AAT0381

UNIVERSIDAD CATOLICA ANDRÉS BELLO
FACULTAD DE CIENCIAS ECONÓMICAS Y SOCIALES
ESCUELA DE ECONOMÍA

ESTUDIO SOBRE LAS VARIABLES SOCIALES Y ECONÓMICAS QUE AFECTAN EL PRECIO INTERNACIONAL DE LAS BITCOINS. PERÍODO 2010-2014

Tutor: José Niño
Autor: Jesús Rangel Lares

Caracas, Mayo 2015

Agradecimientos

Aprovecho la oportunidad para hacer un agradecimiento a varias personas sin las cuales este trabajo no hubiera sido posible. A mis padres, a mis abuelos y a mi hermana por el apoyo durante este largo viaje. Al profesor José Niño por sus conocimientos y valiosas correcciones. A mis compañeros de clase por la amistad durante toda la carrera y por último, a Luis Egan, Eduardo Díaz y Tomás Rodríguez por su apoyo durante la realización del trabajo de grado.

ÍNDICE

INTRODUCCIÓN **6**
CAPÍTULO 1: EL PROBLEMA DE INVESTIGACIÓN **9**
1.1 Hipótesis 9
1.2 Objetivos 9
1.2.1 General 9
1.2.2 Específicos 9
1.3 Tipo de investigación 10
1.4 Glosario 11
CAPÍTULO 2: MARCO TEÓRICO **15**
2.1 Introducción a las bitcoins 15
2.1.1 ¿Qué son las bitcoins? 15
2.1.2 Historia de las bitcoins 15
2.1.3 Características generales 18
2.1.4 Características informáticas 20
2.1.5 Características económicas 22
2.1.5.1 Las bitcoins como dinero 22
2.1.5.2 Las bitcoins como activos de inversión 26
2.1.6 Características legales 30
2.2 Las bitcoins frente al oro 35
2.3 Las bitcoins frente a las monedas de curso legal 37
2.3.1 Ventajas 37
2.3.1.1 Costos transaccionales 37
2.3.1.2 Descentralización 39

2.3.1.3 Seguridad..... 41
2.3.2 Desventajas..... 41
2.3.2.1 51% Attack..... 42
2.3.2.2 Impuestos transaccionales..... 44
2.3.2.3 Goldfinger Attack..... 45
2.3.2.4 Ataques Informáticos..... 46
2.3.2.5 Shocks de demanda..... 48
CAPÍTULO 3: MARCO METODOLÓGICO..... 51
3.1 Formación de precio de las bitcoins..... 51
3.1.1 El mercado de producción de las bitcoins..... 51
3.1.2 Derivación de la función de producción individual..... 55
3.1.2.1 Función de ingreso..... 56
3.1.2.2 Función de costos..... 58
3.1.3 Análisis de la función de producción individual..... 61
3.1.3.1 Análisis de los costos..... 61
3.1.3.2 Análisis de los ingresos..... 65
3.1.3.3 Análisis del beneficio..... 68
3.1.3.4 La función de producción de bitcoins en competencia perfecta... 75
3.1.4 Derivación del costo global de crear una bitcoin..... 78
3.1.5 Análisis del costo global de crear una bitcoin..... 79
3.2 Mercado de oferta y demanda..... 82
3.3 Metodología econométrica..... 84
3.3.1 Descripción de las variables a utilizar..... 85
CAPÍTULO 4: ANÁLISIS DE RESULTADOS..... 91
4.1 Modelo de largo plazo..... 91
4.2 Modelo de corto plazo..... 92
CONCLUSIONES Y RECOMENDACIONES..... 95
BIBLIOGRAFÍA..... 97

ANEXOS **104**
Tabla 1 Anexos. Marco regulatorio de las bitcoins por país..... 105
Demostración 1..... 109
Demostración 2..... 111

Índice de Gráficos y Tablas

Gráfico 1. Cantidad de comercios aceptantes de bitcoins..... 23
Gráfico 2. Oferta total de bitcoins..... 25
Tabla 1. Beta de las bitcoins (β) con mercados de Estados Unidos..... 28
Tabla 2. Desempeño de las bitcoins frente a mercados de Estados Unidos.. 29
Tabla 3. Volatilidad de las bitcoins frente a mercados de Estados Unidos.... 29
Gráfico 3. Crecimiento porcentual de la oferta de las bitcoins 2010-2014..... 39
Gráfico 4. Proyección del crecimiento porcentual de la oferta de las bitcoins 2014-2018..... 40
Gráfico 5. Cuota de las pools de mining de bitcoins..... 43
Gráfico 6. Costos de corto plazo..... 62
Gráfico 7. Costo marginal de corto plazo..... 63
Gráfico 8. Costo marginal de Largo plazo..... 64
Gráfico 9. Ingreso de corto plazo..... 65
Gráfico 10. Ingreso marginal de corto plazo..... 66
Gráfico 11. Ingreso marginal de largo plazo..... 67
Gráfico 12. Beneficio de corto plazo 1..... 69
Gráfico 13. Beneficio de corto plazo 2..... 69
Gráfico 14. Beneficio de corto plazo 3..... 70
Gráfico 15. Beneficio de largo plazo 1..... 72
Gráfico 16. Beneficio de largo plazo 2..... 73
Gráfico 17. Beneficio de largo plazo 3..... 74

Gráfico 18. Beneficio en competencia perfecta..... 75
Tabla 4. Cantidad de descargas porcentuales del software de mining por país..... 80
Tabla 5. Costos energéticos por país..... 80
Gráfico 19. Precio de las bitcoins..... 86
Gráfico 20. Tamaño de la economía..... 87
Gráfico 21. Búsquedas en Google..... 88
Gráfico 22. Hash Rate..... 88
Gráfico 23. Nominal Broad Dollar Index..... 89
Gráfico 24. Dow Jones Index..... 90
Tabla 6. Tests de largo plazo..... 92
Tabla 7. Tests de corto plazo..... 94

INTRODUCCIÓN

Los avances tecnológicos de nuestra era han llegado a todos los rincones del mundo y la forma en la que se pueden llevar a cabo transacciones económicas no es la excepción.

El dinero ha evolucionado a través del tiempo y con él, los métodos de pago. Aun así, esta evolución no ha podido romper con algunos esquemas clásicos como el control del dinero en manos de bancos centrales o la posibilidad de hacer transacciones a cualquier parte del mundo en cuestión de minutos. Estos problemas parecían irresolubles hasta la década pasada cuando se empezaron a crear unas monedas virtuales basadas en una cadena de datos la cual las hace mucho más seguras.

Entre estas nuevas monedas virtuales creadas a finales de la década pasada, la que obtuvo más fama fueron las Bitcoins. Descentralizadas, fácilmente transferibles, pero poco valiosas, las bitcoins se mantuvieron en la clandestinidad durante varios meses hasta que, gracias a una creciente comunidad de usuarios, aceptación de algunas empresas y atención de los medios, empezaron a aumentar de precio.

Los cambios de precio fueron muy volátiles y en espacios de tiempo variados como semanas, meses o años. A principios del 2011 las bitcoins alcanzaron la paridad con el dólar, pocos meses después se cotizaban en 31$ cada una y a finales del año el precio se encontraba en 2$. Estos saltos en el precio no sólo se han dado en períodos largos como de un año, más

recientemente, a finales del 2013, las bitcoins pasaban de 198$ a 1120$ en menos de un mes, para luego caer a 747$ el mes siguiente.

Estos cambios no son producto de la casualidad, el aumento general de precios en períodos prolongados va de la mano con una mayor aceptación por parte de personas y empresas alrededor del mundo en los últimos 3 años, entre ellas se encuentran por ejemplo, Microsoft y Dell. Pero este factor no es suficiente para explicar algunos saltos en el corto plazo. La cobertura de los medios es un factor importante. Los gobiernos de cada país también juegan un papel a la hora de dictar leyes que permitan o prohíban el uso de las bitcoins en sus correspondientes países.

El problema de esta investigación se centra en cuáles son las variables que afectan en mayor medida el precio internacional de las bitcoins. Ciertas variables tienen una relación económica clara con el precio, otras como la atención de los medios, no tanto, pero pueden tener un impacto en el precio tan importante como las anteriores. Se busca identificar también los tipos de efectos de éstas variables, algunos pueden ser inmediatos y otros pueden ser visibles sólo en períodos largos de tiempo.

Este trabajo especial de grado contará con cuatro capítulos los cuales contienen la siguiente información:

• Capítulo I: se describe la hipótesis del trabajo, los objetivos generales, específicos y el tipo de investigación. Contiene un glosario con los términos más recurrentes para los lectores no familiarizados con el tema de las monedas virtuales en general.

• Capítulo II: consiste en una amplia introducción al mundo de las bitcoins desde 4 puntos de vista: generales, informáticos, económicos y legales. También incluye una breve historia, se explica cómo se producen las bitcoins y su estado actual. Se exponen las principales diferencias entre las bitcoins y el oro y entre las bitcoins y las monedas de curso legal de mayor circulación en el mundo.

• Capítulo III: se centra en la parte práctica de la investigación, se realiza un análisis desde el punto de vista de la producción y de las interacciones entre oferta y demanda para determinar cuáles serán las variables que formarán parte del modelo final. Se describe la metodología econométrica y también la relación y signo esperado de cada una de las variables.

• Capítulo IV: consiste en la exposición y análisis de los resultados obtenidos en el capítulo anterior.

CAPÍTULO 1: EL PROBLEMA DE INVESTIGACIÓN

1.1 Hipótesis:

Los cambios del precio internacional de las bitcoins durante el período 2010-2014 pueden ser explicados por variables tales como la cantidad de transacciones, la cobertura de los medios y el Dow Jones Index, entre otras.

1.2 Objetivos:

1.2.1 General:

Determinar cuáles son las variables que contribuyen en mayor medida a la formación del precio internacional de las Bitcoins tanto en el corto como en el largo plazo.

1.2.2 Específicos:

- Realizar una introducción acerca de las Bitcoins, su historia, características y cómo se producen.

- Seleccionar entre un universo de variables que afecten el precio de las Bitcoins las que se utilizarán en el estudio práctico y justificar porque se utilizaran cada una de estas variables.

- Llevar a cabo varias estimaciones econométricas para observar cómo afecta cada una de las variables seleccionadas al objeto de estudio.

- Evaluar la estructura de retardos temporales que tienen cada una de las variables con respecto al precio.

- Analizar si el precio de las Bitcoins se corresponde con diferentes teorías económicas de formación de precios.

- Considerar cual puede ser el desempeño que tendrán estas monedas en la economía mundial en el corto plazo.

1.3 Tipo de Investigación

El tipo de investigación de este trabajo es variado. Por una parte es exploratorio ya que las bitcoins son un fenómeno muy reciente y todavía no se conoce todo su potencial, además de que la naturaleza de las bitcoins puede cambiar en el futuro.

La investigación también es del tipo descriptiva ya que se ocupa gran parte del trabajo en enseñar al lector acerca de todo el universo de estas nuevas monedas virtuales y hacer un análisis de las variables a utilizar y porque se considera que son estas las que ayudan más a esta investigación.

Por último, se puede decir que la investigación es explicativa dado que se busca la relación causal de los cambios de precio de las bitcoins. Se llevará a cabo la realización de ciertos experimentos econométricos para así poder llegar a una conclusión acerca del tema en estudio.

1.4 Glosario:

Altcoin: monedas con el mismo protocolo de las bitcoins pero con algunas características diferentes, por ejemplo: Litecoin o Dogecoin.

ASIC: empresa que se dedica a producir hardware especializado para el mining de bitcoins.

Beta (β): es una medida de correlación de un activo con respecto a otro activo o a una cartera de activos.

Blockchain: cadena de datos donde se encuentra la información histórica de todas las bitcoins en circulación.

Bloque: grupo de bitcoins nuevas creadas, actualmente son de 25 cada uno pero cada cierto tiempo esta cantidad se reduce a la mitad. También incluye las nuevas transacciones.

BTC (฿): abreviación de bitcoin utilizada en las casas de cambio como unidad de cuenta.

Cartera: conjunto de direcciones pertenecientes a un usuario donde se almacenan las bitcoins.

Cliente: software donde se encuentra la información de la cartera virtual y se llevan a cabo las transacciones.

Cloud minning: servicio ofrecido por grandes empresas en el cual ellos alquilan su hardware para producir bitcoins. Esto le permite a otras personas entrar al mercado de producción sin poseer realmente un activo fijo.

Corto Plazo: para efectos de este estudio, el corto plazo comprende períodos menores a un año. En el caso de la producción de las bitcoins, el corto plazo es el período durante el cual los productores no pueden cambiar el activo fijo.

Cold Wallet: cartera de bitcoins que se encuentra en una computadora sin acceso continúo a internet lo que la hace mucho más segura que carteras virtuales normales.

Criptomoneda: moneda virtual.

Dirección: cuenta a donde se envían o donde se reciben bitcoins, una cartera puede contener varias direcciones.

Dificultad: nivel de complejidad de crear un nuevo bloque de bitcoins para los miners.

Dólar Australiano (₳): moneda de curso legal que se utiliza en Australia.

Double Bottom: patrón recurrente que exhibe el precio de algunos activos financieros el cual consiste en 2 picos negativos similares.

Double Top: patrón recurrente que exhibe el precio de algunos activos financieros el cual consiste en 2 picos positivos similares.

Double Spending: acción referida a utilizar las mismas bitcoins para realizar dos transacciones diferentes al mismo tiempo.

Dow Jones Index: índice bursátil que mide el desempeño de las 30 mayores empresas transadas en las bolsas de Estados Unidos.

Fiat Currency: moneda que no tiene ningún respaldo y su valor se basa en la confianza de las personas.

Gigahash: cantidad de hashes por segundo que puede realizar una computadora/miner/pool medido en billones.

Hash: proceso matemático que toma cierta cantidad de data y produce una cantidad de información de longitud fija.

Head & Shoulders: patrón recurrente que exhibe el precio de algunos activos financieros el cual consiste en 3 picos positivos, siendo el segundo mayor que el primero y el tercero.

Key: contraseña para acceder a la cartera virtual usando el cliente de bitcoins.

Largo Plazo: para efectos de este estudio, el largo plazo comprende períodos mayores a un año. En el caso de la producción de las bitcoins, el largo plazo es el período durante el cual los productores pueden cambiar el activo fijo.

Mining: proceso de generar nuevos bloques de bitcoins resolviendo problemas criptográficos.

Miner: puede referirse a las personas que llevan a cabo el mining o a un hardware especializado que realiza este proceso, por ejemplo ASIC Miners.

Mt Gox: una de las casas de cambio de bitcoins más famosas con sede en Japón, actualmente no se encuentra activa.

Nasdaq Composite: índice bursátil de Estados Unidos que incluye todos los valores que cotizan en el mercado Nasdaq.
P2P: interacción entre 2 o más usuarios que forman parte de una red informática.

Pool: grupo de usuarios que se juntan para combinar su poder de mining y tratar obtener el siguiente bloque de bitcoins.

Rama: blockchain alternativa que parte de la original la cual se crea cuando uno o más usuarios empiezan a crear bloques diferentes a los de otro grupo de usuarios. La rama más larga se convierte siempre en la blockchain oficial.

Satoshi: la unidad más pequeña en la que se puede dividir una bitcoin (0.00000001 bitcoins).

Silk Road: página web de venta de productos ilegales como armas o drogas la cual es conocida por aceptar y manejar un gran volumen de bitcoins.

Standard & Poors 500 (S&P): índice bursátil que se calcula en base a la capitalización de 500 grandes empresas que poseen acciones que cotizan en las bolsas Nyse o Nasdaq.

CAPÍTULO 2: MARCO TEÓRICO

2.1: Introducción a las bitcoins

2.1.1 ¿Qué son las bitcoins?

Las bitcoins son unas monedas virtuales creadas a partir del paper publicado por Satoshi Nakamoto (2008) las cuales pueden ser utilizadas mayoritariamente como una inversión dado sus rápidos cambios de valor o para adquirir productos en internet. A diferencia de otras monedas de curso legal, las bitcoins no son controladas por ningún banco central ni tampoco son la moneda oficial de ningún país en el mundo.

Al igual que otras "fiat currencies", no tienen ninguna garantía de cambio como lo tenían algunas monedas durante el uso de "El Patrón Oro", lo que quiere decir que su valor no está respaldado por ningún bien y que este se basa enteramente en la confianza que le tienen las personas que la utilizan.

2.1.2 Historia de las bitcoins

El 3 de Enero de 2009, apenas 2 meses después de la publicación del artículo *A Peer-to-Peer Electronic Cash System* (Nakamoto, 2008), se crea el primer bloque de la blockchain el cual contenía 50 bitcoins. Seis días después salió a luz pública el software oficial para realizar operaciones con estas monedas y se registró la primera transacción el 12 de Enero.

En octubre del mismo año New Liberty Standard publica la primera tasa de cambio referencial entre dólares y bitcoins fijándola en 1$ por 1,309.03 BTC. Esta tasa fue determinada en parte calculando los costos energéticos de crear las bitcoins utilizando una computadora. Varios meses pasaron hasta que en Mayo de 2010 se lleva a cabo la primera transacción que involucraba bienes pagados con bitcoins. La operación cerró en 10.000 bitcoins por el equivalente a 2 pizzas, las cuales tenían un precio equivalente de 25$ (0,0025$ por btc)

El 18 de Julio, abre en Japón Mount Gox, una de las casas de bolsa más importantes hasta la fecha. Un mes después, gracias a una vulnerabilidad en el sistema que no verificaba las transacciones correctamente, billones de bitcoins son creadas al instante. Pocas horas más tarde el error fue hallado y arreglado gracias al uso de un fork en la blockchain el cual reflejaba que dichas monedas creadas maliciosamente nunca existieron. Hasta el día de hoy, este ha sido el único gran error que se ha encontrado en el protocolo de las bitcoins.

En febrero de 2011 se alcanza por primera vez la paridad con el dólar; ese mismo mes es creada la página web de venta de productos ilegales en bitcoins conocida como Silk Road. Durante el resto del año las bitcoins salen a la luz pública varias veces gracias al anuncio de Wikileaks de aceptarlas como donaciones y la redacción de un artículo por parte de la revista TIME, entre otros acontecimientos.

El 24 de abril de 2012 es anunciado SatoshiDice, el sistema de apuestas más famoso de bitcoins. El mes siguiente este servicio fue el responsable de hasta la mitad de las transacciones totales en un mismo día. El 28 de noviembre la cantidad de bitcoins nuevas creadas por bloque cae de 50 a 25.

Durante el 2013 las bitcoins sufren grandes aumentos de precio. El primero de Abril el precio supera por primera vez la barrera de los 100$. A éstos aumentos de precio también se sumaron regulaciones mayoritariamente por parte del gobierno de Estados Unidos; como por ejemplo la del Financial Crimes Enforcement Network (FinCEN), el cual estableció que los miners de monedas virtuales estarían sujetos a registros y otras obligaciones legales.

Durante el mes de Octubre es arrestado Road Ross William Ulbricht en San Francisco, California por presuntamente ser el dueño de Silk Road. Ese mismo mes fue inaugurado en Vancouver, Canadá, el primer cajero de bitcoins el cual permitía vender y comprar bitcoins a personas de la comunidad. El 17 de noviembre se registró en Mount Gox la operación con el mayor precio hasta ahora con un valor de 1216.73$ por cada moneda.

Luego del vertiginoso aumento de precios durante el año 2013, las bitcoins entraron al mapa mundial como una inversión creíble; a pesar de hacerlo, el 2014 fue en general un año negativo para el precio. Las bitcoins abrieron en 770$ y cerraron el año alrededor de los 300$. Pero no todo fueron malas noticias, podría decirse que el 2014 más que un año de crecimiento, fue un año de asentamiento para las bitcoins.

La entrada de China al mercado significó un movimiento importante ya que la decisión durante el mes de abril de no prohibir las bitcoins a sus bancos locales significó un repunte que duró varios meses. La cantidad de cajeros de bitcoins alrededor del mundo aumentó de manera exponencial. La aceptación por parte de empresas también aumentó, incluyendo algunas importantes como Paypal, Dell y Microsoft.

La peor noticia fue el cierre de Mt. Gox, la casa de cambio más grande de bitcoins, lo que significó un duro golpe para el precio. La directiva explicó que fueran víctimas de un ataque cibernético lo que significó grandes pérdidas de bitcoins para sus usuarios. Hoy en día se especula que la quiebra fue producto de un "inside job" y que tales ataques cibernéticos fueron una excusa.

2.1.3 Características generales

¿Cuáles son sus características actuales?

La cantidad de Bitcoins actualmente en circulación es de 13.475.575 cada una con un valor actual de 341,08$ (7 de noviembre de 2014). Las bitcoins no existen físicamente, solo virtualmente, se almacenan en unas carteras virtuales las cuales son, en teoría, totalmente anónimas ya que para transferir fondos de una cuenta a otra solo se necesita la dirección. La cantidad de cuentas activas de este día fueron 163.094 para una cantidad total de 89.542 transacciones (una transacción no siempre es únicamente entre 2 cuentas)

El uso de bitcoins en mercados ilegales

Una característica fundamental de las bitcoins es la anonimidad de las transacciones. Gracias a esto se ha vuelto uno de los más conocidos métodos de pago utilizados en transacciones ilegales a través de internet. El caso más conocido es Silk Road, una página web a la cual sólo se puede acceder anónimamente y tiene a la venta cualquier cantidad de productos ilegales tales como armas o drogas, en un catálogo muy amplio.

La anonimidad de las bitcoins ha causado que sean altamente utilizadas para negocios ilícitos, sin contar además la evasión de impuestos. Cuando

anteriormente enuncié que las carteras virtuales son en teoría totalmente anónimas es porque en la práctica no lo son en un 100%. Entes gubernamentales de Estados Unidos han logrado en más de una ocasión descifrar la identidad del dueño de una cartera de bitcoins el cual las utilizaba en transacciones ilegales (Meiklejohn Pomarole, Jordan, Levchenko, McCoy, Voelker, Savage 2013).

Diferencias fundamentales con otras monedas virtuales anteriores

Lo que hace a las bitcoins diferentes a cualquier moneda virtual creada insatisfactoriamente en el pasado es que se venció el reto de evitar el doble gasto (double-spending) utilizando el sistema propuesto por Nakamoto (2008). Esto se logró gracias a la creación de una cadena de datos (blockchain) donde se almacena toda la información de las bitcoins. Si una persona trata de reflejar una transacción que en verdad no sucedió, esta será rechazada dado que no se encuentra en las blockchains de los demás usuarios.

¿Quiénes son los principales usuarios de las bitcoins?

La adopción de las bitcoins ha sido entre usuarios muy diversos. Dado que una de las mayores ventajas de estas monedas es su anonimidad, se puede inferir que existe un gran número de usuarios que las utilizan con fines ilegales como lavado de dinero y compra de bienes ilícitos.

Un segundo grupo de entusiastas son los ingenieros informáticos o amantes de la programación en general. Ya que el protocolo de las bitcoins es enteramente computacional, estos usuarios fueron unos de los primeros en adquirir estas monedas virtuales.

Los inversionistas llegaron mucho después, mayoritariamente en el 2013, dado el rápido aumento de precio que tuvieron las bitcoins en el transcurso de ese año. Un último grupo podrían ser usuarios de filosofía anarquista, los cuales están en contra de que los gobiernos y bancos centrales controlen algo tan importante como el dinero.

De acuerdo con el estudio de Matthew Wilson & Aaron Yelowitz (2014), el cual tuvo como objetivo determinar cuáles de estos grupos son los que en la práctica tienen la mayor cantidad de usuarios activos en la comunidad de las bitcoins; existe evidencia robusta para decir que los criminales y los entusiastas de la programación superan, por ahora, a los inversionistas y a los anarquistas.

2.1.4 Características informáticas

Actualmente los bloques contienen 25 bitcoins cada uno, pero esto no siempre ha sido así, ni lo será en el futuro. Al principio cada bloque contenía 50 bitcoins, lo que significa que la oferta tanto porcentual como nominalmente crecía mucho más rápido que ahora. En noviembre de 2012, los bloques empezaron a dar 25 bitcoins cada uno, esto no fue al azar. Cada 210.000 bloques nuevos creados, la cantidad de bitcoins que contiene cada nuevo bloque cae a la mitad.

Se espera que para mediados de 2016 esta cantidad caiga de 25 a 12.5 bitcoins y así sucesivamente hasta que se alcance la oferta máxima la cual está fijada en 21 millones. Dado el paso al que se irán creando (cada 4 años aproximadamente la oferta crecerá a la mitad), la oferta llegará al máximo estipulado aproximadamente en el año 2140 según cálculos de diversos usuarios de la comunidad[1].

[1] https://en.bitcoin.it/wiki/Controlled_supply

Estos nuevos bloques de bitcoins son considerados una recompensa por "defender" al sistema y además de eso, aceptar las transacciones realizadas en la comunidad. Dichos bloques se crean cada cierto tiempo, en promedio cada 10 minutos, dependiendo de la cantidad de hardware, medido en hashes para obtener un bloque, que se dedique al mining.

La creación de bloques de bitcoins no es una ciencia 100% exacta, esta depende del proceso de descifrar un algoritmo matemático de cierta dificultad para cual se emplea poder de procesamiento (Hardware). Cada bitcoin puede ser dividida en 10^{-8} partes lo cual garantiza que pueda ser utilizada hasta en las transacciones más pequeñas.

Al día de hoy (31/12/2014), y con un precio de 320$ por bitcoin aproximadamente, solo los miners en lugares de bajo costo energético o con un gran volumen de mining (hardware) pueden obtener una cantidad de ingresos considerable. Los miners individuales dentro de los Estados Unidos en cambio, suelen tener dificultades para obtener un retorno de inversión en el largo plazo.

El mining es una parte esencial del protocolo de seguridad de las bitcoins, ya que este es el que se encarga de alargar la blockchain, haciendo más difícil que se produzcan ataques como el de un cartel que controle el 51% del hashrate. Para evitar que el mining caiga y que las bitcoins sean más vulnerables, existen los costos transaccionales los cuales se pagan a las personas que se encargan de crear las bitcoins como un incentivo extra para que sigan manteniendo la comunidad segura, sobre todo después de que la obtención de nuevas monedas por sí solo no sea rentable. Más adelante serán explicadas las consecuencias del diseño de este sistema con más profundidad.

2.1.5 Características económicas

2.1.5.1 Las bitcoins como dinero

Características del dinero

Para que un bien sea considerado dinero debe cumplir con los siguientes criterios principales: Medio de cambio, Unidad contable y Depósito de valor.

- Medio de cambio: el dinero debe poder ser utilizado para obtener otros bienes de manera eficiente. A su vez debe ser fácil de almacenar y de transportar. Las bitcoins cumplen éstas características indudablemente; pueden ser utilizadas para obtener bienes e incluso son más fáciles de almacenar y transferir que el dinero convencional.

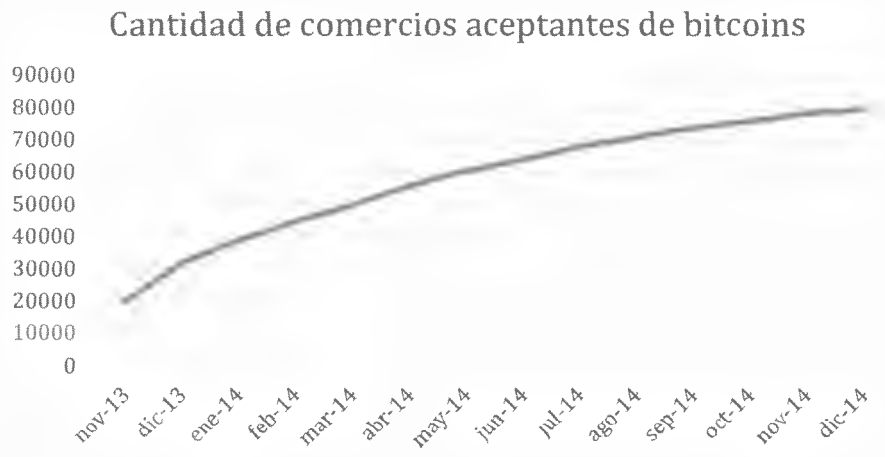
- Unidad de cuenta: todos los bienes de la economía deben poder ser medidos utilizando el dinero, lo que implica que éste debe ser divisible. Además, el dinero debe poder comparar el valor de 2 o más bienes entre ellos. Las bitcoins son capaces de medir el precio de los bienes de la economía utilizando como referencia el precio en dólares (u otras monedas) de dicho bien y el tipo de cambio entre dólares y bitcoins.

- Depósito de valor: dado que el dinero no se utiliza inmediatamente, si no que puede ser guardado para realizar intercambios en el futuro, éste debe ser capaz de conservar su valor en el tiempo. Ésta es la característica del dinero que más le cuesta cumplir a las bitcoins. A pesar de ser un bien no perecedero y que tampoco se puede gastar con el

tiempo, el valor de las bitcoins respecto a los demás bienes de la economía históricamente ha sido muy volátil.

Además de los criterios anteriores, el dinero también debería cumplir con los siguientes:

- Generalmente aceptado: Si muchos agentes de la economía no aceptan el dinero, este pierde una de sus características esenciales como medio de pago. Las bitcoins, a pesar de que todavía no son ampliamente aceptadas, cada vez son más las empresas que ofrecen productos o servicios a cambio de bitcoins u otras monedas virtuales.



Extraído de Coindesk[2] el cual fue construido a partir de la data de bitcoinpulse[3].

- Portátil: el dinero debe ser fácilmente transportable y transferible. Gracias a la tecnología, las bitcoins cumplen ambas características, sobre todo en países desarrollados.

[2] http://www.coindesk.com/state-bitcoin-2015-ecosystem-grows-despite-price-decline/
[3] http://bitcoinpulse.com/

- Almacenable y duradero: poder ser guardado y ser no perecedero son otras características importantes del dinero. Las bitcoins son fácilmente almacenadas en carteras digitales y de esta forma no pueden perecer o desaparecer.

- Divisible: para que el dinero pueda ser utilizado como unidad de cuenta este debe ser fácilmente divisible. En el caso de la mayoría de las monedas virtuales, estas cumplen esta característica mejor que el dinero de curso legal ya que son divisibles entre cualquier valor y hasta 8 decimales en el caso específico de las bitcoins.

Composición y aumento de la oferta

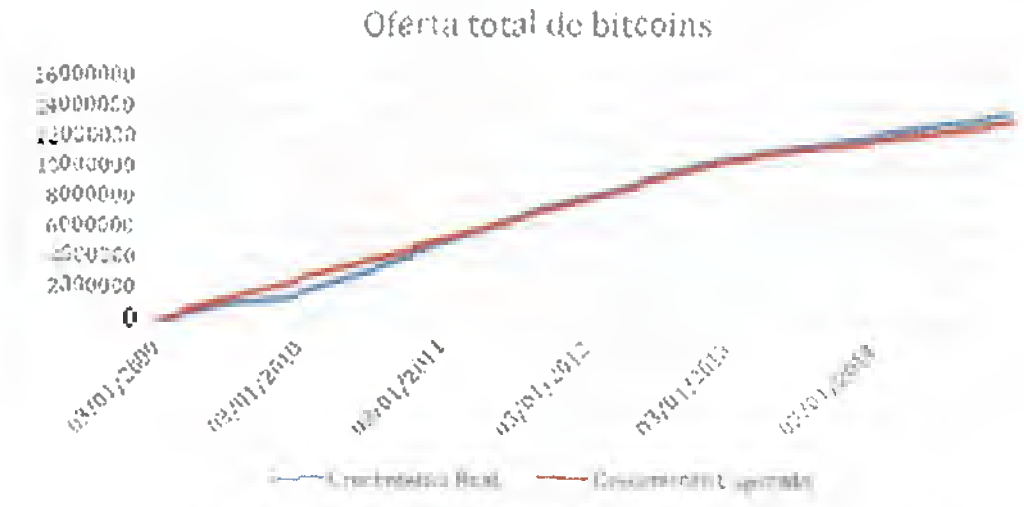
Las bitcoins, al igual que otras monedas de curso legal, tienen una oferta que no se mantiene estática a través del tiempo. Ésta oferta obedece a una función que fue determinada al momento de la creación de las bitcoins y sólo puede ser cambiada bajo un gran consenso de usuarios. Lo anterior implica que las bitcoins son una moneda descentralizada, ningún actor individual en la comunidad tiene el poder de modificar la función de crecimiento de la oferta.

A diferencia de cualquier otra moneda de importante circulación en el mundo, las bitcoins son la única moneda que proporciona información detallada y exacta de oferta y distribución cada segundo.

Como se dijo anteriormente, las bitcoins se crean por bloques, actualmente cada uno contiene 25, pero dicha cantidad cae a la mitad cada cierto tiempo, en promedio cada 4 años (este promedio podría variar en un

futuro). Esto quiere decir que, tanto porcentualmente como nominalmente, el aumento de bitcoins en circulación es decreciente en el largo plazo.

El crecimiento esperado de la oferta, determinado por un algoritmo matemático en el protocolo de las bitcoins es el siguiente: 1 bloque de bitcoins aproximadamente cada 10 minutos, dicho bloque contiene actualmente 25 bitcoins, esto significa 150 nuevas bitcoins cada hora y 3600 cada día. Gracias a ésta fórmula, se puede estimar con bastante certeza la oferta de las bitcoins en cualquier momento determinado.



Como puede observarse en el gráfico, el crecimiento de la oferta real, a pesar de estar muy cerca del crecimiento esperado, no es el mismo ya que el protocolo de las bitcoins se ajusta cada 2 semanas para que el crecimiento real se acerque al esperado. Este rezago en el ajuste crea ciertas diferencias entre la oferta esperada y la real. Actualmente (31/12/2014) esta brecha se encuentra entre el 2 y 3%.

2.1.5.2 Las bitcoins como activos de inversión

Las bitcoins han sido clasificadas legalmente más como activos de inversión que como un medio de pago. Esto puede evidenciarse más adelante en el cuadro de regulación legal por países que fue incluido en los anexos. Dicha clasificación se debe a varias razones, principalmente la volatilidad del tipo de cambio BTC/USD y a la cantidad de bitcoins que se mantienen en las cuentas sin utilizarse, esperando que el precio aumente en el futuro (Glaser, Florian, et al, 2014).

Dado que las bitcoins son consideradas monedas pero también activos de inversión, es necesario hacer un análisis financiero desde ambos puntos de vista.

Las bitcoins en el mercado mundial de monedas

La mayoría de las monedas de curso legal de flotación libre o controlada, a pesar de jugar un papel importante en sus economías locales, también participan en un mercado mundial de monedas. Este mercado es muchas veces responsable de determinar las tasas de cambio nominales entre diferentes monedas.

En este mercado mundial se pueden utilizar 2 tasas de cambio nominales, por ejemplo $/€ y $/£, para determinar una tercera implícita: €/£* (o £/€*). Normalmente, gracias a la existencia del arbitraje, este tasa de cambio implícita, en este caso €/£* (o £/€*), sigue muy de cerca a la tasa de cambio nominal €/£ (o £/€). Al analizar la tasa de cambio de las bitcoins frente a otras monedas, se puede observar que este comportamiento también se da en esta moneda virtual.

De acuerdo con el análisis de Jacob Smith (2014), tomando la tasa de cambio $/฿ y dividiéndolo entre los tasas de cambio €/฿, £/฿ y ₳/฿ se obtienen las tasas de cambio implícitas. Se puede observar que la tasa de cambio implícita sigue a la de los mercados convencionales gracias a la existencia de ocasiones de arbitraje.

Smith acota que el mercado de bitcoins es muy pequeño comparado con los mercados convencionales que se utilizaron en el estudio ($/€, $/£ y $/₳). Esto significa que cambios en los precios relativos (implícitos) en bitcoins pueden estar explicados por cambios en los mercados convencionales. Por otro lado, cambios en los precios relativos en bitcoins no son los suficientemente significativos como para afectar los mercados convencionales.

Por último, Smith concluye que casi la mitad de los cambios en las tasas de cambio implícitas en bitcoins pueden ser explicados por cambios en los mercados convencionales. Este comportamiento es común cuándo se analizan monedas de mercados pequeños frente a otros de mercados más grandes.

Tomando en cuenta la fortaleza del dólar frente a la de las bitcoins y que el precio de las bitcoins esta denominado en dólares, es necesario incluir en este estudio una variable que tome en cuenta cambios en la unidad de medida.

Las bitcoins en los mercados financieros

Uno de los aspectos más importantes de las bitcoins es ¿Qué será de ellas en el futuro? Dado que podrían fracasar rotundamente, o ser un éxito sin precedentes, las bitcoins suelen ser víctimas de una gran especulación.

Este componente especulativo ha sido evidenciable históricamente por una gran volatilidad la cual aproximadamente de un 8% diario lo que significa una volatilidad anualizada aproximada de un 127%. Para tener una idea de que tan alta es, la volatilidad diaria de los índices NASDAQ, Dow Jones y S&P en el mismo segmento de tiempo fue cercana al 1% diario (alrededor de un 15% anualizada).

Para observar de cerca la relación de las bitcoins y los tres mercados nombrados anteriormente se realizó esta tabla que contiene los β históricos y por año de las bitcoins con respecto al Dow Jones Index, Nasdaq y S&P[4].

Beta de las bitcoins (β) con mercados de Estados Unidos					
Mercados	β 20/07/10-2014	β 2011	β 2012	β 2013	β 2014
Dow Jones Index	0,41	0,83	0,44	-1,14	-0,45
Nasdaq	0,25	0,60	0,37	-1,21	-0,11
S&P	0,35	0,77	0,44	-1,16	-0,30

Observando la tabla, se puede concluir que el Dow Jones Index es el que ha tenido la mayor correlación con las bitcoins.

En los mercados de bitcoins (en este caso casas de cambio), estas monedas virtuales han tenido el siguiente desempeño. Este fue calculado tomando el promedio geométrico de los cambios diarios porcentuales y luego anualizándolo.

[4] Series de precio extraídas de https://research.stlouisfed.org/fred2/releases

Desempeño de las bitcoins frente a mercados de Estados Unidos					
Mercados	20/07/10-2014	2011	2012	2013	2014
Bitcoin	540,38%	1316,67%	220,85%	5506,96%	-57,8%
Dow Jones Index	13,42%	5,53%	7,32%	26,5%	7,52%
Nasdaq	18,75%	-1,8%	16,04%	38,32%	13,4%
S&P	15,75%	0%	13,52%	29,6%	11,39%

La volatilidad diaria promedio, la cual fue calculada tomando la desviación típica de los cambios diarios porcentuales, fue la siguiente:

Volatilidad de las bitcoins frente a mercados de Estados Unidos					
Mercados	20/07/10-2014	2011	2012	2013	2014
Bitcoin	7,99%	10,52%	4,26%	9,26%	4,65%
Dow Jones Index	0,88%	1,32%	0,74%	0,64%	0,69%
Nasdaq	1,09%	1,59%	0,95%	0,77%	0,89%
S&P	0,97%	1,47%	0,80%	0,70%	0,72%

En este cuadro se puede evidenciar claramente la alta volatilidad histórica que ha tenido el precio de las bitcoins.

De acuerdo con los estudios de Devavrat Shah & Kang Zhang (2014) y Jonathan Donier & Julius Bonart (2014), las bitcoins exhiben patrones financieros que son observables en otros comodities en sus respectivos mercados tales como Head & Shoulders, Double Top, Double Bottom, entre otros.

Al comparar las bitcoins con otros activos, según el estudio de Briere, Oosterlinck & Szafarz (2013) suceden varias cosas curiosas. La primera es que las bitcoins están muy poco correlacionadas con otros activos. El mayor beta observado fue de apenas un 20% con el oro. El segundo aspecto curioso es que dada esta baja correlación con otros activos y una alta tasa de retorno, la inclusión de bitcoins en portafolios de inversión significó una mejora importante en la relación riesgo/beneficio de dichos portafolios.

Como se explicó al principio del análisis financiero, la volatilidad puede estar relacionada con una alta especulación, ya que existen varios incentivos económicos para comprar bitcoins y esperar a que aumenten de precio:

- El crecimiento de la oferta, el cual es nominal y porcentualmente cada vez menor.
- La probabilidad de que se conviertan en un sistema importante de pagos y transacciones.
- El eventual aumento de los costos de producción (el cual puede influir bastante en el precio) cada vez que haya un Halve (caída inmediata de la tasa de crecimiento de la oferta a la mitad).
- La probable existencia de burbujas que hagan aumentar el precio exponencialmente en el corto plazo, dado que es un bien ligado al área de la informática afectado en gran medida por la cobertura de los medios.

2.1.6 Características legales

La legalidad de las bitcoins en cada país es un tema que ha generado mucha polémica. La sobrevivencia de las monedas virtuales en el largo plazo

puede depender mucho del marco regulatorio que se les aplique. Leyes muy estrictas podrían eliminar ventajas como los bajos costos transaccionales.

La decisión final de cada gobierno acerca del uso de las bitcoins en su país puede depender de varios factores; siendo el más importante la probabilidad de que las bitcoins puedan ser un factor disruptivo en la economía local. Los países con política monetaria constantemente expansiva, como suele ser el caso de países en vías de desarrollo, son los que deberían preocuparse por la adopción de bitcoins por parte de sus ciudadanos, ya que estos puedes estar buscando una moneda de refugio.

Un ejemplo de esto es Argentina, el cual es el país con una de las mayores cantidades de empresas aceptantes de bitcoins en el mundo[5]. La pérdida de valor de su moneda, que según cifras locales ha sufrido un mínimo de 10% de inflación durante los últimos 3 años, es un incentivo para que sus ciudadanos busquen refugio en monedas virtuales.

Tomando en cuenta lo anterior, se puede afirmar que los países con economías inestables presentan incentivos para prohibir las bitcoins, ya que las personas de dicho país pueden preferir las monedas virtuales como refugio a en vez de las monedas de curso legal (por ejemplo la crisis bancaria de Chipre en el 2013[6]).

Pero la capacidad de ser una moneda disruptiva en una economía no es el único factor a tener presente a la hora de decidir el marco legal de las bitcoins. Para monedas consideradas fuertes como el dólar o el euro, que podrían no ver las bitcoins una amenaza, todavía está el problema del lavado de dinero y de la evasión de impuestos.

[5] http://www.coindesk.com/bitcoin-thriving-argentinas-black-market-economy/
[6] http://money.cnn.com/2013/03/28/investing/bitcoin-cyprus/

Dado que las bitcoins no son la única moneda virtual existente, prohibir las bitcoins no disminuiría el lavado de dinero por esta vía. Prohibir las monedas virtuales en su totalidad tampoco significaría un gran golpe para estas actividades ilícitas ya que estas existen desde mucho antes de que se crearan las monedas virtuales. En todo caso, la cooperación entre casas de cambio, servicios de pago y gobiernos locales podría ayudar a disminuir esta actividad.

Para el caso específico de la evasión fiscal, este tampoco debería ser un gran problema para economías desarrolladas. Si las bitcoins son utilizadas en transacciones, estas deben ser registradas por las empresas que prestan servicios o venden productos; al igual que sucede hoy en día con las transacciones que se hacen con dinero en efectivo (que son mucho más difíciles de rastrear que las bitcoins).

Cabe destacar que para aceptar bitcoins como parte de una transacción las empresas deben hacer pública la dirección donde recibirán dichas monedas. Con ésta dirección cualquier ente oficial puede saber cuántas bitcoins recibió dicha empresa lo que hace incluso más difícil la evasión fiscal.

Una tabla con los países que han tomado alguna posición, total o parcial, frente a las bitcoins se encuentra en los anexos (Tabla 1 Anexos).

Los entes gubernamentales de cada país no son los únicos que podrían legalmente afectar, positiva o negativamente, al desarrollo de las bitcoins. La postura que pudiese tomar un organismo internacional de gran importancia, como el Fondo Monetario Internacional, puede determinar la aceptación futura de estas monedas.

Las bitcoins frente al FMI

El Fondo Monetario Internacional (FMI) es un organismo internacional que busca regular las transacciones económicas internacionales para promover un aumento del comercio en el mundo. Su objetivo principal es asegurar la estabilidad monetaria internacional siguiendo de cerca los tipos de cambio y las transacciones entre países.

Cada vez que un país se subscribe al FMI debe pagar una cuota que varía según el tamaño de su economía en proporción con la del resto del mundo. Al menos 75% de dicha cuota debe ser pagada en la moneda de curso legal del país que desea subscribirse, el otro 25% puede ser pagado en monedas de amplia circulación como el dólar, euro, yen o libra esterlina.

Gracias a este sistema de reservas, el cual es usado también para realizar préstamos, el FMI puede contrarrestar ataques especulativos y mantener los tipos de cambio estables. Cuando ocurren ataques especulativos hacia cierta moneda, por ejemplo, al yen, dicha moneda se debilita frente a otra, por ejemplo, el dólar. Si el banco central de dicho país no puede contrarrestar el ataque, ya que no tiene una reserva de dólares lo suficientemente grande como para poner estos en circulación y reducir la oferta de yenes, este suele acudir al FMI para que le haga un préstamo en dólares.

Aquí es donde entra la capacidad disruptiva de las bitcoins, dado que ni los bancos centrales, ni el FMI poseen reservas en bitcoins, un ataque especulativo utilizando monedas virtuales hacia monedas de libre circulación no podría ser contrarrestado utilizando los métodos convencionales.

El FMI obtiene sus reservas en diversas monedas de países miembros. Las bitcoins en sí no son miembros del FMI ni podrían serlo bajo el régimen actual dado que las membresías son exclusivamente para naciones-estado (artículo 2 del FMI). Además, las negociaciones del FMI son hechas exclusivamente con instituciones financieras oficiales de cada país. Las bitcoins, al ser totalmente descentralizadas, no poseen ninguna entidad financiera oficial.

Siguiendo a Plassaras (2013), existen 2 vías para que el FMI incorpore a las bitcoins a su régimen. La primera sería otorgándole control indirecto sobre las bitcoins modificando una provisión existente. La segunda vía sería modificando drásticamente los artículos y condiciones del FMI para permitir la entrada de un actor, en este caso las bitcoins, que no sea una nación estado.

La primera vía puede llevarse a cabo modificando la sección 5 del artículo 4, de tal forma que se les exija a los países miembros un cuota de su subscripción en bitcoins (u otras monedas virtuales) para poder contrarrestar un ataque especulativo en bitcoins contra otra moneda. Para realizar una reforma de este tipo se necesitarían 3 quintas partes de los miembros del FMI con un poder de voto de al menos 85%.

La segunda vía sería modificando la sección 2 del artículo 2, la cual también requiere las 3 quintas partes de los miembros del FMI con un poder de voto de al menos 85% para llevar dicha reforma a cabo. En este caso el FMI en vez de obtener las bitcoins a través de los países miembros, lo haría a través de tenedores de bitcoins. Para hacer esto el FMI tendría que reconocer a las bitcoins u otras monedas virtuales como cuasi-miembros, lo cual sería ventajoso para ambas partes. Por un lado el FMI obtendría fondos en bitcoins y

por otro lado las bitcoins obtendrían mayor reconocimiento mundial y legitimidad.

Ambos casos requieren que los usuarios de bitcoins estén dispuestos a venderle sus monedas a sus gobiernos locales, bancos centrales o al FMI directamente, lo cual podría no ser muy viable. Primero, por el concepto deflacionario que tienen las bitcoins, los usuarios podrían no querer vender sus monedas a menos que estos organismos ofrezcan un precio muy superior al del mercado. Segundo, los ideales de la comunidad de usuarios de bitcoins son anti controles y probablemente no quieran a un organismo como el FMI poniendo en circulación bitcoins que se encontraban fuera del mercado justo cuando el valor de la criptomoneda está aumentando.

2.2 Las bitcoins frente al oro

Uno de los comportamientos más recurrentes en el mundo de las monedas virtuales es comparar dichas monedas con el oro u otros minerales. Aunque existen algunas similitudes, también existen grandes diferencias:

Semejanzas:

- La creación se lleva a cabo a través del mining, en el caso del oro normalmente en minas o ríos y en el caso de las bitcoins, en computadoras.

- No existe un monopolio total en cuanto a la creación, o el mining, del oro o de las bitcoins. Aunque en algunos países la minería de oro puede ser una actividad regulada por el estado (tanto la actividad en sí

como los precios), este no es el caso de todos los países, a diferencia del monopolio de la emisión de las monedas de curso legal. La producción de bitcoins, a excepción de países donde están legalmente reguladas, es totalmente descentralizada.

- Existe un costo de producción intrínseco importante tanto en el mining de oro como de bitcoins. En el caso de las monedas o billetes de curso legal, el costo de producción suele ser ínfimo.

- Ambos poseen un valor más allá de su valor como commodity. En el caso del oro es su valor industrial, en el caso de las bitcoins, es el valor de poder realizar transacciones rápidamente y de bajo costo a cualquier parte del mundo.

Diferencias:

- El crecimiento de la oferta de bitcoins es cuasi-fija. La del oro, en cambio, depende de la extracción de este mineral de la tierra.

- Las bitcoins son fácil y rápidamente transferibles a cualquier parte del mundo, el oro no.

- Las bitcoins son fácilmente divisibles, hasta 8 decimales, a diferencia del oro.

- Es posible utilizar las bitcoins como método de pago para obtener otros bienes al igual que con monedas de curso legal. El oro en cambio, dado su precio (en onzas) y su poca divisibilidad, suele ser poco usado para realizar transacciones.

- El precio del oro es mucho más estable que el de las bitcoins y por ende, suele ser utilizado como un bien de resguardo.

- El oro está sometido a un marco legal importante en varios países, a diferencia de las bitcoins.

2.3 Las bitcoins frente a las monedas de curso legal

2.3.1 Ventajas

Las bitcoins tienen ciertas ventajas con respecto a las monedas de amplio uso actuales tales como el dólar, el euro o el yen. Dichas ventajas pueden clasificarse en tres grupos: costos transaccionales, descentralización y seguridad.

2.3.1.1 Costos transaccionales

Las transacciones en bitcoins ocurren casi inmediatamente, sin importar las personas involucradas o el lugar del mundo en que estas se encuentren. En promedio estas transacciones toman unos 10 minutos para hacerse efectivas y pueden hacerse en cualquier momento del día.

De acuerdo con el cliente actual, una transacción puede no pagar costos transaccionales si se cumplen las siguientes condiciones:

• Pesa menos de 1.000 bytes
• Es menor a 0,01 bitcoins (alrededor de 4$)
• La transacción tiene una prioridad mayor a cierta cantidad[7]

[7] https://en.bitcoin.it/wiki/Transaction_fees

Si no se cumplen estas condiciones, las transacciones deben pagar una tasa actual de 0,0001 btc por cada 1.000 bytes. Cabe destacar que:

- La mayoría de las transacciones son menores a 1.000 bytes así que el promedio de costos por transacciones es de 0,0001 bitcoins (aproximadamente unos 4 centavos de dólar a un precio de 350$ por bitcoin).

- Una misma transacción puede estar compuesta de varios inputs y outputs.

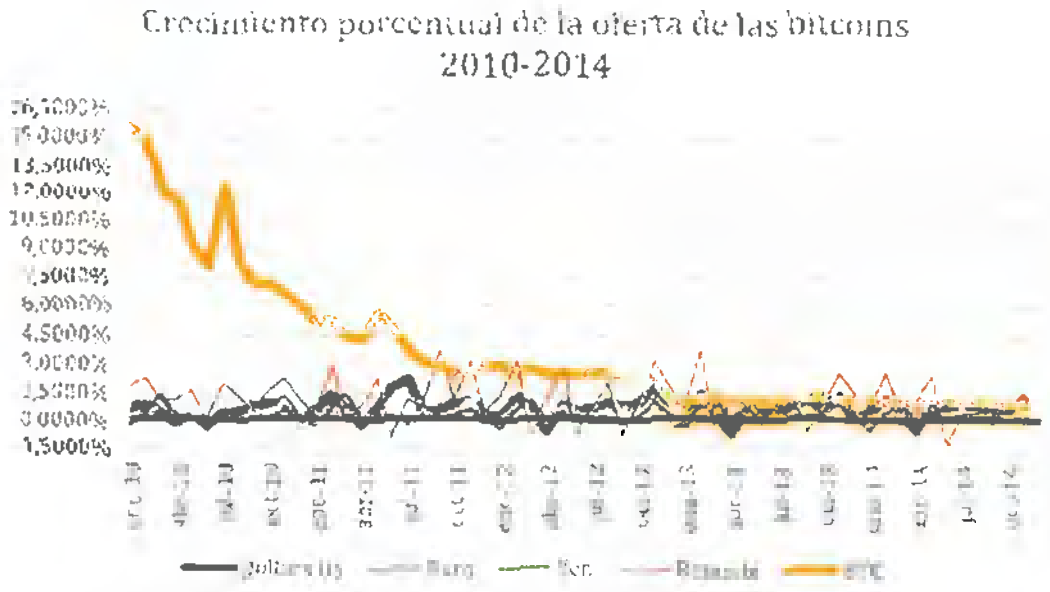
Tomando en cuenta lo anterior, hoy en día, realizar transacciones con bitcoins implica unos costos mucho más bajos que los de los bancos, sobre todo para realizar transferencias entre diferentes países. Los costos transaccionales entre bancos americanos y cualquiera del exterior oscilan entre los 20$ y 70$ aproximadamente, y el tiempo de espera suele ser de al menos 2 días hábiles. Esto demuestra que las bitcoins son más eficientes en la velocidad en que se ejecutan las transacciones y también en cuanto a su bajo costo.

Es necesario recordar que estos costos transaccionales pueden aumentar en un futuro y actualmente son sostenibles gracias a los ingresos devenidos de la creación de nuevas bitcoins. De acuerdo con Kerem Kaşkaloğlu (2014), estos costos aumentarán en un futuro no muy lejano para poder sostener la caída de la rentabilidad del mining y proteger a la comunidad.

2.3.1.2 Descentralización

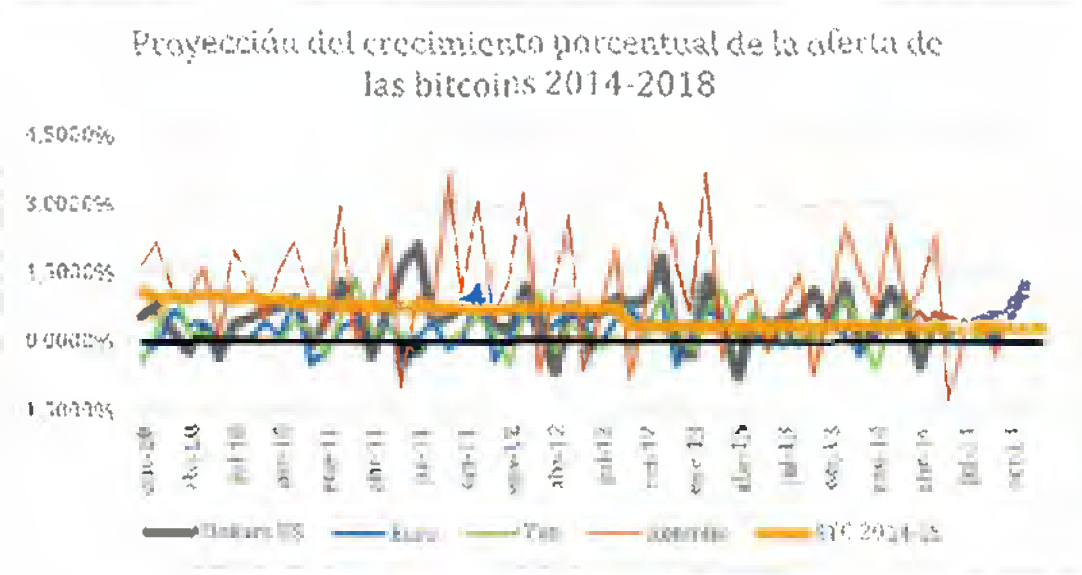
Al no estar controladas por ningún ente, las bitcoins no pueden sufrir de pérdida de valor por un aumento excesivo de la oferta como ha ocurrido con muchas monedas de curso legal en varios paises a lo largo de la historia, sobre todo en paises subdesarrollados. La tasa de crecimiento de la oferta de las bitcoins es menor cada año lo que nos lleva a pensar que en el futuro las bitcoins deberian ganar valor con respecto al dólar u otras monedas en el largo plazo dado que, ceteris paribus, su masa monetaria aumentará más lentamente.

En el siguiente gráfico se puede observar cómo ha sido el crecimiento porcentual de la oferta de las bitcoins desde el año 2010 al año 2014 comparado con el de las monedas de curso legal con las cuales se negocian más estas monedas virtuales.



El crecimiento de la oferta de las bitcoins tiene una tendencia clara decreciente y una volatilidad en el corto plazo bastante baja. Como fue dicho en el capítulo 2, el crecimiento de la oferta puede pronosticarse con mucha certeza gracias a que la fórmula de crecimiento de la oferta de las bitcoins es pública

En el siguiente gráfico fue cambiado el crecimiento de la oferta de las bitcoins entre 2010 y 2014 por el pronóstico entre el 2014 y el 2018 y para efectos de comparación no se cambió el de las demás monedas (2010-2014).



Evidentemente, en el futuro las bitcoins tendrán una tasa de crecimiento mucho menor y mucho menos volátil de lo que la tienen las monedas como el Euro, Dólar, Yen o Renminbi hoy en día.

Ésta rigidez de la oferta puede ser una ventaja a la hora de realizar pronósticos para el futuro de las bitcoins y de evitar caer en escenarios inflacionarios, pero es una desventaja a la hora de enfrentar shocks de

demanda ya que la oferta no puede ajustarse para garantizar la estabilidad del precio. Éste punto será desarrollado en la sección de desventajas.

La comparación anterior es sólo entre las bitcoins y algunas monedas entre las más fuertes del planeta. Con respecto a monedas de países del tercer mundo la balanza se encuentra mucho más a favor de las bitcoins de lo que ya se encuentra en esta comparación.

2.3.1.3 Seguridad

Las bitcoins, al no existir físicamente, tampoco pueden ser robadas usando métodos tradicionales. La única forma en que una persona ajena a una cartera virtual obtenga acceso a ella es con la contraseña, y existen diversas formas muy efectivas de ponerla a salvo, como por ejemplo: Cold Wallets.

Las bitcoins tampoco son guardadas en bancos a diferencia del dinero de curso legal, por lo que no están sujetas al riesgo de quiebras o intervenciones bancarias. Tampoco pueden ser falsificadas ya que, gracias a la blockchain, no es posible utilizar bitcoins que históricamente no hayan sido creadas gracias al mining.

2.3.2 Desventajas

La credibilidad de las bitcoins se fundamenta en que la blockchain no puede ser modificada por un único usuario. Sólo hay una forma, y es controlando más del 50% de los recursos de los usuarios que publican la blockchain. Esta amenaza no está del todo resuelta actualmente ya que un "cartel" que controlase el 51% del Hash Rate podría ejecutar varias acciones en contra de la comunidad de usuarios (Ittay Eyal and Emin G¨un Sirer, 2013).

El incentivo para que dicho ataque no ocurra es que la comunidad de usuarios que tratan de alargar la blockchain crezca bastante, de tal forma que las probabilidades de que un usuario controle más del 50% del poder sean muy cercanas a 0. Incluso, aunque un agente o grupo de agentes controle el 51% o más del hash rate, lo que puede hacer con dicho poder es limitado y sólo acciones muy radicales podrían generarle alguna ganancia (Kroll, Davey, Felten, 2013).

2.3.2.1 51% Attack

Anteriormente se hizo acotación a la importancia del mining de bitcoins para mantener a la comunidad de usuarios segura. Mientras mayor sea el mining, medido en hashes, menor es la probabilidad de que un individuo, o un grupo, de individuos pueda controlar más de la mitad del poder dedicado a alargar la blockchain. Un grupo de usuarios que controle más del 50% del poder puede parecer difícil de creer, pero en la realidad no lo es. Dados los ingresos constantes que ofrecen las pools, los usuarios se agrupan para hacer mining. Es evidenciable que el hash rate sí está concentrado en pocos grupos en el siguiente gráfico.

Cuota de las pools de mining de bitcoins

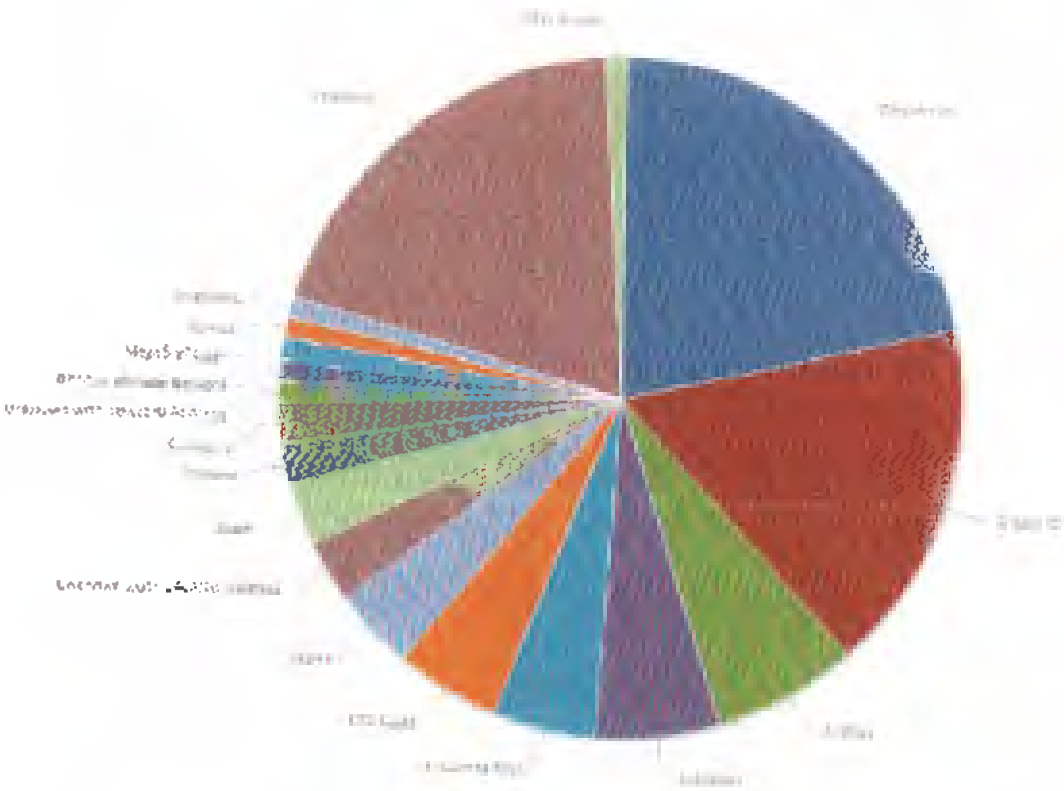


Grafico extraido de blockchain.info[8] 7/11/2014

Como se puede observar, pools como Discush Fish, que controla un 22% del hash rate total, o GHash.IO que posee un 17%, a pesar de no estar tan cerca de un 51%, hacen pensar que el problema de un cartel que controle un porcentaje del hash rate lo suficientemente alto como para realizar un ataque a la comunidad, no está tan lejos de la realidad como muchos piensan. De hecho, una agrupación entre las 4 pools más grandes ya conseguiría el poder necesario para llevar a cabo ese cometido.

Una vez conseguido el porcentaje del Hashrate total deseado, este grupo de usuarios podría realizar las siguientes acciones:

[8] https://blockchain.info/pools

- Crear un fork en la blockchain: esto le permitiría al cartel rechazar las bitcoins que otros miners obtengan producto del mining de tal forma que solo los miembros del cartel puedan obtener bitcoins para sí mismos.
- Double spending: un cartel puede llevar a cabo transacciones para obtener ciertos bienes y luego revertirlas de tal forma que obtengan sus bitcoins de vuelta.

Cabe destacar que todas estas acciones disminuirían la credibilidad de la comunidad en las bitcoins, lo que significaría una caída significativa en su valor. El cartel entonces habría invertido una gran cantidad de recursos en hardware y esta inversión le daría retornos muy bajos. Esto demuestra que un ataque para controlar la comunidad de bitcoins es poco creíble ya que las probabilidades de obtener alguna ganancia monetaria son bajas.

2.3.2.2 Impuestos transaccionales

Dada la naturaleza de crecimiento de la oferta de las bitcoins, la cual es cada vez más baja tanto nominal como porcentualmente, los ingresos de los miners son cada vez menores. Menores ingresos significa menos personas realizando mining y por ende, menos seguridad para la comunidad.

Existen 2 formas de atacar este problema, pero cada una afecta a un grupo de usuarios diferentes:

- Modificar la oferta total y su crecimiento: esto supondría que los ingresos por mining se mantendrían lo suficientemente altos como para no tener que aumentar los costos transaccionales. La oferta podría crecer más rápidamente que la del dólar, lo cual tendría como consecuencia que las

bitcoins, ceteris paribus, pierdan valor a través del tiempo. La elección de qué tan rápido debería crecer la oferta es un problema en sí, y además afectaría a todos los usuarios que actualmente poseen bitcoins.

- Aumentar los costos transaccionales: Una de las mayores ventajas de las bitcoins son sus, hasta ahora, bajos costos transaccionales los cuales son de aproximadamente unos 4 centavos de dólar por transacción. Un aumento significativo de estos costos disminuiría el atractivo de las bitcoins, no sólo para nuevos usuarios, sino también para los que actualmente consideran ésta su mayor ventaja.

Este problema no tiene una solución aparente actualmente dado que todavía los ingresos que se reciben del mining son lo suficientemente altos como para preocuparse por ello, pero es probable que en el futuro se tenga que tomar una medida para evitar una disminución del mining y que la comunidad siga siendo segura.

2.3.2.3 Goldfinger attack

Coloquialmente llamado así por la película de James Bond (Goldfinger, 1961) donde el villano trata de robar el oro de la reserva de Estados Unidos para que la moneda pierda credibilidad.

Dado que un cartel que controle el 51% del hashrate puede obtener muy pocos ingresos al llevar a cabo su ataque, su objetivo puede ser otro, tal como destruir a la comunidad de bitcoins. De acuerdo con Kroll, Davey & Felten (2013), existen 3 grupos de usuarios que podrían desear llevar a cabo tal objetivo.

- Entes gubernamentales: para evitar el lavado de dinero, comercio ilegal, evasión de impuestos, entre otros.
- Ente no gubernamental: para obtener algún tipo de beneficio político o social, tal vez en forma de protesta, por ejemplo el movimiento "Occupy Bitcoin".
- Ente buscando una ganancia: por ejemplo invirtiendo en corto en bitcoins para obtener ingresos por el desplome de su precio.

Es poco probable que se den tanto el caso 2 como el 3 ya que, en el caso de un ente no gubernamental tratando de realizar algún tipo de protesta, es poco probable que dicho ente pueda recaudar los recursos necesarios para realizar dicho ataque. En el caso de algún ente buscando una ganancia, actualmente no existen formas de inversión creíbles en la comunidad que permitan obtener ingresos cuando cae el precio de las bitcoins (podrían existir en el futuro).

Un ente gubernamental es el único que tiene las razones lo suficientemente importantes como para poder querer destruir las bitcoins, y además puede contar con los recursos suficientes como para hacerlo. Es necesario tomar en cuenta que las bitcoins no son la única moneda virtual, existen muchas otras que podrían reemplazarla si esta llegara a desaparecer.

2.3.2.4 Ataques Informáticos

Ataque de maleabilidad: en febrero de 2014 anunció su quiebra la que fue por mucho tiempo la casa de bolsa de mayor volumen de bitcoins, Mt Gox. De acuerdo a una serie de ruedas prensa, anunciaron que un ataque llevado a cabo en su contra utilizando la maleabilidad en las transacciones fue el

causante de la pérdida de más de 850.000 bitcoins, de las cuales alrededor de 750.000 eran de sus usuarios.

Los ataques de maleabilidad se basan en que un atacante, el cual es el recipiente de una transacción, duplica y modifica cierta transacción. Entre las dos transacciones, tanto la original como la modificada, solo una puede ser confirmada. En el caso de que la transacción modificada sea la confirmada, el usuario que envía las bitcoins puede pensar que la transacción nunca se llevó a cabo, realizando así otra transacción causando que el recipiente reciba dos veces la cantidad original de bitcoins. Cabe destacar que este ataque requiere que el emisor de la transacción (víctima) no se dé cuenta de que la transacción original sí se realizó.

Decker & Wattenhofer (2014) realizaron un análisis en el cual concluyeron que la cantidad de bitcoins hurtadas utilizando este sistema durante la quiebra de Mt Gox no se acerca a la cantidad de bitcoins totales robadas a la casa de bolsa. De todos modos el aspecto relevante de esta anécdota es que este sistema para robar bitcoins si funciona y hubo usuarios que fueron víctimas de él, a pesar de que no es un ataque lo suficiente grande como para dañar a toda la comunidad.

Ataques a casas de bolsa: la única forma posible de extraer bitcoins de una cartera personal es estando en posesión de la contraseña (key). El problema es que no todas las bitcoins se encuentran en carteras personales. Muchas se encuentran en carteras comunes, más que todo pertenecientes a casas de cambio de bitcoins. Las casas de bolsa son vulnerables a ataques informáticos dado que siempre están en línea y manejan un volumen considerable de bitcoins. Los métodos para atacar una casa de bolsa de

bitcoins son muy variados. Casi todos consisten en obtener de alguna forma la contraseña de las carteras comunes a través de los servidores.

Es necesario acotar que estos ataques no son ajenos a las bitcoins solamente; los bancos y muchos otros entes financieros son víctimas de ataques cibernéticos sin contar los costos invertidos en prevención y seguridad.

2.3.2.5 Shocks de demanda

Los shocks de demanda son comunes en los escenarios de la economía mundial. En el caso específico del dinero, estos shocks pueden ser contrarrestados con política monetaria para asegurarse de que el valor de una moneda no fluctúe demasiado. Ésta es una característica que no tienen las bitcoins. Al tener una oferta cuasi-fija, los shocks de demanda no pueden ser contrarrestados, lo cual tiene ciertas consecuencias negativas, como por ejemplo, una mayor volatilidad.

Los shocks de demanda por períodos prolongados de tiempo pueden crear burbujas en los precios como ha pasado repetidas veces con las bitcoins como explican en sus respectivos estudios Tim Swanson (2014) y Oscar Wandery (2014). Durante estas burbujas el precio aumenta muy rápidamente en cuestión de días o semanas. Estos aumentos de precio son pro-cíclicos ya que generan cobertura de los medios de comunicación, lo que a su vez hace que más gente demande bitcoins, haciendo que el precio aumente rápidamente. Después de que pasa el shock de demanda, el precio vuelve a su valor fundamental (el cual será analizado en el capítulo 3).

Varios economistas reconocidos creen que las bitcoins, por tener un crecimiento de la oferta tan bajo y además un límite (el cual en verdad puede

ser modificado), pueden caer en una trampa de liquidez dando como resultado una espiral deflacionaria (Krugman NY Times[9]).

Una espiral deflacionaria comienza cuando el valor de una moneda aumenta respecto a los bienes de dicha economía. Cuando esto sucede las personas prefieren no gastar dicha moneda lo cual genera una disminución de la oferta generando un círculo vicioso en el aumento del precio. Esto tiene efectos graves en la economía ya que el dinero perdería su función principal (medio de cambio) y disminuiría el consumo y por ende la producción en general. Las bitcoins, al ser intrínsecamente diferentes a las demás monedas corrientes, no deberían sufrir estas consecuencias por diferentes razones:

- Los precios de productos que pueden ser comprados en bitcoins están denominados en dólares (u otras monedas de curso legal) así que un aumento del precio de esta divisa no tiene efecto en los precios reales de los bienes ya que estos no están denominados en bitcoins (el precio en bitcoins se adapta al precio en la moneda de curso legal).

- Las bitcoins tienen cuasi perfecta convertibilidad y divisibilidad lo que permite que se pueda pagar por obtener cualquier tipo de bienes en cualquier momento.

- Una aumento en el precio de las bitcoins no debería generar una disminución en el consumo, ya que los usuarios de estas monedas deberían tener mayor riqueza y por ende mayor capacidad de gasto. En caso de que disminuyese el consumo en bitcoins, porque se espera que el precio aumente en el futuro, dado que no son monedas de curso legal, no son la mayor fuente de consumo de ningún país así que ésta

[9] http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfetters/

disminución no debería tener mayor efecto en ninguna economía hoy en día.

- Las bitcoins no sólo pueden ser obtenidas a través de la compra-venta. Si los usuarios deciden no vender sus bitcoins (ya que esperan que el precio aumente), otros usuarios pueden obtener bitcoins haciendo mining lo que a su vez aumentaría (leve y transitoriamente) la tasa de crecimiento de la oferta y su valor fundamental.

A pesar de que las bitcoins parecieran no ser propensas a sufrir una espiral deflacionaria, las burbujas de precio producto de shocks de demanda son una realidad que aumenta su volatilidad, lo que les hace perder credibilidad como un bien con un depósito de valor constante en el tiempo.

CAPÍTULO 3: MARCO METODOLÓGICO

3.1 Formación de precios de las bitcoins

3.1.1 El mercado de producción de las bitcoins

Luego de 5 años de la creación de las bitcoins, se puede observar que la producción de estas monedas virtuales se asemeja a un mercado de competencia perfecta ya que cumple, parcial o totalmente, las siguientes características:

- Gran cantidad de compradores y vendedores: tanto la cantidad de productores de bitcoins como usuarios dispuestos a comprarlas es numerosa. Aunque la producción se concentra en pools, estas pools están a su vez compuestas por muchos pequeños productores.

- Producto Homogéneo: las bitcoins son totalmente homogéneas, la única diferencia que existe en el mercado de las monedas virtuales es entre monedas diferentes como las bitcoins y otras altcoins, que pertenecen a la misma industria del mining, pero no son productos sustitutos.

- Información Completa y gratuita: La información de los precios es completa y gratuita. La de los factores de producción no es perfecta pero es bastante homogénea, los únicos que tienen información adicional son

los que se encargan de construir los activos fijos (hardware) que se utilizan en la producción.

- No hay barreras de entrada o salida: como no hay ningún régimen que regule en todo el mundo el mining de las bitcoins, no existen barreras de entrada ni tampoco de salida, ya que se puede dejar de hacer mining en cualquier momento. El único costo real de entrada al igual que cualquier industria de producción es el activo fijo, el cual en el caso de las bitcoins se encuentra disponible en un catálogo de precios bastante amplio permitiendo que cualquier persona entre al mercado.

- Maximización del beneficio: dado que ningún productor puede modificar la oferta ni la demanda así aumente o disminuya su producción, la única forma de maximizar el beneficio es produciendo la mayor cantidad de tiempo posible.

- Perfecta movilidad de factores: los factores de producción, desde computadoras normales hasta miners especializados, pueden ser transportados fácilmente a cualquier parte del mundo y están a la venta al público.

- Rendimientos constantes a escala: en el caso de la producción de bitcoins, los rendimientos a escala no son fácilmente observables dado que hay un componente tecnológico que dificulta el análisis.

Si existiesen rendimientos crecientes a escala se puede pensar que una sola empresa podría crecer lo suficiente como para adueñarse del mercado, creando así un monopolio. Esto es poco probable porque, como se dijo anteriormente, si una sola empresa o ente controlase mayoritariamente la

producción (oferta) de las bitcoins, estas perderían su valor y todos los costos invertidos en adueñarse del mercado se desperdiciarían.

Adicionalmente, dado que la tasa de crecimiento de la oferta de las bitcoins es cuasi-rígida, una empresa monopólica produciría casi la misma cantidad de bitcoins que todas las empresas conjuntas en competencia perfecta. La única diferencia sería que esta única empresa lo haría con menores costos (a diferencia de otros monopolios donde el productor podría controlar más fácilmente la cantidad y con eso el precio).

Un mercado oligopólico es probable teóricamente en caso de que el precio se encuentre por encima del costo de producción de los oligopolistas, y por debajo del costo de producción de todos los demás. Para que esto suceda tienen que darse las siguientes condiciones:

- Que todos los productores oligopólicos posean activos fijos de mayor rendimiento que el resto de los productores. Esto no solo implica que tienen los activos de mayor rendimiento un solo día, sino también a medida que pasa el tiempo (para que el mercado no pase a ser uno de competencia perfecta) lo cual, a menos de que ellos sean los creadores de dicho hardware, es poco probable que ocurra.

- Que todos los productores oligopólicos tengan costos energéticos menores que todo el resto de los productores. Cabe destacar que los costos energéticos pueden varias según el país, el tipo de empresa (descuentos legales), la existencia de descuentos (o aumentos) por volumen, la cercanía a las fuentes de producción energéticas (como plantas hidroeléctricas), la época del año, el tipo de cambio (ya que se

diferencian en sólo centavos), entre muchos otros factores; así que es poco probable tener los menores costos energéticos a lo largo del tiempo. Si es ya es difícil que una sola empresa tenga los menores costos energéticos a través del tiempo, es incluso más difícil que varias empresas los tengan.

- El precio debe estar muy cercano a los costos de los productores oligopólicos para que no entren más productores al mercado. Esto significaría un beneficio casi nulo o nulo en su totalidad si se toman en cuenta costos friccionales como impuestos, mantenimiento de los equipos, entre otros. Hay que agregar también que, como los costos energéticos no son totalmente uniformes, en caso de que estos aumenten, incluso sólo por cortos períodos de tiempo, se podría incurrir en pérdidas.

- La uniformidad del precio. Si este cae, incluso levemente, los productores incurrirían en pérdidas, ya que en el caso del oligopolio este se encuentra muy cercano a los costos de producción. En caso de que este aumente, entrarían nuevos productores al mercado para los cuales antes no era rentable producir. El precio de las bitcoins es particularmente volátil así que ésta es otra condición con pocas probabilidades de que se cumpla.

Luego de este análisis, se puede concluir que la cantidad de factores necesarios para que la producción de bitcoins sea un oligopolio no son muchos; pero si es poco probable que se cumplan por separado, es mucho más difícil que se den todos a la vez, y además, por un tiempo prolongado.

Todo parece que indicar que el mercado de producción de bitcoin se asemeja a un mercado de competencia perfecta, y además es poco probable que se convierta en un mercado dominado por un monopolio o un oligopolio. A pesar de tener muchas características de un mercado de la naturaleza mencionada, este tiene algunas particularidades que lo diferencian de otros mercados de competencia perfecta.

Una de estas características es la rigidez de la oferta. En un mercado convencional de competencia perfecta, la entrada de nuevos competidores tiene un efecto de aumento en la oferta disminuyendo así el precio. En el mercado de producción de las bitcoins, dado que la oferta es rígida, la entrada de nuevos competidores en vez de aumentar la oferta y disminuir el precio, lo que genera es una caída de la producción de todos los demás y por ende, de su ingreso.

Como el ajuste en el mercado de producción no es vía oferta y por último precio como en los mercados convencionales, si no por el lado de la cuota de producción, lo que se deriva en menores ingresos, la cuota de producción debe estar relacionada con el precio.

3.1.2 Derivación de la función de producción:

Antes de derivar la función de producción es necesario analizar un aspecto importante de las bitcoins. Tomando en cuenta el algoritmo de producción, el cual establece una tasa de crecimiento cuasi fija, los productores individuales no pueden elegir cuantas bitcoins producir. Para hacer frente a restricción, la unidad de producción en este trabajo será el tiempo medido en días, pero puede hacerse indistintamente en minutos, horas, semanas, etc.

Una segunda razón para hacer el análisis en función al tiempo es que el precio de las bitcoins es tan volátil que se puede incurrir en ganancias (o pérdidas) muy grandes, incluso con una cantidad estable de bitcoins producidas.

Para derivar una función de producción para un productor individual primero se derivará la función de ingreso.

3.1.2.1 Función de ingreso

Para crear un bloque de bitcoins los miners deben encontrar un hash por debajo de un valor *X*. Mientras menor sea *X*, más difícil es obtener un bloque.

La dificultad (*D*) se define como $D = \frac{Xmax}{X}$

Xmax según el protocolo[10] de bitcoins es 2^224

La probabilidad de encontrar el hash requerido de acuerdo con el protocolo es:

$$\frac{X}{2^{\wedge}256}$$

Despejando *X* de la primera ecuación se obtiene que $X = \frac{Xmax}{D}$

Si se sustituye *X* en la segunda ecuación por la anterior, la probabilidad de obtener un bloque de bitcoins sería:

$$\frac{Xmax}{2^{256}D}$$

Ahora se sustituye *Xmax.*

[10] https://en.bitcoin.it/wiki/Difficulty

$$\frac{2^{224}}{2^{256}D} = \frac{1}{2^{32}D}$$

La probabilidad de obtener un bloque de bitcoins con un solo hash (*h*=1) es entonces:

$$\frac{1}{2^{32}D}$$

El número de hashes suele ser medido en cantidad de hashes por segundo y está determinado por el activo fijo. La cantidad de hashes (*h*) que puede ejecutar un miner en cierta cantidad de tiempo (*t*) es *h.t*, así que si se desea saber la cantidad de hashes que puede ejecutar un miner en un día, esto equivale a *h*.86400 (cantidad de segundos en un día).

$$\frac{h.86400}{2^{32}D}$$

Si se desea saber la probabilidad de obtener una sola bitcoin basta con multiplicar dicha ecuación por la cantidad de bitcoins que contiene un bloque para el momento del cálculo, en este caso son 25.

$$\frac{h.86400}{2^{32}D}.25$$

Como se desea conocer una función de producción en dólares y no en bitcoins (porque el precio es muy volátil), se debe multiplicar la ecuación anterior por el precio (*P*) de las bitcoins en dólares.

$$\frac{h.86400}{2^{32}D}.25.P$$

Para determinar el ingreso que obtendrá el productor en cierta cantidad de días basta con multiplicar la ecuación anterior por la cantidad de días (*N*).

$$\frac{h.86400}{2^{32}D}.25.P.N$$

Esta es la función de ingreso de un productor de bitcoins en (*N*) días. Las variables *P* y *D* son ajenas al productor y *h* solo puede ser modificada cambiando el activo fijo. La única variable sobre la que el productor tiene verdadero control en todo momento es cuantos días producir (*N*). Más adelante se analizará cómo influye esta variable.

Cabe destacar que la función de ingresos derivada anteriormente depende de la probabilidad de obtener un bloque de bitcoins, la cual se distribuye como una función de Poisson (Nakamoto, 2008). Para hacer frente a esta situación los productores individuales se juntan en pools para obtener ingresos más homogéneamente.

3.1.2.2 Función de costos

Los costos de producción pueden ser separados en 2, costos variables y costos fijos.

El costo fijo es el costo del miner (hardware) el cual será denotado como *F*.
Costo Fijo:
F

Este costo como es fijo no varía según la cantidad de días así que permanece igual a través del tiempo.

Al costo fijo hay que sumarle el costo variable el cual viene determinado por el gasto energético del miner (*kW*), el costo en dólares de la energía local (*c)* y la cantidad de tiempo (*t*).

Los costos energéticos locales se miden en *kWh/$* lo que es igual al costo de usar 1000 kW en una hora. El costo variable de los miners medido en *kW* refleja la cantidad de kW que utiliza el miner en 1 hora. Para saber cuál es el costo en dólares de utilizar el miner en 1 hora es necesario dividir la variable *kW* entre 1000 y multiplicarla por el precio *c*.

El costo variable quedaría entonces de la siguiente forma:

$$\frac{kW}{1000}.c.t$$

Como la función de ingreso fue derivada en función de una unidad de tiempo igual a un día, se debe hacer lo mismo con la función de costos. Como el lado izquierdo de la ecuación está calculado en horas, *t* debe ser igual a 24 para conocer los costos del mining en un día.

Los costos variables son finalmente:

$$\frac{kW}{1000}.c.24$$

Para saber en qué gastos incurrirá el productor en cierta cantidad de días basta con multiplicar la ecuación anterior por *N*.

$$\frac{kW}{1000}.c.24.N$$

Los costos totales, como resultado de la suma de los costos fijo más los costos variables son:

$$F + \frac{kW}{1000}.c.24.N$$

La función de producción final, en función a la cantidad de tiempo, medido en días (*N*), queda de la siguiente forma:

$$(\frac{h.86400}{2^{32}D}.25.P.N) - (F + \frac{kW}{1000}.c.24.N)$$

Es necesario hacer varias acotaciones respecto a esta función de producción:

- Esta es la función para una persona que produce por su cuenta. La mayoría de los miners pequeños hacen mining en pools ya que esto normaliza sus ingresos.
- Las pools tienen comisiones, lo que significa que el lado de ingresos de la ecuación suele ser menor en la mayoría de los casos (dependiendo del porcentaje que se cobre como comisión).
- No todas las pools usan sistemas de pagos proporcionales, algunas premian también la cantidad de tiempo que los usuarios están

conectados, así que el lado de los ingresos de usuarios que no están siempre produciendo suele ser menor.

- La función no toma en cuenta costos como impuestos o de mantenimiento del activo fijo.
- Los ingresos por impuestos transaccionales no están contemplados en esta función por ser actualmente muy bajos. Podrían jugar un papel mucho más importante en el futuro si aumenta la cantidad de transacciones.

A continuación se analizarán las implicaciones que tiene dicha función para el mercado de producción de bitcoins.

3.1.3 Análisis de la función de producción individual

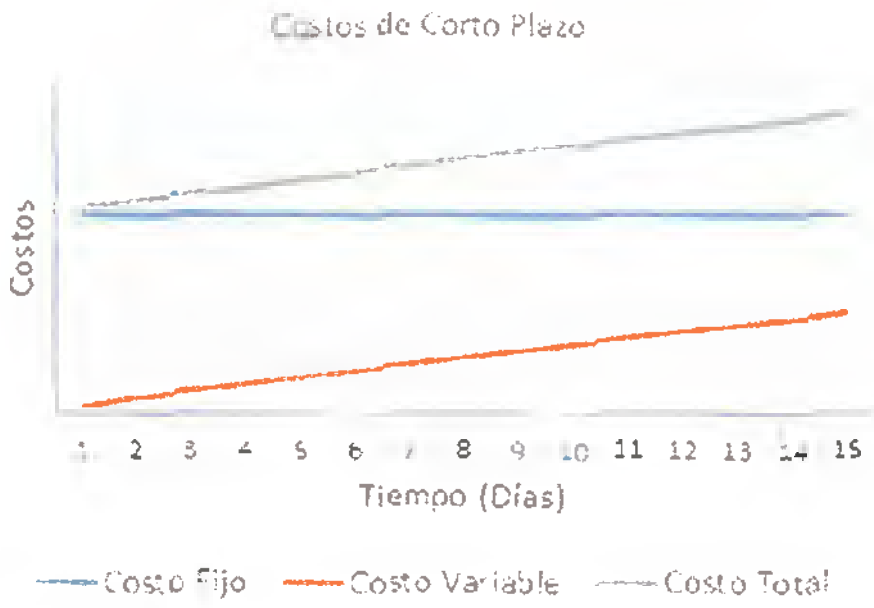
Para determinar los efectos de la función de producción de las bitcoins en el mercado de producción, se procede a hacer el análisis por partes. Se empezará por los costos por ser más fáciles.

3.1.3.1 Análisis de los costos

Costos de corto plazo

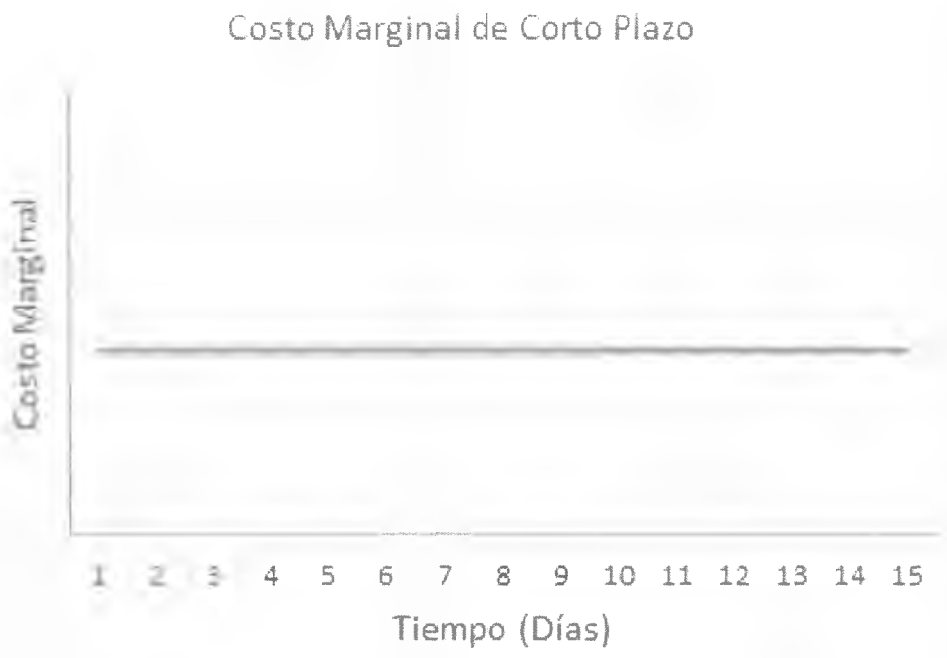
F y kW están dados por el activo fijo, lo que significa que en el corto plazo se mantienen constantes y c es exógeno para el productor y también es fijo en el corto plazo, la función de costos tiene la siguiente forma en el corto plazo:

Si se deriva el costo marginal diario de la función de costos, se obtiene que el costo marginal no solo es lineal, sino que además es constante ya que *kW* y c se mantienen fijos.



$$CMg = \frac{kW}{1000} \cdot c \cdot 24$$

Que el costo marginal sea constante obedece al postulado que se hizo anteriormente el cual dice que el productor no tiene control sobre el nivel de producción solo de la cantidad de tiempo que este se dedique producir.

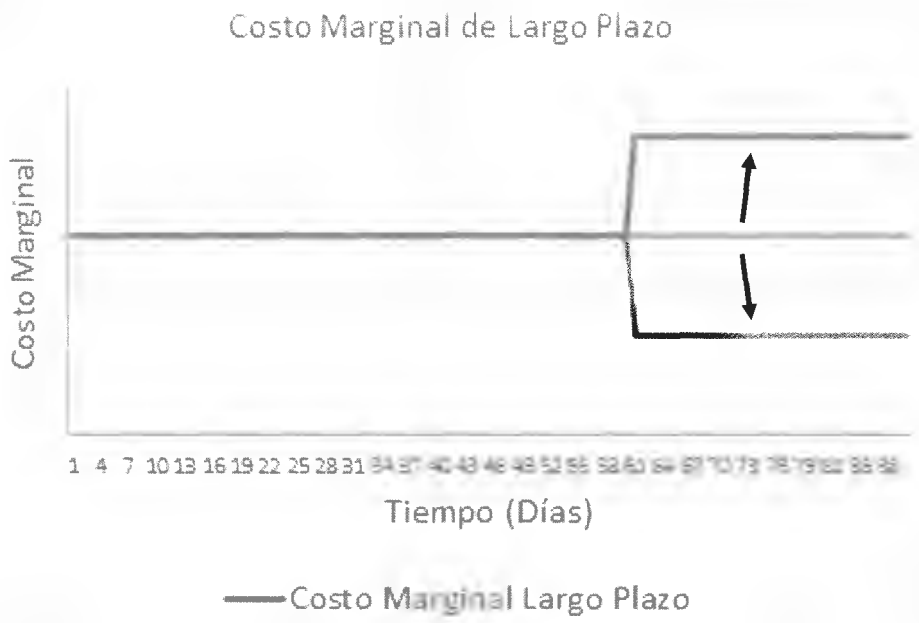


Costos de largo plazo

El largo plazo es bastante similar al corto plazo, la diferencia es que ahora los productores pueden cambiar el activo fijo. Cambios en *F* tienen efectos directos en *kW*. Estos cambios de *kW* tienen efecto directo en el costo marginal desplazándolo hacia arriba o hacia abajo, dependiendo del cambio en el activo fijo.

En el largo plazo también pueden cambiar los costos energéticos locales, lo que también afecta directamente al costo marginal, desplazándolo hacia arriba o hacia abajo.

Si ambos factores aumentan (disminuyen), el costo marginal aumenta (disminuye). Si los factores se mueven en direcciones opuestas, el efecto sobre el costo marginal dependerá del cual cambie en mayor proporción.



Es necesario acotar que cambios en *kW* no siempre son proporcionales a cambios en el activo fijo (*F*) ya que existen muchos activos fijos disponibles en el mercado y no todos tienen la misma relación *kW/F*. Los cambios serían proporcionales si se obtiene más (o menos) del mismo producto.

Por ejemplo, suponiendo que el productor posee un activo fijo con un costo de 1000$ y un consumo energético de 1000 kW por hora, si se adquiere un nuevo producto que también cuesta 1000$, pero su consumo energético es de 500 kW por hora, *F* habrá aumentado en un 100% pero *kW* solo en un 50%. A pesar de que los cambios no siempre son proporcionales, casi siempre son en la misma dirección, ya que la única forma de que un aumento (disminución)

en *F* me genere una disminución (aumento) en *kW*, es desincorporando activos y cambiándolos por otros.

3.1.3.2 Análisis de los ingresos

Ingreso de corto plazo

La función de ingresos para un productor contiene cierta volatilidad dado que contiene la variable precio (*P*) y la dificultad (*D*).

En la gráfica anterior, para la cual se tomó como ejemplo el comportamiento del ingreso durante los últimos 15 días de la serie de datos, la volatilidad no es observable porque existe una tendencia. Al derivar la función

de ingreso marginal y realizar un ejemplo con los mismos datos si se puede observar mejor la volatilidad:

$$Img = \frac{h.86400}{2^{32}D}.25.P$$

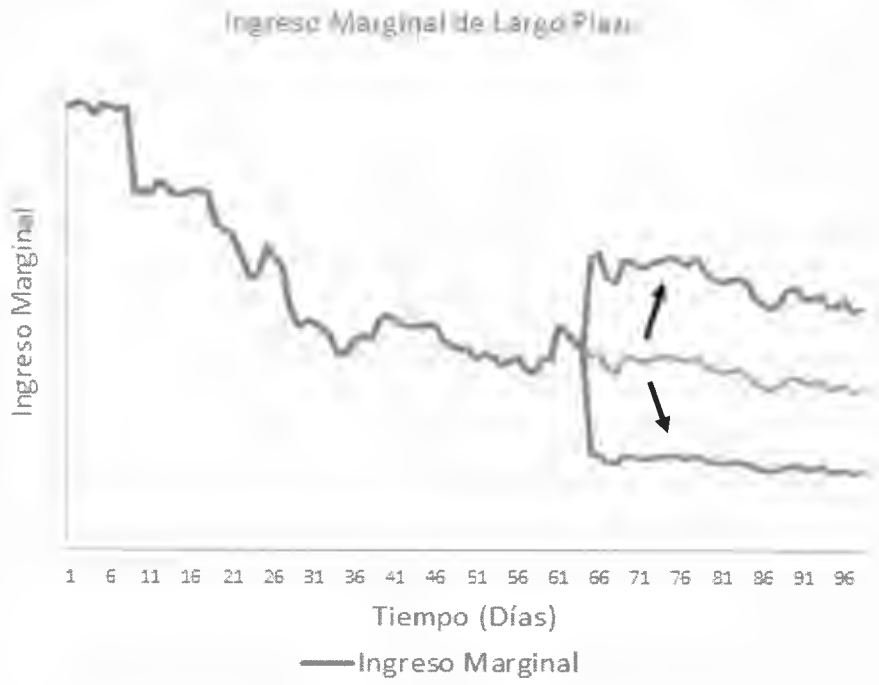
En la función de ingreso marginal a corto plazo, todas las variables se mantienen fijas excepto por *P* y *D*. La dificultad varía aproximadamente cada 2 semanas así que la volatilidad del ingreso marginal en el corto plazo se debe más que todo a la volatilidad del precio.

Ingreso de largo plazo

Al igual que en el caso de los costos, los ingresos de largo plazo son similares a los de corto plazo. Cambios en *F* tienen efectos directos en *h*. Estos cambios en *h* desplazan el ingreso marginal hacia arriba o hacia abajo.

La otra variable de la ecuación de costo marginal que puede cambiar en el largo plazo es la cantidad de bitcoins que contiene un bloque de bitcoins (actualmente es 25). Esta variable solo cambia cayendo a la mitad (12,5 la próxima vez) aproximadamente cada 4 años. Dado que estos cambios solo ocurren en márgenes de tiempo bastante amplios (y predecibles), será omitida del análisis de largo plazo. Para modelar el ingreso marginal se tomaron las últimas 100 muestras de la data.

Un aumento en h genera un aumento en la misma proporción en el ingreso marginal y lo mismo pasa en caso de una disminución.



Es necesario acotar que cambios en *h* no siempre son proporcionales a cambios en el activo fijo (*F*) porque existen muchos activos fijos disponibles en

el mercado y no todos tienen la misma relación *h/F*. Los cambios serían proporcionales si se obtiene más (o menos) del mismo producto.

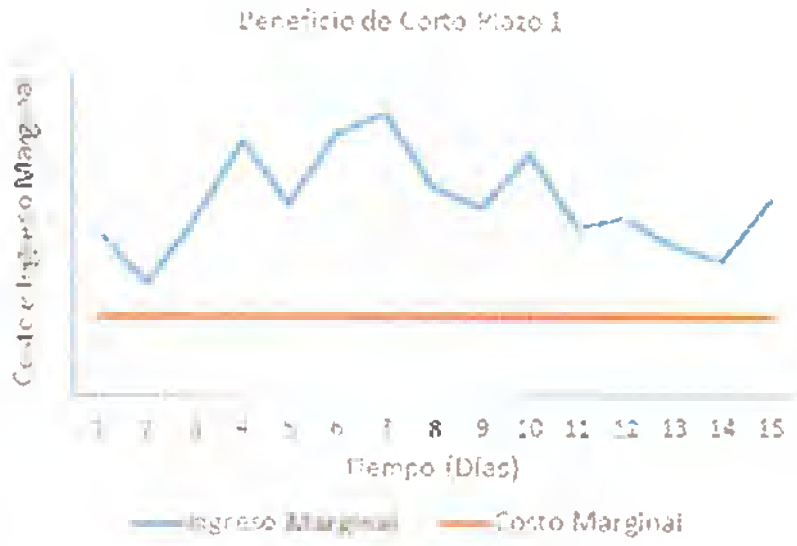
Por ejemplo, suponiendo que el productor posee un activo fijo con un costo de 1000$ y este calcula 1000 hashes por segundo, si se adquiere un nuevo producto que también cuesta 1000$, pero puede calcular 2000 hashes por segundo, *F* habrá aumentado en un 100% pero *h* habrá aumentado en un 200%. A pesar de que los cambios no siempre son proporcionales, casi siempre son en la misma dirección ya que la única forma de que un aumento (disminución) en *F* me genere una disminución (aumento) en *h* es desincorporando activos y cambiándolos por otros.

3.1.3.3 Análisis del beneficio

Beneficio de corto plazo

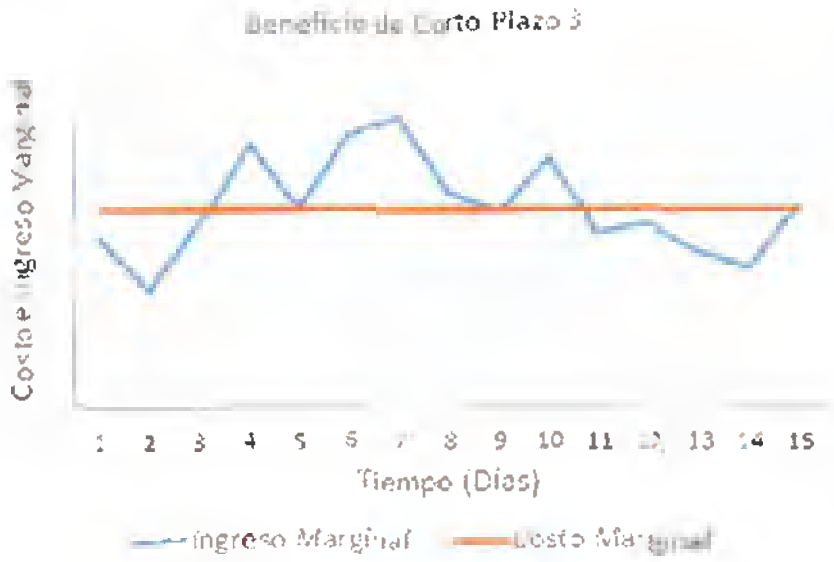
Tomando el ingreso marginal y el costo marginal, se puede construir una gráfica que contenga a ambos para observar el beneficio.

En el corto plazo pueden darse 3 casos:



En el primer caso, el ingreso marginal se encuentra siempre por encima del corto plazo, lo que significa que el productor si quiere maximizar el beneficio deberá producir en todo momento.

En el segundo caso, el ingreso marginal se encuentra siempre por debajo del corto plazo, lo que significa que el productor, si quiere maximizar el beneficio, no deberá producir hasta que el ingreso marginal supere a su costo marginal. Existe la posibilidad de que aún en este caso se decida producir, más *adelante serán analizadas las razones.*



En el tercer caso el ingreso marginal oscila alrededor del costo marginal. Si el productor quiere maximizar el beneficio deberá producir sólo cuando el ingreso marginal se encuentre por encima. Al igual que en el caso 2, es posible que se produzca aun cuando el costo sea mayor que el ingreso marginal.

En este análisis del beneficio se puede evidenciar la importancia de la variable N, ya que el productor no puede elegir cuanto producir, pero si cuando.

Beneficio de largo plazo

En el largo plazo sucede lo siguiente con el beneficio. Asumiendo que los productores no desincorporan activos, cambios en el activo fijo tiene efectos directos en h y kW en la misma dirección. Las dos variables tienen efecto en el beneficio marginal.

Las variables h y kW cambian en una proporción α y β respectivamente. Si el productor adquiere activos fijos iguales al que ya posee, α será igual a β. Si el productor adquiere un activo fijo nuevo diferente al que poseía anteriormente, α será diferente de β. Tomando en cuenta que hay avances tecnológicos (ley de Moore[10] y ley de Koomey[11]) y el supuesto de que el productor busca maximizar su beneficio, α será siempre mayor o igual que β.

El beneficio marginal crece (o decrece) en una tasa entre α y β. (Demostración 1 en los anexos).

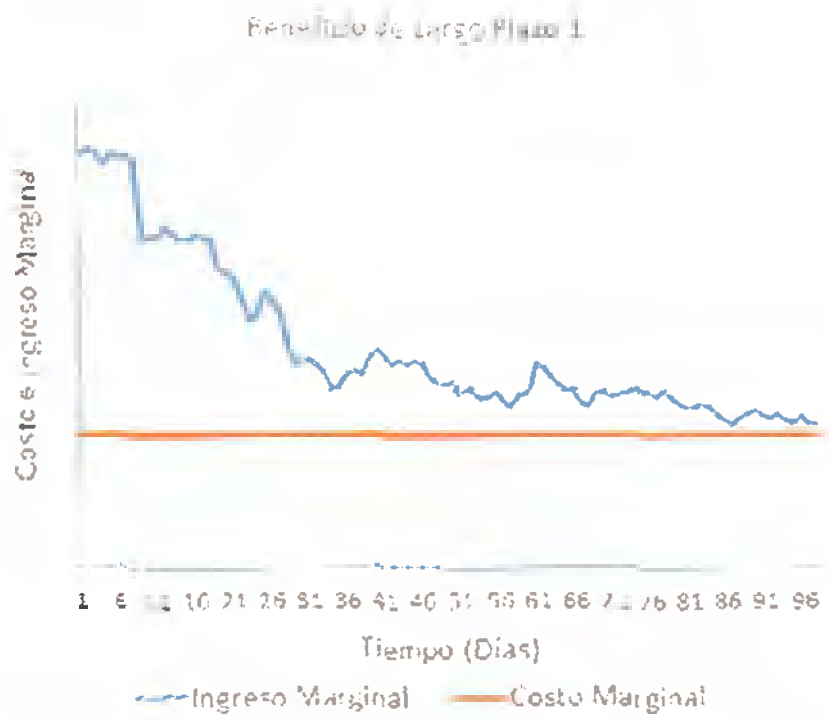
La importancia de esta conclusión para el largo plazo es la siguiente:

- Si el ingreso marginal se encuentra por encima del costo marginal, es posible maximizar el beneficio adquiriendo más activo fijo
- Si el ingreso marginal se encuentra por debajo del costo marginal, la única forma de minimizar las pérdidas sería dejando de producir ya que modificando el activo, las pérdidas aumentarían o disminuirían proporcionalmente. Existen 2 vías en las que las pérdidas podrían convertirse en beneficios:

- La primera vía seria con un α muchisimo más grande que β lo cual no es tecnológicamente probable (dado que la ley de Moore y la ley de Koomey suponen una barrera de crecimiento a través del tiempo bastante fuerte para los valores de α y β).

- La segunda forma seria desincorporando los activos de menor productividad. Esto permitiria mover con mayor holgura los ingresos marginales sin afectar tanto los costos marginales. Para este análisis seria mejor recalcular la función de producción desde el principio, en vez de calcular cual fue el cambio al hacer una modificación tan importante en el activo fijo.

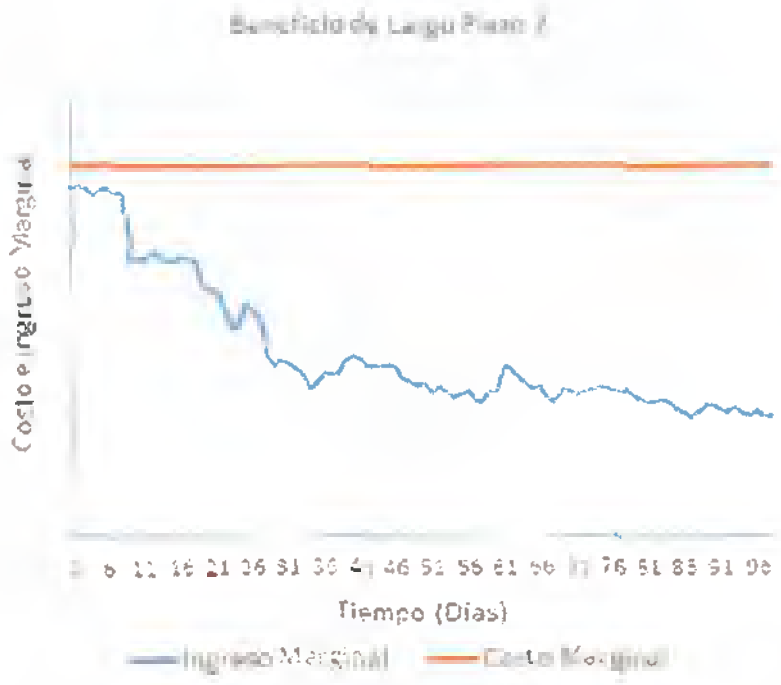
Ahora se procederá a realizar un análisis de 3 casos al igual que se hizo anteriormente en el corto plazo.



[11] http://es.wikipedia.org/wiki/Ley_de_Moore

[12] http://en.wikipedia.org/wiki/Koomey%27s_law

En el primer caso, el análisis es similar al de corto plazo. Si el costo marginal se encuentra siempre por encima del ingreso marginal, para maximizar el beneficio lo recomendable es producir todos los días. Como el productor se encuentra en el largo plazo, este puede aumentar su beneficio adquiriendo más activo fijo.

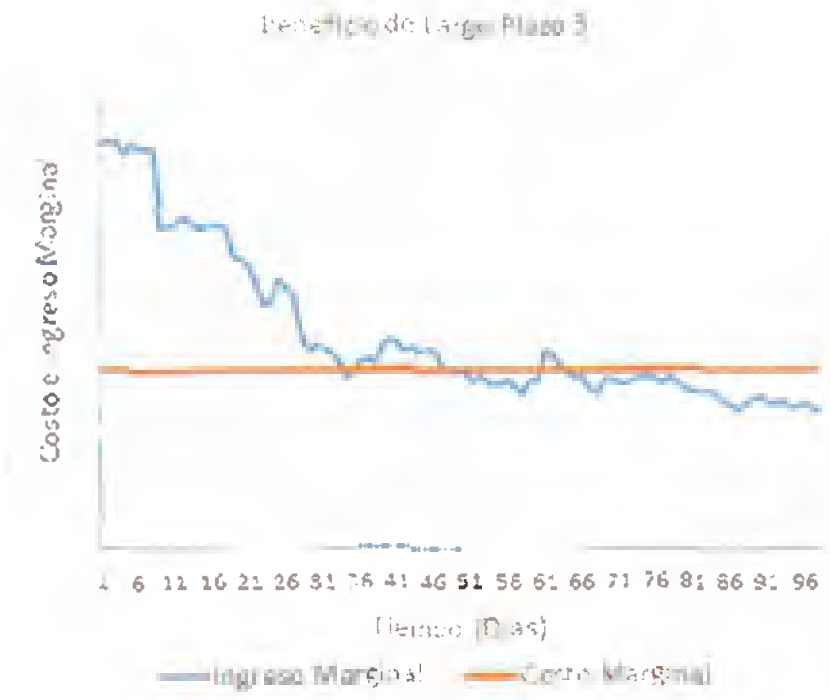


En el segundo caso del corto plazo, la decisión óptima era no producir hasta que el ingreso marginal aumentase por encima del costo marginal. Ahora que el productor se encuentra en el largo plazo, si esto no sucede, este debe cambiar el activo fijo si quiere que sea rentable producir.

Como se dijo al principio del análisis de beneficio de largo plazo, la única forma de mover curva de ingreso marginal sin mover en el mismo sentido la de

costo marginal es desincorporando activo y cambiándolo por uno mucho más productivo.

En este caso en especifico es muy probable que el productor se encuentre *en un lugar donde los costos energéticos so altos y por ende no le sea rentable* producir, incluso en el largo plazo.



En el tercer caso, el análisis también es similar al de corto plazo. Para *maximizar el beneficio lo recomendable seria producir los dias* que el costo marginal se encuentre debajo del ingreso marginal. Como ahora el productor se encuentra en el largo plazo, este puede aumentar su beneficio durante los dias que si es rentable producir adquiriendo más activo fijo.

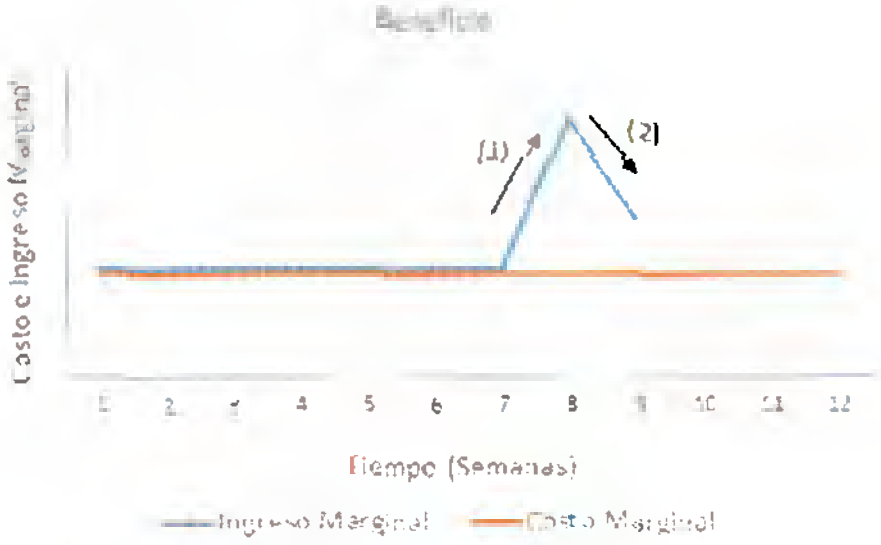
3.1.3.4 La función de producción de bitcoins en competencia perfecta

Ahora se contrastará este comportamiento con la teoría económica de mercados de competencia perfecta.

En competencia perfecta, un bien debe ser producido en cierta cantidad de tal forma que el ingreso marginal iguale al costo marginal.

En el mundo de las bitcoins, el ingreso marginal es el único que es variable en el corto plazo. Se analizará entonces que pasa si hay una perturbación en el ingreso:

- Dado un estado de equilibrio (Img = Cmg), si aumenta el precio (1), aumenta el ingreso marginal para todos los productores. Ahora pueden entrar nuevos productores para los cuales previamente no era rentable producir. Cuando esto ocurre, el hash rate y la dificultad aumentan, disminuyendo el ingreso marginal (2), haciendo que la curva de ingreso, que se había separado del costo, se acerque nuevamente al equilibrio.



- El análisis es análogo para el caso en que disminuya el precio luego de un estado de equilibrio. Se salen productores del mercado, disminuyendo el hash rate y la dificultad, haciendo que la curva de ingreso marginal, la cual se había alejado del precio, se acerque equilibrio.

En el largo plazo, el ajuste hacia el equilibrio es el mismo, la única diferencia es que ahora los productores pueden ajustar grandes desviaciones entre el ingreso marginal y el costo marginal modificando su activo fijo.

Este análisis concuerda con la teoría económica ya que, aunque el ingreso marginal y el costo marginal no son iguales en todo momento (dada la volatilidad del precio), el mercado tiende a corregir sus imperfecciones.

Es necesario hacer varias acotaciones al análisis anterior tanto al corto como al largo plazo. La primera es que la volatilidad del precio es mayor que la de la dificultad, ya que esta cambia solo cada 2 semanas aproximadamente, por lo que los movimientos en el precio no suelen ser inmediatamente compensados por los movimientos de la dificultad. En el largo plazo esto puede causar burbujas en el precio como se expuso en la sección de shocks de demanda.

En segundo lugar, no todos los productores dejan de producir bitcoins si el costo marginal se encuentra por encima del ingreso marginal, ya que muchos productores esperan que las bitcoins aumenten de precio en un futuro y que este aumento de precio compense sus pérdidas actuales.

La existencia de cloud mining, el cual absorbe todos los costos variables para los inversionistas, hace que sea mejor producir a cualquier costo y a

cualquier precio para al menos recuperar parte de la inversión en caso de que se incurra en pérdidas, lo que significa que estos productores tampoco saldrían del mercado en caso de una disminución en los precios.

Los dos aspectos nombrados anteriores hacen que la dificultad suela encontrar barreras temporales a la baja. Éstas barreras pueden desplazarse también al precio dado que, como se explicó anteriormente, los productores podrían preferir mantener sus bitcoins esperando que aumenten de precio a venderlas e incurrir en pérdidas inmediatamente.

El papel de la tecnología en el largo plazo no es del todo claro. Los avances tecnológicos mejoran h, pero dado que su difusión es amplia, esto trae como consecuencia que también aumente D casi en la misma proporción, lo que significa que el efecto de la tecnología en el ingreso marginal tiende a ser nulo. Solo tienen ventaja los que puedan hacerse con dichos avances antes de que el resto del mercado se adapte por completo, por ejemplo, la migración de CPU (unidad central de procesamiento) a GPU (unidad gráfica de procesamiento).

Por el lado de los costos, el efecto de los avances tecnológicos si es claro. A pesar de que los miners son cada vez más eficientes tanto en hashes por segundo como en hashes por joule (cantidad de hashes por kW consumido), el aumento exponencial del hash rate en los últimos años implica, tecnológicamente (ley de Koomey), un mayor consumo energético. Esto significa mayores costos variables y marginales.

Si en el largo plazo la tecnología no genera un aumento del ingreso marginal, ya que esta se difunde perfectamente, los aumentos en el hash rate

global deben ser compensados con un aumento del precio para que siga siendo rentable producir.

3.1.4 Derivación del costo global de crear una bitcoin

Anteriormente se concluyó que el ingreso marginal de una crear una bitcoin debe ser igual al costo marginal, es posible inferir que el costo global de producirla debe ser igual al precio global.

Para determinar costo global de crear una bitcoin basta con agregar las funciones de costos de los productores individuales.

$$\sum \frac{kW}{1000} . c = \frac{kWt}{1000} . cg$$

En la función anterior *kWt* es la suma de todos los *kW* individuales y *cg* es un promedio ponderado de los costos energéticos de los diferentes productores de bitcoins (demostración 2 en los anexos). Dado que ambas variables están medidas en horas y actualmente las bitcoins se producen en bloques de 25 aproximadamente cada 10 minutos, es necesario dividir estos costos entre 6 y entre 25.

$$\frac{\frac{kWt}{1000} . cg}{6.25}$$

Luego de simplificar, se concluye que la función de producción global es:

$$\frac{kWt . cg}{150000}$$

3.1.5 Análisis del costo global de crear una bitcoin

En este punto el análisis encuentra varias barreras. La primera es que no se conoce kWt dado que el mining de bitcoin se realiza en activos muy diversos, desde computadoras caseras hasta hardware especializado, y cada uno tiene un kW por hora muy diferente. La segunda es que, no solo no se conocen los costos energéticos que paga cada miner alrededor del planeta, sino que tampoco se sabe cuál es la cuota de producción de cada uno como para realizar un promedio ponderado.

Incluso si se conociese la ubicación perfecta de todos los productores en el planeta, a 2 productores ubicados exactamente en la misma ciudad podrían aplicarles costos energéticos muy diferentes (por ejemplo si uno de los dos paga la electricidad como hogar, o como empresa). Además, en algunas ciudades no existe un solo proveedor de energía si no varios, como por ejemplo en Berlín, lo que hace la estimación mucho más difícil.

Solo para ilustración del lector, se determinó que actualmente la mayor cantidad de descargas del software para mining de bitcoin[13], como proxy de la ubicación de los productores, se ha realizado en Estados Unidos, China, Alemania, Rusia y Reino Unido.

[13] http://sourceforge.net/projects/bitcoin/files/stats/timeline

Unidos	33,9%	34,0%	32,8%	26,9%	26,2%
China	1,4%	6,8%	5,4%	13,7%	13,3%
Alemania	3,8%	9,4%	7,9%	6,0%	6,3%
Rusia	15,4%	5,8%	6,2%	5,6%	5,8%
Reino Unido	5,4%	5,3%	5,8%	5,4%	5,2%
Canadá	5,5%	4,5%	4,3%	3,9%	3,8%
Holanda	2,1%	2,3%	2,4%	2,4%	2,4%
Australia	2,7%	2,5%	2,7%	2,4%	2,3%
Polonia	2,0%	3,3%	2,9%	2,3%	2,3%
Francia	3,2%	2,0%	1,8%	1,9%	2,0%

Para tener una idea de los costos energéticos promedio de estos países, se realizó la siguiente tabla:

Costos energéticos por país	
Países	Costos energéticos promedio (Centavos de $ por kWh)[14 15]
Estados Unidos	8-37
China	7,5-10,7
Alemania	36,25
Rusia	2,4-14
Reino Unido	20
Canadá	7,78-11,17
Holanda	28,89
Australia	30,817
Polonia	19
Francia	19,39

[14] http://en.wikipedia.org/wiki/Electricity_pricing

[15] http://shrinkthatfootprint.com/average-electricity-prices-kwh

Utilizando las descargas del software de Bitcoins como proxy de la cantidad de productores en cada país, se puede observar un aumento de la cantidad de productores en China y una caída en Estados Unidos lo que sugiere que el mining, al ser un mercado de libre entrada, se ha ido desplazando hacia países donde los costos energéticos son mucho menores. En el caso de Rusia, a pesar de tener costos energéticos bastante bajos, su disminución en cuanto a la cantidad de descargas de software puede deberse al marco legal local, el cual dice que las bitcoins son ilegales.

Cabe destacar que el futuro de la concentración del mining es incierto por varias razones. A pesar de que la creación de bitcoins se asemeja a una industria de competencia perfecta, podría presentar rendimientos crecientes a escala gracias al uso extensivo de capital basado en productos tecnológicos y menores costos energéticos en algunos países. Los mayores rendimientos a escala implican mayor concentración de la producción.

Por otro lado está el futuro de las pools las cuales concentran más del 70% de la producción actual. De acuerdo con los estudios de Ittay Eyal (2014), Emin Gun Sirer & Ittay Eyal (2013) y Nicolas Courtois & Lear Bahack (2014), las pools pueden ser objeto de varios ataques, tanto por parte de algunos usuarios, como por parte otras pools. La forma más efectiva de evitar todos estos ataques es haciendo las pools privadas. La mayoría de las pools grandes son públicas así que ocurriría un gran cambio en la concentración del poder de mining si estas pools se disuelven o cambian sus políticas de aceptación de miembros.

Como existen variables importantes que apuntan en distintos sentidos en cuanto a la concentración de la producción, no es posible afirmar de ninguna forma cómo será la concentración del mining en el futuro.

3.2 Mercado de oferta y demanda:

De acuerdo con Carl Menger, el precio de un bien depende de su escasez relativa. Para determinar dicho valor por esta vía se utilizará la ley de oferta y demanda.

La interacción entre oferta y demanda puede ser derivada del modelo de Barro (1979) de determinación del precio del oro modificado por Ciaian, Rajcaniova y Kancs (2014) para adaptarlo a las bitcoins.

La función de oferta de bitcoins es la siguiente:

$$M^s = P^b B$$

P^b = Precio de las bitcoins denominado en dólares.
B = Total de bitcoins en circulación.

Para la demanda se utilizará la siguiente ecuación:

$$M^d = \frac{PY}{V}$$

P = Nivel general de precios de bienes y servicios.
Y = Tamaño de la economía de las bitcoins.
V = Velocidad de circulación de las bitcoins.

El equilibrio está dado por la igualdad entre la oferta y la demanda la cual sería:

$$P^b = \frac{PY}{VB}$$

Esta ecuación implica que:

(1) A mayor velocidad de circulación (V), menor precio
(2) A mayor oferta (B), menor precio
(3) A mayor precio de los bienes y servicios de la economía (P), mayor es el precio de las bitcoins
(4) A mayor tamaño de la economía de las bitcoins (Y), mayor precio

Aplicando logaritmos a la ecuación de equilibrio entre oferta y demanda resulta la siguiente ecuación:

$$p^B_t = \beta_0 + \beta_1 p_t + \beta_2 y_t + \beta_3 v_t + \beta_4 b_t + \epsilon_t$$

De acuerdo con el modelo de Barro, β_1 y β_2 deberían ser positivos y β_3 y β_4 negativos, lo cual también sería consistente con la ecuación original.

Para el mercado de las bitcoins se puede inferir que:

(1) La velocidad de circulación no es lo suficientemente grande actualmente ya que las bitcoins han sido adoptadas por relativamente pocos usuarios y su aceptación todavía no es generalizada. Debería jugar un papel más importante en el futuro.

(2) Dado que se conoce casi perfectamente la tasa de crecimiento de la oferta, incluso para el largo plazo, esta tampoco debería jugar un papel importante. Además es muy poco volátil.
(3) El precio de los bienes y servicios de las economías desarrolladas (las que tienen más usuarios de bitcoins) varía poco en el corto plazo.
(4) El tamaño de la economía, medido utilizando como proxi la cantidad total de transacciones, varía bastante, tanto en el corto plazo como en el largo plazo.

Estas conclusiones indican que, entre estas variables, el tamaño de la economía es la variable que explica mayoritariamente los cambios de precios de las bitcoins ya que las demás variables se mantienen relativamente fijas con el paso del tiempo.

3.3 Metodología econométrica

La metodología a utilizar es un modelaje econométrico utilizando el método de Engle y Granger de 2 etapas (1987).

Según Engle & Granger (1987) regresiones de series de tiempo interdependientes y no estacionarias puede llevar a resultados espurios. Para asegurar que los resultados no sean de esta naturaleza se procederá a realizar los siguientes tests: Augmented Dicky-Fuller (ADF) y Phillips-Perron (PP). La cantidad de rezagos a utilizar para cada variable está determinada por el criterio de informacion de Akaike (AIC). Si 2 series de tiempo no son estacionarias, su combinación si debe serlo (Engle & Granger, 1987). En este caso la serie se considera cointegrada implicando que existe un equilibrio de largo plazo entre las series.

El primer paso consiste en realizar un modelo de largo plazo, utilizando la primera etapa de la metodología de Engle y Granger de 2 etapas, el cual contenga todas las variables del estudio. Dada la no estacionariedad en varianza, se transformarán las variables empleando el logaritmo. Esta transformación permite, igualmente, obtener en forma directa las elasticidades.

El segundo paso consiste en determinar la relación de corto plazo para examinar las relaciones entre las variables y el precio. Esto puede hacerse utilizando la metodología Johansen (1990), Engle & Granger (1987) o un modelo de rezagos distribuidos (ADL).

En el tercer paso se estimará un modelo de corrección del error (MCE) para las series que están cointegradas. Este modelo incluye un término que indica la velocidad de ajuste de cada desequilibrio en relación a un equilibrio de largo plazo.

Como último paso, se realizarán los tests tradicionales para verificar las hipótesis de Gauss-Markov. En este sentido, se emplearán los contrastes sobre la normalidad de los residuos (Jarque-Bera), forma funcional correcta (Ramsey), ausencia de heterocedasticidad (Arch), autocorrelación entre los residuos (Breusch-Godfrey), y ausencia de raíz unitaria (Dickey-Fuller).

3.3.1 Descripción de las variables a utilizar

La periodicidad de la data a utilizar para el estudio es semanal, tomando como muestra el valor del día viernes de cada semana. El período muestral comprende entre el 23 de julio de 2010 y el 26 de diciembre de 2014.

A continuación se describen una por una las variables a utilizar en el modelo econométrico y su relación con el precio:

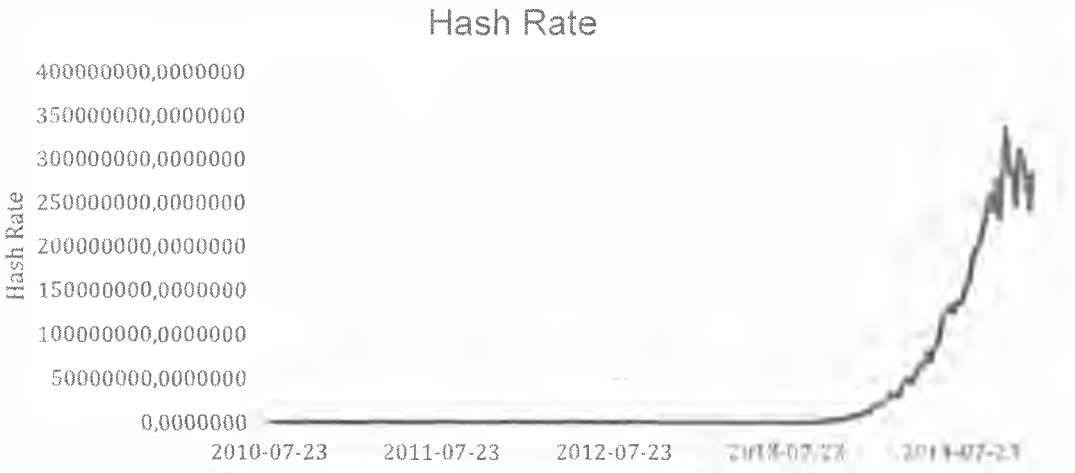
Precio de las Bitcoins: el precio de las bitcoins denominado en dólares estadounidenses es la variable a explicar. Existen varios índices y casas de cambio disponibles que publican el precio de las bitcoins. El índice a utilizar será el publicado por Coindesk, el cual calcula un promedio de los precios de diferentes casas de cambio disponibles. La información se encuentra disponible en http://www.coindesk.com/price/ diariamente y la metodología que utilizan para calcular el precio se encuentra explicada en http://www.coindesk.com/price/bitcoin-price-index/.

Tamaño de la economía: de acuerdo con Ciaian, Rajcaniova & Kancs (2014), para determinar el tamaño total de la economía pueden utilizarse 2 proxis: la cantidad de cuentas y el total de transacciones. En este caso se utilizarán la cantidad de transacciones. Como en el mundo de las bitcoins ocurren muchas transacciones espurias, más que todo con el incentivo de obscurecer la fuente de dichos fondos, se excluirán transacciones en cadena mayores a 1000 (una cadena de transacciones es un grupo de transacciones que pasa por las

mismas direcciones cierto número de veces). De acuerdo con el análisis en el mercado de oferta y demanda, se espera que este variable tenga un signo positivo. Se encuentra disponible diaria y semanalmente en: https://blockchain.info/charts

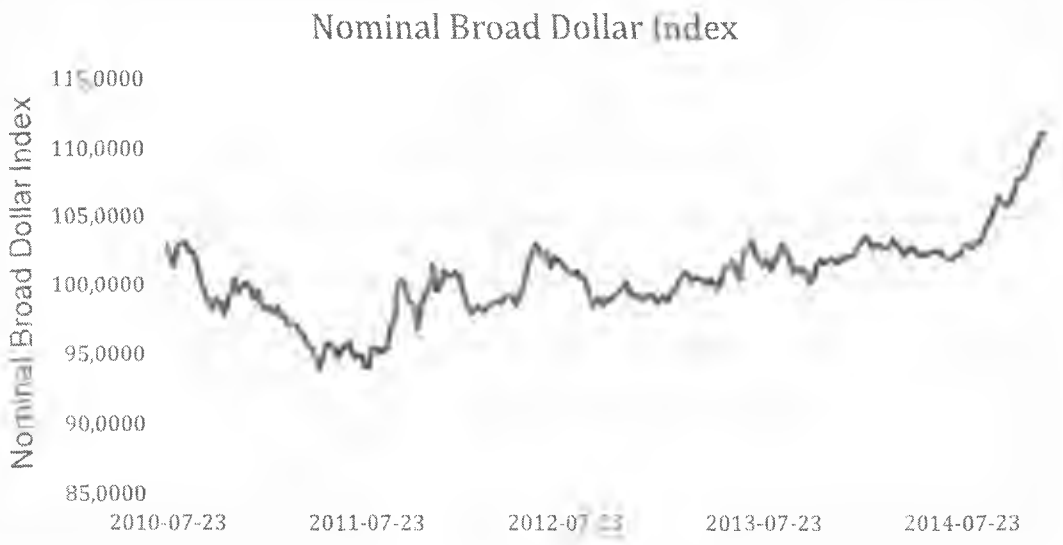
Búsquedas en Google: La data se encuentra en http://trends.google.com en la categoría "web" de forma porcentual siendo el día con más búsquedas el 100% y los demás días una proporción de este. Se espera que tenga un signo positivo ya que mayor atención puede aumentar la cantidad de transacciones y esto a su vez el precio. Puede obtenerse diaria, semanal o mensualmente.

Hash Rate: la variable explicativa de mayor peso en el modelo de producción fue la dificultad, pero ésta es una función de otra variable. La dificultad es una función del promedio de la tasa del hash rate el cual se ajusta cada 2016 bloques (aproximadamente 2 semanas). El hash rate se refiere a la cantidad de poder medido, en Gigahashes, que los miners dedican a proteger el sistema y a su vez ser recompensados. Un aumento del Hash Rate significa un aumento en la dificultad lo que debería aumentar el precio. Se encuentra en forma diaria y semanal en https://blockchain.info/charts

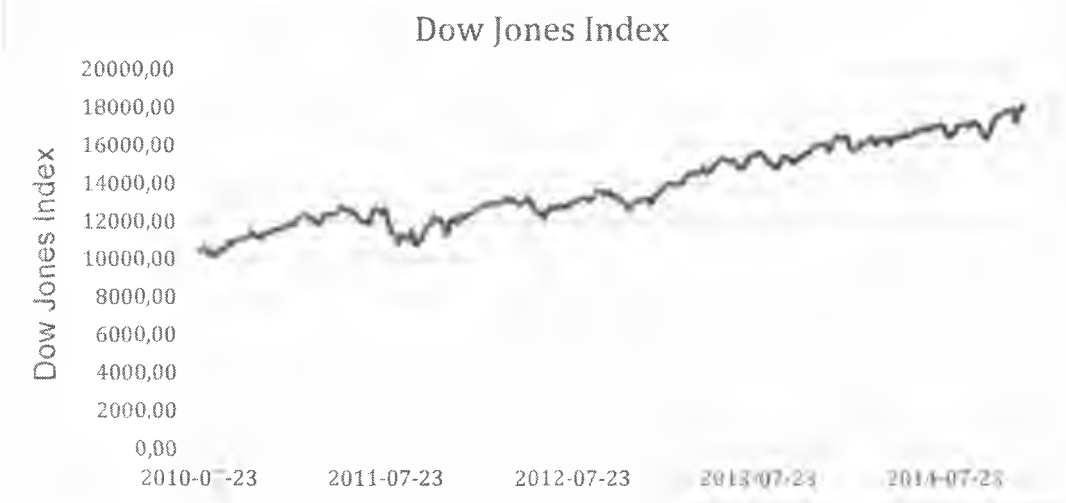


Nominal Broad Dollar Index: ya que el objetivo consiste en encontrar cuales son los aspectos que afectan en mayor medida al precio de las bitcoins, la unidad de cuenta para medir el precio también es una variable importante. Si el dólar se hace más fuerte con respecto a varias monedas, es posible que haya aumentado su poder adquisitivo y que por ende se haya fortalecido también con respecto a las bitcoins, lo cual significaría una caída en el precio. El signo esperado entonces es negativo.

Para medir el poder del dólar a través del tiempo con respecto a otras monedas se utilizará el Nominal Broad Dollar Index el cual toma en cuenta el tipo de cambio del dólar contra una cesta de monedas de forma ponderada dependiendo de las exportaciones e importaciones de los Estados Unidos. La información está disponible de forma diaria y mensual en la página web de la Reserva Federal de Estados Unidos en la sección de índices:http://www.federalreserve.gov/releases/h10/summary/



Dow Jones Index: el Dow Jones Industrial Average Index es un indicador financiero que nos da información acerca del estado del mercado estadounidense. Un aumento en el Dow Jones Index debería causar un aumento en el precio dado que una mejora en la economía de Estados Unidos debería aumentar la cantidad de transacciones y por ende el precio. La información se encuentra disponible diariamente en http://research.stlouisfed.org/fred2/series/DJIA/



CAPÍTULO 4: ANÁLISIS DE RESULTADOS

Siguiendo el método Engle y Granger de 2 etapas sobre cointegración entre las variables consideradas, se comprobó la no estacionariedad de la varianza y se transformaron las series tomando logaritmos. Luego se procedió a determinar si las series cointegran, realizando los contrastes de raíz unitaria de las variables. Las variable resultaron ser I(1) lo que significa que si cointegran.

4.1 Modelo de largo plazo

En el modelo de largo plazo fueron utilizadas las 5 variables originales: la cantidad de transacciones, las búsquedas en google, el hash rate, el nominal broad dollar index y el dow jones index. Se incluyó una única variable dummy el 2 de abril de 2011.

El resultado de la primera etapa, el cual corresponde al modelo de largo plazo, fue el siguiente:

$$LogP_t = -32{,}169 + 0{,}165.LogHash + 0{,}575.LogGoogle + 0{,}207.LogTrans + 4{,}72.LogDJI - 3{,}13.LogBDI + 0{,}99.Dum020411$$

Las 5 variables demostraron ser significativas en todos los niveles, lo que quiere que si afectan al precio de las bitcoins en el largo plazo. El modelo aprobó los tests de Dickey-Fuller, Jarque-Bera, y Breusch-Godfrey. Los resultados de los tests se encuentran en la tabla siguiente.

Tests de largo plazo				
Test	Hipótesis Nula	Valor crítico	Valor Observado	Decisión
Dickey Fuller	Presencia de raíz unitaria	-1,94	-6,66	Se rechaza la hipótesis nula
Jarque-Bera	Los residuos se distribuyen normalmente	5,99	0,99	Se acepta la hipótesis nula
Breusch-Godfrey	Ausencia de autocorrelación	3,88	191,57	Se acepta la hipótesis nula

Después de realizar la estimación de largo plazo, se comprobó que los residuos son I(0) mediante la prueba de raíz unitaria para proceder al modelo de corto plazo.

4.2 Modelo de corto plazo

Luego de determinar el modelo de largo plazo, se procede a la segunda etapa del método de Engle y Granger, correspondiente al modelo de corto plazo, mediante un "Modelo con Corrección del Error". Debido a la volatilidad extrema en los datos al comienzo del período muestral, se decidió modificar el período de estudio para este modelo. La data comprende el período entre el 30 de diciembre de 2011 y el 26 de diciembre de 2014.

Se diferenciaron los logaritmos de las series de cada una de las 5 variables, y se incluyeron los residuos del modelo de largo plazo para medir la velocidad de ajuste hacia el equilibrio. Se agregaron también los rezagos de cada variable hasta un máximo de 4 semanas, y se procedió a utilizar la metodología de Hendry "De lo general a lo particular" para determinar cuáles variables o rezagos son significativos en el corto plazo. Se incluyeron variables dummies en los días 05/04/2013, 22/11/2013, 06/12/2013 y 20/12/2013.

El modelo resultante fue el siguiente:

$DLogP_t$ = -0,022 - 0,101.RES + 0,22.DLogHash + 0,256.DLogHash(-1) + 0,125.DLogHash(-2) + 0,073.DLogGoogle(-1) + 0,113.DLogGoogle(-2) + 0,14.DLogTrans + 1,23DLogDJI(-2) + 0,363Dum050413 + 0,519.Dum221113 + 0,431.Dum061213 + 0,332.Dum201213

La variable RES son los residuos de largo plazo lo cual nos indica que el modelo tiene una velocidad de ajuste del 10% hacia el equilibrio.

El hash rate y sus primeros 2 rezagos fueron significativos, lo que es congruente con la teoría económica, ya que el precio está afectado por la dificultad inmediata. La dificultad a su vez está determinada por el hash rate de hasta 2 períodos (semanas) anteriores.

La cantidad de vistas en google fue significativa solo en su primer y segundo rezago. Esto significa que la atención de los medios y del público no afecta inmediatamente al precio de una manera significativa, si no en un período de 1 a 2 semanas aproximadamente.

La cantidad de transacciones como proxy del tamaño de la economía fue significativa sin ningún rezago. Esto significa que la cantidad de transacciones afecta al precio inmediatamente.

La última variable significativa en el modelo de corto plazo fue el índice Dow Jones con un rezago de 2 períodos, lo que significa que, al igual que la atención de los medios, no afecta al precio inmediatamente.

El Broad Dollar Index no fue significativo en el modelo de corto plazo y tampoco ninguno de sus rezagos. Esto puede deberse a que varía muy poco en el corto plazo.

El modelo aprobó los tests de Dickey-Fuller, Jarque-Bera, Breusch-Godfrey, Arch y Ramsey. Los resultados de los tests se encuentran en la tabla siguiente.

Tests de corto plazo				
Test	Hipótesis Nula	Valor crítico	Valor Observado	Decisión
Dickey Fuller	Presencia de raíz unitaria	-1,94	-11,11	Se rechaza la hipótesis nula
Jarque Bera	Los residuos se distribuyen normalmente	5,99	3,78	Se acepta la hipótesis nula
Breusch-Godfrey	Ausencia de autocorrelación	1,82	1,99	Se acepta la hipótesis nula
Arch	Ausencia de heterocedasticidad	1,59	1,71	Se acepta la hipótesis nula
Ramsey	El modelo está especificado correctamente	1,66	2,37	Se acepta la hipótesis nula

CONCLUSIONES Y RECOMENDACIONES

Esta investigación buscaba demostrar que el precio internacional de las bitcoins se ve afectado por ciertas variables como la cantidad de transacciones, la atención de los medios y el público, el Dow Jones.

Como las bitcoins son un fenómeno bastante reciente, se procedió a realizar una amplia introducción al lector acerca de las características informáticas, económicas, y legales más importantes. La alta volatilidad que presentaron las bitcoins durante el período de estudio demostró ser una debilidad importante a la hora de compararlas con monedas de curso legal.

Al realizar un análisis financiero, se concluyó que el índice con el cual han estado más correlacionados es el Dow Jones Industrial Average. Se determinó que cambios en la fortaleza del dólar, al ser ésta la unidad de medida del precio de las bitcoins, también deberían afectar al precio.

Se observó que el mercado de producción de las bitcoins cumple con la mayoría de las características de un mercado de competencia perfecta. Se procedió luego a derivar y analizar una función de producción individual. A partir de dicha función se determinó que la dificultad es una de las variables que afecta al precio.

Al realizar un análisis del mercado de oferta y demanda de las bitcoins se concluyó que la variable determinante del precio más importante en este mercado específico es el tamaño de la economía.

El estudio econométrico reflejó que todas las variables del estudio son significativas en el largo plazo y sólo el broad dollar index no lo es en el corto plazo.

Por último, se determinó la estructura de rezagos de cada una de las variables en el corto plazo y se comprobó que esta coincide con la teoría económica y las características de las bitcoins expuestas anteriormente. El valor 0,10 de los residuos nos indica que los desequilibrios de corto plazo tienden a corregirse aproximadamente un 10% en cada período, lo que refleja que el ajuste hacia el largo plazo es lento.

Para finalizar, se concluye que la investigación logró cumplir con los objetivos. Se analizaron cada una de las variables propuestas y se determinó que si afectan al precio internacional de las bitcoins.

Se considera que para futuras investigaciones se puede ampliar la cantidad de variables a analizar agregando otras que podrían no encontrarse dentro de los modelos de producción o de oferta y demanda que fueron realizados en este trabajo; por ejemplo, un índice de distribución global de las bitcoins similar a un índice de Gini. También puede llevarse a cabo la estimación econométrica con una metodología que se adapte mejor a la volatilidad de las bitcoins, por ejemplo un modelo GARCH.

BIBLIOGRAFÍA

- AFP (15/09/2014) Why Bangladesh will jail Bitcoin traders. [En línea]. Disponible en: http://www.telegraph.co.uk/finance/currency/11097208/Why-Bangladesh-will-jail-Bitcoin-traders.html
- Asamblea Nacional de la República Nacional de Ecuador (24/07/2014) Aprobación del Proyecto de Código Orgánico Monetario y Financiero. [En línea]. Disponible en: http://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-20/Aprobaci%C3%B3n%20del%20Proyecto%20de%20C%C3%B3digo%20Org%C3%A1nico%20Monetario%20y%20Financiero%20%28Urgente%20en%20materia%20econ%C3%B3mica%29.pdf
- Banco Central de la Federación Rusa (27/01/2014). Sobre el uso en las transacciones de "monedas virtuales", en particular, Bitcoin. [En línea]. Disponible en: http://www.cbr.ru/press/PR.aspx?file=27012014_1825052.htm
- Bank Indonesia (06/02/2014). Statement of Bank Indonesia Related To Bitcoin and Other Virtual Currency. [En línea]. Disponible en: http://www.bi.go.id/en/ruang-media/siaran-pers/Pages/SP_160614.aspx
- Banque de France (5/12/2013) Les dangers liés au développement des monnaies virtuelles: l'exemple du bitcoin. [En línea]. Disponible en: http://www.banque-france.fr/fileadmin/user_upload/banque_de_france/publications/Focus-10-stabilite-financiere.pdf
- Barro, R. J. (1979). Money and the price level under the gold standard. The Economic Journal, 13-33.

- Belén Marty (19/06/2014) Bolivia Not Revolutionary Enough to Tolerate Bitcoin. [En línea]. Disponible en: http://panampost.com/belen-marty/2014/06/19/bolivia-not-revolutionary-enough-to-tolerate-bitcoin/
- Bouoiyour, J., Selmi, R., & Tiwari, A. (2014). Is Bitcoin business income or speculative bubble? Unconditional vs. conditional frequency domain analysis.
- Briere, M., Oosterlinck, K., & Szafarz, A. (2013). Virtual currency, tangible return: portfolio diversification with bitcoins. Tangible Return: Portfolio Diversification with Bitcoins (September 12, 2013).
- Central Bank of Iceland (19/03/2014). Significant risk attached to use of virtual currency. [En línea]. Disponible en: http://www.cb.is/publications-news-and-speeches/news-and-speeches/news/2014/03/19/Significant-risk-attached-to-use-of-virtual-currency/
- Christin, N. (2013, May). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In Proceedings of the 22nd international conference on World Wide Web (pp. 213-224). International World Wide Web Conferences Steering Committee.
- Courtois, N. T., & Bahack, L. (2014). On subversive miner strategies and block withholding attack in bitcoin digital currency. arXiv preprint arXiv:1402.1718.
- Decker, C., & Wattenhofer, R. (2014). Bitcoin Transaction Malleability and MtGox. In Computer Security-ESORICS 2014 (pp. 313-326). Springer International Publishing.
- Donier, J., & Bonart, J. F. (2014). A million metaorder analysis of market impact on the Bitcoin. Available at SSRN.
- Engle R.F., and Granger, C.W.J. (1987). "Co-integration and error correction: Representation, estimation and testing", Econometrica, 55(2), 251-276
- Esther Han (21/08/2014). Australian Tax Office decides bitcoins are assets, not currency. [En línea]. Disponible en: http://www.smh.com.au/technology/technology-news/australian-tax-office-decides-bitcoins-are-assets-not-currency-20140820-1063gq.html

- European Parliamentary Research Service (11/04/2014). Bitcoin Market economics and regulation. [En línea]. Disponible en: http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI(2014)140793_REV1_EN.pdf
- Evans, D. S. (2014). Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms. University of Chicago Coase-Sandor Institute for Law & Economics Research Paper, (685).
- Eyal, I. (2014). The Miner's Dilemma. arXiv preprint arXiv:1411.7099.
- Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In Financial Cryptography and Data Security (pp. 436-454). Springer Berlin Heidelberg.
- Fairfield, J. A. (2014). Smart contracts, Bitcoin bots, and consumer protection. Washington and Lee Law Review Online, 71(2), 36.
- Financial Crimes Enforcement Network (27/10/2014). Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System. [En línea]. Disponible en: http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf & http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R011.pdf
- FG/Agencies (10/12/2013) Cyprus Central Bank warns about risks in use of Bitcoin. [En línea]. Disponible en: http://famagusta-gazette.com/cyprus-central-bank-warns-about-risks-in-use-of-bitcoin-p21692-69.htm
- Garcia, D., Tessone, C. J., Mavrodiev, P., & Perony, N. (2014). The digital traces of bubbles: feedback cycles between socio-economic signals in the Bitcoin economy. Journal of The Royal Society Interface, 11(99), 20140623.
- Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., & Siering, M. (2014). Bitcoin-Asset or Currency? Revealing Users' Hidden Intentions. Revealing Users' Hidden Intentions (April 15, 2014). ECIS.
- Guadamuz, A., & Marsden, C. (2014). Bitcoin: the wrong implementation of the right idea at the right time. Available at SSRN.

- Inland Revenue Authority of Singapore (27/01/2014). Income Tax Treatment of Virtual Currencies [Recuperado del 21/05/2015] en: https://www.iras.gov.sg/irasHome/page04.aspx?id=15471
- Iwamura, M., Kitamura, Y., & Matsumoto, T. (2014). Is Bitcoin the Only Cryptocurrency in the Town? Economics of Cryptocurrency and Friedrich A. Hayek. Economics of Cryptocurrency And Friedrich A. Hayek (February 28, 2014).
- Johansen, S. and Juselius, K. (1990). "Maximun Likelihood Estimation and Interference on Cointegration with Applications to the Demand for Money", Oxford Bulletin of Economics and statics 52(2): 169-210
- Johnson, B., Laszka, A., Grossklags, J., Vasek, M., & Moore, T. (2014). Game-theoretic analysis of DDoS attacks against Bitcoin mining pools. In Financial Cryptography and Data Security (pp. 72-86). Springer Berlin Heidelberg.
- Kaminski, J., & Gloor, P. (2014). Nowcasting the Bitcoin Market with Twitter Signals. arXiv preprint arXiv:1406.7577.
- Kashmir Hill (31/01/2014) Bitcoin's Legality Around The World [En línea]. Disponible en: http://www.forbes.com/sites/kashmirhill/2014/01/31/bitcoins-legality-around-the-world/
- Kaskaloglu, K. (2014). Near Zero Bitcoin Transaction Fees Cannot Last Forever. In The International Conference on Digital Security and Forensics (DigitalSec2014) (pp. 91-99). The Society of Digital Information and Wireless Communication.
- Kristoufek, L. (2014). What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis. arXiv preprint arXiv:1406.0268.
- Kroll, Joshua A., Ian C. Davey, and Edward W. Felten. "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries." Proceedings of WEIS. Vol. 2013. 2013.

- Kondor, D., Pósfai, M., Csabai, I., & Vattay, G. (2014). Do the rich get richer? An empirical analysis of the Bitcoin transaction network. PloS one, 9(2), e86197.
- Legality of bitcoin by country (s.f.) En Wikipedia. http://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country
- Lütkepohl, H., & Krätzig, M. (Eds.). (2004). Applied time series econometrics. Cambridge University Press.
- Matonis, J. (2012, November). ECB: "Roots of Bitcoin Can Be Found in the Austrian School of Economics" [Forbes.com] from: http://www.forbes.com/sites/jonmatonis/2012/11/03/ecb-roots-of-bitcoin-can-be-found-in-the-austrian-school-of-economics/
- Ministerio de Finanzas de Slovenia (23/12/203) Tratamiento fiscal de operaciones en moneda virtuales. [En línea]. Disponible en: http://www.durs.gov.si/si/davki_predpisi_in_pojasnila/dohodnina_pojasnila/dohodek_iz_kapitala/dobicek_iz_kapitala/vrednostni_papirji_in_delezi_v_gospodarskih_druzbah_zadrugah_in_drugih_oblikah_organiziranja_ter_investicijski_kuponi/davcna_obravnava_poslovanja_z_virtualno_valuto_po_zdoh_2_in_zddpo_2/
- Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013, October). A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference (pp. 127-140). ACM.
- Möser, M. (2013). Anonymity of Bitcoin Transactions. In Münster Bitcoin Conference.
- Möser, M., & Böhme, R. (2015, January). Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees. In 2nd Workshop on Bitcoin Research, affiliated with the19th International Conference on Financial Cryptography and Data Security, Puerto Rico.

- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Consulted, 1(2012), 28.
- Pavel Ciaian & Miroslava Rajcaniova & d'Artis Kancs, 2014. "The Economics of BitCoin Price Formation," EERI Research Paper Series EERI RP 2014/08, Economics and Econometrics Research Institute (EERI), Brussels.
- Pete Rizzo (22/09/2014) Belgian Tax Body: Bitcoin Trades Not Subject to VAT [En línea]. Disponible en: http://www.coindesk.com/belgium-tax-vat-bitcoin-transactions/
- Pete Rizzo (23/06/2014). Canada Amends National Law to Regulate Bitcoin Businesses. [En línea]. Disponible en: http://www.coindesk.com/canada-amends-national-law-regulate-bitcoin-businesses/
- Plassaras, N. A. (2013). Regulating digital currencies: bringing Bitcoin within the reach of IMF. Chi. J. Int'l L., 14, 377.
- Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system (pp. 197-223). Springer New York.
- Reserve Bank of India (24/12/2013). RBI cautions users of Virtual Currencies against Risks. [En línea]. Disponible en: http://www.banque-
- Reserve Bank of New Zeland (s.f.) Notes & coins frequently asked questions. [En línea]. Disponible en: http://www.rbnz.govt.nz/notes_and_coins/0094941.html
- Rogojanu, A., & Badea, L. (2014). The issue of competing currencies. Case study–Bitcoin. Theoretical and Applied Economics, 21(1), 103-114.
- Roio, D. Bitcoin, the end of the Taboo on Money. Media-N: ISEA2012 Machine Wilderness, 40.
- de Roure, C., & Tasca, P. (2014). Bitcoin and the PPP Puzzle.
- Saito, T. (2013). Bitcoin: A Search-Theoretic Approach. Tokyo, Nihon.
- Shah, D., & Zhang, K. (2014). Bayesian regression and Bitcoin. arXiv preprint arXiv:1410.1231.

- Skatterättsnämnden (14/10/2013). Mervärdesskatt: Handel med bitcoins. [En línea]. Disponible en: http://skatterattsnamnden.se/skatterattsnamnden/forhandsbesked/2013/forhandsbesked2013/mervardesskatthandelmedbitcoins.5.46ae6b26141980f1e2d29d9.html
- Smith, J. B. (2014). An Analysis of Bitcoin Exchange Rates. Available at SSRN 2493797.
- Superintendencia Financiera de Colombia (26/03/2014) Riesgos de las operaciones realizadas con "Monedas Virtuales". [En línea]. Disponible en: https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=10082781
- Swanson, T. (2014). Learning from Bitcoin's past to improve its future.
- The Law Library of Congress (01/2014) Regulation of Bitcoin in Selected Jurisdictions. [En línea]. Disponible en: http://www.loc.gov/law/help/bitcoin-survey/
- Van Wikj, D. (2013). "What can be expected from the BitCoin?" Working Paper No. 345986, Erasmus Rotterdam Universiteit.
- Vasek, M., & Moore, T. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams.
- Wandery, O. (2014). Bitcoin: A Seemingly Rampant Elevator, or is Someone Pushing its Buttons?: A Case Study on Bitcoin's Fluctuations in Price and Concept.
- Wang, J. C. Y. (2014). A Simple Macroeconomic Model of Bitcoin. Available at SSRN 2394024.
- Wesner, N. (2014). The Time Value of a Digital Currency: Bitcoin Interest Rates Dynamics. Available at SSRN 2432367.
- Wilson, M. G., & Yelowitz, A. (2014). Characteristics of Bitcoin Users: An Analysis of Google Search Data. Available at SSRN 2518603.

Anexos

Tabla 1 Anexos. Marco Regulatorio de las bitcoins por país

País	Estatus	Fecha
Alemania	El ministro de finanzas anunció que las bitcoins son una unidad de cuenta y que pueden ser usadas con propósitos fiscales y comerciales. Están clasificadas como monedas privadas.	19/08/2013
Australia	La oficina de impuestos de Australia clasifica las bitcoins como un activo y no como una moneda. En Diciembre del 2013 el presidente del Banco Central dijo que no existe una ley en contra de realizar transacciones en otras monedas.	20/08/2014
Bangladesh	Advertencia oficial del banco central de Bangladesh acerca del riesgo y del uso de las bitcoins como herramienta de lavado de dinero.	15/09/2014
Bélgica	El Servicio Público Federal de Finanzas emitió un comunicado en el que exonera a las monedas virtuales a pagar impuestos al valor agregado.	09/09/2014
Bolivia	El banco central de Bolivia prohibió en su totalidad el uso de cualquier moneda que no sea emitida o regulada por el estado, incluyendo las bitcoins.	06/05/2014
Brasil	La ley N° 12865 que regula las transacciones electrónicas permite el uso de bitcoins dado que entran en la categoría de monedas virtuales que se encuentran en un dispositivo y sistema electrónico.	09/10/2013

Canadá	El parlamento de Canadá emitió una ley que enmienda la ley previa de lavado de dinero y terrorismo para regular legalmente a las bitcoins. No prohíbe el mining ni las transacciones.	19/06/2014
China	El banco central de China prohibió a las instituciones financieras llevar a cabo transacciones en bitcoins. Individualmente es legal realizar transacciones.	05/12/2014
Colombia	La Superintendencia Financiera de Colombia emitió una carta en la que alerta acerca de los riesgos de las monedas virtuales. No prohíbe de ninguna forma el uso de las bitcoins excepto para entidades vigiladas.	26/03/2014
Croacia	El Banco Nacional de Croacia concluyó que las monedas virtuales no son monedas de curso legal pero pueden usadas legalmente.	06/12/2013
Chipre	El Banco Central de Chipre emitió un comunicado en el que alerta acerca de los peligros de las monedas virtuales, aun así no prohíbe en ningún modo el uso de estas.	11/12/2013
Dinamarca	La Autoridad Financiera Supervisora declaró que las bitcoins no son monedas y su uso no estará sujeto a regulación ni garantías.	18/07/2014
Ecuador	La asamblea Nacional de Ecuador prohibió totalmente las bitcoins y cualquier otro tipo de criptomonedas dado que están implementado un nuevo sistema monetario electrónico controlado por el gobierno.	24/07/2014

Eslovenia	El Ministerio de Financia hizo un anuncio en el cual explica que las ganancias de capital en bitcoins no están sujetas a impuestos pero si el mining y la venta de bienes.	23/12/2013
Estados Unidos	La FinCEN emitió 2 decretos en los cuales explica que cualquier persona que acepte cualquier sustituto de dinero con fin de realizar transacciones es clasificado como un trasmisor de dinero según las regulaciones actuales de la FinCEN	27/10/2014
Estonia	La junta de Impuestos y Aduanas de Estonia público en su web un documento acerca de los impuestos en transacciones denominadas en bitcoins en el cual obliga a individuos y entidades legales a registrarse como proveedores de servicios de negocios. También explica las bitcoins están sujetas a impuestos sobre la renta e impuesto al valor agregado.	13/03/2014
Finlandia	La Autoridad Tributaria de Finlandia publicó instrucciones acerca del régimen aplicado a las monedas virtuales. Al ser intercambiadas por otras monedas debe pagarse un impuesto a ganancias de capital. Al utilizarse como método de intercambio éstas ganancias también están sujetas a impuestos. La pérdida de valor de las bitcoins en cambio no puede contarse como un deducible.	28/08/2013

Francia	El Banco Central de Francia realizó un reporte donde explica que las monedas virtuales no pueden ser consideradas monedas reales o medios de pago bajo las leyes actuales. A pesar de esto no existe regulación o prohibición alguna sobre las bitcoins.	05/12/2013
Hong Kong	El secretario de Servicios Financieros y Tesorería expresó en un concejo legislativo que aunque no existe regulación alguna sobre monedas virtuales, las leyes existentes contemplan acciones contra actividades ilegales que utilicen bitcoins tales como fraudes y lavado de dinero.	08/01/2014
India	El Banco de La Reserva de India emitió un comunicado en el cual sugiere al público no involucrase en operaciones con monedas virtuales. El panorama legal no es del todo claro ya que 2 días después fue allanada la oficina del sitio web de trading buysellbit.co.in	24/12/2012
Indonesia	El Banco Central de Indonesia publicó una rueda de prensa en la que indica que las bitcoins u otras monedas virtuales no son monedas o instrumentos de pago legales.	06/02/2014
Islandia	El Banco Central de Islandia emitió un comunicado en el que prohíbe la compra de bitcoins, esto no afecta el mining.	19/03/2014
Noruega	La Autoridad Tributaria de Noruega emitió un comunicado el cual explica que las bitcoins serán	11/11/2013

	tratadas como activos sujetos a impuestos (o deducciones) y las transacciones denominadas en bitcoins también estarán sujetas a impuestos.	
Rusia	El Banco Central de Rusia publicó una carta en la que hace énfasis en que substitutos de las rupias son ilegales	27/01/2014
Singapur	La Autoridad Monetaria de Singapur decidido no interferir con las transacciones pero si serán sujetas a impuestos.	08/01/2014

La fuente de cada estatus se encuentra en la bibliografía

Demostración 1

Caso 1: α y β iguales

Si $\alpha = \beta > 0$

$$\Delta Bmg = \frac{h.86400.\alpha}{2^{32}D}.25.P - \frac{kW.\alpha}{1000}.c.24$$

$$\Delta Bmg = \alpha(\frac{h.86400}{2^{32}D}.25.P - \frac{kW}{1000}.c.24)$$

$$\Delta Bmg = \alpha(Bmg)$$

Si $\alpha = \beta < 0$

El análisis es recíproco pero el cambio en el beneficio marginal es negativo:

$$\Delta Bmg = -\alpha(Bmg)$$

Caso 2: α y β diferentes

Si $\alpha > \beta > 0$

$$\Delta Bmg = \frac{h.86400.\alpha}{2^{32}D}.25.P - \frac{kW.\beta}{1000}.c.24$$

α se puede reescribir como $\alpha = (\beta + \varphi)$ donde φ es mayor a 0

$$\Delta Bmg = \frac{h.86400.(\beta + \varphi)}{2^{32}D}.25.P - \frac{kW.\beta}{1000}.24$$

$$\Delta Bmg = \frac{h.86400.\beta}{2^{32}D}.25.P + \frac{h.86400.\varphi}{2^{32}D}.25.P - \frac{kW.\beta}{1000}.c.24$$

$$\Delta Bmg = \frac{h.86400.\varphi}{2^{32}D}.25.P + (\frac{h.86400.\beta}{2^{32}D}.25.P - \frac{kW.\beta}{10000}.c.24)$$

$$\Delta Bmg = \frac{h.86400.\varphi}{2^{32}D}.25.P + \beta(Bmg)$$

$$\Delta Bmg > \beta(Bmg)$$

Tenemos que el beneficio marginal crece en una proporción mayor a β. El análisis es análogo para $(\alpha - \varphi) = \beta$ donde φ es mayor a 0. Sustituyendo β en la ecuación en vez de α nos daría como resultado que el beneficio marginal crece en una proporción menor que α.

El análisis es el mismo para:

$\beta > \alpha > 0$
$\alpha < \beta < 0$
$\beta < \alpha < 0$

En todos los casos el cambio en el beneficio marginal siempre se encuentra entre α y β.

Demostración 2

$$\sum \frac{kW}{1000}.c = \frac{kW_1}{1000}.c_1 + \frac{kW_2}{1000}.c_2 + \frac{kW_3}{1000}.c_3 + \ldots + \frac{kW_n}{1000}.c_n$$

$$= \frac{kW_1.c_1 + kW_2.c_2 + kW_3.c_3 + \ldots + kW_n.c_n}{1000}$$

Calculando un promedio ponderado de *c* según cada *kW* resulta la siguiente ecuación:

$$= \frac{(kW_1. + kW_2. + kW_3. + \ldots + kW_n).cg}{1000}$$

$$\sum \frac{kW}{1000}.c = \frac{kWt.cg}{1000}$$