desde el punto de vista del fraude, *Bitcoin* presenta una importante debilidad en comparación a otros medios de pago extendidos en el mundo online como pudieran ser las tarjetas. Por su configuración a modo de cadena de transacciones, el traspaso de *Bitcoins* entre usuarios es firme e irreversible, lo que impide poder disfrutar de un mecanismo de protección equivalente al derecho de reembolso.

No obstante, para paliar esta deficiencia, el propio ecosistema ha propiciado la aparición de una serie de servicios paralelos que, en cierta medida, recuperan la figura de los intermediarios en el proceso. Así las cosas, estos nuevos

actores pueden bien actuar como depositarios temporales de los fondos, liberándolos una vez los compradores han recibido los artículos[9].

[9] No obstante, algunas de estas empresas han sido recientemente noticia por fallas importantes de seguridad que han permitido a hackers el robo de los fondos que mantenían en custodia lo que ha provocado un cierto pánico entre la comunidad de usuarios con la consiguiente pérdida de confianza en el nuevo instrumento.

ANEXO I – EL PROCESO TÉCNICO

La pieza fundamental sobre la que se asienta todo el sistema *Bitcoin* es la existencia de un registro público compartido de transacciones denominado "cadena de transacciones" o "*block-chain*" en su terminología anglosajona. Todas las transacciones confirmadas o validadas se incluyen en la cadena de bloques. Esta circunstancia permite que las nuevas transacciones puedan ser verificadas garantizando el buen fin de las mismas. La integridad y el orden cronológico de la cadena de bloques se asegura por el uso de criptografía asimétrica de suerte que toda tenencia de *Bitcoins* está asociada a una dirección que, a su vez, sirve de punto de origen o de destino de las posibles operaciones.

Técnicamente, esta dirección equivale al hash de la clave pública del usuario[10] y tiene la apariencia de una secuencia única y fija de caracteres alfa-numéricos similar a la del ejemplo siguiente: 15VjRaDX9zpbA8LVnbrCAFzrVzN7ixHNsC. Esta clave, junto con la correspondiente "llave" privada, se almacena en la aplicación de monedero de los usuarios que es, por otro lado, donde residen las "unidades monetarias" de *Bitcoins* a su disposición[11].

En consecuencia, cuando se desea transferir *Bitcoins* entre dos direcciones es necesario que el ordenante firme la transacción mediante su clave privada, proporcionando así una prueba matemática de que los fondos provienen de los propietarios de esas direcciones. La firma evita, además, que la transacción sea alterada por cualquier persona una vez que se ha emitido. Todas las transacciones son transmitidas entre los usuarios y confirmadas por la red en los siguientes minutos, a través de un proceso llamado minería.

La minería se activa a partir de los nodos (ordenadores) conectados al sistema con una periodicidad aproximada de 10 minutos en promedio una vez se ha comunicado al conjunto de la red la posible cesión. Cuando se trata de incorporar bloques por importes significativos es habitual que se espere para procesar varios bloques de forma acumulada. Esta circunstancia puede llevar aparejada una demora de hasta 60 minutos.

---

[10] Es el valor resultante de aplicar un algoritmo a dicha clave pública y en el que se recoge, de forma resumida, toda la información que sirve de input al algoritmo. Al deshacer la operación se puede identificar quién está detrás.

[11] En la práctica, con el fin de no limitar el uso de *Bitcoin* exclusivamente a usuarios avanzados que cuenten con una alta capacidad de proceso en sus ordenadores, existe también la posibilidad de subcontratar con terceros el servicio de almacenamiento del valor de dicho monedero (por ejemplo, *Flexicoin* o *Instant Wallet*). Al estar residiendo en los servidores de un tercero el acceso al mismo se realiza mediante un nombre y una contraseña de usuario. Esta modalidad ofrece además la ventaja de la ubicuidad puesto que el titular no queda limitado al dispositivo en el que almacenó inicialmente los fondos sino que puede acceder a los saldos de manera flexible desde cualquier otro lugar como, por ejemplo, un teléfono móvil.

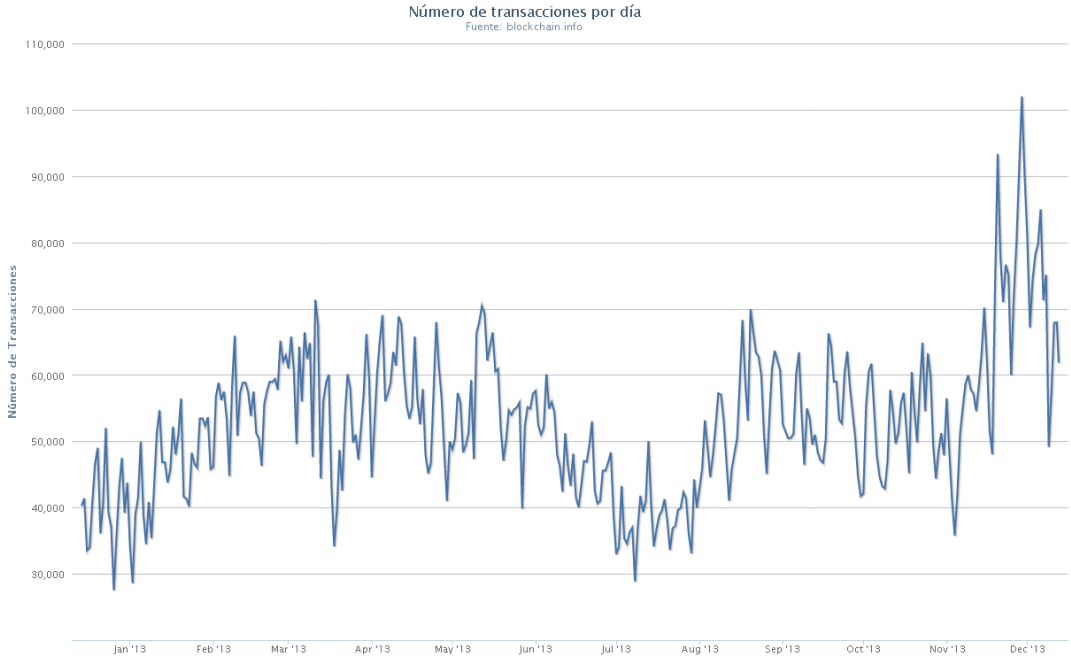
Para completar la validación de las transacciones los nodos ponen en marcha una secuencia de actuaciones encaminadas a encontrar la solución a un problema matemático no trivial. Se sigue el procedimiento de prueba y error, también conocido como “búsqueda por fuerza bruta”.

De una manera sencilla, de lo que se trata es de hallar el valor que toma una variable x de tal manera que se cumpla la siguiente expresión $h(x) \leq y$, donde la función h es una función hash conocida, así como el valor y. Cuanto menor sea el valor de y, mayor dificultad entraña el problema porque el universo de soluciones posible se acorta.

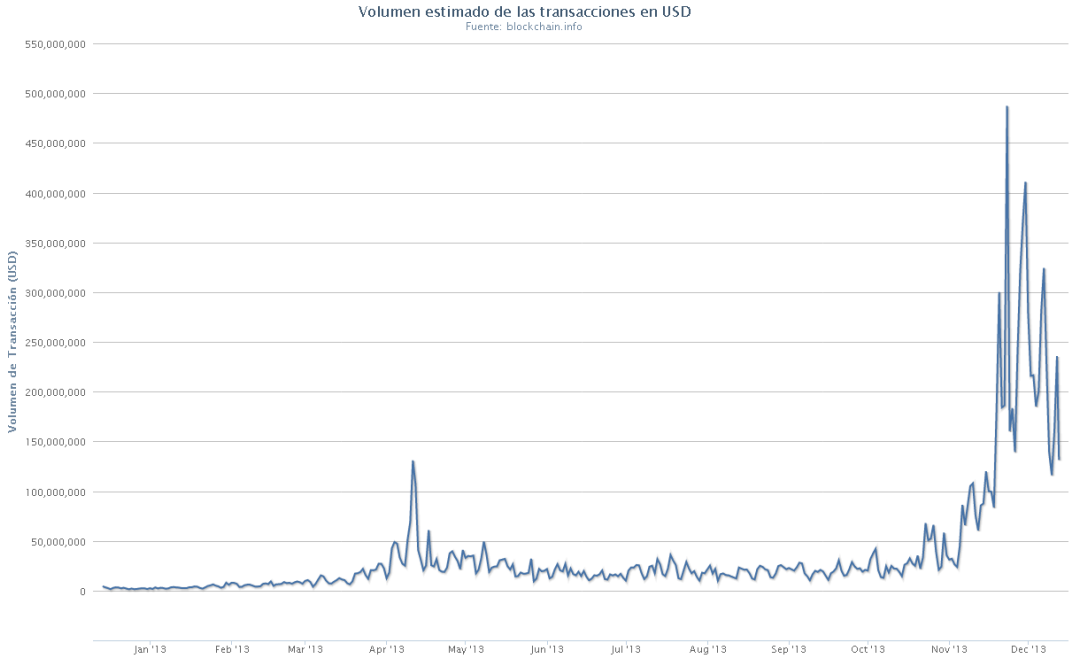
A efectos prácticos, los puntos de origen y destino de la red constituyen elementos integrales de los términos de la ecuación. El primer nodo que identifique este número x lo publicita al resto. La idea es que la comunidad de usuarios pueda verificar su validez y lograr, así, que dicha transacción se incorpore definitivamente a la cadena de operaciones. Una vez conocido el valor concreto de x que resuelve la ecuación, el proceso de comprobación resulta inmediato y accesible para cualquier persona. Sin embargo, por las propiedades de la función hash, la derivación de este número a partir del resultado de la misma no es tarea sencilla.

Conviene señalar que una de estas transacciones que debe ser objeto de confirmación es la propia acuñación de las monedas. En este caso, las nuevas unidades monetarias irán a parar al “minero” que ha resuelto la ecuación compleja. Del mismo modo, los mineros reciben una recompensa (en forma de *Bitcoins* o comisión) por completar con éxito uno de los problemas asociados a la transferencia de fondos.

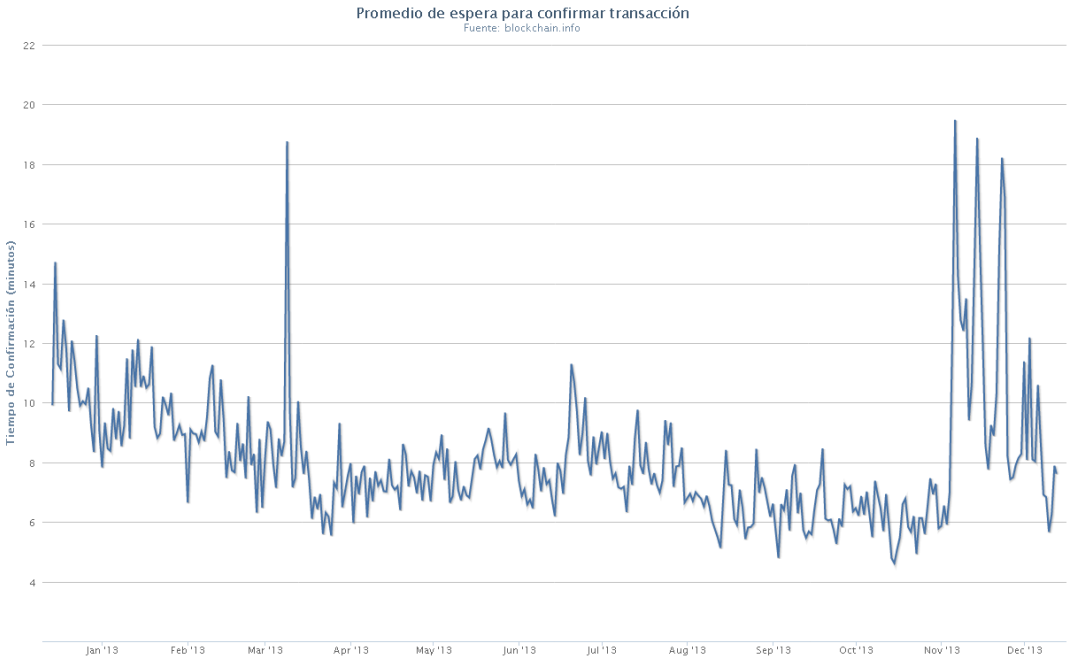
ANEXO II – ALGUNAS ESTADÍSTICAS



Fuente: Blockchain



Fuente: Blockchain



Fuente: Blockchain