Estudio de la red Bitcoin

June 14
2013

Trabajo Final de Máster (TFM)

Máster interuniversitario en seguridad de las tecnologías de la información y de las comunicaciones (MISTIC)

Área: Seguridad en redes y aplicaciones distribuidas

Autor: Andrés Cisneros Campos

Director: Cristina Pérez Solà

UOC Universitat Oberta de Catalunya
UAB Universitat Autònoma de Barcelona
Universitat Rovira i Virgili
UIB Universitat de les Illes Balears

Resumen del proyecto:

Bitcoin [1] es una moneda digital basada en el uso de la criptografía. De hecho, Bitcoin es una de las primeras implementaciones de una cripto-moneda. A diferencia de la mayoría de las monedas convencionales Bitcoin está diseñada para trabajar en una red Peer2Peer. Es decir, Bitcoin no está controlada por una autoridad central que regula la emisión de moneda ni pone restricciones en las operaciones. La red Bitcoin permite observar todas las operaciones que se llevan a cabo en ella, ya que estas son públicas. En los primeros seis meses de 2013 Bitcoin ha aparecido en los medios y se ha dado a conocer a un público más general.

El objetivo de este proyecto es el estudio de las transacciones Bitcoin. Para ello, este trabajo pretende introducir a Bitcoin, sus direcciones, las monedas y las transacciones. Después se analizará el bloque de transacciones para ver como estos y otros parámetros han ido variando a lo largo de la vida de la red. Para concluir el trabajo se estudiará el proceso de creación de moneda o también llamado minería y se verá si es económicamente viable dedicar tiempo, energía y recursos de computación a la creación de monedas.

Abstract:

Bitcoin [1] is a digital currency based on the use of cryptography. In fact, Bitcoin is one of the first implementations of a crypto-currency. Unlike most conventional currencies Bitcoin is designed to work in a Peer2Peer network. Hence, Bitcoin is not controlled by a central authority that regulates the issuance of currency and place restrictions on operations. The Bitcoin network allows everybody to monitor all operations that are performed on it. In the first six months of 2013 Bitcoin has appeared in the mass media and has become known to a wider audience.

The objective of this project is to study the Bitcoin transaction graph. To this end, this project aims to introduce Bitcoin addresses, currencies and transactions. Then analyze the block chain to see how these and other parameters have varied over the life of the network. To conclude the project we examine the process of money creation, also known as mining and will see if it is economically viable to allocate time, energy and computing resources to create coins.

CONTENTS

1 INTRODUCCIÓN

1.1 JUSTIFICACIÓN DEL TFM Y CONTEXTO

Decidí inscribirme en el máster del MISTIC por la UOC para aumentar los conocimientos sobre la seguridad de las TIC y aprender nuevos conceptos y tecnologías. Cuando me encontré en la situación de que debía hacer un trabajo de final de máster (TFM) tenía dos opciones: hacer un proyecto a medida basándome en el trabajo que realizo a diario u optar por algo nuevo empezando desde cero. La decisión estaba clara, me informe a fondo sobre los tema que se ofrecían para hacer el TFM y elegí el que me resultaba más desconocido. Por ello he enfocado este trabajo para entender realmente lo que significa tanto a nivel tecnológico como social la introducción de una moneda virtual que está respaldada por los propios usuarios de esta.

1.2 OBJETIVOS DEL TFM

Objetivo 1: Analizar la red Bitcoin desde su creación. Para ello se analizará superficialmente el número de direcciones, el balance de las cuentas y las transacciones. Además se pretende entender como ha variado el tipo de cambio y detectar los eventos significativos que ha habido el red Bitcoin.

1. Analizar el número de monedas de la red en el grafo de transacciones
2. Analizar número de transacciones totales
3. Analizar número de monederos totales.
4. Identificar los eventos más significativos de la red
5. Analizar el tipo de cambio de la red de Bitcoin desde que se ofreció cambio de Bitcoin a dólar $ hasta la actualidad.

Objetivo 2: Analizar el número de monedas de la red Bitcoin y su comportamiento. Se pretende entender como se generan las monedas, cuantas se usan para transacciones, si existen cuentas de ahorro y si hay monedas que se han perdido y no pueden volver a usarse.

1. Analizar la tasa de creación de monedas de la red Bitcoin.
2. Que pasará cuando no se creen más monedas y en cambio algunas se vayan perdiendo.
3. Análisis de la media de monedas por dirección.
4. Cuantas monedas de las que se generan son intercambiadas por $ dólares

Objetivo 3: Entender y estudiar las direcciones de la red. Se pretende ver como es posible asociar varias direcciones a una sola persona o entidad. Si hay direcciones que no se usan y están latentes en la red, tiempo de vida, etc.

1. Contar el número de direcciones actuales y entender su tasa de creación
2. Es posible asociar varias direcciones a una sola persona/entidad
3. Detectar el patrón de uso de las direcciones y el tiempo medio de vida
4. Detectar si hay direcciones de un solo uso

Objetivo 4: Entender y estudiar los tipos de transacciones y ver como han evolucionado en la red Bitcoin. Se pretende entender el tamaño de las transacciones en función del número de monedas que mueven y ver quien genera esas transacciones.

1. Analizar la primera transacción.
2. Analizar la transacción más grande la historia, ver el origen de las monedas
3. Analizar la transacción estándar de Bitcoin (tamaño, número de receptores, etc.)

4. Analizar la evolución del número de transacciones por día y su cantidad

Objetivo 5: Analizar y estudiar la generación de bloques y su evolución en el tiempo. Se pretende entender como varían los timestamps entre bloques.

1. Estudiar la evolución del número medio de transacciones por bloque
2. Estudiar la evolución del número medio de monedas por bloque
3. Estudiar como varia el tiempo de creación entre bloques.
4. Estudiar el "generation transaction" para ver si hay ciertos usuarios que suelen resolver más bloques que otros.

Objetivo 6: Estudiar y entender el componente de minería de la red Bitcoin. Se pretende ver como han evolucionado las técnicas de minería (CPU, GPU, FPGA, ASIC). También se estudiará el comportamiento de la red respecto a las recompensas de minería y su incremento de dificultad con el tiempo. Se estudiará la distribución de mineros y como se distribuyen los nuevos BTC.

1. Estudiar la evolución de las técnicas de minado (CPU, GPU, FPGA, ASIC)
2. Estudiar el aumento de la dificultad en la generación de monedas. ¿Se puede correlar con el punto anterior?
3. Entender como funcionan las mining pools
4. Estudiar como la red se ha ajustado para mantener la tasa de creación de monedas constante.
5. Estudiar que pasará cuando se dejen de generar monedas

Objetivo 7: Analizar la rentabilidad de una inversión para hacerse minero de la red Bitcoin. Se pretende analizar tanto desde el punto de vista de la minería como de la aplicación de costes de gestión a las transacciones.

1. Analizar el coste del hardware necesario para hacerse minero.
2. Calcular el tiempo necesario para generar monedas con el hardware seleccionado en el punto anterior.
3. Análisis del coste de electricidad usado.
4. Calcular el tiempo de retorno de la inversión del hardware seleccionado.
5. Analizar si es rentable vivir de las comisiones de los costes por transacción.

Objetivo 8: Identificar como han afectado los eventos más significativos a la red Bitcoin. Aparición y desaparición de servicios, posibles ataques a la red, etc. ¿En qué fase de la curva de Gartner está la red Bitcoin?

1. Estudiar los ataques MTGox y ver que se pretendía hacer.
2. Estudiar las últimas noticias acerca de la red Bitcoin y como ha afectado al número de direcciones creadas y al número de transacciones.
3. Determinar en que punto de la curva de Gartner se encuentra Bitcoin

1.3 ENFOQUE Y MÉTODO

En Bitcoin es posible consultar todas las operaciones que se han hecho en la red, ya que estas se encuentran publicas (chain block). Gracias a estos podemos investigar sobre la red y cada uno de sus parámetros. Para realizar esta memoria la directora de está me proporciono 30GB de datos para importar en una base de datos MySQL donde poder hacer consultas sobre la red. Haciendo consultas SQL, exportando datos a tablas nuevas y a ficheros de CSV, he podido analizar la red y ofrecer la información que se encuentra en este trabajo.

Por tanto el método de trabajo ha sido investigar sobre la Bitcoin para aprender en que consiste y después usar el block chain para obtener los datos reales del comportamiento de la red durante los primeros años de vida.

1.4 PLANIFICACIÓN DEL PROYECTO

La metodología que se ha usado en este trabajo de final de máster puede ser considerada de cascada. Durante las primeras semanas se realizó una investigación inicial en el concepto de Bitcoin y sus particularidades. Tras esto se definieron los objetivos que pretendía abarcar este proyecto. En la primera fase del proyecto se analizaron los parámetros que se deseaban seguir del grafo de transacciones. Tras esta definición se importó la cadena de boques de Bitcoin en una base de datos, la cual me ha servido para poder ir obteniendo la información de la red. Tras obtener los resultados se han estudiado y se han realizado las conclusiones.

A pesar de ser una metodología en cascada, si durante alguna de las tareas se necesitaba retocar tareas pasadas. Como por ejemplo una definición más exhaustiva de los objetivos, se han reabierto tareas acabadas para acabar de retocar esos detalles.

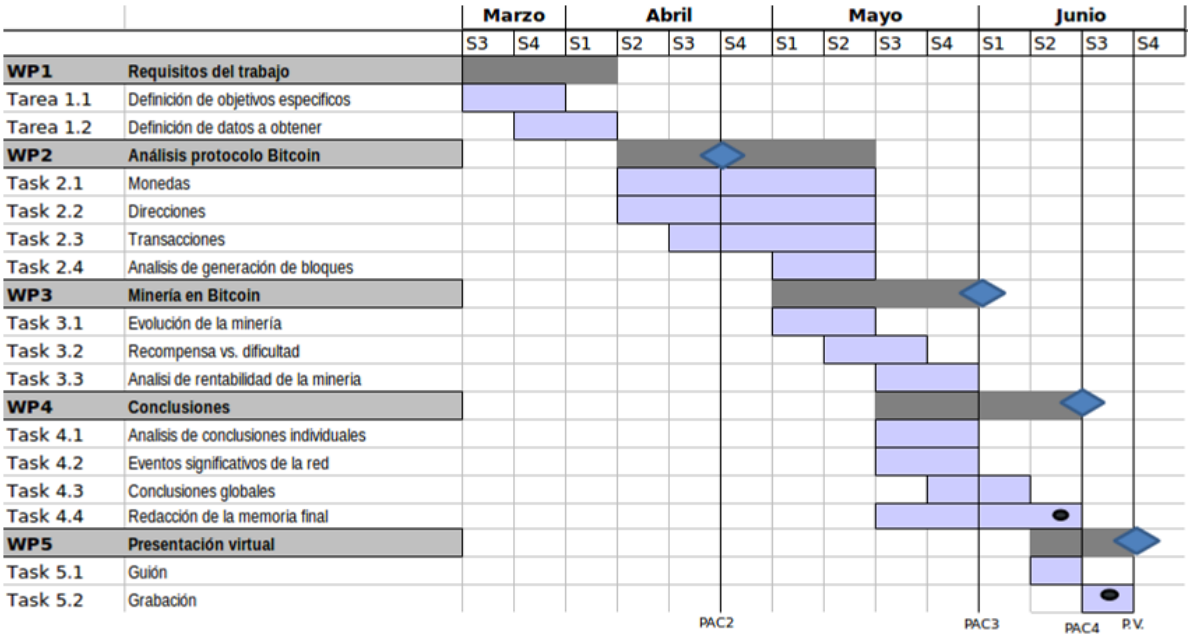


Fig. 1 - Diagrama de Gantt de la planificación del proyecto

A continuación se presentan los paquetes de trabajo o work package (WP) en los que he dividido la planificación del TFM. Además en la Fig. 1, se muestra la distribución temporal de los paquetes de trabajo y de las tareas.

1.4.1 REQUISITOS DEL TRABAJO (WP1)

En este bloque de trabajo se definirán los objetivos y se realizará el análisis de los parámetros a medir. Esta tarea pretender definir los requisitos del trabajo. Los objetivos descritos anteriormente son globales y en esta tarea se extenderán para que sean específicos y cuantificables.

1.4.2 ANÁLISIS PROTOCOLO BITCOIN (WP2)

En este bloque se estudiaran los 3 principales elementos del protocolo de la red Bitcoin: monedas, direcciones y transacciones. De estos 2 elementos se estudiará su evolución y características singulares de cada una. De las monedas se estudiará los conceptos de ahorro y pérdida de monedas. De las direcciones se estudiará el concepto de entidad que controla varias direcciones. Y de las transacciones se analizarán los tipos que hay y como han evolucionado. Además se englobará lo visto anteriormente con el análisis de la generación de bloques.

1.4.3 MINERÍA EN BITCOIN (WP3)

En esta tarea se estudiará el componente de minería de Bitcoin y como ha evolucionado con el tiempo a medida que nuevos sistemas más eficientes han aparecido (CPU, GPU, FPGA, ASIC).También se estudiará el comportamiento de la red respecto a las recompensas de minería y su incremento de dificultad con el tiempo. Además en esta tarea se analizará la rentabilidad de la red desde el punto de vista de la minería y de las comisiones por transacciones.

1.4.4 CONCLUSIONES (WP4)

En este bloque se pretende analizar en su conjunto todas las conclusiones individuales extraídas de cada bloque de trabajo. Además se analizarán de manera general como han afectado los eventos más significativos de Bitcoin a los aspectos estudiados. El output de este bloque será la realización de la memoria final.

1.4.5 COMENTARIOS SOBRE LA PLANIFICACIÓN

Debido a algunos problemas de agenda y disponibilidad, el WP2 no pudo ser empezado hasta dos semanas más tarde de lo que estaba previsto. Esto quedo reflejado en la entrega intermedia PAC2. No obstante, el trabajo pendiente pudo ser recuperado antes de la PAC3.

1.5 BREVE DESCRIPCIÓN DE LOS OTROS CAPÍTULOS DE LA MEMORIA

Para ayudar a seguir esta memoria, la siguiente tabla resume en que consiste cada uno de los capítulos.

Tabla 1 Breve descripción de los capítulos de la memoria

Capítulo	Descripción
1 Introducción	Introducción es este TFM, su formato y contenido.
2 Descripción sobre el sistema Bitcoin	Descripción teórica para entender que es la red Bitcoin.
3 Análisis del protocolo Bitcoin	Análisis realizado sobre las partes descritas en la sección 2.
4 Conclusiones	Conclusiones del trabajo realizado y pasos futuros.
5 Bibliografía	Fuentes usadas para la elaboración de este TFM.
6 Anexos	Incluye los Scripts y consultas SQL usadas en la sección 3.

2 DESCRIPCIÓN SOBRE EL SISTEMA BITCOIN

2.1 ACERCA DE BITCOIN

Bitcoin es una moneda electrónica descentralizada, fue lanzada en febrero de 2009, desde entonces ha ido ganando más adeptos y ha pasado por varias fases. Las transacciones de la red Bitcoin son totalmente públicas, es posible consultar cualquier movimiento que se ha realizado desde que se empezó hasta la actualidad. Por ello, usando estos datos, se pretende estudiar la red y su evolución al cabo del tiempo.

La red Bitcoin es usada para intercambian monedas Bitcoin o BTC. Estas monedas pueden ser fraccionadas en mili Bitcoins/mBTC (1BTC=1000mBTC), micro Bitcoins/µBTC (1mBTC=1000µBTC) o satoshis (1µBTC=100 satoshis).

Las monedas son almacenadas en monederos virtuales. Estos monederos tienen asociados una clave pública y una clave privada. La clave privada solo es conocida por el dueño y le permite poder usar las monedas que contiene su monedero. La clave pública es usada entre otras cosas para obtener la dirección de un monedero al cual poderle enviar fondos. Los monederos tienen asociada una dirección. Esta dirección puede ser comparada al número de cuenta de nuestro banco.

Para transferir fondos entre cuentas, se usan las transacciones. Para simplificar, diremos que estas transacciones indican la cuenta de origen, la cuenta de destino y el importe a transferir. Una vez realizada una transacción está será compartida a través de la red P2P entre todos los usuarios.

Cada cierto tiempo, unos 10 minutos, todas las transacciones que han sido ordenadas en ese periodo son almacenadas en bloques. El creador de este bloque es un usuario de la red que destina la capacidad computacional de su ordenador a ejecutar operaciones matemáticas que dan como resultado una cadena de caracteres. Como recompensa a ese trabajo, por cada bloque que genera la red le otorga un número concreto de BTC.

2.2 MONEDAS

2.2.1 ACERCA DE LAS MONEDAS

Bitcoin es una moneda digital. Las monedas se otorgan como premio a las personas que aportan tiempo de computación a la red creando bloques. Estas monedas son generadas de la nada (término “mining”). El número de monedas en la red es limitado y nunca superará los 21 millones de BTC. Existen casas de cambio que permiten intercambiar Bitcoins por monedas de curso legal. Las monedas pueden destruirse (al perderse la clave privada de un monedero) y ya no podrán ser recuperadas nunca más.

2.2.2 ECONOMÍA EN BITCOIN

El número de monedas total que existe en la red Bitcoin se puede cuantificar perfectamente y preveer sin error el ritmo de generación de nuevas monedas. Actualmente hay unos 6 millones de Bitcoins en circulación y se llegará a 21 millones en el año 2140, cuando ya no se podrán en circulación nuevas monedas. Por tanto la oferta de monedas de la red Bitcoin es predecible y limitada. Además la red en si no está controlada por una autoridad centralizada (como FED o BCE). Aunque previsiblemente se vea sometida a algún tipo de regulación en un futuro. Desde finales de mayo de 2013, la principal casa de cambio de la red MTGOX requiere verificar las cuentas para evitar problemas de lavado de dinero y otras actividades delictivas [11].

La ley de la oferta y la demanda determinará la equivalencia con otras monedas y el valor de las Bitcoins. Visto como un dibujo, es una curva casi sin fin que determina exactamente cuándo se generarán nuevas monedas.

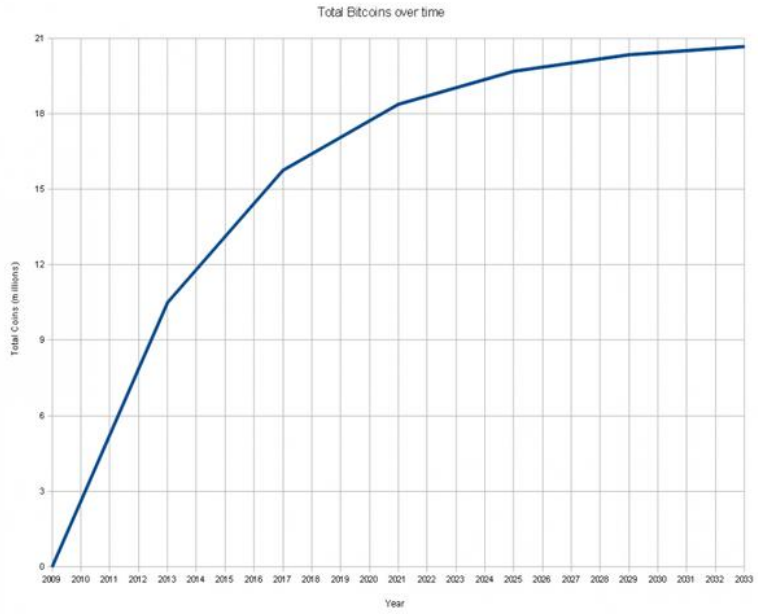


Fig. 2 - Número de monedas BTC en circulación

Fuente: https://en.bitcoin.it/wiki/File:Total_bitcoins_over_time_graph.png

Las monedas son creadas y regaladas a la persona que genera un bloque. El número de Bitcoins generado por bloque comienza en 50 y se irá dividiendo entre dos cada 210.000 bloques (unos cuatro años). Para el año 2140 la recompensa será 0 y por tanto el número de monedas no crecerá. Siguiendo esta regla, sabemos que para el año 2013 más de la mitad de todas las monedas posibles de la red Bitcoin ya habían sido minadas. Ahora mismo nos encontramos en la era donde se otorgan 25BTC por bloque. El primero de esta lista de bloques fue el bloque 210.000[1].

2.3 DIRECCIONES

Las direcciones Bitcoin generadas correctamente proceden de un número secreto al que se denomina clave privada, un tipo de clave criptográfica que se utiliza en una firma electrónica, y que es la única información necesaria para poder gastar los fondos asociados a la dirección.

Cuando se utiliza un programa cliente de Bitcoin, las claves privadas se guardan en un tipo de archivo llamado archivo monedero. El monedero consta de una clave pública y una clave privada. La clave privada es imprescindible para crear nuevas transacciones que envíen Bitcoins de una dirección a otra. Si se pierde la clave privada correspondiente a una dirección (por ejemplo, por una avería o un accidente como un incendio o una inundación que destruya el dispositivo), los Bitcoins en esa dirección se pierden para siempre.

2.3.1 ACERCA DE LAS DIRECCIONES

Una dirección BTC es un identificador de entre 27 y 34 caracteres alfanuméricos, comenzando por el número 1 o el 3, que representa un destino u origen de un pago en Bitcoins. Las direcciones se pueden

[1] http://blockexplorer.com/b/210000

generar muy fácilmente (prácticamente instantáneamente) y en número arbitrario desde cualquier programa cliente de Bitcoin, a través de servicios en Internet o monederos en línea. Además es posible hacerlo Offline. Poseer una dirección no tiene asociado ningún gasto. La dirección no contiene información sobre el dueño y son generalmente anónimas (a no ser que se publicite en una página web, foro, etc.). Pueden usarse para un solo uso y luego ser desechadas y no volver a usarse nunca más. Las direcciones aparecen por primera vez en la red Bitcoin cuando forman parte de una transacción. Cuando una dirección no ha sido usada nunca no aparece en la red Bitcoin.

El total de direcciones diferentes pueden existir en la red Bitcoin es 2^160 o lo que es lo mismo, 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976. Una de las dudas iníciales que contemplé fue que si no hay ninguna entidad central que controla la creación de direcciones y esto se hace de manera individual, es posible que dos usuarios diferentes generen la misma dirección. La respuesta corta es que sí. Pero tras investigar un poco encontré una frase que resumía la probabilidad de que esto pasase:

<<<Just to give some perspective: in order to run out of addresses, each human currently living on the planet (±6 billions) has to generate 500 million of addresses for each single nano-second (10^{-9}s) during the entire age of the universe (15 billions of years)>>> [12]

Como se puede observar de la frase anterior, la probabilidad de que alguien pueda generar la misma dirección Bitcoin es prácticamente 0, por tanto consideramos que es improbable que dos personas generen la misma dirección.

2.3.2 ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)

ECDSA es el algoritmo criptográfico usado por Bitcoin para asegurar que solo puede gastar los fondos el dueño legítimo de estos. En ECDSA encontramos los siguientes conceptos clave:

Clave privada: Es un número secreto, que sólo conoce la persona que lo ha generado. Una clave privada es esencialmente un número generado aleatoriamente o elegido por el usuario que lo genera. Es posible generar clave privadas escribiendo un texto que podemos recordar. En Bitcoin solo la persona con la clave privada que está asociada a unos fondos podrá gastarlos. En Bitcoin, una clave privada es un entero de 256 bits (32 bytes).

Clave pública: Es un número que está asociado a una clave privada, pero que puede ser anunciado y compartido. Una clave pública se puede calcular a partir de una clave privada, pero no viceversa. Una clave pública se puede utilizar para determinar si una firma es auténtica (en otras palabras si se ha generado usando la clave privada concreta) sin requerir la clave privada para ser comprobado. En Bitcoin, la clave pública se puede representar de manera comprimida o sin comprimir. Las claves públicas comprimidas son de 33 bytes, que consta de un prefijo o bien 0x02 o 0x03, y un entero de 256 bits llamado x. Las claves sin comprimir son de 65 bytes, que consta de prefijo constante (0x04), seguidas de dos números enteros de 256 bits llamados “x” e “y” (2 * 32 bytes). El prefijo de una clave comprimido permite calcular el valor de “y” a partir del valor “x”.

Firma: Es un número que demuestra que un mensaje ha sido creado por un usuario concreto. Una firma es generada matemáticamente a partir de un hash de algo que debe ser firmado y de la clave privada. La firma en si, consiste en dos números conocidos como “r” y “s”. Usando la clave pública y un algoritmo matemático se puede verificar que dicha firma ha sido realizada con la clave privada y con el hash de lo que se pretendía firmar. Las firmas son de 73, 72, o 71 bytes de longitud, con probabilidades aproximadamente el 25%, 50% y 25%, respectivamente, aunque tamaños aún más pequeños son posibles con probabilidad decreciente exponencialmente.

Tabla 2 - Resumen de los elementos de las direcciones

Elemento	Función
Clave privada	Genera la clave pública Genera firmas (permite transferir dinero) No se puede compartir Si se pierde o destruye no se podrán recuperar los fondos
Clave pública	Identifica una clave privada Se usa para verificar firmas
Dirección	Es el identificador público del monedero Identificar la cuenta para enviar BTC
Firma	Permite verificar que un mensaje ha sido firmado por el propietario de la clave privada sin conocerla.

2.3.3 DIRECCIONES MULTIFIRMA

Se pueden generar direcciones que requieran una combinación de varias claves privadas. Este tipo de direcciones dependen de algunas características añadidas al protocolo con posterioridad al lanzamiento original de Bitcoin, por lo que se las diferencia de las direcciones originales a través de un carácter inicial '3', en lugar del '1' de las direcciones convencionales. Este tipo de direcciones avanzadas equivaldrían a un cheque con más de un beneficiario, para cobrar el cual hace falta la firma de todos los beneficiarios.

El requisito concreto, como el número de claves privadas necesario para acceder a los fondos, se decide al generar la dirección. Una vez creada, no es posible cambiar esos requisitos de acceso a los fondos.

2.3.4 CODIFICANDO UNA DIRECCIÓN BITCOIN

Sería posible usar solo la clave pública para transferir dinero, pero en el protocolo Bitcoin se creo las direcciones. Ello es por una razón concreta. Las direcciones Bitcoin tienen una codificación especial. Bitcoin usa la codificación de binario a texto Base58. La respuesta de porque no se usa la base-64 la encontramos en el código fuente del cliente de Bitcoin (Tabla 3).

Tabla 3 - Cabecera del fichero base58.h

```
// Why base-58 instead of standard base-64 encoding?
// - Don't want 0OIl characters that look the same in some fonts and
//      could be used to create visually identical looking account numbers.
// - A string with non-alphanumeric characters is not as easily accepted as an account number.
// - E-mail usually won't line-break if there's no punctuation to break at.
// - Doubleclicking selects the whole number as one word if it's all alphanumeric.
```

Las principales razones son:

- Se eliminan los caracteres que se parecen para evitar el error humano al copiarlas.
- Se parecen a números de cuenta a los que las personas están más acostumbrados al no usar símbolos especiales y ser solo alfanumérico.
- Con una doble pulsación de ratón se selecciona todo el texto automáticamente.

En la Fig. 3 se puede observar cuales son las funciones matemáticas para obtener la dirección de un monedero a partir de su clave pública.

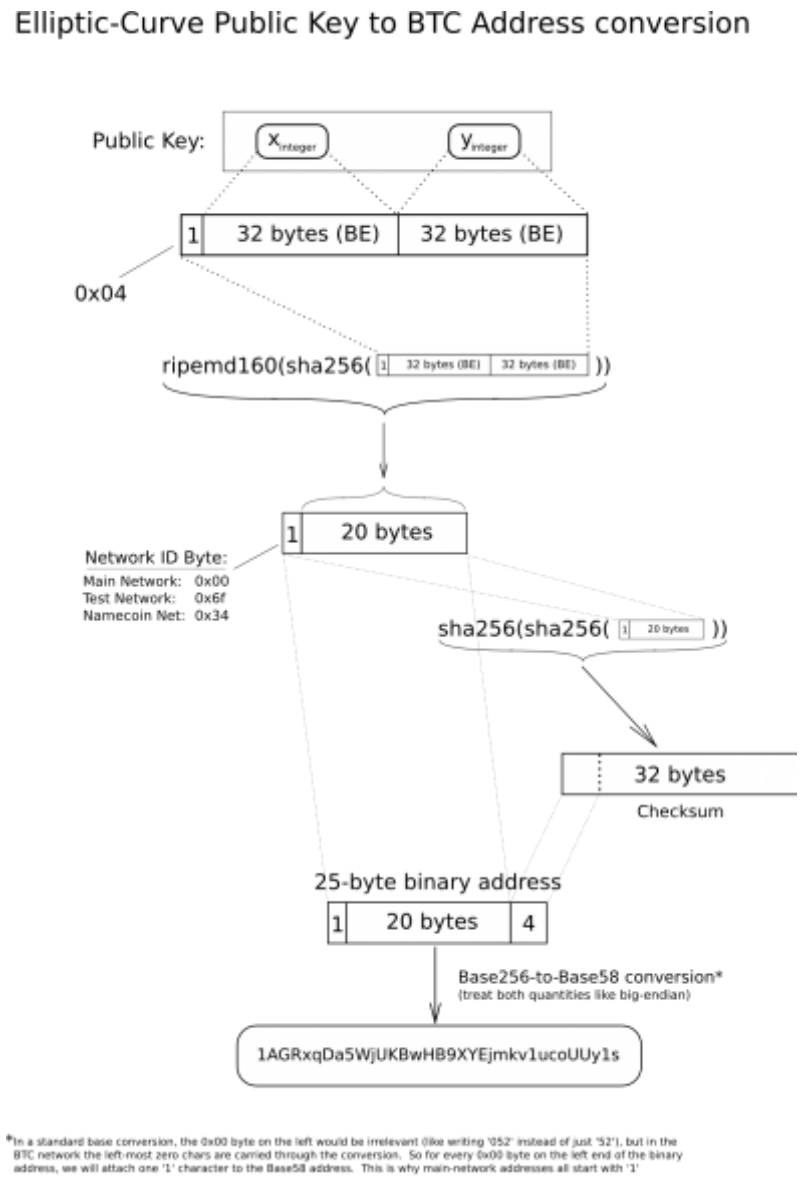


Fig. 3 - De clave pública a dirección BTC

2.4 TRANSACCIONES

Una transacción es cuando un usuario transfiere BTC a otro. El usuario difunde a los nodos de la red P2P a los que está conectado dicha transacción. Esos nodos validan las firmas criptográficas y el valor de la transacción antes de aceptarla y retransmitirla. Este procedimiento propaga la transacción de manera indefinida hasta alcanzar a todos los nodos de la red P2P. Para que los usuarios no tengan problemas, las transacciones no están encriptados con lo cual toda la red puede saber los detalles de las transacciones de todos los usuarios. Gracias a esto los usuarios pueden saber si las monedas ya han sido usadas con anterioridad. Así Bitcoin resuelve el gran problema de las monedas digitales, evitar que la moneda se pueda usar más de una vez. Hay 3 tipos de transacciones: a dirección IP, a dirección Bitcoin y generación.

Cada transacción puede ser dividida en dos partes: la entrada (de donde viene el dinero) o txinput y la salida (a donde va el dinero) o txoutput.

Input: Un input es una referencia a una salida en una transacción diferente. Es posible que un input pueda referenciar a varios outputs en una misma transacción. Cuando pasa esto, se suman los valores de las salidas mencionadas arriba, y el total se puede utilizar en las salida o txoutput de esta transacción. Para referencias a dichas transacciones usamos el hash de estas. Para verificar que la persona que ha creado la transacción tiene derecho a usar los fondos referenciados añade en el campo ScriptSig la clave pública del txoutput original y la firma (con lo que demuestra que tiene la clave privada del monedero).

Output: Un output contiene las instrucciones para enviar Bitcoins. Indica las direcciones a las que tienen que ser enviadas y la cantidad de BTC que hay que enviar a cada uno. Para evitar tocar números con decimales, los valores se dan en Satoshis y no en BTC (1 BTC = 100000000 Satoshi). El valor de todos los outputs no puede superar el que viene del Input, pero si que puede ser inferior. Es decir que podemos sacar de unas transacciones anteriores todo el dinero, por ejemplo 100BTC y solo enviar 90BTC en outputs. Pero aquellos 10BTC que no usemos no los podremos recuperar. Para ello lo que se puede hacer es crear un output que nos envíe los 10BTC a nosotros mismos, sería como tener cambio de la operación. Si por alguna razón sobra dinero al sumar los outputs, está cantidad será otorgada al que solucione el bloque como regalo o fee.

2.5 GENERACIÓN DE BLOQUES

2.5.1 BLOQUE

Todos los datos son grabados permanentemente en la red Bitcoin a través de bloques. Cada bloque contiene las últimas transacciones que han sido enviadas a la red y no están incluidas en un bloque anterior. Los bloques se utilizan para probar que las transacciones existían en un momento determinado.

Para crear un bloque se necesitan diferente información cómo el hash del bloque anterior. Además todos los bloques tienen un campo llamado 'nonce'. Que incluye un número aleatorio elegido por la persona que publica el bloque. Este campo tiene una importancia vital a la hora de crear el bloque ya que existen ciertas restricciones que veremos en el siguiente apartado.

2.5.2 TASA DE CREACIÓN DE BLOQUES

La red Bitcoin está diseñada para crear una media de 6 bloques cada hora. Por ello se usa el término dificultad para reducir la probabilidad de crear un bloque válido. Para crear un bloque válido se considera que el hash SHA-256 de todo el bloque está por debajo de un objetivo. Recordemos que el bloque tiene una parte variable que es el 'nonce' y que esto hace que cambiando el 'nonce' pueda cambiar el hash. Pues bien, la dificultad en Bitcoin es establecida con el número de ceros que tiene que poseer el hash al principio de este.

Dificultad ajustable

La red trata de crear seis bloques por hora. Cada 2016 bloques (alrededor de dos semanas), todos los clientes Bitcoin comparan el número real creado con este objetivo y modifican el objetivo por el porcentaje que ha variado. Esto aumenta (o disminuye) la dificultad de generación de bloques.

Cargo por transacciones

Como se ha explicado anteriormente existe la posibilidad de pagar tasas o 'Fees' para intentar que los mineros incluyan antes tu transacción en el próximo bloque. Cuando no se recompense con nuevas monedas a los mineros, está será la única manera de obtener beneficios por crear bloques.

2.6 MINERÍA EN BITCOIN

La minería de un bloque es difícil debido a que el hash SHA-256 de la cabecera de un bloque debe ser menor que o igual a un valor marcado por la red. El hash tiene que empezar con cierto número de ceros. La probabilidad de calcular un hash que comienza con muchos ceros es muy baja, por lo tanto, muchos intentos se debe hacer. Con el fin de generar un hash diferente cada vez, uno de los campos de la cabecera debe variar. Este campo es el 'nonce' y se incrementa cada vez para calcular el nuevo hash. Para medir la capacidad de un equipo de generar hash los datos se dan en Hash/segundo.

2.6.1 EVOLUCIÓN DE LA MINERÍA

Con Bitcoin, los mineros utilizan software especial para resolver problemas matemáticos y se emiten una serie de Bitcoins a cambio. Con el aumento de valor del BTC respecto al dólar ha habido un gran interés en optimizar la forma en la que se pueden obtener los hashes ya sea incrementado el ratio (más probabilidad de resolverlo) o con herramientas que tengan un menor consumo de energía. En esta sección se mostrará la evolución de las soluciones usadas durante los 4 años de Bitcoin.

CPU MINING

Las primeras versiones de cliente de Bitcoin usaban la potencia de la unidad CPU para minar los bloques. Las nuevas técnicas con el uso de la GPU hicieron que la minería CPU no fuera nunca más rentable. Por tanto, la opción se eliminó desde el cliente Bitcoin.

GPU MINING

La minería por GPU es drásticamente más rápida y más eficiente que la minería CPU. Este tipo de minería usa las tarjetas gráficas de última generación que son expertas en resolver problemas matemáticos que usan para las operaciones 3D y los adaptan al cálculo de hash.

FPGA MINING

La minería usando FPGA es una forma muy eficiente y rápida, comparable a la minería GPU y superando drásticamente la minería CPU. FPGAs suelen consumir cantidades muy pequeñas de energía con relativamente altas calificaciones de hash, haciéndolos más viables y eficientes que la minería GPU.

ASIC MINING

Un circuito integrado específico de la aplicación o ASIC, es un microchip diseñado y fabricado para un propósito muy específico. Los primeros ASICs diseñados para la minería Bitcoin fueron lanzados por primera vez en 2013, y están en manos de un número muy limitado de mineros. Por la cantidad de energía que consumen y el ratio de hashes que pueden producir hará que de descarte la minería por GPU por ser menos económica.

ANÁLISIS DE BUSQUEDA DE TECNOLOGIA DE MINERÍA

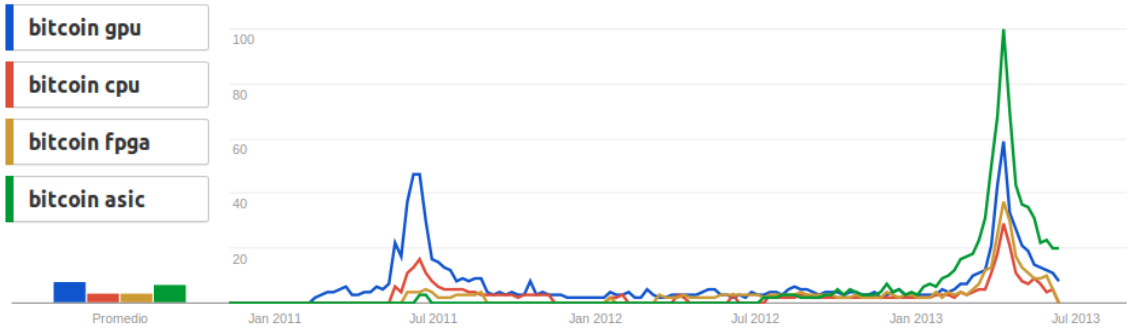


Fig. 4 - Búsqueda en Google Trends de tecnologías de minado

Como vemos en la Fig. 4 gracias a Google Trends, podemos observar como las búsquedas de las diferentes tecnologías de minado han ido evolucionando. En 2011 la mayor era GPU y en 2013 domina las búsquedas la tecnología ASIC.

2.6.2 RECOMPENSA VS. DIFICULTAD

LA DIFICULTAD

La dificultad es la medida de lo difícil que es encontrar un nuevo bloque en comparación con lo más fácil que podría ser. La dificultad se ajusta cada 2016 bloques a un valor tal que los 2.016 bloques anteriores se habrían generado en exactamente dos semanas (estimando la capacidad de proceso de la red en ese tiempo). Esto dará lugar, en promedio, a un bloque cada diez minutos. A medida que más mineros trabajan en los bloques, la tasa de creación de bloques sube. A medida que la tasa de generación de bloques aumenta, la dificultad aumenta para compensar la que empujará la tasa de creación de bloques hacia abajo. Los bloques liberados que no cumplan las restricciones son obviados por los miembros de lar red y por tanto no reciben la recompensa. Al igual que los datos de transacciones los datos sobre la dificultad son extraídos de la red. En cambio la capacidad de computación de la red solo puede ser estimada, este valor es calculado según el tiempo medio que tarda la red en resolver un bloque y la dificultad de la red.

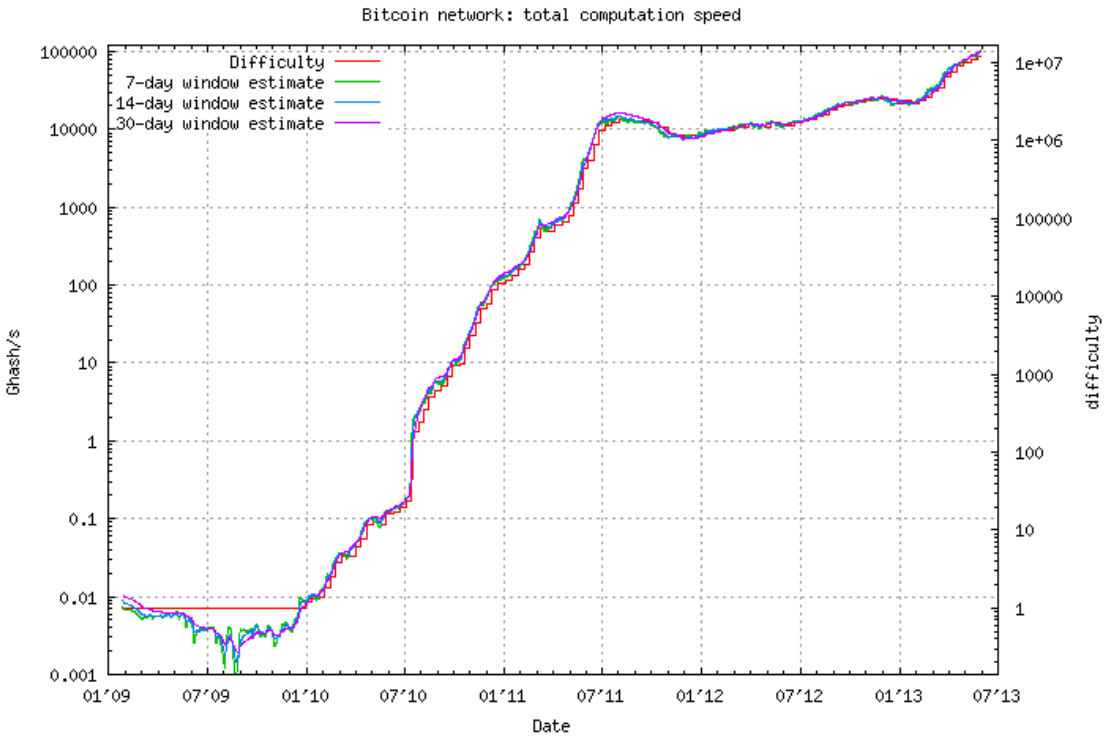


Fig. 5 – Evolución de la dificultad de resolución de bloques y de la capacidad computacional estimada

Fuente: http://bitcoin.sipa.be/

Como se puede observar en la Fig. 5 el eje vertical izquierdo muestra cual es el poder computacional de la red en orden de giga hashes por segundo. Podemos observar varias cosas curiosas en el gráfico sabiendo cuales han sido los momentos históricos de la red [13]:

La dificultad no cambió durante aproximadamente los primeros 12 meses de vida hasta el 3012/2009.

En julio de 2010 en apenas 5 días el valor del cambio de divisas se multiplicó por 10. Además a mediados de julio se estableció la casa de cambio MtGox. Esto puede verse como se dispara exponencialmente la capacidad computacional de la red. Además durante el último semestre de 2010 el cliente GPU de minería fue lanzado.

El aumento de la dificultad durante 2010, 10.000 veces en un año hace que surja la necesidad de crear las primeras pools para repartir las monedas obtenidas por bloque.

El 6 de marzo de 2011 en un periodo corto de tiempo la red alcanza 900Ghash/segundo para luego bajar a 500Ghash/ segundo. Se especula que alguna supercomputadora fue conectada a la red durante ese tiempo. Debido a esto la dificultad aumento para mantener estable el ratio de creación de bloques. Tras este periodo, al cesar el funcionamiento de este minero misterioso la dificultad decreció por primera un 10%.

A mediados de 2011 la dificultad se estabilizo alrededor de 1.000.000 y solo un año más tarde volvía a empezar a crecer de nuevo. Durante febrero de 2013 a Mayo de 2013 la dificultad se ha multiplicado por ~10. Este es debido a la inclusión de los nuevos equipos y técnicas de minado.

Una de las cosas interesantes del grafico es poder ver como se modifica la dificultad al detectarse nuevos tipos de tecnología de minada. Por ejemplo en julio de 2010 se detectó el primer bloque minado usando GPU [14] y como vemos la dificultad creció de forma exponencial. El otro gran cambio

ha sido la introducción de ASIC, no obstante, estos equipo solo están disponibles desde principios de 2013 y solo a ciertos usuarios. Pero cuando empiecen a ser enviados a los clientes veremos otro subida drástica en la dificultad.

RECOMPENSA

Cuando se descubre un bloque, el descubridor puede otorgar a sí mismos un cierto número de Bitcoins, que es acordada por todos los miembros de la red. Actualmente esta recompensa es de 25 Bitcoins, este valor se reducirá a la mitad cada 210.000 bloques. Además, el minero recibe las tasas pagadas por los usuarios que envían las transacciones. La cuota es un incentivo para que el minero para incluir la operación en su bloque. En el futuro las tasas representarán un porcentaje mucho más importante de la renta minera ya que la recompensa cada vez será menor.

Tabla 4 - Evolución de la recompensa por bloque

De	A	Recompensa	Hasta el año
0	209.999	50	2009,01
210.000	419.999	25	2013,00
420.000	629.999	12,5	2016,99
630.000	839.999	6,25	2020,99
840.000	1.049.999	3,125	2024,98
1.050.000	1.259.999	1,5625	2028,97
1.260.000	1.469.999	0,78125	2032,96
1.470.000	1.679.999	0,390625	2036,96
1.680.000	1.889.999	0,1953125	2040,95
1.890.000	2.099.999	0,09765625	2044,94
2.100.000	2.309.999	0,048828125	2048,93
2.310.000	2.519.999	0,024414063	2052,93
2.520.000	2.729.999	0,012207031	2056,92
2.730.000	2.939.999	0,006103516	2060,91
2.940.000	3.149.999	0,003051758	2064,90
3.150.000	3.359.999	0,001525879	2068,90
3.360.000	3.569.999	0,000762939	2072,89
3.570.000	3.779.999	0,00038147	2076,88
3.780.000	3.989.999	0,000190735	2080,88
3.990.000	4.199.999	9,53674E-05	2084,87
4.200.000	4.409.999	4,76837E-05	2088,86
4.410.000	4.619.999	2,38419E-05	2092,85
4.620.000	4.829.999	1,19209E-05	2096,85
4.830.000	5.039.999	5,96046E-06	2100,84
5.040.000	5.249.999	2,98023E-06	2104,83
5.250.000	5.459.999	1,49012E-06	2108,82
5.460.000	5.669.999	7,45058E-07	2112,82
5.670.000	5.879.999	3,72529E-07	2116,81
5.880.000	6.089.999	1,86265E-07	2120,80
6.090.000	6.299.999	9,31323E-08	2124,80
6.300.000	6.509.999	4,65661E-08	2128,79
6.510.000	6.719.999	2,32831E-08	2132,78

6.720.000	6.929.999	1,16415E-08	2136,77
6.930.000	7.139.999	5,82077E-09	2140,77

MINERIA COLABORATIVA (MINNING POOLS)

La minería colaborativa es un enfoque de la minería, donde múltiples clientes contribuyen a la generación de un bloque, y luego se dividen la recompensa bloque según la potencia de procesamiento que ha contribuido cada uno. La minería colaborativa reduce eficazmente la granularidad de la recompensa generación de bloque, extendiéndola más suavemente a través del tiempo. Es decir, al cabo del tiempo obtendrás el mismo número de Bitcoin pero si se hiciese individualmente se haría de golpe en un futuro y en cambio colaborando es de manera progresiva. Cada pool tiene una manera diferente de gestionar que parte de la recompensa se asigna a cada cliente. Algunas pools cobran comisiones cada vez que se resuelve un bloque, mientras que otras se quedan tan solo con las tasas que ha obtenido ese bloque. La potencia de las pools varía en función del número de clientes que la usen, podemos encontrar pools como BTC Guild [15] que soluciona 36,000 GH/s. Comparando estas cifras con las de Fig. 5 vemos que tan solo BTC Guild tiene un tercio de la capacidad total de la red Bitcoin (~110.000GH/s).

3 ANÁLISIS DEL PROTOCOLO BITCOIN

3.1 MONEDAS

3.1.1 CALCULANDO LAS MONEDAS EN CIRCULACIÓN

De la base de datos con la que trabajamos es posible extraer fácilmente el número total de monedas de la red. Para ello simplemente tenemos que consultar el campo "block_total_satoshis" del último bloque disponible en el grafo (226.203) que equivale al bloque 226202[2] de 2013-03-16 17:43:47. El resultado era 10.905.061,8697. El problema es que algo no cuadra con este resultado, ya que aún no se han empezado a generar Bitcoin con parte decimal. Si analizamos los cálculos a mano vemos que ha fallado algo en la base de datos.

- Tenemos 210.000 bloques que han sido recompensados con 50 BTC = 10.500.000 BTC
- El resto de bloques 16.203 (226.203-210.000) han recibido 25 BTC = 40.5075 BTC
- Sumando el total de monedas creadas (10.500.000+40.5075) Obtenemos 10.905.075 BTC
- Teniendo una diferencia con el dato de la base de datos de 13,1303 BTC

Investigando en la base de datos, he visto algunos bloques donde la generación no ha sido sumada de manera correcta (Ver Tabla 5).

Tabla 5 - Errores en el total de monedas en circulación de la BBDD

Identificador (block_id)	Total de monedas en circulación (block_total_satoshis)
73327	3.666.350,00000000 BTC
73328	3.666.399,99000000 BTC

3.1.2 TASA DE CAMBIO

Existen casas de cambio, entre ellas la más importante es MtGox [16]. Ya que tiene un mayor número de volumen de cambio diario, lo que permite que sea más fácil y rápido cambiar entre divisas si el precio que marcas está cerca de la oferta y demanda del mercado.

Es posible consultar el histórico de los datos de cambio desde mediados de 2010 cuando se estableció MTGox. En la Fig. 6 podemos ver la evolución tanto a nivel de volumen como en precio.

[2] http://blockexplorer.com/b/226202

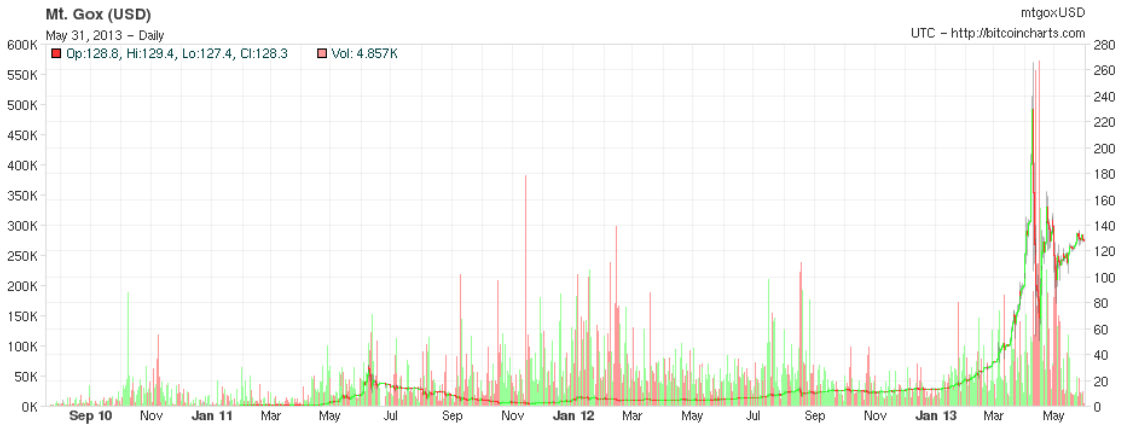


Fig. 6 - Tipo de cambio y volumen Dolar/Bitcoin

La gráfica muestra una cierta estabilidad hasta el año 2013 cuando empezó a crecer el valor hasta el gran pico tanto de valor como de transacciones que se dio en marzo de 2013.

¿Por qué ocurrió esto?

En el mes de abril de 2013 [17] MtGox ha sufrido una interrupción en su servicio de cambio de divisas en un par de ocasiones. Esto ha generado una caída del valor de BTC respecto al dólar. El problema radica en la dependencia de esta casa de intercambio de divisas con la red como se puede apreciar en la Fig. 7.

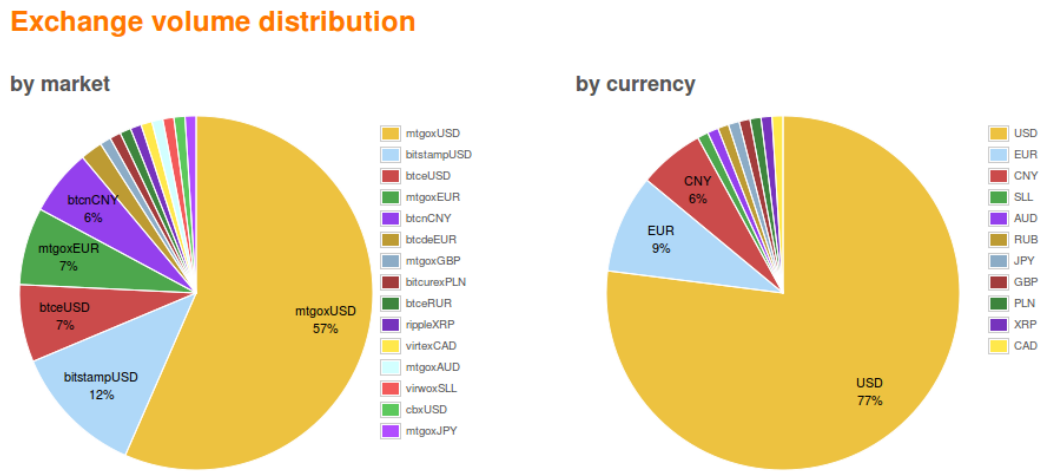


Fig. 7 - Volumen de cambio de divisas por mercado y por moneda. Fuente: http://bitcoincharts.com/charts/volumepie/

Por ello tanto si es debido a una interrupción del servicio por causas naturales o si es debido a un ataque contra el mayor sitio de intercambio de monedas esto afecta gravemente a la tasa de cambio.

3.1.3 PERDIDA O DESTRUCCIÓN DE MONEDAS

En la red Bitcoin las monedas están asociadas a un monedero, si por algún casual ese monedero se perdiese (olvidar la clave privada). Esas monedas no se podrían recuperar nunca más y por tanto desaparecerían de circulación. Debido a la falta de tiempo este aspecto no ha podido ser estudiado en el presente TFM.

3.1.4 MONEDAS AHORRADAS

En la siguiente tabla se puede ver que direcciones solo han recibido monedas y nunca las han transferido.

Tabla 6 - Top 5 monederos que solo han recibido monedas

Pubkey_id	Número ingresos	Total BTC	Total Dólares (1BTC = 103$)
1083445	61	111.111,11257544	11.444.444
268522	6	79.957,04210000	8.235.571
297910	12	50.000,04110001	5.150.000
2518480	3	50.000,04110000	5.150.000
10267771	1	44.864,20534842	4.620.992

Un punto interesante es saber el total de monedas que están guardadas en estas cuentas. El total repartido en 2.281.397 ingresos es de 8.253.452,93854854 BTC o 850.105.652 $ que lo mismo que el PIB de un país como Granada [18] de 90.000 habitantes.

3.1.5 MONEDAS EN CIRCULACIÓN

Direcciones con más monedas en la actualidad

Tabla 7 - Top 5 de direcciones con entradas y salidas con más monedas

Pubkey_id	Entradas	Salidas	Total BTC	Total Dólares (1BTC = 103$)
9551884	4	3	53.880,04210000	5.549.644
811397	18	9	53.000,04210000	5.459.000
3638721	23	1	47.458,04110000	4.888.174
3802960	122	16	47.230,15410977	4.864.690
6919902	41	22	42.660,49317786	4.393.980

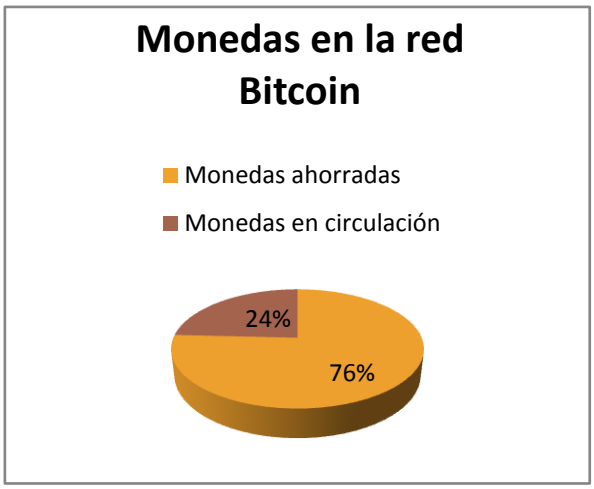


Fig. 8 - Monedas en la red Bitcoin

El análisis de las direcciones que son usadas para transmitir y recibir Bitcoins muestra que solo 2.636.221,43842568 BTC ($271.530.763) están en circulación. Esto es solo una pequeña cantidad comparado la cantidad de monedas que están ahorradas y no circulan 8.253.452,93854854 BTC. Podemos decir que un 75% de las monedas de la red no circulan. Esto es un aspecto interesante que indica que las monedas se usan más para almacenar y/o especular en un futuro que para actividades comerciales en el día a día.

El total de monedas teórico en la red en el momento de captar los datos era de 10.905.075 BTC el cual está un poco por encima de la suma de las monedas en circulación y las monedas ahorradas que sale a 10.889.674,38. Como explicaré más adelante he tenido algún problema en consultas de las transacciones donde había algunas que no apuntaban a ninguna dirección y por tanto no han sido representadas en los datos anteriores.

3.2 DIRECCIONES

3.2.1 DATOS SOBRE DIRECCIONES

Como se ha explicado en la sección anterior, crear una dirección no tiene ningún tipo de coste, ni económico, ni computacional ni de tiempo. Por ello es interesante estudiar las direcciones y como son usadas por los miembros de la red Bitcoin. En este apartado pretendo analizar que uso se les da a las 11.068.199 direcciones que aparecen en la base de datos usada en el TFM.

Direcciones usadas alguna vez pero que ahora no tienen fondos

Sabiendo los datos anteriores de número de direcciones usadas, creí necesario entender cuantas de esas cuentas han sido usados por un tiempo limitado para después dejarlas con una balance 0. Usando la consulta del anexo (6.1.10) conseguí calcularlo. Este análisis me proporcionó la información de que un total de 9.542.423 direcciones ya no tienen fondos en la red.

Direcciones usadas para transferencias que tienen fondos

Usando la consulta del anexo (6.1.10) conseguí calcularlo. Este análisis me proporcionó la información de que únicamente un total de 450,657 direcciones son las únicas que tienen fondos.

Total de direcciones de ahorro

Estas direcciones se caracterizan por solo ser usadas para recibir Bitcoins. Un Total de 840,427 solo han sido usados para almacenar monedas. Es decir son direcciones que solo reciben monedas y nunca las han transmitido a otras cuentas. Muchas de estas direcciones se encuentran en la primera fase de Bitcoin donde direcciones que solo recibían la recompensa por crear bloques iban almacenando monedas sin usarlas nunca.

Análisis de direcciones

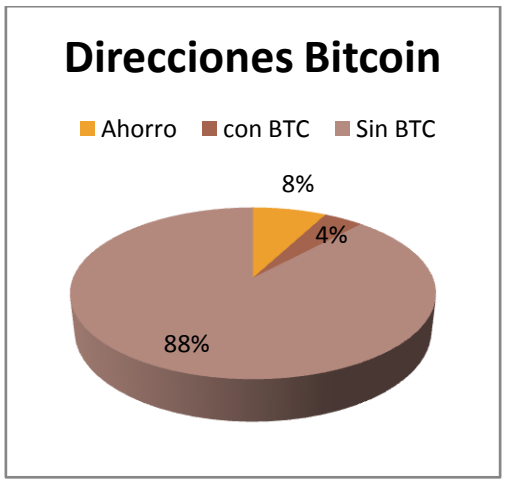


Fig. 9 - Clasificación de direcciones

Con los datos anteriores estaba claro que muchas de las direcciones de Bitcoin se habían abandonado lo cual tiene sentido ya que no cuesta nada crear una nueva. Pero para ver gráficamente que proporción de cuentas activas con y sin Bitcoins y compararlas con el número de cuentas de ahorro se ha incluido la Fig. 9. En ella vemos que las direcciones sin Bitcoins representan un 88% del total de direcciones usadas durante la vida de la red.

3.3 TRANSACCIONES

3.3.1 LA PRIMERA TRANSACCIÓN

La primera transacción[3] de la red se produce en el bloque 0[4]. Como antes de este bloque no existían transacciones previas esta transacción solo podía ser de generación. La transacción es si tenía los siguientes detalles:

Hash	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Número de inputs	1
Número de inputs	1
Total	50 BTC
Número de outputs	1
Total out	50 BTC
Tamaño	204 bytes
Fee	0 BTC

Input

Output Previo	Cantidad	De	Tipo	ScriptSig
N/A	50 BTC	N/A	Generación	04ffff001d0104455468652054696d65732030332f4a616e2f323030392043 68616e63656c6c6f72206f6e206272696e6b206f66207365636f6e6420626 1696c6f757420666f722062616e6b73

Output

Índice	Usado	Cantidad	A dirección	Tipo	ScriptPubKey
0	No	50 BTC	1A1zP1eP5QGefi2DM PTfTL5SLmv7DivfNa	Clave pública	04678afdb0fe5548271967f1a67130b7105cd6a828e03909 a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112d e5c384df7ba0b8d578a4c702b6bf11d5f OP_CHECKSIG

Como detalle, analizando toda la cadena de bloques y veremos que estos 50BTC no han sido nunca usados. Esta dirección fue usada para ingresar la recompensa del primer bloque. Durante la vida de la red ha habido diferentes transacciones de pequeñas cantidades de monedas que han tenido destino está dirección, pero los fondos nunca han sido transferidos a otra dirección.

3.3.2 DATOS SOBRE TRANSACCIONES

Analizando las transacciones con más BTC de la historia de la red

Tx_id (BBDD)	Total BTC	Bloque	Fecha	Valor en $Dólares[5]
1867247	550.000,00000000	153509[6]	2011-11-16 05:59:08	1.375.000
1868080	500.020,70037663	153527[7]	2011-11-16 09:17:36	1.250.050
1873035	499.743,98238996	153634[8]	2011-11-17 04:53:35	1.124357
1873399	499.660,08738996	153649[9]	2011-11-17 06:31:31	1.249.150
1873615	499.620,97474996	153657[10]	2011-11-17 07:25:54	1.249.052

[3] http://blockexplorer.com/t/3pTRm5YNJz
[4] http://blockexplorer.com/b/0
[5] Se ha calculado mediante el histórico de MTGox
[6] http://blockexplorer.com/b/153509
[7] http://blockexplorer.com/b/153527
[8] http://blockexplorer.com/b/153634
[9] http://blockexplorer.com/b/153649

Como podemos observar estas transacciones tienen un valor superior a un millón de dólares. Sin poder citar una fuente oficial solo puedo comentar que parece ser que fue MtGox que quería consolidar sus cuentas.

3.4 ANÁLISIS DE GENERACIÓN DE BLOQUES

3.4.1 DATOS SOBRE BLOQUES

Para analizar los siguientes puntos sin sobrecargar la base de datos con consultas, he realizado los siguientes pasos:

Exportar a un fichero de texto CSV los datos que extraje de la base de datos usando la consulta recogida en el anexo (6.1.2). Después he podido usar programas como Matlab, Octave, R, Bash script o programas escritos en Java para dibujar las tablas que necesito. En mi caso he decidido hacer el análisis de los datos usando Bash scripting.

El primer paso es agrupar los datos por días. He considerado que el día natural no tiene ninguna importancia debido a las diferentes zonas horarias, por tanto considero un día como el primer tiempo del primer bloque más 24 horas. Todo lo que este entre esos dos tiempos formará parte del mismo día.

El script me devolverá los datos agregados por día de EPOCH, Numero de Bloques, número total de monedas transmitidas por día, número medio de monedas movidas por bloque, máximo número de monedas de bloque, total transacciones, número media de transacciones por bloque, número máximo de transacciones bloque y tiempo medio que pasa entre bloques. El script tiene como parámetro de entrada el fichero sacado de la base de datos en el punto anterior. El script puede encontrarse en los anexos.

La salida del script ha sido importada en una hoja de cálculo para obtener los siguientes gráficos.

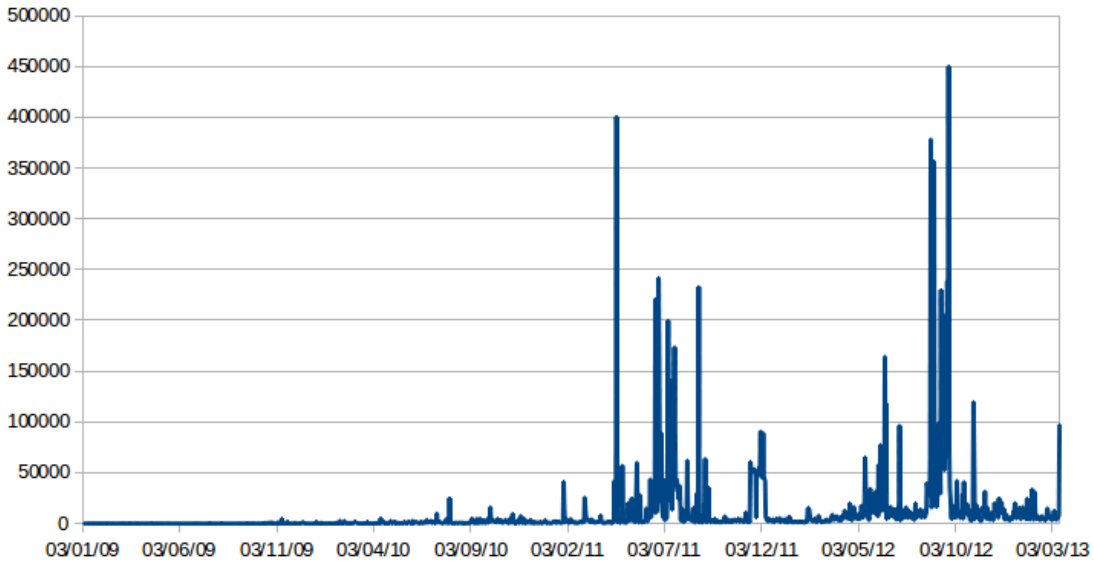


Fig. 10 – Máximo número de monedas transferidas por bloque y por fecha (en BTC)

[10] http://blockexplorer.com/b/153657

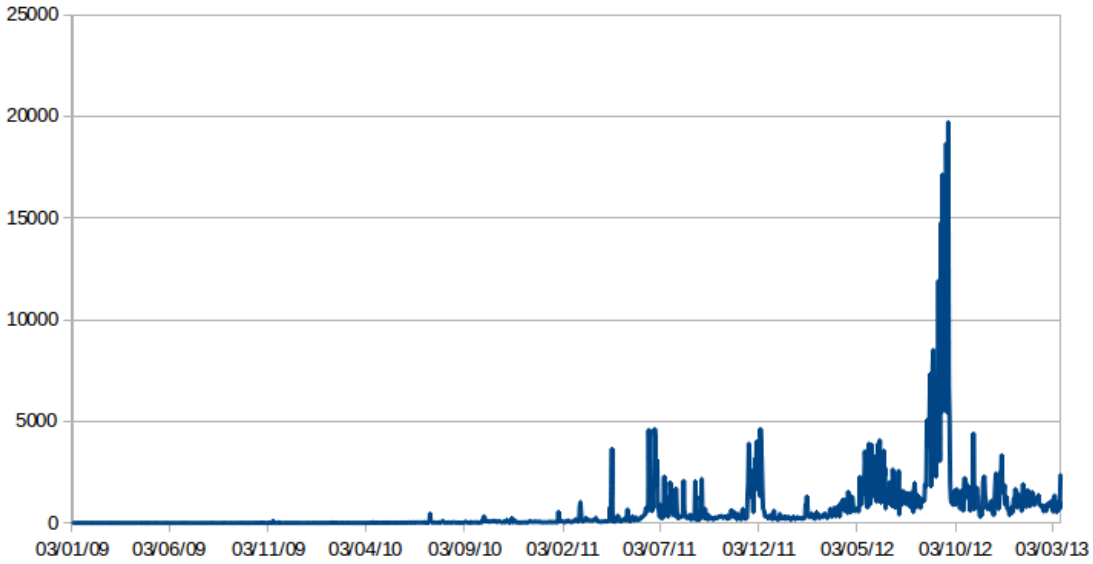


Fig. 11 – Media de número de monedas transferidas por bloque y por fecha (en BTC)

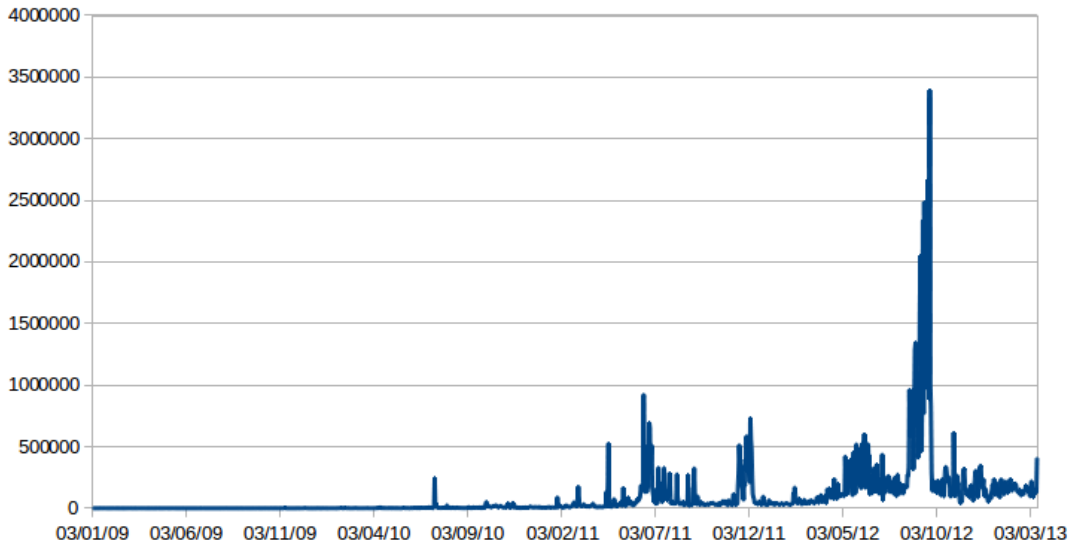


Fig. 12 – Total de dinero transferido por día en BTC

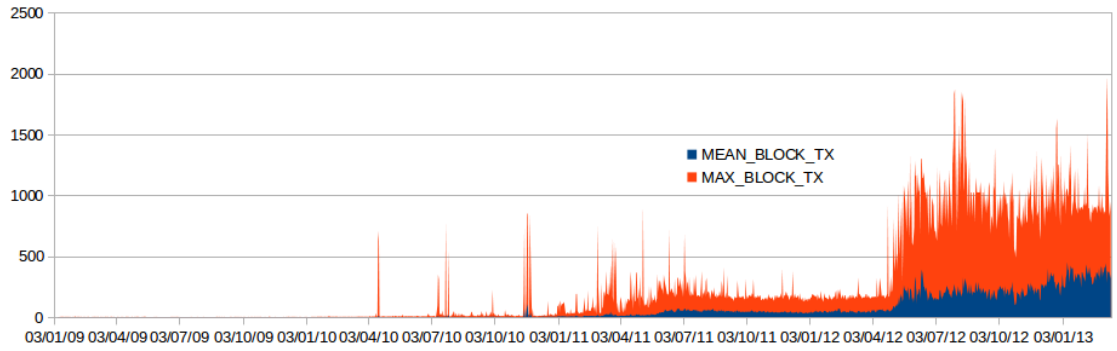


Fig. 13 - Número medio de transacciones por bloque

Tras analizar las gráficas vemos que ha habido un periodo donde la red se ha mantenido muy calmada y a partir del año 2011 empieza ha haber más actividad. A partir de mediados de 2012 hay otro gran crecimiento que se mantiene estable hasta ahora.

Bloques con más transacciones

Resultado en detalle

Bloque	Total de transacciones	Fecha
225203	1976	2013-03-10 15:20:35
191716	1871	2012-07-31 19:44:18
193271	1852	2012-08-10 21:14:36
193645	1836	2012-08-13 05:20:13
191652	1833	2012-07-31 08:29:54

El bloque con más transacciones hasta la fecha fue el Block 225203[11] (225204 en nuestra BD) que alcanzó el número de transacciones almacenadas en 1976.

Bloques con más outputs

Resultado en detalle:

Bloque	Total de transacciones	Fecha
203181	2793	2012-10-14 02:21:46
206692	2615	2012-11-06 06:50:27
225634	2597	2013-03-13 10:15:17
204704	2360	2012-10-24 05:31:52
206537	2355	2012-11-05 06:06:49

3.4.2 VARIANZA DE TIEMPO ENTRE SOLUCION DE BLOQUES

Analizando el campo block_nTime de cada bloque podemos averiguar cada cuanto se generan los bloques. El problema es que debido a que este tiempo lo decide el creador del bloque. Puede que haya casos donde el problema radique en ordenadores que no tienen el reloj bien ajustado o que son manipulados de manera premeditada por el creador del bloque. Como resultado de esto, se pueden dar casos de que haya bloques que hayan sido creados antes que su anterior (según el campo nTime) cosa que no es posible. Por esta razón estos bloques no han sido contados para el siguiente estudio. En total he encontrado 5286 bloques los cuales tienen error en el campo nTime. Un ejemplo puedes ser:

Bloque	Tiempo de creación (block_nTime)
226149	2013-03-16 10:41:32
226150	2013-03-16 10:41:22

Después de analizar los bloques podemos obtener los siguientes datos:

- Máximo tiempo entre bloques: 90532 segundos (+25 horas)
- Tiempo medio entre bloques: 590.7 segundos (9.8 Minutos)
- Desviación estándar: 799.470 segundos

[11] http://blockexplorer.com/b/225203

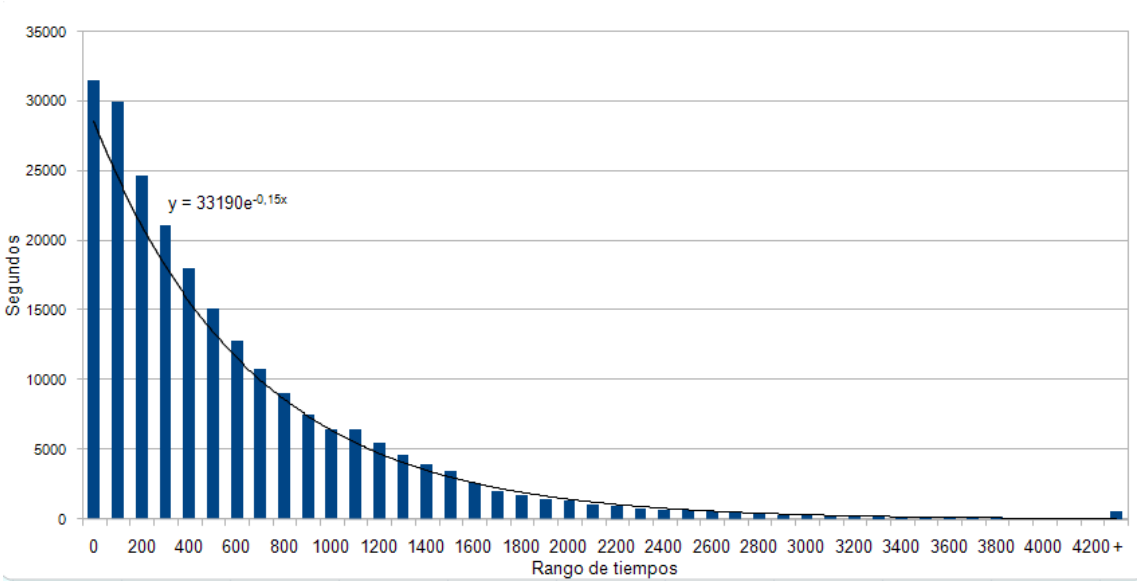


Fig. 14 - Distribución de tiempo de resolución entre bloques

Como podemos apreciar en el histograma de la Fig. 14, la distribución de creación entre bloques se puede aproximar por la formula $y=33190e^{-0.15x}$. La media de tiempo se marca en los 600 segundos (10 minutos).

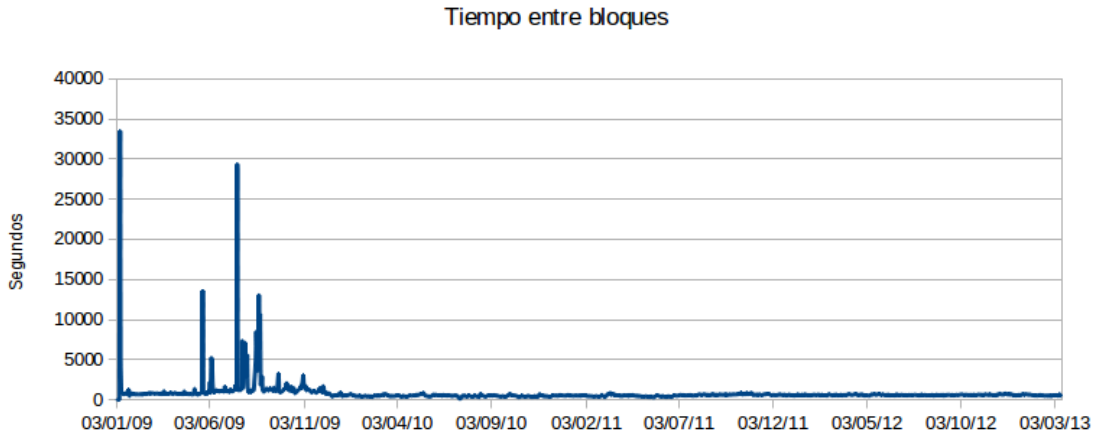


Fig. 15 - Media de tiempo entre bloques por fecha

El primer máximo es normal debido al tiempo que tardo la red en resolver el segundo bloque después del bloque génesis. Para los siguientes conviene que veamos la Fig. 5, donde se aprecia como la red descendió en número capacidad computacional.

3.4.3 CADENA DE BLOQUES (BLOCKCHAIN)

Una cadena de bloques es una base de datos de transacciones compartidas por todos los nodos que participan en el sistema basado en el protocolo de Bitcoin. Una copia completa de la cadena de bloques contiene cada transacción ejecutada en la red. Con esta información, se puede averiguar la cantidad de monedas que pertenecía a cada dirección en cualquier momento de la historia de la red.

Cada bloque contiene un hash del bloque anterior. Esto tiene el efecto de crear una cadena de bloques desde el bloque de Génesis hasta el bloque actual. Cada bloque está garantizado para llegar después de

que el bloque anterior cronológicamente, ya que uno de los campos del bloque es el hash del bloque anterior. Como los siguientes bloques incluyen el hash del bloque anterior, es poco práctico modificar bloques antiguos ya que habría que generar también los nuevos hash de los bloques. Estas propiedades son las que hacen doble gasto de Bitcoins muy difícil. El bloque de la cadena es la principal innovación de Bitcoin.

3.4.4 EL PRIMER BLOQUE (GÉNESIS)

El bloque génesis es el primer bloque de la cadena de bloques de Bitcoin. Se dice que fue creado por Satoshi Nakamoto. La recompensa del primer bloque valorado en 50BTC la recibió la dirección 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa. De todas formas debido a una particularidad en la forma que está expresado este bloque hace que estos 50BTC no puedan usarse. Al ser el primer bloque parece que fue hecho de manera voluntaria.

Tabla 8 - Detalles del bloque de génesis

Campo	Valor
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Time	2009-01-03 18:15:05
Difficulty	1
Transactions	1
Total BTC	50
Size	285 bytes
Merkle root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Nonce	2083236893
Campo	Valor
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Time	2009-01-03 18:15:05
Difficulty	1
Transactions	1
Total BTC	50
Size	285 bytes
Merkle root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

3.5 ANÁLISIS DE LA RENTABILIDAD DE LA MINERÍA

En esta sección se analizará la rentabilidad que tendría montar un sistema dedicado a la minería de Bitcoin. En este apartado se pretende analizar costes e ingresos de manera bisemanal para poder aumentar la dificultad y plantear 3 escenarios (aumenta mucho, aumenta poco, sigue como está). El análisis se hará a un año vista para ver si es posible recuperar la inversión. A fecha de 13 de junio de 2013, la dificultad está en 15.605.633 y se prevé que aumente un 18% en la próxima subida.

3.5.1 SELECCIÓN DEL HARDWARE

Uno de los aspectos que siempre se menosprecia el coste hora de la persona que va a gestionar el sistema. Por esto, lo que haré es intentar seleccionar un sistema que sea lo más sencillo posible y que requiera la menor intervención humana posible.

Por ello he seleccionado un equipo de hardware que puede funcionar de manera autónoma gracias a su puerto Ethernet. Este equipo puede reservarse pero por ahora no envían unidades.

Product	Mhash/s	Watts/h	Price	Type	Other
Avalon ASIC #1	66300	620	1299	ASIC	Ethernet

3.5.2 SELECCIÓN DEL POOL

Para este ejemplo he preferido seleccionar una pool en vez de hacer el minado por mi cuenta. Consultando la tabla de pools [10] he decidido optar por BTCGuild ya que tiene la mayor cuota de mercado. La parte negativa radica en que hay que destinar un 5% de los ingresos a las fees del mining pool.

3.5.3 RETORNO DE LA INVERSIÓN (PROVISIONAL)

Antes de calcular cuales son los ingresos, se plantean los costes derivados que tiene la minería de Bitcoin. Además del coste que tiene la adquisición del hardware nos podemos encontrar con los siguientes costes (Tabla 9). Los costes variables dependen de la cantidad de bloques que resolvamos. He incluido en la categoría de costes variables las comisiones que cobre el pool y la comisión que se quede la casa de cambio. Después de sumar los ingresos y restar los costes he calculado cual es el importe final antes de impuestos y después de impuestos. He considerado que la tasa de cambio estará estable durante el periodo en cuestión. Es importante ver que para el estudio he dividido los periodos de tiempo en bloques de dos semanas ya que cada dos semanas es cuando cambia la dificultad.

Tabla 9 - Costes asociados a la minería de Bitcoin

Costes		
Electricidad	0,138658	€/kWh
Internet	39	€/Mes
Uptime	99%	
Pool fee	5%	
Recompensa	25	BTC
Comision cambio	5%	
Impuestos	20%	
Gastos 2 semanas		
Internet	19,5	€
Electricidad	28,89	€

Tabla 10 - Resumen de rentabilidad de los 5 primeros meses

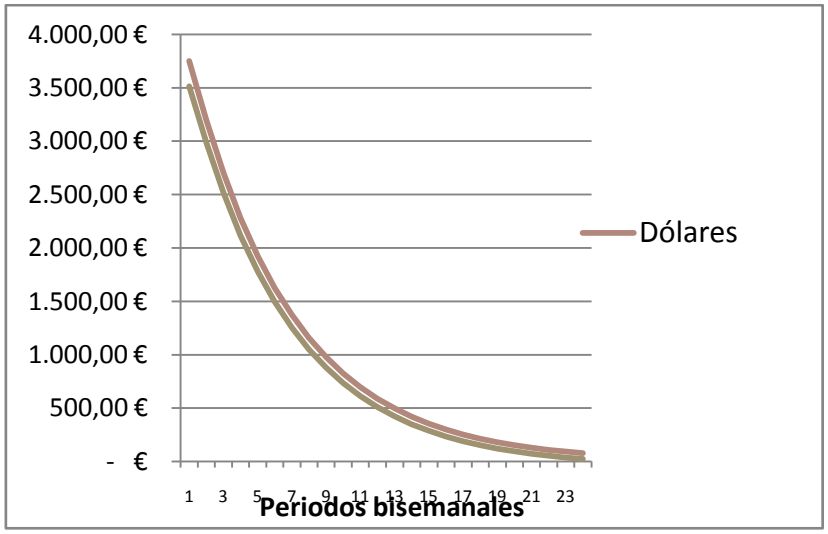
Periodos (2 semanas)	1	2	3	4	5	6	7	8	9	10
Dificultad	15.605.633	18.490.341	21.908.289	25.958.045	30.756.401	36.441.735	43.178.005	51.159.478	60.616.330	71.821.285
$ por BTC	128	128	128	128	128	128	128	128	128	128
Time/block (seg)	4,7E+28	5,6E+28	6,6E+28	7,8E+28	9,3E+28	1,1E+29	1,3E+29	1,5E+29	1,8E+29	2,2E+29
Time/block (dias)	11,7	13,8	16,4	19,4	23,0	27,3	32,3	38,3	45,4	53,8
Block Periodo	1,20	1,01	0,85	0,72	0,61	0,51	0,43	0,37	0,31	0,26
BTC periodo	29,96	25,28	21,34	18,01	15,20	12,83	10,83	9,14	7,71	6,51
BTC periodo(Con Uptime)	29,66	25,03	21,13	17,83	15,05	12,70	10,72	9,05	7,64	6,44
BTC/dia	2,12	1,79	1,51	1,27	1,07	0,91	0,77	0,65	0,55	0,46
Comision pool (BTC)	1,48	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Costes										
Electricidad	28,89 €	29 €	29 €	29 €	29 €	29 €	29 €	29 €	29 €	29 €
Internet	19,50 €	20 €	20 €	20 €	20 €	20 €	20 €	20 €	20 €	20 €
Amortización HW										
Total costes	48,39 €	48 €	48 €	48 €	48 €	48 €	48 €	48 €	48 €	48 €
Total										
Dólares	3.751,96 €	3.204 €	2.704 €	2.282 €	1.926 €	1.626 €	1.372 €	1.158 €	977 €	825 €
Comisión cambio	187,60 €	160 €	135 €	114 €	96 €	81 €	69 €	58 €	49 €	41 €
Ingresos-Gastos	3.515,98 €	2.995 €	2.520 €	2.120 €	1.781 €	1.496 €	1.255 €	1.052 €	880 €	735 €
Beneficios (impuestos)	3.515,98 €	2.995 €	2.520 €	2.120 €	1.781 €	1.496 €	1.255 €	1.052 €	880 €	735 €
Acumulado	**3.516 €**	**6.511 €**	**9.031 €**	**11.151 €**	**12.932 €**	**14.428 €**	**15.683 €**	**16.735 €**	**17.615 €**	**18.350 €**

3.5.4 EXPLICACIÓN DEL ESTUDIO

La Tabla 11 y La dificultad ha sido estimada para que aumente un ratio de un 18% en cada etapa. Esto ha sido calculado mediante la dificultad actual (15.605.633) y la prevista para el siguiente ciclo (18.490.341).

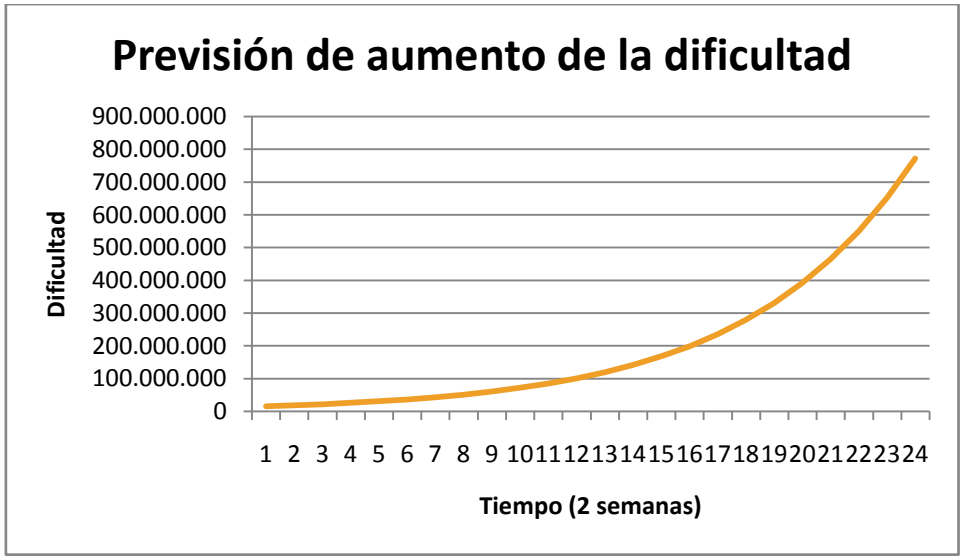
Tabla 12 muestran como se va reduciendo los ingresos a medida que van pasando las semanas y la dificultad aumenta. Es interesante ver como los costes no son muy elevados y se mantienen constantes (electricidad, internet) y los variables como las comisiones que se pagan al realizar el cambio de divisa o al mining pool también son constantes. Por ello la mayor incógnita que encontramos es saber cuanto valdrá la dificultad en el futuro.

Tabla 11 - Previsión de ingresos a 1 año



La dificultad ha sido estimada para que aumente un ratio de un 18% en cada etapa. Esto ha sido calculado mediante la dificultad actual (15.605.633) y la prevista para el siguiente ciclo (18.490.341).

Tabla 12 - Previsión de aumento de la dificultad a 1 año



3.5.5 CONCLUSIONES SOBRE EL NEGOCIO DE LA MINERIA

La conclusión que he extraído de este estudio es que parece que merece la pena durante unos meses. Económicamente sale viable y se recupera la inversión enseguida, pero también es verdad que debido a los nuevos ASIC que llegaran al mercado la dificultad crecerá tanto que bajará mucho la cantidad de Bitcoins conseguidos.

Además teniendo en cuenta la volatilidad de la moneda esto hace que sea una inversión arriesgada. El mayor problema radica en el plazo de entrega que no está siendo respetado por los distribuidores de hardware ASIC. Por ello creo que invertir en tecnología de minería para Bitcoin no es recomendable.

Además hay una duda que me inquieta, los fabricantes de hardware ASIC ofrecen equipos cuyo costes se amortiza en menos de una semana. Por ello creo que quizás algunos fabricantes están retrasando la salida al mercado de estos mientras lo usan para minar sus propias monedas, ya que a la tasa de cambio actual obtienen más beneficios minando que no vendiendo ese hardware.

4 CONCLUSIONES

4.1 ANÁLISIS DE CONCLUSIONES INDIVIDUALES

Problemas de trabajar con base de datos tan grande y el tiempo que tarda en realizar las consultas. Haría falta tener más experiencia en consultas MySQL para poder optimizarlas. Además he encontrado algunos problemas con algunos registros, como por ejemplo pubkey_id=NULL, que han hecho que algunos resultados no sean exactos. Por ejemplo he encontrado transferencias que no apuntaban a ninguna dirección, y por tanto esas monedas no han sido interpretadas correctamente.

Este TFM me ha permitido entender a nivel tecnológico como funciona la red, que partes tiene y como soluciona los problemas de la moneda digital. La curva de aprendizaje ha sido un poco lenta al principio pero después he conseguido entender como funcionan las cosas y como obtener la información que buscaba. No obstante no me ha sido posible indagar en algunos aspectos de la red tan a conciencia como hubiera deseado.

Del análisis de bloques, vemos que la red Bitcoin no es usada de manera constante, sino que cada cierto tiempo toda la red sufre un gran número de movimientos que se reflejan en los picos.

La aceptación del gran público de Bitcoin es un tema complicado, analizando el interés de este a través de Google Trend podemos ver que el mayor interés ha sido cuando la red ha sufrido problemas o el ratio de cambio se ha disparado. Esto hacer que las personas pensando que pueden obtener dinero gratis empiecen a usar la red Bitcoin. Además el ratio de cambio de 1BTC por a 103$ hace que se despierte el interés por la minería.

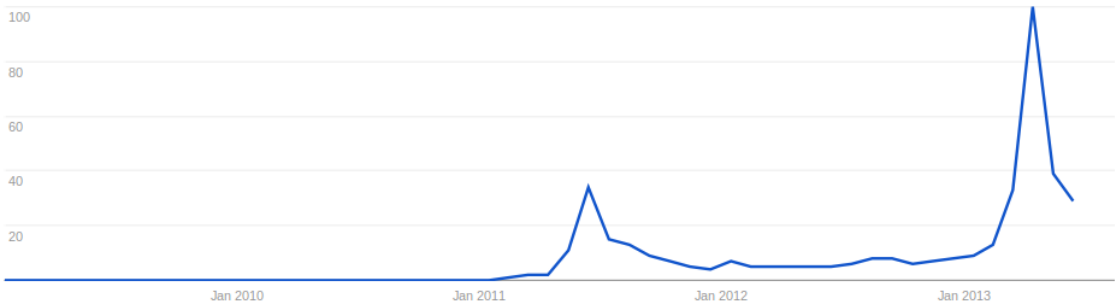


Fig. 16 - resultado de búsquedas en Google Trend del término Bitcoin

Si comparamos Bitcoin con la curva de Gartner no es muy sencillo hacer una relación directa entre las fases. Desde mi punto de vista ahora mismo se encontraría en el segundo “Peak of Inflated Expectations” gracias a la subida de la cotización respecto al dólar, pero veremos poco a poco como baja la expectación cuando la dificultad aumente de manera exponencial y no parezca tan atractivo conseguir dinero “gratis”.

4.2 LÍNEAS DE TRABAJO FUTURAS

Debido a la falta de tiempo hay ciertos aspectos de la red Bitcoin que podrían haber sido estudiados con más detenimiento. Por ello me gustaría hacer una pequeña lista de los aspectos de la red que deberían ser analizados para mejorar el entendimiento de esta.

- Análisis de la destrucción o perdida de monedas y ver como afectará a largo plazo a la red cuando esta no pueda fabricar más monedas.

- Estudiar los picos puntuales que aparecen en la red y saber a que son debidos, que los origina y si se pueden prever para ver como afecta al cambio con el dólar.
- Seguimiento de las direcciones para averiguar si hay usuarios que poseen más de una dirección.
- Analizar la fecha de creación (primera aparición en la red) de las direcciones que son usadas y de las que no, para comparar los dos gráficos y ver si hay correlaciones.
- Analizar como si se esta usando la red para transmitir dinero como pago por actividades delictivas.

4.3 CONCLUSIONES GLOBALES DEL TFM

Para mi el mayor problema es la utilidad de la moneda en si, ya que ahora mismo Bitcoin está siendo usada para especular, usando la minería y el ahorro, y no para comerciar. Se hace más negocio con el cambio de moneda, la minería y con repartir monedas gratis que no con ofrecer servicios o bienes. Existen servicios como los del juego, pero todos se basan en lo mismo, obtener más monedas y más dinero. Por ello creo que mientras no exista un comercio como tal Bitcoin solo puede ser considerado oro y no una moneda.

Uno de los aspectos que me ha resultado más interesante es como Bitcoin ha innovado en el concepto de la seguridad. Siempre se ha dicho que la seguridad por ofuscación no es buena y en Bitcoin se ve claramente como publicando toda la información, la red puede seguir siendo segura gracias a la criptografía de claves públicas y privadas.

En conclusión y a pesar de los aspectos que no he podido investigar como hubiera deseado estoy muy contento de haber elegido este tema y haber tenido la oportunidad de aprender de primera mano lo que representa la moneda digital y como lidiar con los problemas y dudas que puedes surgir de su uso.

5 BIBLIOGRAFÍA

1. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

2. Dorit Ron and Adi Shamir: Quantitative Analysis of the Full Bitcoin Transaction Graph, 2012.

3. Wallace, B.: The Rise and Fall of Bitcoin, Wired Magazine, 23 November 2011,

http://www.wired.com/magazine/2011/11/mf_bitcoin/all/

4. Bitcoin in plain English. - http://codinginmysleep.com/bitcoin-in-plain-english/

5. Bitcoin Mining in Plain English - http://codinginmysleep.com/bitcoin-mining-in-plain-english/

6. Bitcoin Cold Storage In Plain English - http://codinginmysleep.com/bitcoin-cold-storage-in-plain-english/

7. Bitcoin Attacks in Plain English - http://codinginmysleep.com/bitcoin-attacks-in-plain-english/

8. Wikipedia http://es.wikipedia.org/wiki/Bitcoin

9. 28c3: Bitcoin - An Analysis. http://www.youtube.com/watch?v=hlWyTqL1hFA

10. Comparison of mining pools - https://en.bitcoin.it/wiki/Comparison_of_mining_pools

11. Nota de prensa MTGox - https://mtgox.com/press_release_20130530.html

12. Bitcoin talk forum sobre probabilidad de generar la misma dirección - https://bitcointalk.org/index.php?topic=1387.msg150668#msg150668

13. Historia de la red Bitcoin - https://en.bitcoin.it/wiki/History

14. Bio del minero ArtForz https://en.bitcoin.it/wiki/ArtForz

15. BTC Guild - https://www.btcguild.com

16. MtGox - https://mtgox.com/

17. Mt. Gox Press Release - April 24th, 2013 - https://mtgox.com/pdf/20130424_ddos_statement_and_faq.pdf

18. Información sobre Granada (Pais) - http://es.wikipedia.org/wiki/Granada_%28pa%C3%ADs%29

6 ANEXOS

6.1 CONSULTAS SQL

6.1.1 ANALIZANDO LAS TRANSACCIONES CON MÁS BTC DE LA HISTORIA DE LA RED

```
SELECT tx_id, SUM(`txout_value`) as total FROM `txout` group by tx_id ORDER by  total DESC LIMIT 0,5
```

6.1.2 OBTENIENDO DATOS SOBRE BLOQUES

```
SELECT `block_id`,`block_nTime`,`block_value_in`,`block_num_tx`
FROM `block`
INTO OUTFILE '/tmp/blocks.txt'
FIELDS TERMINATED BY ''
ENCLOSED BY ''
LINES TERMINATED BY '\n';
```

6.1.3 OBTENER BLOQUE CON MÁS TRANSACCIONES

```
SELECT block_id, COUNT(*) as total FROM `block_tx` group by block_id order by total DESC LIMIT 0,5
```

6.1.4 BLOQUES CON MÁS OUTPUTS

```
SELECT block_id, count( * ) AS total
FROM block_tx, txout
WHERE block_tx.tx_id = txout.tx_id
GROUP BY txout.tx_id
ORDER BY total DESC
LIMIT 0 , 5
```

6.1.5 CREANDO TABLA AUXILIAR PARA CONSULTAR TRANSACCIONES DE ENTRADA

```
CREATE TABLE IF NOT EXISTS `ingresos` (
  `ultimo_ingreso` decimal(26,0) NOT NULL,
  `primer_ingreso` decimal(26,0) NOT NULL,
  `pubkey_id` decimal(26,0) NOT NULL,
  `total_ingreso` bigint(20) NOT NULL,
  `num_ingresos` bigint(20) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

INSERT INTO  ingresos
select max(tx_id) as LastIngreso_txid, min(tx_id) as CreacionCuenta_txid, pubkey_id, sum(txout_value)
as TotalValue, count(txout_value) as TotalIngresos
from txout
group by pubkey_id
```

6.1.6 CREANDO TABLA AUXILIAR PARA CONSULTAR TRANSACCIONES DE SALIDA

```
CREATE TABLE IF NOT EXISTS `retirados` (
```

```
  `ultimo_retirado` decimal(26,0) NOT NULL,
  `primer_retirado` decimal(26,0) NOT NULL,
  `pubkey_id` decimal(26,0) NOT NULL,
  `total_retirado` bigint(20) NOT NULL,
  `num_retirado` bigint(20) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

INSERT INTO   retirados
select   max(txout.tx_id) as LastRetiro, min(txout.tx_id) as Primer_retiro, pubkey_id, sum(txout_value)
as TotalRetirado, count(txout_value) as total_retiros
from txin, txout
where txin.txout_id=txout.txout_id
group by pubkey_id
```

6.1.7 CUENTAS DE AHORRO

```
CREATE TABLE IF NOT EXISTS `cuentasAhorro` (
  `ultimo_ingreso` decimal(26,0) NOT NULL,
  `primer_ingreso` decimal(26,0) NOT NULL,
  `pubkey_id` decimal(26,0) NOT NULL,
  `total_ingreso` bigint(20) NOT NULL,
  `num_ingresos` bigint(20) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

INSERT INTO   cuentasAhorro
select * from ingresos where not exists
(SELECT pubkey_id FROM retirados where retirados.pubkey_id = ingresos.pubkey_id )
```

6.1.8 CALCULAR RIQUEZA ACUMULADA EN CUENTAS DE AHORRO

```
SELECT SUM(total_ingreso), SUM(num_ingresos)
FROM `cuentasAhorro`
ORDER BY `cuentasAhorro`.`total_ingreso`
```

6.1.9 DIRECCIONES USADOS CON MÁS BITCOINS

```
SELECT retirados.pubkey_id,
(ingresos.total_ingreso-retirados.total_retirado) as bitcoins,
 ingresos.num_ingresos, retirados.num_retirado
FROM retirados,ingresos
WHERE retirados.pubkey_id = ingresos.pubkey_id
ORDER BY bitcoins DESC
```

6.1.10 DIRECCIONES USADAS CON FONDOS EN LA ACTUALIDAD

```
SELECT retirados.pubkey_id
FROM retirados,ingresos
WHERE retirados.pubkey_id = ingresos.pubkey_id and ingresos.total_ingreso!=retirados.total_retirado
```

6.1.11 DIRECCIONES USADAS SIN FONDOS EN LA ACTUALIDAD

```
SELECT retirados.pubkey_id
FROM retirados,ingresos
```

```
WHERE retirados.pubkey_id = ingresos.pubkey_id and ingresos.total_ingreso==retirados.total_retirado
```

6.1.12 CALCULANDO MONEDAS EN CIRCULACIÓN

```
SELECT SUM( (ingresos.total_ingreso-retirados.total_retirado))
        FROM retirados,ingresos
        WHERE retirados.pubkey_id = ingresos.pubkey_id
```

6.2 SCRIPTS

6.2.1 INFORMACIÓN ADICIONAL DE BLOQUES

```
#!/bin/bash
#Script para crear un summary file de los datos exportados de MYSQL
#Devuelve un fichero con: EPOCH NUM_BLOCKS TOTAL_BTC_IN MEAN_BTC_IN MAX_BLOCK_IN TOTAL_TX MEAN_BLOCK_TX  MAX_BLOCK_TX MEAN_TIME_GENERATION
reset

EPOCH_DAY=86400
EPOCH_ACTUAL=0
EPOCH_FUTURO=0
MEAN_TIME=0
EPOCH_LAST=0

function clearVars(){
        COUNT_BLOCKS=0
        MEDIA_in=0
        MEDIA_tx=0
        MAX_in=0
        MAX_tx=0
        MEAN_TIME=0
}

function updateMediaEpoch(){
        TMP=$(($block_epoch-$EPOCH_LAST));
        #no quiero diferencias negativas
        if [ $TMP -lt 0 ];then
                TMP=0
        fi
        MEAN_TIME=$(($MEAN_TIME+$TMP));
        EPOCH_LAST=$block_epoch
}

function updateSample(){
        COUNT_BLOCKS=$(($COUNT_BLOCKS+1));
        MEDIA_in=$(($MEDIA_in+$block_in));
        MEDIA_tx=$(($MEDIA_tx+$block_tx));
        updateMediaEpoch
        if [ $block_in -gt $MAX_in ];then
                MAX_in=$block_in
        fi
        if [ $block_tx -gt $MAX_tx ];then
                MAX_tx=$block_tx
        fi
}
clearVars
```

```
echo EPOCH NUM_BLOCKS TOTAL_BTC_IN MEAN_BTC_IN MAX_BLOCK_IN TOTAL_TX MEAN_BLOCK_TX MAX_BLOCK_TX MEAN_TIME_GENERATION

cat $1 | while read block_id block_epoch block_in block_tx; do

#inicializamos las variables
if [ $EPOCH_FUTURO -eq 0 ];then
        EPOCH_FUTURO=$(($block_epoch+$EPOCH_DAY));
        EPOCH_ACTUAL=$block_epoch
        EPOCH_LAST=$block_epoch
fi

#Comprobamos si la muestra está en el dia que le toca
if [ $block_epoch -lt $EPOCH_FUTURO ]; then
        updateSample
else

        echo -n $EPOCH_ACTUAL $COUNT_BLOCKS
        echo -n " "
        echo -n $MEDIA_in $(($MEDIA_in/$COUNT_BLOCKS)) $MAX_in
        echo -n " "
        echo $MEDIA_tx $(($MEDIA_tx/$COUNT_BLOCKS)) $MAX_tx $(($MEAN_TIME/$COUNT_BLOCKS))


#Reseteamos variables
        clearVars
        EPOCH_ACTUAL=$EPOCH_FUTURO
        EPOCH_FUTURO=$(($EPOCH_FUTURO+$EPOCH_DAY))

#Por si no existen muestras ese dia (Del genesis al siguiente)
while [ $block_epoch -gt $EPOCH_FUTURO ]; do
        echo $EPOCH_ACTUAL 0 0 0 0 0 0 0

        EPOCH_ACTUAL=$EPOCH_FUTURO
        EPOCH_FUTURO=$(($EPOCH_FUTURO+$EPOCH_DAY))
done
        #Contamos bloque actual
        updateSample
fi
done
```