UNIVERSIDAD AUTÓNOMA METROPOLITANA IZTAPALAPA

DIVISIÓN DE CIENCIAS SOCIALES Y HUMANIDADES

DEPARTAMENTO DE ANTROPOLOGÍA

LICENCIATURA EN ANTROPOLOGÍA SOCIAL

“¿Águila o sol?:
Qué es lo que bitcoin está cambiando con sus prácticas”

Trabajo terminal

que para acreditar las unidades de enseñanza aprendizaje de
Trabajo de Investigación Etnográfica y Análisis Interpretativo III
y obtener el título de

LICENCIADO EN ANTROPOLOGÍA SOCIAL
Presenta

Rodrigo del Castillo Negrete Eissa
Matrícula No. 209347493

Comité de Investigación:

Director: Dr. Luis Bernardo Reygadas Robles Gil

Asesores:

México, Ciudad de México. Abril 2018

Índice

Introducción

La manera en la que llegué a bitcoin fue principalmente por un interés en las redes descentralizadas de par a par, conocidas como p2p en inglés, y por un vago recuerdo que tuve alrededor del 2011 al intentar explicar qué eran dichas monedas y cómo funcionaban a mi papá, quien siempre me ha inculcado un interés por la computación y las nuevas tecnologías. Al escuchar los proyectos que fueron abiertos por los profesores del departamento de antropología de la UAM Iztapalapa, mis dos opciones fueron el proyecto de Redes Cognitivas dirigido por Luis Reygadas y el proyecto para ir a hacer investigación de campo en el sitio arqueológico del Tajín dirigido por Daniel Nahmad Molinari. Ambos son y han sido temas de interés personal, sin embargo he sido usuario de las redes de par a par por ya algunos años, y el hacer un estudio, ver la relevancia de estas redes dentro de la sociedad mexicana, es algo que ya había reflexionado a lo largo de toda la carrera en antropología.

La religión prehispánica y lo que queda de ella cómo reflejo en la sociedad mexicana es también una cuestión que me interesa mucho, pero se ha convertido gracias a la antropología y las enseñanzas de la planta docente del departamento, más en algo personal que en un tema de estudio. En comparación, las redes de par a par y la transferencia de archivos por internet, que es el principal uso de estas redes que conocía antes de acercarme a bitcoin, me es familiar pues he tenido acercamiento desde hace ya varios años. Concretamente he tenido la experiencia de primea mano de usar aplicaciones como Napster, Kazaa, eDonkey, eMule, iMesh, Morpheus, LimeWire, y gtk-gnutella entre otras, así como páginas de torrents como Demonoid y The Pirate Bay, que utilizan de un modo u otro las redes descentralizadas de par a par.

De tal modo, unos minutos antes de proceder a la entrevista con Luis Reygadas, yo estaba seguro de que llegaría a tener una propuesta relacionada a la piratería y las redes de par a par. Sin embargo al estar revisando nerviosamente los detalles y las aplicaciones prácticas de estas redes para tener la información fresca, antes de pasar a la entrevista, re-encontré lo que había visto en el 2011 llamado bitcoin. En el 2011 intenté entenderlas y explicarlas, no obstante lo único que encontré fueron videos en YouTube demasiado técnicos de cómo funcionaba la cadena de bloques, y aunque entendiera algunos de los términos y cosas que se explicaban en el video, esto no fue suficiente para explicarme la noción de una moneda como tal en Internet. Por la misma razón no exploré mucho más el tema en esa fecha. Pese a esto, 5 años después existía ya mucha más información explicando qué es, cómo funciona

y dónde comprarla, misma que consulté antes de entrar a la entrevista y tener de ese modo dos opciones para plantear la investigación, las redes de par a par y bitcoin.

Aunque tuviera una vaga comprensión de qué eran dichas monedas y aunque fuera algo confuso en un inicio comprenderlas y explicarlas, consideré que sería buen tema para la investigación. No sólo encajaba con el tema de las redes cognitivas, sino que se relaciona profundamente con el tema de la antropología económica. En mi manera de ver las cosas las redes descentralizadas de par a par, y el Internet, se relacionan profundamente con la economía, pues ayudan a mantener un mercado informal muy grande en México, que es la piratería. Fue como si hubieran mejorado mi tema de investigación y en lugar de películas y datos transferidos en Internet lo que se transfiere ahora son monedas. Es así como comprendí bitcoin en sus primeras instancias y la explicación general que yo mismo me di para comprenderlas.

De este modo, con el tiempo que me quedaba antes de proceder a la entrevista del trabajo de campo con quien ha sido mi asesor de tesis, hice rápidamente una revisión de qué era bitcoin. En ese entonces no lo comprendí del todo bien comparado al momento de escribir estas líneas, pero logré explicar con cierto grado de certeza qué era y por qué era relevante estudiarla. En ese momento lo poco que encontré en donde podría hacer investigación de campo fue FAMSA México S. A. de C. V. y Bitso, una casa de cambio de pesos a bitcoin, la cual se profundiza en la tesis. En ese momento Bitso se asoció con una empresa llamada BitPay, ellos se encargan de ofrecer el servicio de procesamiento de pagos en bitcoin a cualquier empresa y es en la actualidad la empresa más grande en hacerlo. Algunos de los clientes con los que están asociados son Microsoft y Warner Bros. Records, entre otros (Bitso, 2015). Con esto se dibujaba un panorama positivo para estudiar la moneda, pues se encontraba en crecimiento la principal casa de cambio mexicana.

La manera en que se hizo la investigación fue con trabajo de campo en presencial y virtual. Profundizando en el primero, éste fue principalmente en la Ciudad de México y en segunda instancia en Acapulco, Guerrero, haciendo entrevistas a aquellas personas que trataban con bitcoin directamente. Es decir, personas ya sea que estaban vendiendo bitcoin, o que aceptaban pago de bitcoin en sus restaurantes o negocios. Hablando del trabajo de campo virtual, éste fue desde hacer un perfil de Satoshi Nakamoto (el creador de bitcoin) con todas sus entrevistas y publicaciones en foros para poder entender quién es este personaje y lograr hacer un tipo de semblanza, hasta incluso hacer entrevistas en

línea, recabar datos y cifras que me ayudaran a comprender mejor la magnitud de bitcoin en lo virtual y en la realidad offline. El recabar datos no sólo se refiere a buscar conversaciones de un personaje anónimo que ya desapareció, sino que fue también buscar análisis e información de personas respetadas en criptografía y en general del tema para poder obtener una visión más cercana al movimiento virtual con el cual bitcoin se conformó y avanza.

Ya que se explicó la premisa de la investigación en materia a mis intereses personales y el por qué decidí estudiar este tema, daré ahora la explicación de los intereses académicos. Los propósitos de la investigación son diversos pues al ser un tema de actualidad en el cual se unen diversos factores, como la computación, la criptografía, las matemáticas y el dinero entre muchos otro. El primero es el de dar a conocer y hacer que los lectores comprendan de qué fenómeno estamos hablando. El segundo de ellos es dar un acercamiento desde la antropología a un factor que es tratado en la mayoría de las veces desde la economía pues uno de los objetos principales de ella es el dinero. Por último y tal vez el más ambicioso es generar en el lector, algo que espero se vea reflejado a lo largo de toda la investigación, cierto grado de conciencia en relación a qué es una moneda.

Hablo del simple hecho de reflexionar en que constituye para nosotros una moneda. Por qué la aceptamos con sus características en la actualidad; es decir expedida de un país y con instituciones ya sean de ese mismo país o internacionales. Y tal vez la pregunta más interesante que me generó la investigación es: ¿Por qué no existen actualizaciones en los mecanismos e instituciones que la regulan? O dicho de otro modo: ¿Por qué al ser algo tan versátil y tener tantos diferentes aspectos dentro de la vida de las personas es vista como algo absoluto? Absoluto en el sentido que no son rediseñadas y es difícil cambiar la noción de qué es una moneda, más no los significados y todas las cosas posibles que puede representar.

Hablando ahora de la pregunta central de la tesis, tenemos: ¿Cuáles son las prácticas que hacen de bitcoin una moneda? Claro que los detractores de bitcoin podrán pensar en lo tendencioso de la pregunta pero se analizan también los casos en los que falla en ser una moneda como tal. De mismo modo se invita al lector a sumergirse en este críptico mundo para que se forme una opinión en relación a la pregunta de investigación y de no ser suficientes las conclusiones a las que se llegan, que formule las propias pues es un tema difícil de abarcar en una investigación de licenciatura.

Podemos observar varias caras a esta pregunta central y los aspectos que la conforman son, en primera instancia, ¿Qué características hacen única a bitcoin de otro tipo de monedas? Y en segunda ¿Qué prácticas se dan y se han dado con esta moneda? Se analizan las características que hacen a la moneda única pues, históricamente no se habían tenido monedas digitales con la misma infraestructura, seguridad y practicidad. Del mismo modo resulta evidente preguntarnos sobre las prácticas que rodean a bitcoin para poder entender en su totalidad, desde su uso, aquello que queremos investigar.

Antes de dar un esquema de los capítulos de la tesis citaré brevemente fragmentos del prefacio de la obra de Simmel, Filosofía del Dinero, en la cual tenemos una explicación mucho más formal de por qué estudiar el dinero de esta forma, es decir con el uso y sus prácticas.

De acuerdo a Simmel: "la filosofía del dinero se encuentra más allá y más acá de la ciencia económica". De igual manera nos menciona que "su función es representar los presupuestos que otorgan al dinero su sentido y su posición práctica en la estructura espiritual, en las relaciones sociales, en la organización lógica de las realidades y de los valores." (Simmel, 2016, p. 34) Es así que se pretende hacer un aporte a la representación de presupuestos que otorgan, en nuestro caso a bitcoin, un sentido y una posición práctica.

Hablando de los fenómenos sociales y de cómo nos podemos acercar a ellos para estudiarlos, nos dice que "la totalidad de un fenómeno social, como la aparición de un fundador de una religión, nunca se puede agotar con las diferentes perspectivas que tenemos para estudiarlo. Sean desde la religión, la psicología, patología, historia en general y sociología. Similarmente, "como una poesía no solo pertenece a la historia de la literatura, sino que también pertenece a la estética, la filosofía y biografía. Por ello, el hecho de que dos personas intercambien el producto de su trabajo, no solo pertenece a la economía política", pues de acuerdo a Simmel, "no existe posibilidad en lo absoluto de que el contenido de ese hecho se agote dentro de ella." (Simmel, 2016, p. 35) Es así que pretendo acercarme al hecho en el cual dos personas intercambian el producto de su trabajo desde la antropología, del uso y prácticas de bitcoin. Que como se verá y aunque es una moneda virtual, sí existe trabajo detrás de ella para su distribución.

El esquema bajo la cual la tesis está escrita es el siguiente: en el primer capítulo como es de esperarse tenemos la explicación de qué es esto que llamamos bitcoin. Nótese, y que sirva de observación, este fue uno de los capítulos más difíciles de redactar, pues para poder explicarlo en términos que fueran

comprensibles, fue necesario adentrarme en sus mecanismos internos. Es decir, entender y ver cómo es que funciona realmente esta moneda y por qué es que funciona. A mi modo de ver las cosas, tenía yo que darme una idea y entender por qué de verdad funciona esta moneda y que mecanismos de seguridad están detrás de ella, para poder no sólo explicarla sino tener la certeza de que la moneda funciona.

Como pequeño paréntesis sobre la explicación, he incluido un anexo técnico en el cual se explican los detalles más finos de bitcoin. Esto es para que los que necesiten o tengan la misma necesidad con la que yo me enfrenté, de entender a fondo por qué funciona, tengan donde consultar los aspectos de la computación y matemáticas que hacen viable esta moneda.

En este primer capítulo se incluye también una explicación a fondo de los llamados mineros, quienes, como se verá, son las personas encargadas de administrar la red, de par a par, sobre la cual bitcoin está construida. Se analiza desde el producto de su trabajo, hasta los costos y ganancias que un minero obtendría si comenzara a minar, es decir hacer el trabajo para administrar la red, en una determinada fecha.

En el segundo capítulo se analiza todo lo relacionado al complejo personaje que es Satoshi Nakamoto, quien es la persona, entidad o grupo, que desarrolló la idea de bitcoin. Como se verá en el capítulo, Nakamoto es el nombre de un personaje anónimo, del cual tenemos solamente algunas conversaciones, así como publicaciones en diversos foros de criptografía. Aún con este contexto otro punto que se toca es el de su identidad. Paralelo a todo lo relacionado a Nakamoto se habla también del contexto sobre el cual se desarrolla la moneda, el cual se le conoce como la comunidad de software libre.

Por último el tercer capítulo, que es el más sustancioso, habla de mi experiencia en concreto del trabajo de campo. En ésta nos encontramos y vemos a bitcoin desde muchos aspectos diferentes. El primero y más creativo es aquel en que introduzco y se hace un ejercicio creativo para ver bitcoin como algo más allá de una moneda. Una vez que es introducida de este modo se procede a ver los primeros usos que yo tuve de esta moneda, al igual que los trayectos o viajes que tuve que hacer para encontrar esta moneda virtual en la realidad. De traslados dentro de la Ciudad de México, hasta un viaje a un congreso de anarquistas capitalistas en Acapulco, Guerrero.

Este capítulo es de los más interesantes pues se introducen formalmente las primeras cifras de la investigación, analizando el volumen de intercambio cada 24 horas, así como la capitalización total de bitcoin. Paralelo a las cifras también se explora la idea de un negocio piramidal, que llega a ser un tanto recurrente en los detractores. Se tiene también una mirada crítica a la cadena de bloques que, como se verá más adelante, no sólo es la tecnología detrás de bitcoin, sino también es una base de datos muy grande con todos los registros y movimientos de un primer bitcoin que se creó hasta la última transacción registrada en tiempo real.

En este mismo capítulo se analizan los actores que hacen posible el uso de bitcoin en la Ciudad de México y en parte del resto del mundo. Estos son los llamados exchanges o casas de cambio, en el caso de mi investigación Bitso S. A. P. I. de C. V. es de las primeras empresas en México en proporcionar este servicio, y fue la encargada de procesar todas menos una de las compras que hice a lo largo de toda mi investigación. Se analiza la cantidad de dinero que esta empresa procesa, así como su relevancia a nivel mundial entre otras cifras.

Por lo tanto y remitiéndome a la práctica que tenemos de resolver dudas o decisiones al lanzar una moneda al aire, se invita al lector a decidir entre el águila del escudo real mexicano o la pirámide del sol, a manera de volado, para resolver esas dudas y cuestiones que podemos tener de esta compleja moneda.

La explicación del millón: Bitcoin.

Definición características y funcionamiento de bitcoin

Explicar bitcoin ha sido uno de los temas más difíciles de la investigación y este capítulo tal vez dará cuenta de ello. El objetivo de este capítulo es que al terminar de leerlo se explique bitcoin y le quede al lector una idea clara de con qué estamos tratando. Hablamos de una moneda electrónica que se apoya en una tecnología compleja[1], que usa importantes mecanismos para garantizar su seguridad; pero también tenemos en nuestras manos una moneda internacional, con una gran practicidad, seguridad y velocidad entre muchas otras características únicas.

Se han mencionado muchas características, pero algo que no debe ignorarse es lo que se dice implícitamente antes de éstas, y es: moneda electrónica. Esto puede parecer un oxímoron, pues con algunas cosas electrónicas o digitales existe una gran dificultad de imaginar cómo serían en la vida real. Más cuando se trata de información digital o electrónica y en nuestro caso de una moneda como tal. Otro ejemplo es la unidad más chica de información que contiene una computadora, el byte. Ambas cosas pueden ser muy difíciles de imaginar, pero son la base de sistemas con un funcionamiento complejo. Esta es la primera complicación al explicarla, pues no se tiene un objeto físico en la realidad que sea bitcoin como tal, pero sí existen aplicaciones, programas y sitios donde podemos checar su precio o valor y la cantidad que uno tiene.

Esto no significa que sea una moneda que no tenga ningún tipo de materialidad o sustento, pues se puede adquirir con muchas divisas, como por ejemplo: Pesos mexicanos, Rupias de la India, Dólares, Euros, Yenes, Yuanes y en última instancia se puede adquirir con cualquier divisa, siempre y cuando en la compra venta ambas partes estén de acuerdo en el tipo de cambio. Es decir, bitcoin aunque carezca de materialidad es una moneda digital que se puede conseguir o comprar con dinero común y

[1] Lo que nos interesa explicar y dejar claro es el segundo conjunto de características mencionadas. El primer conjunto de características más técnicas estará en el Anexo 1, donde se proporcionará una explicación detallada del funcionamiento interno.

corriente. Asi como las aplicaciones y programas donde podemos almacenar y administrar nuestras bitcoins son llamadas carteras o wallets en inglés.

Bitcoin entonces puede considerarse como una moneda digital que se maneja con las carteras o wallets, cuya practicidad y velocidad es comparable a cualquier transacción que se hace hoy en día a través de internet. Como nos menciona Tomás Álvarez Melis, cofundador de Volabit y Mifiel[2], cuando le pregunté sobre experiencias memorables de bitcoin: "Lo que siempre me sigue dando satisfacción es cuando te aparece el código Qr, lo escaneas con el teléfono, mandas los bitcoins, y en un segundo te aparece pagado el invoice". Aquí podemos observar la facilidad de hacer un pago usando bitcoin, en donde se genera un código Qr, que es una imagen que se escanea con el teléfono y después de escanearla lo único que se tiene que hacer es confirmar la transacción. A continuación un ejemplo:

Imagen 1:Ejemplo de código Qr.

Este código es uno que generé con mi teléfono celular, con mi cartera usando una aplicación llamada Copay, en cuestión de segundos. La imagen puede ser escaneada por cualquier móvil que tenga una cartera de bitcoin. Una vez escaneada la imagen anterior la persona que quisiera mandarme dinero solamente indica la cantidad a enviar junto con una comisión, que es muy baja, y confirmar la transacción, que como nos menciona Tomás, en unos segundos aparece completada. El enviar bitcoins a mi dirección se puede entender como algo que muchos sitios en internet hacen, y esto es poner una

[2] Donde Volabit es una Casa de Cambio o exchange de bitcoin y Mifiel una Empresa para frimar documentos legales mexicanos a distancia con validez jurídica (Mifiel, 2017)

dirección en la que están abiertos a recibir fondos. Todo este proceso puede ser completado en menos de 2 minutos.

El siguiente punto que se menciona en la lista de características de bitcoin es la seguridad. Para poder hacer la transacción anterior es necesario ser el dueño de las monedas. Similar al PIN que es pedido en las transacciones de cajero automático, o pagos de tarjeta bancaria, para nuestro caso se usan dos tipos de PIN[3]. El primer PIN es el más importante, le llamaremos PIN privado, éste nos permite controlar las monedas y nos habilita como dueños de ellas. El segundo PIN el lector acaba de verlo en la página anterior, se obtiene usando el primer PIN (el privado), con un proceso prácticamente irreversible, y nos sirve para recibir bitcoins. Le llamaremos PIN público, representa una cadena de números y letras en minúsculas y mayúsculas. Ejemplificando: el código Qr (Imagen 1) representa este PIN Público: 1PnV1XhcXEo6FUVayEcXgBcFUS4gDiGDoG.

El PIN privado se genera y se debe de guardar con el mismo cuidado que una contraseña bancaria. En mi caso usé un método[4] que en caso de que alguien quiera adivinar u obtener mi contraseña con fuerza bruta[5], le llevaría aproximadamente 2 años y medio (StackExchange, 2013), usando tecnología que permite obtener en 6 horas cualquier contraseña del sistema operativo de Windows, es decir un sistema con grandes capacidades (Goodin, 2012). En el caso de Copay, que es la cartera que he empleado durante toda la investigación, mi PIN privado es almacenado localmente en mi teléfono celular, y nadie más que yo puede verlo.

Como cualquier contraseña existen maneras de recuperarlas y en este caso de respaldarlas. Al momento de descargar nuestra cartera, la aplicación nos da una frase de 5 palabras, independiente de nuestro PIN privado, con la cual podemos restaurar nuestra cartera en caso de extraviar el teléfono celular. Concluyendo con el tema de la seguridad, en cualquier móvil se tiene una contraseña para desbloquearlo e incluso, Copay ofrece la posibilidad de fijar un número de 4 dígitos para abrir la aplicación, añadiendo aún más capas de seguridad. Específicamente en este caso podríamos decir que

[3] Personal Identifiaction Number en inglés, o NIP¨en español Número de Identifiación Personal
[4] Use un método llamado Diceware, y el modo en que funciona es el siguiente: Se tiran 5 dados al azar, el resultado de 5 números corresponde a una palabra dentro de una lista de 7776 palabras diferentes. Se repite el proceso y después de 6 palabras uno obtiene su contraseña. (Reinhold, 2017),
[5] A lo que se refiere con fuerza bruta es intentar cada posible contraseña hasta obtener la correcta. El ejemplo canónico es el probar todos los números posibles de un candado de 4 números, hasta de ese modo obtener la contraseña.

la cartera como objeto en la realidad que ayuda a guardar billetes y tarjetas de crédito es el teléfono celular como tal.

La última de las características que se menciona es la velocidad y será la última característica que explicaré antes de adentrarme en las características únicas. Por diseño nuestra transacción queda registrada en la red después de 10 minutos de haberla procesado. Similarmente después de un aproximado de 60 minutos la misma transacción queda firmada en la red como irreversible, al igual que tenemos la garantía de que nuestras monedas se transfirieron correctamente. Ésta puede parecer una diferencia sutil para el lector, pues una cosa es hacer un registro y otra cosa es firmar ese registro. Puede ser análogo a un libro mayor, en donde se toma la hora de la transacción para hacer el registro, sin embargo es después de 60 minutos que las personas encargadas en administrar el libro mayor garantizan que verdaderamente somos dueños de las monedas que decimos tener y por lo tanto se firma ese registro como correcto. Esto se retomará en donde se hable de la internacionalidad de bitcoin.

En mi experiencia los pagos que hice usando la moneda fueron prácticamente inmediatos y en cuestión de minutos, si no es que segundos, mi pago ya había sido realizado. Al comprar tuve que esperar alrededor de 20 minutos para obtener mis fracciones de bitcoin[6], al comprarlos en un cajero automático localizado en una tienda de comics llamada Fantástico Comics S de RL de CV.

Una vez explicadas las características básicas notables podemos hablar de las que son únicas y que hacen verdaderamente interesante bitcoin. La primera es el hecho de que no tiene ninguna entidad centralizada para el control, distribución o producción de las monedas, sino que es una red descentralizada la que administra estas funciones. A lo que se refiere con descentralizada es que todas las personas involucradas en la red tienen la misma importancia y existe una igualdad en las actividades que desarrolla cualquier persona involucrada en la red. En términos más concretos, no existe un banco o gobierno que controle bitcoin. Esto significa que no existe ningún tipo de respaldo o control que los gobiernos pueden tener sobre la moneda como tal, y la implicación más importante es que no se encuentra respaldada por ningún país, banco, gobierno o institución central, esto entre otras implicaciones que no se desarrollarán en este momento.

[6] Como se verá más adelante, una bitcoin es divisible en muchos centavos. Los centavos de bitcoin son conocidos como Satoshis, mismos que llevan el nombre de su creador, Satoshi Nakamoto.

La siguiente característica deriva casi automáticamente del punto anterior, y es una que se menciona implícitamente o tal vez sea obvia para algunos lectores. Esta es la internacionalidad de bitcoin. Al no tener un banco central o un país que la regule y estar conectada a una red descentralizada usando internet, las posibilidades que adquiere bitcoin para ser usada a lo largo del mundo son realmente grandes. Al 12 de Octubre del 2017 tenemos que hay una participación total de 9,000 computadores diferentes a lo largo de 96 países. Todos colaboran activamente en la red de bitcoin, cada uno con diferente incidencia, es decir hay unos que tienen un porcentaje más alto de participación que otros, y hay otros países que solamente tienen una computadora pero todos colaboran. (Yeow, 2017).

Para no confundir al lector es necesario distinguir entre las computadoras que se conectan a la red, y a los usuarios. En el primer caso las computadoras que se conectan son las encargadas de compartir una misma copia del libro mayor, que se mencionó hablando de la velocidad de bitcoin. Los usuarios por otra parte son las personas que usan la moneda con una cartera o wallet, y se conectan como usuarios a la red de bitcoin a través de la cartera. A diferencia de una computadora, cuyo trabajo es mantener actualizado y público el libro mayor y ser parte de la red descentralizada de bitcoin.

Por consiguiente tenemos, no solo una red mantenida globalmente en 96 países diferentes, sino que existe la oportunidad de conectarnos desde cualquier lugar del mundo, siempre y cuando se tenga una conexión a Internet, y usar bitcoin con una cartera. Por ambas razones anteriormente expuestas considero que la moneda es internacional y se puede emplear en prácticamente cualquier parte del mundo.

La tercera característica única es lo que llamo el libro mayor. La red se puede considerar como la infraestructura sobre la cual el libro mayor está distribuido, y éste es, como lo hemos dicho ya, un registro con firmas de todas las transacciones que se tienen de bitcoin. Hablando propiamente a este libro mayor se le conoce con el nombre de: cadena de bloques, o blockchain en inglés, y es uno de los motivos gracias a los cuales bitcoin funciona, al igual que es una de las explicaciones más difíciles del tema.

La cadena de bloques entonces es la tecnología detrás de bitcoin. Pero en lugar de que dos personas involucradas en una transacción tengan sus propios libros mayores, como en la contabilidad clásica, así como sus propias entradas sin que haya algún tipo de verificación entre ellos, o que la verificación dependa de una tercera persona para validar las transacciones, como podrían ser auditores, la cadena de

bloques permite tener un solo libro mayor. Es decir que tenemos un libro mayor que todos los usuarios y actores de la red pueden obtener y consultar, en donde una transacción es vista como un intercambio entre dos usuarios, en el cual cada transacción es agregada al libro mayor con una firma[7]. Esta firma garantiza que las entradas no sean falsas y que no se puedan borrar o duplicar, garantizando un registro fidedigno de todos los participantes, y de todas las transacciones que se hacen.

Ya se ha hablado de muchas de las características de bitcoin, desde las más simples a las más complejas o únicas, sin embargo de algo esencial en las monedas como lo es la adquisición aún no se menciona explícitamente. Existen diversos modos de adquirirla, la manera más simple es que alguien que ya tenga la moneda te venda algunas fracciones de bitcoin. Se puede dar el caso en el que la persona sea un conocido o amigo, y paralelo a la venta sucede también una explicación, por lo menos básica de que es, o de cómo usar las carteras y dónde encontrar más información. Otra manera de adquirirla es en línea, existen páginas como LocalBitcoins en la cual los usuarios proporcionan el precio al que están vendiendo o comprando bitcoin y la forma de pago, al igual que cada usuario tiene un porcentaje de reputación. Esta página es similar a Mercado Libre u otros mercados en línea en donde se intercambien bienes en general.(LocalBitcoins, 2017)

Otra manera en la que se pueden conseguir es en un cajero automático, esto se mencionó ya en mi experiencia recibiendo bitcoin. El cajero que yo usé, ya más de una vez, se localiza en la Ciudad de México en una tienda de comics llamada Fantástico, sin embargo existen un total de 10 cajeros en todo México, y solamente 3 en la Ciudad.(“Bitcoin ATM Mexico – find bitcoin machine locations,” 2014) Coincidentemente los 3 cajeros de la ciudad están en 3 diferentes tiendas de Fantástico.

Un tercer modo de adquirir bitcoin es a través de empresas de fintech[8] que se llaman Casas de Cambio o exchanges. Como su nombre lo indica uno puede cambiar la moneda local por bitcoin o viceversa. Muchos exchanges o Casas de Cambio tienen su propia aplicación y es muy fácil confundir una cartera o wallet con estos exchanges. La diferencia fundamental es que en una cartera el usuario es dueño de sus monedas y controla su PIN privado, mientras que en un exchange o Casa de Cambio uno tiene una cuenta con la que compra y vende bitcoin y no necesariamente es dueño directo de sus monedas, sino

[7] Por el momento no es necesario especificar cómo es esta firma, sino que es necesario comprender que la firma valida la transacción. Hablando en términos muy básicos de criptografía y cifrado podríamos decir que es un número que se genera después de hacer una gran cantidad de cálculos y se agrega como apéndice para toda transacción agregada en el Libro Mayor.

[8] Palabra formada del inglés usando finance y technology, son empresas que dan un servicio financiero usando tecnologías de la información.

que es dueño de una cuenta del exchange en donde tiene las monedas que ha adquirido. Por razones obvias existe un contrato al hacer una cuenta en un exchange, así como condiciones y términos de uso.

Las ventajas de tener una cuenta en una Casa de Cambio es que uno puede recuperar su contraseña si la pierde, existe una garantía en contra de hackers[9] y tiene también servicio al cliente entre otros beneficios. Sin embargo la desventaja más grande es que el exchange actúa como un tercero, entre nosotros y nuestra cartera al hacer una transacción (Prahalad, 2016). Otra desventaja que se desprende de esto es la anonimidad, por razones obvias el exchange al hacer nuestra cuenta nos pide información de contacto; nombre completo, fecha de nacimiento, correo electrónico, país y número de celular en general. Perdiendo de ese modo la anonimidad que es otra de las características de bitcoin.

Existe un último modo de adquirir bitcoin y como es de esperarse es un modo más complicado de los mencionados anteriormente. Este modo es produciéndola y está relacionado con la cadena de bloques[10] que se mencionó ya un par de veces. Tal vez el lector ya se haya hecho la pregunta de: ¿Quién se encargaría de un libro mayor Público, disponible al Internet, con el cual se procesan de miles a millones de transacciones diarias sin remuneración alguna? Pues la respuesta es simple, nadie. Las personas encargadas en administrar este libro mayor, llamado Block Chain o cadena de bloques, se les llama Mineros y hacen este servicio a cambio de bitcoin.

Antes de seguir se tiene que hacer otra aclaración de todos los diferentes agentes involucrados y conectados en la red. Se tenía ya una diferenciación entre las computadoras y los usuarios. Los primeros son los encargados en compartir y actualizar el libro mayor, Block Chain, con internet, en una red descentralizada. Los segundos se conectan a la red de bitcoin, ya sea con su cartera como tal, o representados por un exchange o Casa de Cambio. El tercer agente, el que se acaba de introducir, está conectado también a la red de bitcoin, pero cumple con la tarea de firmar las transacciones para validarlas. Como se mencionó al momento de explicar la velocidad es hasta después de 60 minutos, aproximadamente, que queda como irreversible nuestra transacción y con la garantía de que recibimos y/o enviamos nuestras monedas satisfactoriamente. Esta irreversibilidad es la que nos garantiza que no se puedan gastar dos veces una misma moneda, es decir el gasto doble.

La labor de los mineros puede parecernos redundante o irrelevante, pues podríamos tener un solo registro en una página de Internet con nuestro libro mayor contable. Pero este caso sería un caso

[9] Piratas informáticos
[10] Introducido también como el Libro Mayor con registros y firmas de transacciones.

análogo a un banco o institución financiera central, pues se tendría un solo sitio, en este caso una página, donde están todos los registros de nuestro libro mayor. Siguiendo con la comparación, si alguien quisiera entrar y modificar algún registro, bastaría con quebrar la seguridad del sitio en donde está guardado el Libro Central y modificar a su gusto todas las entradas. Por el hecho de ser una moneda digital los cambios serían inmediatos y sería, una vez que el intruso logró entrar al sitio donde se guarda el libro mayor, muy difícil detener a esta persona.

Otro punto que no podemos olvidar es la naturaleza digital de la moneda, pues se ha probado que con dinero fiduciario las instituciones centrales son capaces, hasta cierto grado, de administrar y resguardar el dinero de sus usuarios. Si comparamos entonces esta situación, central, a un libro mayor que está distribuido a 9 mil computadoras diferentes alrededor de 96 países, al 12 de Octubre del 2017. (Yeow, 2017) Un agresor tendría que hacer una modificación en tiempo real, con la firma de los Mineros, a todos los registros de las computadoras conectadas a la red, para poder modificar y poder obtener un beneficio o causar algún tipo de daño.

Esto nos lleva entonces a cómo es la firma de los Mineros y por qué es tan importante. En términos muy simples, lo que los Mineros hacen es estar calculando con procesadores cada vez más complejos, eficientes, y costosos, una gran cantidad de cálculos por segundo. En el momento en que un Minero obtiene el resultado deseado de lo que está calculando, entonces se obtiene una firma que nos ayudará a validar el registro en nuestro Libro Contable. Algo muy importante de entender es que el resultado que buscan los Mineros, para la solución de su cálculo, es muy fácil de verificar. Pero por otra parte como ya se dijo toma mucho tiempo y recursos para obtener ese resultado.

Sin embargo, antes de continuar con la explicación de la firma de los Mineros, debemos concluir con lo que comenzamos, y esto fue la cuarta manera de obtener bitcoin. Los mineros al obtener la firma que valida el registro de una transacción, obtienen una recompensa, y esta recompensa son bitcoins. Paradójicamente se generan bitcoins verificando transacciones de bitcoin. Puede sonar tautológica la manera en la que esta moneda es “minada”, pero nos revela algo muy íntimo de la moneda, y es que la cantidad total de bitcoins está relacionada directamente con la recompensa por el minado.

Citando una conversación de Satoshi Nakamoto, en la que nos habla sobre las recompensas del minado, obtenemos una dimensión más profunda del diseño de bitcoin. Esta conversación es con Martti Malmi,

un finlandés que es administrador actual del foro BitcoinTalk[11], colaboró con Satoshi para hacer las primeras versiones de bitcoin, y es quien hizo la primera transacción en la historia de la moneda a cambio de dólares. (Malmi, 2015). La conversación: "¿La comisión, que reciben los mineros, será siempre la manera para garantizar la rentabilidad de hacer el minado de bitcoin, aún cuando generarla deje de ser rentable?", y la respuesta de Satoshi: "Cierto. De lo contrario no podríamos tener un límite finito de 21 millones de monedas, porque tendría que haber siempre una recompensa mínima para generarla. En unas décadas cuando la recompensa sea demasiada chica, la comisión de la transacción será la principal compensación para los nodos[12]. Estoy seguro que en 20 años habrá o bien un volumen de transacción muy grande o no lo habrá." (Nakamoto, 2010a) Traducción propia.

Una vez dicho esto podemos hablar de otra particularidad de la moneda, y es que bitcoin tiene una cantidad limitada de unidades que serán creadas en toda su historia, específicamente 21 millones. No serán minadas o creadas más de este número. Al 10 de Octubre del 2017 se tenían 16,617,750 bitcoins en circulación (Blockchain Luxembourg S.A.R.L, 2017a), y para cuando se lean estas líneas el número de monedas en circulación estará ya más elevado.

Como se mencionó ya, tener un número fijo de monedas y una producción constante de monedas fue por diseño, no se hablará por ahora más del diseñador de bitcoin pero, para no dejar al lector en blanco, podemos decir que es un personaje polémico, en el anonimato y existe la posibilidad que sea millonario o incluso billonario. Sin embargo en el apartado de Satoshi Nakamoto profundizaremos en todo lo relevante a su identidad e historia, y por ahora nos atendremos a su creación.

Hablando sobre la circulación total y la producción de monedas, podemos citarlo cuando publicó en Internet la primera versión de bitcoin: "La circulación total será de 21,000,000 monedas." … "reduciendo la cantidad a la mitad cada 4 años. Primeros 4 años: 10,500,000 monedas. Siguientes 4 años: 5,250,000 monedas. Siguientes 4 años: 2,625,000 monedas. Siguientes 4 años: 1,312,500 monedas. etc… Cuando se termine (la distribución), el sistema puede soportar comisiones de transacciones. Está basado en una competencia de mercado abierto, y siempre habrá probablemente

[11] Uno de los principales foros y el más viejo, en donde se habla del desarrollo de bitcoin y de sus detalles técnicos, entre otras cosas.
[12] En este caso Satoshi, como especialista en computación, utiliza la palabra de "nodo" que tiene su definición en la computación, pero para nuestro caso podemos intercambiarla por los "mineros". Pues los mineros son los encargados de validar transacciones y recibir una compensación por ello.

nodos[13] dispuestos a procesar transacciones gratuitamente." Traducción hecha por el autor (Nakamoto, 2009)

Los primeros 4 años tendremos solamente 10,500,000, y como podrá haberse dado cuenta el lector, en los siguientes años la producción[14] será la mitad del periodo anterior, así sucesivamente cada 4 años hasta llegar al número acordado. Ya que se mencionó que a los encargados en procesar transacciones se les llama mineros, ayudaría pensar en una mina para entender la distribución planteada por Satoshi. Si imaginamos entonces que las primeras 10,500,000 monedas, que se "minan" están en la parte superior y la más accesible, entonces su obtención es muy sencilla y se puede hacer con pico y pala. Eventualmente esta primera zona se agota, procedemos a la segunda zona en donde es necesario ir más profundo que la anterior, y donde se encuentran las siguientes 5,250,000 monedas, similarmente la dificultad de obtención resulta más difícil que la anterior y se necesitaría ya un taladro hidráulico o utensilios más eficientes que un pico y pala.

Entre más profundo se vaya en la mina más difícil resulta la obtención y refinamiento de las monedas y menor número de monedas están disponibles en las siguientes zonas. Como se indicó ya: los mineros usan procesadores cada vez más complejos eficientes y costosos, y la cantidad de bitcoins al escribir estas líneas es de aproximadamente 16 millones, por lo tanto estamos en la tercera zona de la "mina".

La dificultad que representa la tercera zona de la mina es aquella que no puede ser superada ya por el pico y la pala, ni tampoco con un martillo hidráulico. En términos reales y de computación, ya no se pueden verificar transacciones con una simple computadora personal (primera zona), o con una computadora construida para validar transacciones (segunda zona), sino que hoy en día se tienen procesadores, diseñados exclusivamente con la finalidad de validar transacciones de bitcoin, conectados entre sí. A continuación una fotografía de un ejemplo del minado de tercera zona:

[13] Mineros. Vease nota al pie número 10.
[14] Una anotación importante que hacer es que dentro de la comunidad de bitcoin he notado que no se usan los términos usuales de producción para hablar sobre la creación de las monedas, sino que se ve como el minado de las monedas y se les ve como algo más relacionado a imprimir o generar dinero que a producir algún bien.

Imagen 2: *("Inside North America's $8m a Month bitcoin Mining Operation," 2014)*

Es importante recordar que la analogía de la mina es solamente un ejercicio imaginativo y que realmente lo que se hace por parte de los mineros es procesar transacciones y estar calculando la solución a un problema matemático poco predecible y de gran dificultad, como ya se explicó.

Un último detalle del que se habló ya, pero aún no se desarrolla, son las fracciones. Si bien recuerda el lector cuando hablé de la velocidad y la compra de mis primeras bitcoins, hablé sobre recibir fracciones, no una bitcoin completa. Para plantearlo en términos más cercanos, así como las fracciones de los pesos se les conoce como centavos, a las fracciones de bitcoin más pequeñas se les conoce como satoshis, en honor al creador. Sin embargo una bitcoin puede fraccionarse en 100 millones de partes. Este es un concepto difícil de digerir, y resulta impráctico imaginarnos todos los satoshis físicos, a manera de centavos de peso, que tendríamos que tener en nuestra bolsa para poder pagar algo con 1 BTC. Sin embargo por la naturaleza electrónica de bitcoin, que es una divisa digital, los satoshis representan solamente un número decimal y son fáciles de manejar, en número y con decimales un Satoshi se ve así: 0. 000 000 01.

Esta es otra de las características que se menciona que es por diseño, sin embargo tenemos una conversación de Satoshi en el foro de BitcoinTalk, en donde muestra cierto grado de confianza por elegir este número de decimales hablando de inflación y de ver bitcoin como un bien. El título del tema en el foro es: "Que tan divisible es bitcoin y otras preguntas de mercado/economía" lo abrió un usuario llamado BlueSky: y su duda sobre este tema es: "¿Qué tan divisibles son las bitcoins? Hago esta pregunta pues prácticamente la producción de bitcoins es finita & será muy costoso en términos de tiempo & poder en el futuro, y si el sistema se hace más popular habrá más bienes que BC's (bitcoins)".

A lo que Nakamoto responde: "Eventualmente como máximo solamente 21 millones de monedas para 6.8 mil millones de personas en el mundo si realmente se hace enorme. Pero no te preocupes, existen otros 6 lugares decimales que no se muestran, para un total de 8 lugares decimales internamente.

Muestra 1.00 pero internamente es 1.00 000 000. Si hay una deflación masiva en el futuro, el programa podría mostrar más lugares decimales" (Nakamoto, 2010b).

Como podemos observar, Nakamoto nos habla nuevamente del número total de bitcoins, mismo que relaciona con la población mundial en el 2010, que es cuando escribió esa respuesta. Paralelo a vincular el número total de monedas con la población mundial nos menciona que existen internamente 8 lugares decimales adicionales. Es importante recordar que esto fue en el 2010 y en ese entonces se tenían solamente dos lugares decimales. Hoy en día ya se han implementado los 8 lugares.

Por lo tanto para tener satisfactoriamente una bitcoin es necesario tener 100,000,000 de satoshis. Haciendo cálculos, si obtenemos la cantidad de satoshis que cada persona del mundo tendría al 2010 y teniendo todas las monedas de bitcoin en distribución tendríamos que hacer la división de 2,100,000,000,000,000 entre la población mundial en el 2010 de acuerdo a Nakamoto: 68,000,000,000, dándonos un total de 30,882 satoshis por persona. Esto se puede calcular para ver qué tantos centavos se tendrían mundialmente, o también se puede ver como una respuesta de Satoshi para generar un bien que no sea escaso como plantea el usuario del foro BlueSky.

Un punto que se dejó en el aire y aún no se explica es la anonimidad. Se habló de ella en las desventajas de las Casas de Cambio, y es algo que al usar bitcoin con carteras, sin tener que depender de exchanges, y con un poco de cuidado puede ser realizado satisfactoriamente. A lo que se refiere específicamente cuando se dice que bitcoin es anónima es en sus transacciones. La anonimidad en las transacciones ocurre con el uso adecuado del PIN público y las medidas adecuadas para no dejar rastro con su uso en Internet. Para cada transacción nueva es necesario usar un PIN nuevo pues es muy fácil generarlo, su uso repetido puede hacer más fácil relacionar una identidad a cierto PIN público y de ese modo perder la anonimidad.

La anonimidad depende también de nuestros hábitos con los que usemos Internet, es decir si publicamos nuestra identidad con nombre y correo junto con un PIN público, como lo he hecho yo anteriormente, se pierde la anonimidad. Todas las transacciones que recibo y envío de esa dirección quedarán registradas en el libro mayor. Sin embargo, si se tiene el cuidado suficiente se pueden hacer transacciones de bitcoin completamente anónimas. Si agregamos a esto la rapidez, seguridad, practicidad, lo descentralizado y la no regulación gubernamental tenemos una moneda con crecimiento sin igual con un volumen de transacción muy alto. Con estas características es muy fácil entonces hacer

y lucrar con cuestiones ilícitas, como puede ser el mercado negro o el lavado de dinero.

Una de las últimas cosas por explicar para concluir con la explicación de qué es bitcoin, es lo que se conoce como el *Genesis Block* en inglés y en español *Bloque Génesis*. Antes, sin embargo tenemos que hacer una simple aclaración de que es un bloque, se ha dicho que los mineros lo que validan son transacciones para simplificar la explicación del minado, pero en realidad lo que verifican con su firma, es un conjunto de transacciones. A este conjunto de transacciones se le llama bloque o Block en inglés, y por cuestiones de practicidad y velocidad los mineros agrupan las transacciones en estos bloques pues verificar individualmente cada transacción sería poco eficiente[15].

En los términos que se ha explicado bitcoin tenemos que el *Bloque Génesis* en nuestro caso sería la creación del libro mayor Público como tal. Como ya se sabe cada que se verifica un bloque, es decir cierto número de transacciones, se tiene una recompensa o incentivo para los mineros. En este caso la recompensa que se obtuvo del primer bloque que se minó no se puede gastar (Bitcoin Wiki, 2017), sin embargo todas las demás son ya efectivas para transacciones. Regresando al Libro Público Mayor podemos considerar el *Bloque Génesis* como la primera impresión oficial que se hizo, con la seguridad adecuada y propia para poder identificarlo como el original y no estar usando otro libro mayor.

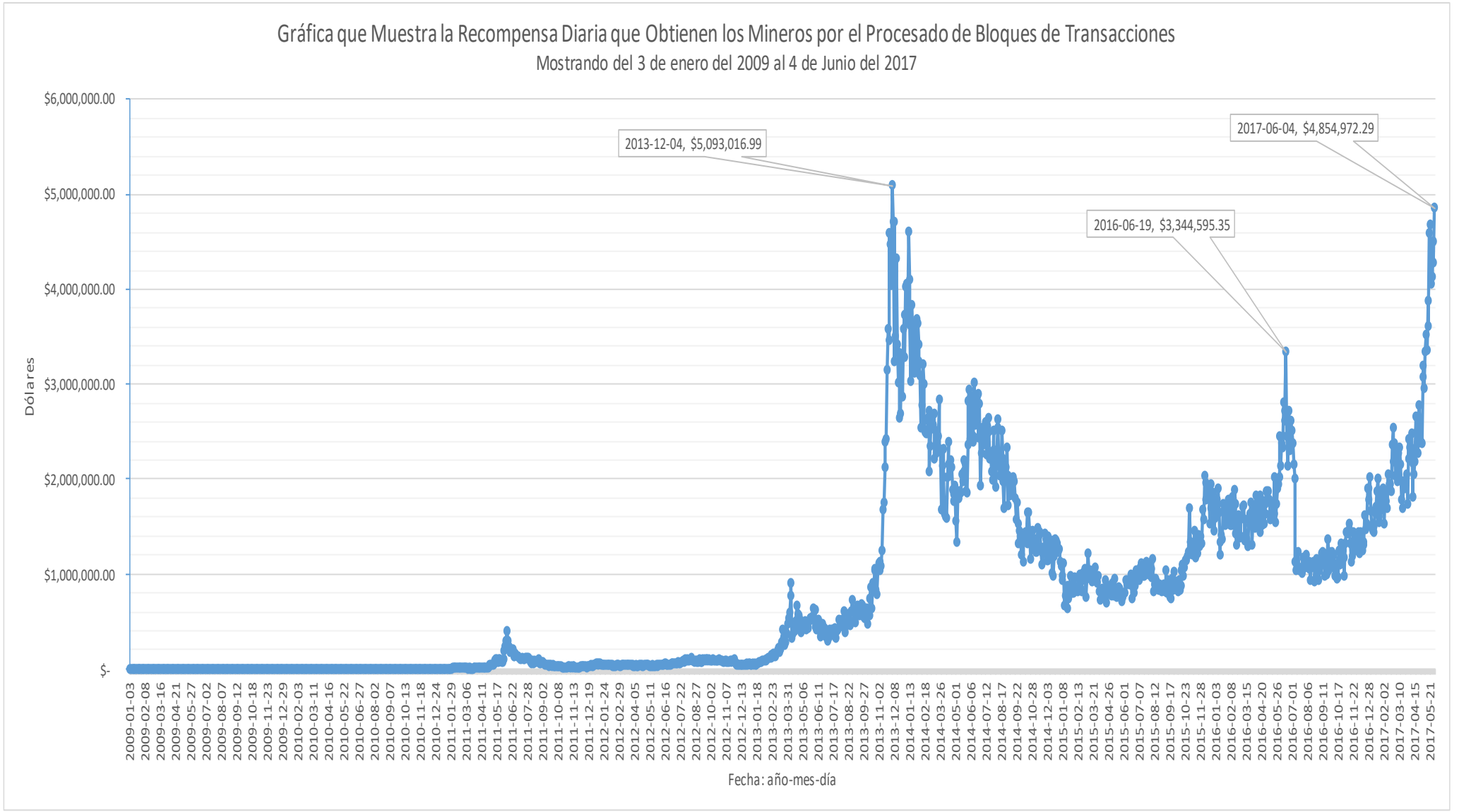
Concluyendo sobre algunos temas podemos hacer las siguientes reflexiones. En relación al tema de la seguridad en gran medida depende del conocimiento del usuario de aquello que está usando, cómo lo está usando y qué mecanismos de seguridad están detrás de aquello a lo que confía sus monedas. Para grandes cantidades de bitcoin se recomienda otro tipo de cartera a diferencia de la que se habló aquí y una seguridad mucho más robusta.

Que la red sea par a par y que todos tengan la capacidad de unirse no significa que la red sea completamente democrática e igualitaria, pues tenemos una gran cantidad de mineros que acaparan muchos de los nodos de la red. Con lo cual generan una capacidad de decisión mayor para el futuro de la moneda cuando se llega a necesitar una votación de los mineros para acordar algo, a diferencia de los mineros independientes.

Para explicar un poco más a fondo el minado y ver las cifras correspondientes a esta actividad tengo dos gráficas. En la primera podemos ver la cantidad de dólares que ganan por minar satisfactoriamente

[15] Por esta razón se le llama cadena de bloques o blockchain a la tecnología detrás de bitcoin, pues quedan registrados todos los bloques que ya se han verificado por los mineros y forman parte de una cadena de transacciones validadas.

un bloque, esto es la recompensa que obtienen al obtener la “firma” con la cual validan como correcta un conjunto de transacciones. La segunda es la cantidad de dólares que obtienen por el cobro de comisiones. A continuación las gráficas:



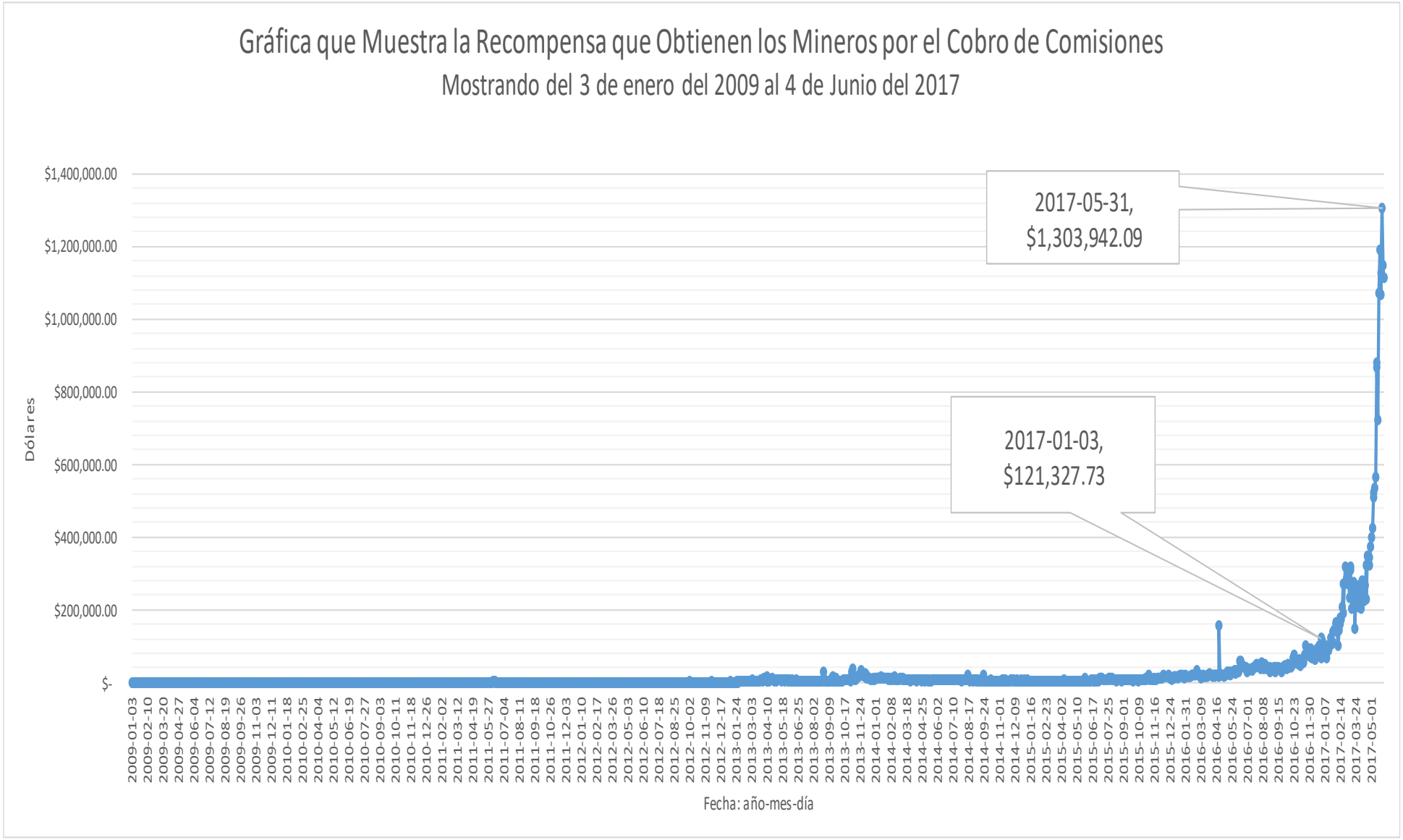
Gráfica 1: Datos obtenidos de: (Blockchain Luxembourg S.A.R.L, 2017b)

Como podemos observar en la gráfica anterior existe una recompensa muy grande por ser parte de la red de bitcoin y ser un minero. Existen días como los que están subrayados, 4 de diciembre del 2013, 19 de junio del 2016 y 4 de junio del 2017 en donde se llegó a obtener una recompensa por minado de bloques de 5, 3 y 4 millones de dólares. En la fecha del 4 de diciembre del 2013 y del 19 de junio del 2016 se estaba todavía en la "zona 2" de la mina, es decir la recompensa por bloque en ese entonces era de 25 BTC, mientras tanto en la última fecha señalada se estaba ya en la "zona 3" de la mina, en donde la recompensa por bloque minado es de 12.5 BTC.

Como se explicó ya, la distribución de bitcoin está controlada, en promedio los mineros tardan 10 minutos en generar[16] un bloque, un día tiene 1440 minutos, por lo tanto cada día se generan en promedio 144 bloques. Si estamos en la zona 2 se generan en promedio 3600 bitcoins al día pues la recompensa por bloque es de 25 bitcoins, consecuentemente en la zona 3 se generan 1800 bitcoins, pues la recompensa es de 12.5 BTC. Estos son números aproximados y pueden variar dependiendo de la eficiencia de los mineros, si observamos las bitcoins creadas los días señalados anteriormente podemos ver reflejada la variación de la que se habla. El 4 de diciembre del 2013 se generaron 5020, el 19 de junio 2016 se generaron 4021 y el 4 de junio del 2017 se generaron 2941 bitcoins (Bitcoin.com, 2017a). Aunque esta es una razón por la cual hubo una ganancia elevada el tipo de cambio también influye. En diciembre el tipo de cambio fue de 1,147 dólares una bitcoin, el 19 de junio del 2017 fue 764 dólares y el 4 de junio del 2017 fue de 2,552.(coindesk, 2017a).

No podemos olvidar que en la gráfica anterior se hace la conversión de bitcoin a dólares y se puede considerar como el valor de lo que minan, pues si observamos las monedas que obtienen como tal los mineros estas van descendiendo por el mismo diseño del que ya se platicó. La siguiente gráfica que es relevante ver ahora es sobre las comisiones que cobran los mineros.

[16] Generar es la palabra usada en la jerga de bitcoin, pero lo que se hace es validar y verificar un bloque de transacciones.

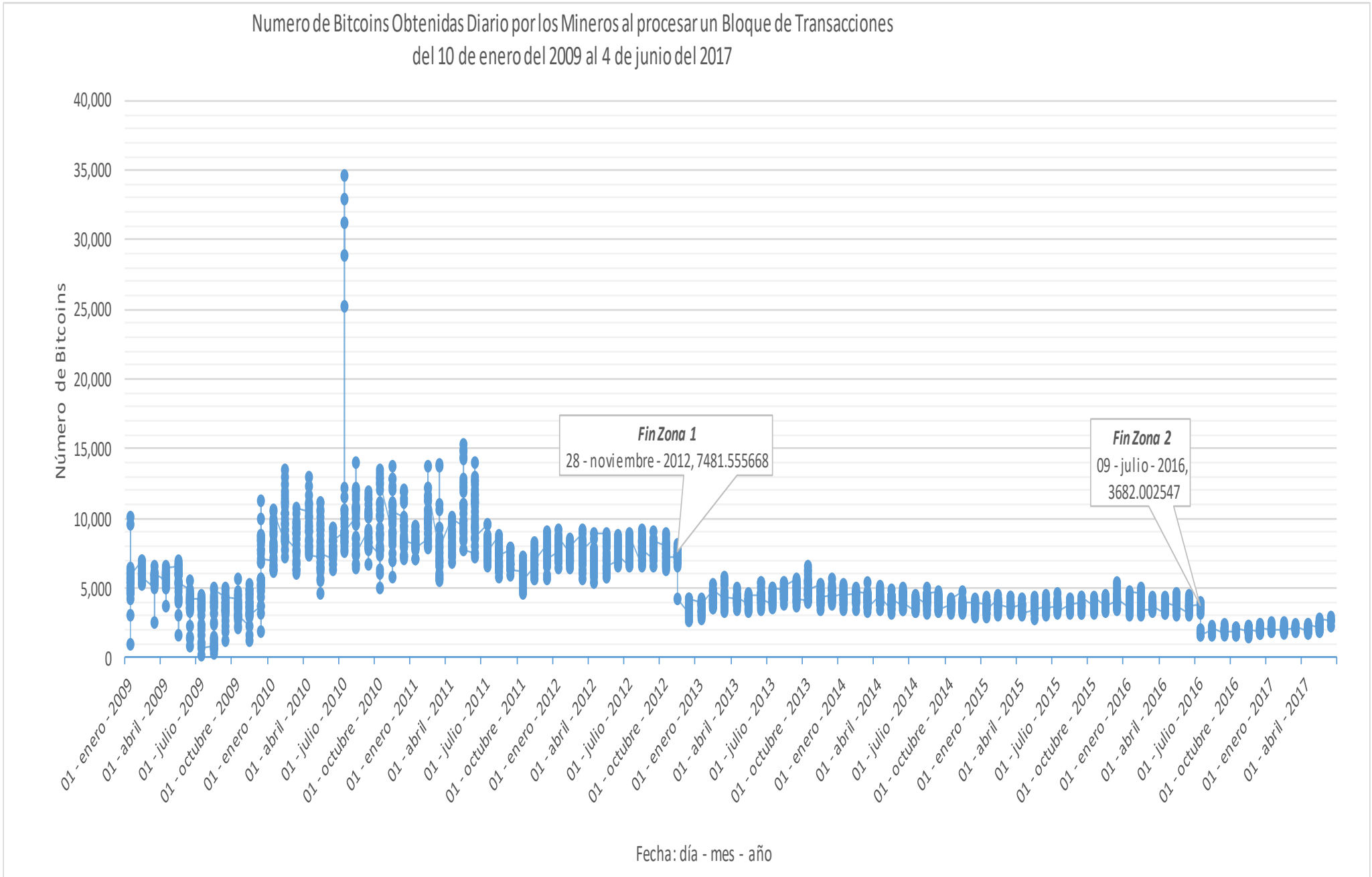


Gráfica 2: Datos obtenidos de: (Blockchain Luxembourg S.A.R.L, 2017b)

En la gráfica del cobro de comisiones podemos observar la realidad sobre las ganancias de los mineros, esta es una en la que dependen de procesar bloques, al igual que el tipo de cambio al vender las bitcoins que obtienen del minado y las comisiones son realmente pocas en comparación a la recompensa por bloque, esto por lo menos del 2009 al 2016. Otro punto a comentar es el reciente incremento del cobro de comisiones en el 2017, de enero a mayo podemos observar un incremento aproximado de 10 veces el valor. La comisión en enero fue de 121,327 dólares y el 31 de mayo ascendió a 1,303,942 dólares es decir un incremento de 10 veces el valor de enero.

Otro punto que podemos retomar de la discusión anterior es cuando Satoshi menciona que en un futuro la comisión por transacción será la principal compensación para los nodos. Como podemos observar en la gráfica las comisiones finalmente después de 8 años están siendo relevantes y están dando ganancias equiparables o comparables a la recompensa por el minado de un bloque. Este comentario nos lleva a nuestro siguiente punto y es uno que es fácil de olvidar tomando en cuenta y viendo las grandes ganancias que nos puede dar la minería y es: cada vez menos bitcoins son minadas y el número de bitcoins minadas está decreciendo. Es decir independiente del precio de las bitcoins y de cuan elevado sea su valor, un hecho que es fácil de olvidar es que habrá solamente 21 millones de monedas en circulación.

A continuación la gráfica:

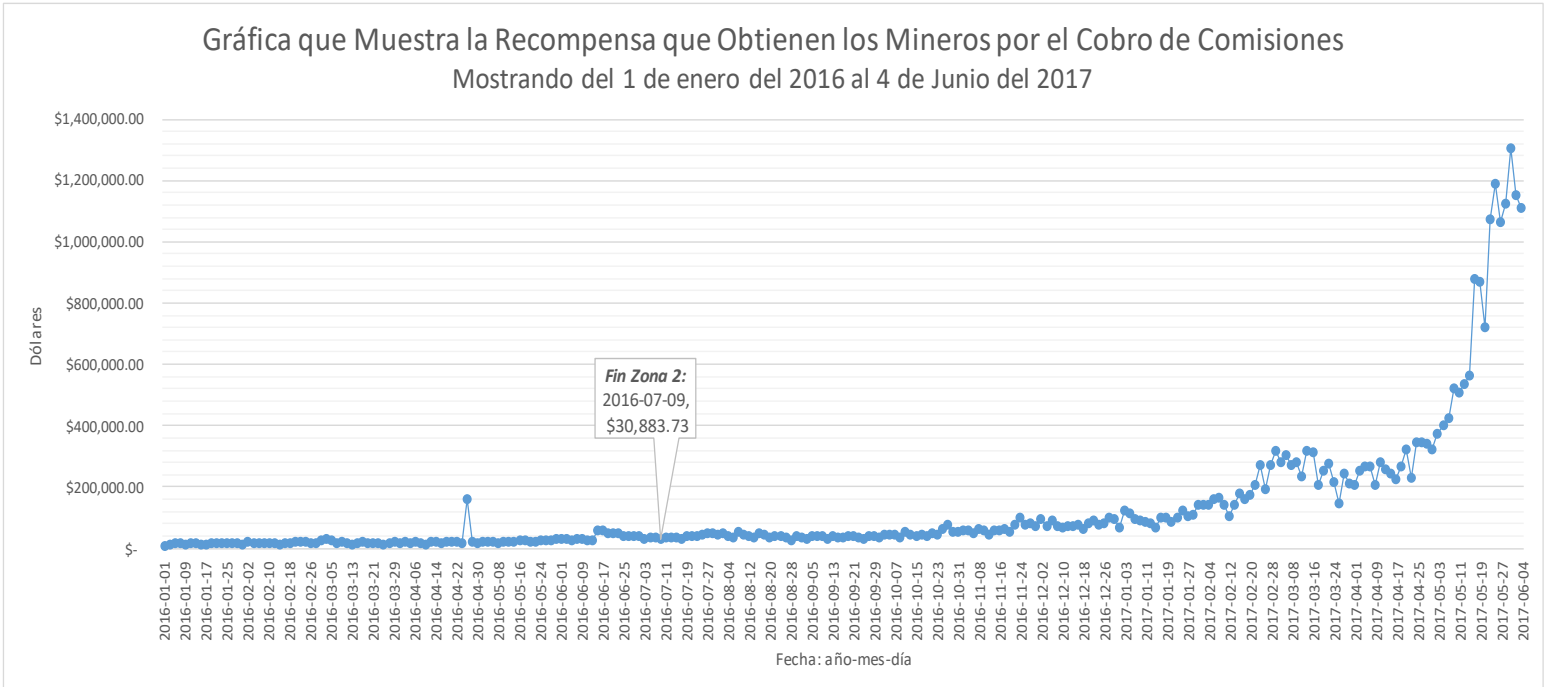


Gráfica 3: Datos obtenidos de (Bitcoin.com, 2017)

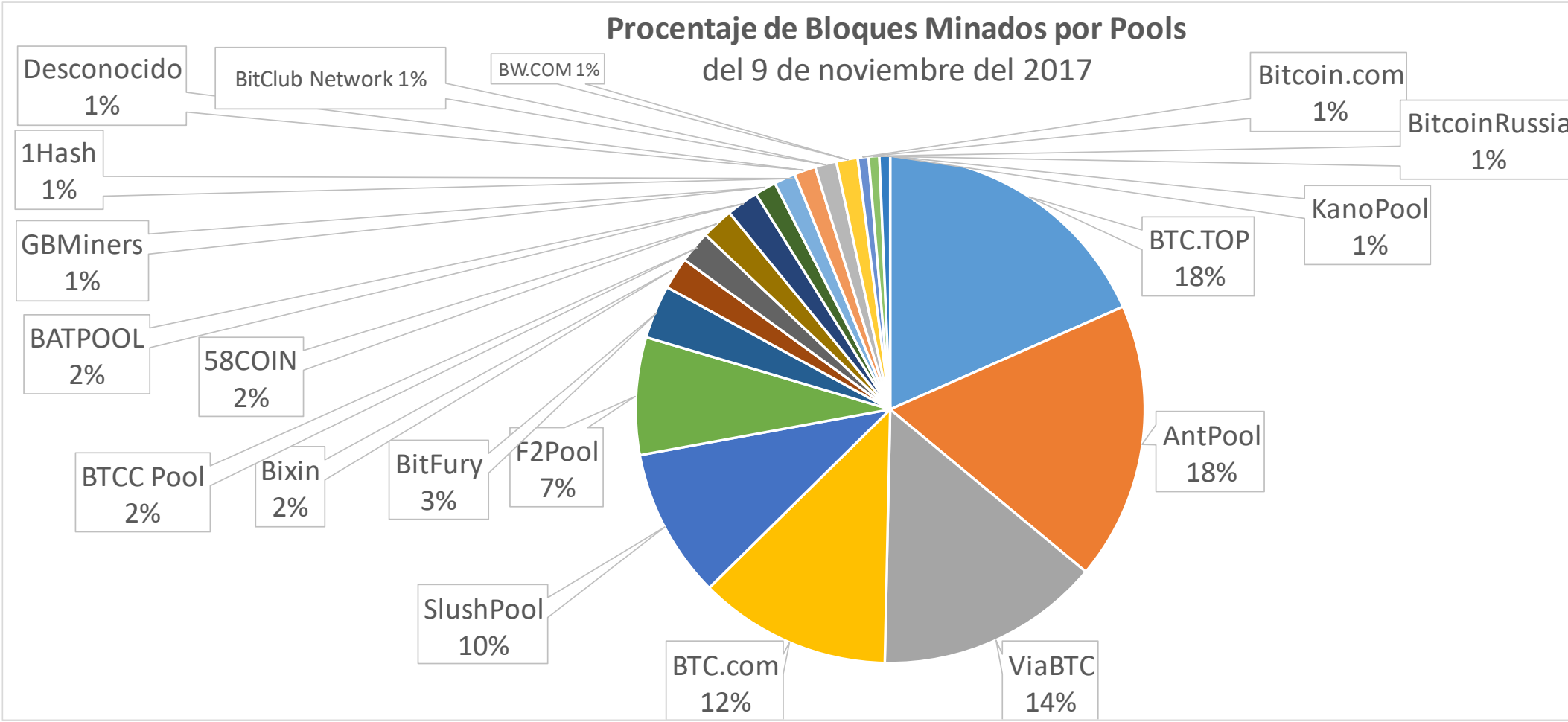
Como es de esperarse y es algo obvio, esta es una gráfica que tiene que, por diseño y por lo que ya se comentó, ir en decremento. Otro punto que podemos observar de la gráfica anterior son las zonas de las que se ha hablado. Se puede observar la transición de la *Zona* 1 a la *Zona* 2 el 28 de noviembre del 2012, en donde se nota considerablemente como se reduce el número de bitcoins creadas a la mitad. En promedio se tenía, con algunas variaciones de las fechas iniciales de bitcoin, una generación promedio de 7,800 al día. Esto hasta el 28 de noviembre del 2012, después de esta fecha el número baja a un promedio de 3,600. Después de lo cual se repite nuevamente, de 3,600 monedas pasamos a 1,800, esto se puede observar en el "***Fin de la Zona***" ***2*** en la gráfica.

Si vinculamos la gráfica anterior con la gráfica 2 podemos observar que paralelo a la baja en la producción de monedas, 1,800 ***Zona 3***, tenemos un aumento considerable en el cobro de comisiones. Es decir tenemos aproximadamente por noviembre del 2016 con la nueva regla de distribución un incremento considerable en el cobro de comisiones. En esta zona solamente se hacen 12.5 bitcoins por cada bloque procesado, o 1,800 bitcoins al día y como podemos observar en la siguiente gráfica, al aumento al entrar el año 2017 comienza a incrementarse.

Viendo entonces esta gráfica obtenemos una visión un tanto más positiva si fuéramos a participar en el minado de bitcoin, pues existe a partir del 2017 un incremento notable en las ganancias, a diferencia de la gráfica 2 en donde desde el 2009 al 2016 no existe un cambio notable. Sin embargo esto nos lleva a la gráfica 6:



Gráfica 4: Datos obtenidos de (Bitcoin.com, 2017)



Gráfica 5: Datos obtenidos de (Blockchain Luxembourg S.A.R.L, 2017b)

En la gráfica anterior tenemos el término de Pools, esto se refiere a un Fondo o a un conjunto de personas reunidas para minar bitcoin. Como ya se explicó el minado individual es propio de la *Zona* 1 en donde la dificultad para minar era muy baja, esto no quiere decir que uno no pueda hacer minería individual en las zonas siguientes, sin embargo es muy difícil competir como individuo para minar cuando existen estos fondos de mineros, los cuales hacen en colaboración la minería. Adicionalmente se tendría que tener mucha suerte para estar minando individualmente y poder minar un bloque y obtener la solución, es posible pero poco probable.

Analizando los costos de unirse a un fondo o invertir en la minería de bitcoin podemos observar páginas que hacen estimados con las siguientes cifras: Capacidad de procesamiento de nuestra computadora, su consumo en watts, el costo por Kilowatt hora, la comisión que el Fondo (Pool) nos cobra, la dificultad de minado de bitcoin, la recompensa por minar un bloque, el precio de un bitcoin en pesos y los costos de inversión.

A continuación dos tablas de las cifras y el estimado en cuestión:

Capacidad de Procesamiento (GH/s)	**Consumo (Watts)**
14000	1375
Costo de Luz ($/kWh)	**Comisión de Fondo (Pool)**
0.15	0%
Dificultad de Minado de Bitcoin	**Recompensa por Bloque**
1,452,839,779,145.92	12.5
Bitcoin en Pesos	**Costos de Inversión**
$ 140,674.21	$ 38,180.00

Tabla 1: Datos obtenidos de (CoinWarz, 2017)

Tiempo	Bitcoins Minadas	Conversión de Bitcoins Minadas a Pesos	Costo de Luz en Pesos	Comisión de Pool	Ganancia en Pesos
Cada Hora	0.00010096	$14.13	$4.01	0%	$10.12
Cada Día	0.00242312	$340.95	$94.50	0%	$246.45
Cada Semana	0.01696181	$2,386.25	$661.47	0%	$1,724.78
Cada Mes	0.07269348	$10,226.51	$2,834.87	0%	$7,391.65
Cada Año	0.88443734	$124,422.51	$34,490.86	0%	$89,931.65

Tabla 2: Datos obtenidos de (CoinWarz, 2017)

Es necesario decir que el estimado fue hecho para el 9 de noviembre del 2017 pues cambia diariamente el precio de la bitcoin, no se sabe cuántos mineros se estarán uniendo a la red, la dificultad de minado puede variar y por último depende la eficiencia de la Pool en la que estamos para obtener nuestras ganancias. Adicional a los cálculos anteriormente presentados nos da tres cifras más la página. La primera son los días para generar un bloque si estamos minando solos y es con las cifras que dimos de 5,158 días aunque se nos menciona que puede variar dependiendo de la suerte de uno. La segunda cifra son los días para generar una bitcoin completa y son 412 días y por último los días para recuperar nuestra inversión inicial que son 154 días. (CoinWarz, 2017)

El estimado fue haciendo la compra de uno de los procesadores que vende el Fondo (Pool), llamado AntPool que tiene 18% de los nodos minados al 9 de noviembre del 2012, ver gráfica 6. En este caso existen Pools que venden sus propios procesadores y con un simple registro nos podemos unir a dicho fondo, al igual que AntPool no cobra comisiones. En este caso su procesador AntMiner S9 se encuentra en 27,012[17] pesos y se están calculando 11,168 pesos de costo extra, pues se deben de comprar más cosas que el procesador y la posible mano de obra.

Por último regresando a la gráfica 6, podemos observar no sólo la eficiencia de los Fondos o Pools para hacer el trabajo del minado, sino que podemos ver lo que ya se había mencionado pero de una manera más concreta, en donde la capacidad de decisión está controlada por los mineros. Pues son ellos los que mantienen la red y en última instancia los Fondos tienen un poder de decisión muy grande, no sólo en la votación, sino también en el procesamiento de las transacciones, y en el caso de AntPool proveen a la comunidad de bitcoin con los procesadores más veloces y de cierto modo son un referente muy claro hablando de la red de bitcoin.

Una última conclusión comentando sobre la minería es que las ganancias, al igual que las comisiones, son cobradas en bitcoin, es decir no podemos pagar una comisión con dólares o pesos mexicanos, sino que la comisión que pagamos a los mineros se paga en bitcoin, o satoshis (fracciones de bitcoin). Con lo cual generamos una dependencia de los mineros con la moneda, en el sentido de que ganan en bitcoin y tienen ellos que vender sus bitcoin a dinero fiduciario, ya sea para subsistencia o como una ganancia u inversión, o pueden reinvertir en equipo de minado y minería. Este es un punto que puede

[17] El precio es de 1415 dólares y el tipo de cambio al 9 de noviembre fue de 19.09 pesos (Banxico, 2017a)

ayudarnos a ver quiénes son las personas que están realmente en las entrañas de la moneda, pues un minero de tiempo completo dedica toda su energía y tiempo a estar procesando transacciones mejorando sus cálculos y manteniendo su equipo de cómputo funcional, con el cual gana bitcoin y tiene que, por el poco uso presencial de la moneda, cambiarla a otra divisa para poder gastarla.

Hablando sobre la centralidad existe un cierto grado en la medida en que es usada para hacer movimientos grandes de capital. Es decir, la mayor centralidad que ocurre usando bitcoin es para movimientos grandes de capital, los demás usos, como se verán en mi experiencia etnográfica, que fueron comprando comics, tacos, pizzas y pagando una entrada a una conferencia, son los menos significativos. En términos simples tenemos una moneda con un movimiento de capital masivo internacional, con la posibilidad de ser anónima en la cual, a diario, son transferidos miles de millones de dólares, sin necesidad de instituciones bancarias o gobiernos.

Con la internacionalidad, depende de dónde tenemos internet, si alguien no tiene internet entonces no puede usar bitcoin, llevándonos a la conclusión inmediata de que es una moneda digital o electrónica, tal vez podemos decir que es una moneda de internet como tal. Otra conclusión de la internacionalidad es que no en todos lados se pueden conseguir bitcoins, es verdad se puede usar la moneda en muchos lugares, pero si inicialmente nadie o pocas personas lo tienen, o existen pocos lugares donde podemos obtenerla, su internacionalidad se ve limitada a donde la podemos conseguir o a la conexión a Internet como tal.

Concluyendo ahora con la cadena de bloques, sabemos que se puede entender de muchas maneras y vista de una manera más general tiene muchas diferentes aplicaciones, es por esto que fue difícil explicar su funcionamiento. Sin embargo para terminar de explicar y entender la cadena de bloques podemos intentar dar dos descripciones. Entendido desde la computación, si lo vemos como una base de datos, entonces al 16 de noviembre del 2017, contamos con una base con un tamaño de 133.2 GB. (Bitcoin.com, 2017b) Esto puede no decirnos mucho, pero si quisiéramos analizar esta base tendríamos que tener un poder de computo considerable para poder analizar y observar con eficacia a detalle todas las transacciones que son hechas.

En números más lejanos a la computación, entendido desde la contabilidad, tenemos que nuestro libro mayor cuenta con 494,544 (Bitcoin.com, 2017c) bloques. Recordando brevemente un bloque es un conjunto de transacciones, que por practicidad los mineros hacen para no estar verificando solamente

una transacción a la vez. El número de transacciones dentro de cada uno de estos bloques varía y tenemos en total de 271,640,369 transacciones (Bitcoin.com, 2017d) distribuidas entre los 494,544 bloques mencionados. Por lo tanto, si congelamos el tiempo y suponemos que no crecerán más las entradas de nuestro libro mayor, el libro que estamos describiendo necesitaría tener la capacidad para poder tener los 494,544 bloques o 271,640,369 entradas de transacciones. Sin embargo tendríamos que tener, por lo menos dentro de la "*Zona* 3" que es en la que estamos actualmente, un libro al que se le agregaran diariamente un promedio de 263,270[18] transacciones diarias. O alternativamente 150 bloques diarios.[19] De tal forma, como sea que imaginemos nuestro libro mayor es uno que crece muy rápidamente y tiene ya muchas entradas. Si lográramos tener una página por cada bloque hablaríamos de un libro de 494,544 páginas al 16 de noviembre del 2017.

Ahora que se ha hablado de las características generales y específicas y se ha dado una explicación de todos los términos generales de bitcoin se procederá a hablar sobre Satoshi Nakamoto. Persona de la cual se ha hablado ya indirectamente y se ha citado un par de veces a lo largo de este capítulo.

[18] Cifra que se obtuvo calculando el promedio de transacciones diarias del inicio de la *Zona* 3 al 16 de noviembre del 2017. Datos de (Bitcoin.com, 2017d).
[19] Se obtuvo el promedio con el intervalo del 9 de julio del 2016, que es el inicio de la *Zona* 3 al 16 de noviembre del 2017 con datos obtenidos de www.bitcoin.com: (Bitcoin.com, 2017c)

¡Está vivo! ¡Está vivo!: Satoshi Nakamoto y su White Paper

Biografía de Satoshi Nakamoto y un análisis de su Informe Blanco

Hasta ahora se ha hablado solamente de las características de bitcoin, y se ha mencionado el nombre de su creador, Satoshi Nakamoto, sin embargo este personaje es muy complejo. Es uno que se conoce solamente en un entorno virtual, que escribió un Informe Blanco planteando las bases de un sistema que, gracias a su desarrollo, es capaz de tener un volumen y movimiento de capital muy alto, pues hablamos de miles de millones de dólares. Todo esto sin tener que depender de ningún banco o gobierno, y como cereza del pastel, es anónimo, nadie sabe quién es en la realidad, y tiene probablemente un gran número de bitcoins.

Dentro de este apartado se hablará de este personaje virtual, y simultáneamente se analizarán algunos detalles de su Informe Blanco. Los detalles que se abordarán serán solamente aquellos que influyen en las cuestiones que hacen bitcoin única, en el sentido de ser una moneda descentralizada y un proyecto desarrollado por su comunidad en Internet y no las cuestiones técnicas, pues eso ya se vio en la explicación de bitcoin. En relación a Satoshi Nakamoto se hablará y se construiría una semblanza desde las citas y conversaciones que se tienen en Internet, así como de información disponible de este personaje, e incluso hablaremos de las personas que afirman ser Nakamoto.

Dado su anonimato y desaparición[20], estas conversaciones y citas, son la única manera de acercarnos a su pensamiento y manera de diseñar la moneda, pues al buscar una explicación concreta de los detalles más finos de bitcoin no tenemos información precisa. Es por ello que muchas veces al explicar, o leer sobre la moneda y sus propiedades específicas se dice que son por diseño, en lugar de dar una razón particular.

A lo largo de la investigación se ha usado ya varias veces la palabra de Informe Blanco o White Paper, ambos términos se refieren a la misma cosa y esto es; un ensayo persuasivo, que usa lógica y hechos para promover cierto producto, servicio o punto de vista. Su contenido provee información práctica a empresarios que buscan comprender un tema, resolver un problema o tomar una decisión (Graham, 2017). En nuestro caso Satoshi plantea resolver el problema de doble gasto o double spending en inglés, que es una de las razones por la cual no se había tenido antes una moneda digital.

[20] Estamos hablando de una desaparición de Internet o virtual, pues en la realidad no existe, por ahora, una figura pública que haya probado ser Satoshi Nakamoto.

A lo que se refiere por doble gasto es que se pueda gastar una misma moneda más de una vez. En nuestro caso sería pagar con 1 bitcoin un libro y con esa misma bitcoin pagar un café. Como bitcoin es en última instancia un bien digital, y como es muy fácil de generar copias exactas de los archivos digitales existe la posibilidad de hacer un doble o múltiple gasto, al igual que multiplicar fácilmente la moneda. Otra propiedad de los archivos digitales es la velocidad con la que se pueden enviar a través de Internet. Por lo tanto, diseñar una moneda en un entorno que cuenta con la capacidad de hacer copias fácilmente y una velocidad de envío alta, ha sido un reto por los desarrolladores y criptógrafos desde los inicios de la década de los 90as. El modo en el que se logra resolver este problema es con la cadena de bloques, y con el problema que deben resolver los mineros para validar las transacciones. Esto es lo que se explicó en el primer capítulo a lo que se refiere con el libro mayor, el verificar y firmar las transacciones.

Ejemplificando, el informe tiene en las primeras líneas de su resumen: "Una versión de efectivo digital completamente de par-a-par permitiría enviar pagos en línea directamente de una entidad a otra sin tener que atravesar por una institución financiera. Las firmas digitales proveen parte de la solución, pero los beneficios principales se pierden si un tercero de confianza es requerido para evitar el doble gasto. Nosotros proponemos una solución al problema de doble gasto usando una red de par-a-par."(Nakamoto, 2008a). A lo que se refiere cuando menciona usar una red de par a par, es lo que ya se mencionó en la explicación de bitcoin cuando se habla que la moneda usa una red descentralizada. Para recordar; es una red en la que cada par tiene igual de importancia que los demás, todos comparten la misma información y trabajan juntos para lograr un objetivo.

Lo que debemos observar es que en las primeras líneas Satoshi ya nos indica el problema que pretende resolver, el doble gasto, usando una red de par-a-par sin tener que depender de una institución financiera, unas primeras líneas muy poderosas para abrir el informe. Algo también importante de mencionar es la forma de redactar en donde usan el plural, concretamente: "Nosotros ponemos una solución…"(Nakamoto, 2008a). En estos momentos puede considerarse solamente como una forma de redactar, sin embargo, nos ayuda a introducir la idea de que Satoshi puede ser más de una persona. Dada la anonimidad de Satoshi no se sabe con certeza quién es, por eso mismo no se puede descartar la posibilidad que sea un grupo de personas, idea que se desarrollará más adelante, cuando se discuta su identidad.

Antes de seguir hablando sobre el Informe es relevante introducir la lista de correos en donde Satoshi

no solo publicó el informe, sino que también tuvo varias conversaciones en dónde defendió su idea y probablemente terminó de pulirla. La lista de correos en cuestión se llama *Metzdowd*, es abierta al público, cualquier persona se puede suscribir, su tema de especialización es la criptografía. Concretamente: "los aspectos técnicos de criptosistemas, repercusiones sociales de criptosistemas y políticas de la criptografía tales como controles de exportación o leyes restringiendo la criptografía". ("Metzdowd - cryptography Info Page,")

El momento en que la idea de bitcoin, es decir el informe blanco, se publicó al Internet fue el 1 de noviembre del 2008 en *Metzdowd* (Nakamoto, 2008b). Menciono que solamente fue la idea la que se expuso, pues el programa, que aunque era experimental y estaba en su primer iteración[21], fue publicado el 9 de enero del 2009 en un sitio llamado Sourceforge. Este sitio es uno en donde se le permite a los usuarios administrar y controlar proyectos de software libre.[22] Esta es una diferencia sutil, y puede causar un poco de confusión al lector, es análogo al caso en el que se tienen un plano para una construcción y la fecha siguiente es cuando ya tenemos el edificio construido. El programa sería en nuestro caso el edificio ya construido y el plano para la construcción sería el informe blanco.

Si analizamos una conversación en particular que tuvo Nakamoto con Hal Finney, vemos un hecho importante que nos ayuda a entender como trabajó Satoshi, al igual que nos sugiere la imposibilidad de plantear una fecha exacta de su creación. La conversación también nos sugiere la posibilidad de que Nakamoto sea más de una persona por la manera en desarrollar bitcoin.

La conversación ocurre el 9 de noviembre del 2008 entre Hal Finney y Satoshi. Como pequeña introducción a Hal Finney tenemos que fue la primera persona en recibir bitcoins directamente de Nakamoto. Específicamente recibió 10 bitcoins y dice que minó aproximadamente el bloque número 70[23] (Finney, 2013). En la plática virtual de Satoshi, tras responder varias preguntas de Hal sobre cómo resolver algunos problemas que sucederían con implementar bitcoin, después de que le pide una descripción orientada a los procesos de su idea, al igual que detalles concretos de cómo piensa programar todo, responde: "Aprecio tus preguntas. Yo hice esto un poco al revés. Yo tuve que escribir

[21] El programa que inicialmente se publicó en enero del 2009 ya no es el que se usa actualmente y como se verá más adelante, las versiones del programa van mejorándose cada cierto tiempo.
[22] La versión original del programa de Satoshi Nakamoto que es la versión 0.1, no se encuentra ya en el sitio de Sourceforge. Sin embargo podemos encontrar una copia de la versión 0.1.5, que es muy similar a la primera versión, en la siguiente referencia: (Nakamoto, 2017)
[23] En el capítulo de La Explicación de bitcoin se menciona que es el minado, al igual que los bloques, sin embargo no se menciona que los bloques, que son un conjunto de transacciones tienen un número que los identifica. El *Bloque Génesis* es el bloque número cero y mientras más bloques se agregan a la cadena de bloques los números van ascendiendo.

todo el código antes de que me pudiera convencer a mí mismo que podía resolver cada problema, luego escribí el artículo. Yo pienso que seré capaz de liberar el código antes de lo que podría escribir una especificación detallada. Ya estás en lo correcto en la mayoría de tus suposiciones donde llenas los espacios en blanco."[24] Traducción hecha por mí. (Nakamoto, 2008c)

Esta conversación nos plantea, como sugerí antes, que la fecha exacta de la creación de bitcoin, nos será ajena, pues su implementación ya llevaba siendo desarrollada antes de la publicación del famoso "White Paper". Esto por lo menos en la medida en la que no sepamos quien es Satoshi Nakamoto en la realidad. Algo más que podemos obtener de esta conversación es saber de la manera en la que desarrolló su idea. Ésta fue de una manera poco convencional, se implementó la idea directo al código. Esta es una de las maneras de trabajar en la comunidad de código abierto; en lugar de proceder de un modo más tradicional y académico o del sector privado en el que se hace la propuesta o un plan y luego se programa. Esto nos puede sugerir un gran número de conclusiones. Sin embargo pienso que la principal o más importante es la conclusión que se desprende de la manera en la que desarrollaron el código.

Al tener un desarrollo que es directo al código nos habla de que Satoshi es una persona experimentada en la programación, o como se menciona anteriormente la manera en la que se desarrolla el programa es similar a la efectuada en la comunidad del código abierto. Agregando a esto último, que proponen un sistema de efectivo digital sin tener que depender de instituciones financieras o de terceros, reforzamos la idea de que se pudo haber desarrollado bitcoin en una comunidad muy cerrada de personas anónimamente. Antes de seguir con la identidad de Satoshi y una vez que se ha tocado el tema del desarrollo comunitario profundicemos en el software libre.

Este es uno de los puntos que hace de bitcoin una moneda única y un proyecto administrado por su comunidad. En el software libre el programa o software otorga libertades al usuario, que van desde correr el programa, estudiarlo y cambiarlo como le parezca relevante. Comparativamente, los programas y softwares privados, o de empresas, cuentan con protección interna y externa, esto es, que no se puede estudiar cómo es que funciona ni proponer alguna modificación o mejora a su funcionamiento. Así como solamente se puede correr de la manera específica en que fue diseñado y cómo indican sus términos de uso.

[24] Otra aclaración que es pertinente de hacer es que una especificación detallada del código, es diferente al informe blanco, pues la especificación es una descripción de los procesos de la computadora y del programa con términos de programación pero comprensibles para una persona.

Éstas son dos maneras que se tienen de desarrollar programas, la manera tradicional o privada, en la cual el desarrollo depende de la institución, de las personas que contrata así como del objetivo de la empresa. A diferencia del desarrollo de programas o software libre, en donde depende de las personas que quieran colaborar al proyecto y de una comunidad que decide a dónde se dirige el proyecto. Concretamente, si observamos el caso de bitcoin, desde la primera versión a la más reciente, tenemos que es: "un proyecto gratuito de código abierto impulsado por la comunidad, liberado bajo la licencia MIT."(Bitcoin Project, 2017a)

Esta consigna está en la página de descarga de bitcoin, que es la licencia bajo la cual está liberado al público el programa. La licencia como su nombre lo indica es una licencia que surgió en el Instituto de Tecnología de Massachusetts, y es conocida como una licencia permisiva ("Licencia MIT," 2017). A lo que se refiere con permisiva es que puede utilizarse y reutilizarse el programa desde una manera libre hasta privada, es decir se puede reescribir públicamente el programa y redistribuir abiertamente hasta, incluso, vender copias siempre y cuando incluyamos la licencia MIT. Aunque puede sonar contradictoria esta elección, podemos entender la preferencia de Satoshi al liberar la primera versión de su programa bajo esta licencia, pues es una de las más usadas hoy en día para desarrollar programas de software libre. Es la que permite la mayor difusión, pues se permite el desarrollo en ambas esferas; pública y privada.

A otra cosa que se refiere esta licencia es que la libertad otorgada para cambiar el programa está regulada por una comunidad de desarrolladores, al igual que se deben de seguir pautas para colaborar al proyecto. Es así que los posibles cambios al programa son revisados por desarrolladores y no es aceptado cualquier cambio sin antes una revisión. (Bitcoin Project, 2017b) La libertad otorgada al usar bitcoin es la de correr, estudiar y cambiar el programa, todos con el impulso de la comunidad.

El usar una licencia tan contradictoria que permita ambos tipos de desarrollos privados y libres, o públicos puede sonarnos contradictorio, pero si observamos unos datos podemos entender la decisión de Nakamoto. De acuerdo a una página que analiza 2 millones de proyectos de software libre de 9,000 lugares diferentes, esta licencia, del MIT, ocupa el primer lugar con 32% de los proyectos. ("Top Open Source Licenses,") Es importante notar que el programa de bitcoin sigue siendo un proyecto gratuito y se sigue distribuyendo con la licencia de MIT desde la primera versión del programa en enero del 2009, hasta el momento en que se escriben estas líneas. Como es de suponerse y pueda el lector suponer, existen muchas implementaciones diferentes de la tecnología de bitcoin, concretamente tenemos en

nuestras manos toda una categoría de monedas llamadas criptomonedas, que funcionan con criptografía y con variaciones al funcionamiento de bitcoin. En la jerga de bitcoin a todas las criptomonedas alternas a bitcoin se les llama Altcoins, del inglés: alt de alternativas y coin de moneda.

Esto no quiere decir que las demás criptomonedas, Altcoins, sean copias al código original, sino que cada criptomoneda diferente tiene su "White Paper" o su artículo de creación, en donde se explica y justifica cómo funciona, qué tipo de criptografía usa y por qué funciona. Este es un hecho que en mi opinión es posible por la apertura que tiene bitcoin gracias a las licencias mencionadas, y que no se tengan seguros o secretos detrás de su idea principal.

Terminando con el tema del software libre tenemos también el software privado, y se tienen desarrollos privados de la tecnología como pueden ser las instituciones llamadas exchanges, que operan muy similarmente a las casas de cambio, o también empresas como IBM que están desarrollando su propia implementación de la tecnología de bitcoin. Es gracias, entonces, a este tipo de licencia que se pueden permitir diversos desarrollos, todos dentro de bitcoin o usando de un modo u otro su tecnología. Desde los que lucran y obtienen dinero funcionando como una Casa de Cambio, exchanges, hasta las instituciones privadas como IBM que están haciendo uso de la cadena de bloques, Block Chain en inglés. ("Banking consortium awards Digital Trade Chain contract to IBM," 2017)[25].

Podemos hablar de las consecuencias que este tipo de diseño tiene. Son importantes para la investigación y nos sirven para entender cómo funciona en sus fundamentos y se ha desarrollado. Menciono que tiene consecuencias importantes pues tocamos indirectamente la regulación. Cuando se habla de la criptomoneda se dice que no existe ningún tipo de regulación, este es un hecho verdadero, no existe ningún órgano o institución central que regule la moneda como tal a manera de banco o gobierno. Sin embargo podemos observar que existe una regulación activa y libre[26] para el programa que establece las reglas de su uso. Es una diferencia sutil y se puede generar confusión. En términos simples podemos decir que no se regula el qué, ni cuándo, ni dónde, pero sí cómo.

Este tipo de diseño tiene sus ventajas y desventajas. La ventaja de un diseño libre yace en que el código

[25] El Consorcio de Cadenas de Comercialización Digital o Digital Trade Chain Consortium fundado en enero del 2017, que consiste en la participación de los bancos: Deutsche Bank, HSBC, Natixis, Rabobank, Societé Générale y Unicredit, eligió a IBM para administrar, monitorear y asegurar las transacciones nacionales e internacionales, de todos los usuarios en su plataforma. Ésta es una plataforma que ayuda al desarrollo y comercialización de una cadena compartida de suministro, así como una plataforma de intercambio financiera.

[26] Libre en el sentido que se ha mencionado que otorga el programa los usuarios, con la bibertad de correrlo, estudiarlo y cambiarlo.

lo puede obtener cualquier persona, estudiarlo e incluso cambiarlo. Los desarrolladores y las personas que proponen cambios al programa ofrecen mejoras que benefician a todos los usuarios de la aplicación, al igual que mejoran la aplicación progresivamente. Este es un hecho que se puede demostrar o visualizar con bitcoin, pues el programa comenzó con muy pocas personas colaborando en él, al igual que un bitcoin cuando se empezó a usar tenía un valor nulo o muy bajo. A diferencia de hoy en día, en la que tenemos la versión 0.14.2 de la aplicación (Bitcoin Project, 2017c), misma que permite un volumen muy elevado de transacciones que oscila en los miles de millones de dólares. Sugiriendo que las mejoras que se han hecho al programa original de bitcoin, entre otros factores, han llevado al programa a lo que es hoy en día.

La desventaja que conlleva este tipo de diseño es que se deposita la confianza en los programadores, desarrolladores, matemáticos, criptógrafos y las personas que están detrás del desarrollo de la aplicación. Esta parece ser una clara desventaja, pero si comparamos lo que pasa con el desarrollo de las plataformas de intercambio que usan los bancos y las instituciones financieras no tenemos una situación tan desventajosa. En un banco el código de las plataformas y los programas están cerrados al público e incluso están protegidos por derechos de autor, esto hace que no haya ningún tipo de revisión, estudio o proposición de cambio externa, solamente la interna. Depositando entonces la confianza en una empresa privada en lugar de personas públicas, o accesibles por lo menos en el internet, que dado el caso podrían explicar el código o justificar su funcionamiento, mejoras y propuestas si entendiéramos del tema. Situación que sería muy difícil de lograr con las empresas financieras y bancos, pues parte de su éxito está en tener un mejor sistema y programas que su competencia y si revelan al público la manera en que funcionan sus programas se verían afectados por sus competidores o habría consecuencias de este tipo.

Una vez agotado el tema del software libre y del desarrollo comunitario de bitcoin podemos comenzar a hablar sobre las múltiples identidades de Satoshi Nakamoto. Han aparecido algunas personas que dicen ser él; ya sea es el caso de Dorian Satoshi Nakamoto nombrado por la revista Newsweek (McGrath Goodman, 2014) o el nombramiento de Craig Wright hecho por la revista digital Wired y Gizmodo. (Hern, 2015). Sin embargo al tener esta ambigüedad podemos no saber nunca quién es realmente Satoshi Nakamoto, pues podría ser una mujer, un hombre o un grupo de personas, quienes escribieron y publicaron el informe blanco.

Independiente del número de personas que aclamen ser Satoshi Nakamoto, que por ahora han sido dos

solamente, pero podríamos tener más a futuro, hay un hecho un poco tautológico y frágil para demostrar que alguien es Satoshi Nakamoto. Esto sería usando las primeras bitcoins iniciales que fueron creadas en la red, o usar la llave publica de Satoshi Nakamoto a modo de firma. Es un hecho a mi parecer tautológico, pues se demuestra dentro de la red que alguien tiene la llave del usuario, pero de ahí a garantizar que esto refleja la persona o entidad que escribió, pensó y desarrolló bitcoin en la realidad es un paso muy grande. Frágil pues las bitcoins que tendría Satoshi Nakamoto al momento de que todas las bitcoins fueran minadas es de 5%, y podría generar repercusiones importantes en la red al hacer algún tipo de movimiento o transacción (Bradbury, 2014).

Sin embargo, independientemente de quien sea Satoshi Nakamoto el informe blanco está basado en hechos y nociones de criptografía modernos, así como en nociones que se han demostrado funcionales dentro de la computación. Tema que ya se discutió a profundidad en el capítulo uno, o se puede ver la explicación técnica en el anexo.

Se dijo ya que se publicó la idea bitcoin en la lista de correos de *Metzdowd*, sin embargo, el informe blanco como tal está en una página web llamada Bitcoin.org, el enlace web es el siguiente https://bitcoin.org/bitcoin.pdf. Como se habrá podido imaginar el lector, hay también controversia sobre quién y cómo se registró el dominio de bitcoin.org, que es en donde está almacenado al público el artículo original. De acuerdo al foro BitcoinTalk, mismo del que ya se habló en el primer capítulo, la página en cuestión fue registrada por Satoshi Nakamoto usando un portal de correos anónimos https://www.anonymousspeech.com. (“How did Satoshi register bitcoin.org?,” 2016). La información del registro la dio el administrador del foro llamado Micheal con apodo de theymos, que tuvo contacto con Satoshi desde el 2010.

Como se dijo, Nakamoto es un personaje virtual y no sabemos quién es en la realidad, para terminar de hablar de él tenemos sus dos últimas publicaciones en la página de la Fundación de par-a-par que fueron en marzo y septiembre del 2014. En la publicación de marzo Satoshi publica que él no es Dorian Satoshi Nakamoto, que como ya se mencionó, era una persona que de acuerdo a Newsweek era el creador. (Posted by Satoshi Nakamoto on February 11 and Discussions, 2014a) La otra publicación, ocurrió el 8 de septiembre de 2014 a las 23:10, en donde alguien usando la cuenta de Satoshi, dice: “Querido Satoshi. Tu dox,[27]contraseñas y direcciones IP están siendo vendidas en la darknet. Aparentemente no configuraste bien Tor y tu IP se filtró una vez que usaste tu cuenta de correo

[27] Dox es el termino en inglés de distribuir públicamente la información privada y de contacto de alguien.

electrónico en el 2010. Tú no estás seguro. Necesitas salir de donde estás tan pronto como sea posible antes de que estas personas puedan dañarte. Gracias por inventar bitcoin." (Posted by Satoshi Nakamoto on February 11 and Discussions, 2014b)

La publicación del 8 de septiembre se confirma también con lo que se puede observar en otro hilo en el foro de BitcoinTalk, en donde Theymos, el administrador de dicho foro, del que se habló anteriormente, dice que recibió un correo de Satoshi confirmando que su cuenta fue comprometida. Theymos también advierte que cualquier correo a partir del 8 de septiembre debe de ser descartado y no debería de reconocerse como Nakamoto, del mismo modo es de los primeros en sugerir que alguien para comprobar la identidad de Satoshi así como para comprobar que es Nakamoto con el que estamos hablando debe de tener la firma digital con la que siempre ha firmado en sus correos. ("satoshin@gmx.com is compromised," 2016)

Es relevante incluir este dato pues marca lo que podríamos considerar un lapso de tiempo de vida digital de nuestro personaje/entidad en cuestión, por lo menos hasta que se demuestre lo contrario, y no regrese con algún tipo de actividad, ya sea la persona en físico, movimiento de sus monedas o un mensaje con su firma, o todas las anteriores. Tenemos entonces el 2008 como una fecha de "nacimiento" con la publicación del artículo en *Metzdowd*, y la defunción en el 2014.

Para hacer unos últimos comentarios y reflexiones sobre este personaje, tenemos que es uno de los pilares sobre los cuales está construido bitcoin. Paradójicamente es un pilar anónimo y el legado que dejó, no sólo es bitcoin, como la primer plataforma o moneda en línea sin ninguna institución central o gobierno con la capacidad de manejar miles de millones de dólares, sino que inspiró, directa o indirectamente, la creación de 1,278 Altcoins al 13 de Noviembre del 2017 (CoinMarketCap, 2017a). Al igual que, como ya se vio, la Block Chain o cadena de bloques ha llegado incluso a las instituciones privadas para mejorar algunos de sus procesos, e incluso al Grupo Banco Mundial (World Bank Group), que abrió una Solicitud de Información[28] a "personas o grupos que quieran participar en actividades prácticas para descubrir y explorar las posibilidades de la tecnología de libros mayores distribuidos o servicios de blockchain en el contexto de los retos mundiales más urgentes", que cierra en diciembre del 2017.

Como se puede ver en el anexo y tal vez un poco en el primer capítulo, es difícil explicar y entender en

[28] Request For Information en inglés, y consiste en un proceso empresarial en el cual se reúne información escrita de la capacidad de varios proveedores. Normalmente sigue un formato el cual es fácil hacer comparaciones. (Wikipedia, 2017a)

su totalidad el funcionamiento de bitcoin, a lo que agregamos que no se tiene a la persona o personas que tuvieron la idea inicial disponibles como figuras públicas, o para hacer consultas de a dónde se deba dirigir el proyecto, el por qué de cuestiones de su funcionamiento. Esto hace a la moneda no sólo más difícil de entender, también es parte del atractivo de bitcoin. Es decir, si nos hablan de una moneda descentralizada pero al comenzar a observar su historia viéramos a un personaje como Satoshi aún activo y siendo un miembro importante para la toma de decisiones de bitcoin tendríamos una clara contradicción, pues quien mejor que el mismo creador para decidir del futuro de bitcoin o de las decisiones importantes.

De manera similar el hecho de que el creador sea anónimo refuerza la idea de bitcoin como una moneda digital con la cual se puede lograr el anonimato. Por lo tanto tenemos dos incentivos como el anonimato y la descentralización que se ven reflejados desde el creador de bitcoin, aunque, como ya se vio, puede llegar a existir cierto grado de centralización, con los Fondos o Pools de mineros, y se tienen que tomar medidas específicas para que sea anónimo el uso de bitcoin.

Que exista poca información sobre el creador de bitcoin y que haya que buscarla en sitios específicos puede ser un hecho a favor para que las personas se unan a usar bitcoin y lo hagan con más facilidad. Paralelo a esto, si las principales noticias y la información que tenemos de bitcoin es su aumento de precio constante y no la noticia de que cada vez que sube de precio bitcoin, aumenta la riqueza o el valor de las personas que compraron o adquirieron bitcoin en sus inicios, o como en la jerga se les conoce como los “early adopters”, es decir pioneros, resulta mucho más atractivo como inversión. Es decir, es muy diferente que se nos diga que tienen un rendimiento y un aumento de valor muy bueno, a que nos digan que existen personas que adquirieron bitcoin en 11.04 dólares el 15 de noviembre del 2012 (coindesk, 2017b), es decir hace 5 años desde que se escriben estas líneas, las cuales están actualmente experimentando un aumento de aproximadamente 65,145 %.[29]

Específicamente si hablamos de Nakamoto se tiene un estimado que será el dueño de aproximadamente 5% de todas las bitcoins cuando éstas se terminen de minar y como se indicó en el primer capítulo en la explicación del *Bloque Génesis* y de las *Zonas de la Mina*, generar sus monedas le costó muy poco trabajo. Es decir no tuvo que usar super computadoras o procesadores específicos para la minería, sino que computadores de escritorio del 2009. Este es el caso más extremo en el cual no compró ni invirtió nada más que tiempo electricidad para generar bitcoins que ahora valen 7192 dólares. (coindesk,

[29] Al 15 de noviembre del 2017 tenemos un precio de 7192.07 dólares por un bitcoin

2017b)

Para finalizar de explicar este punto podemos observar una gráfica del precio de bitcoin desde sus inicios hasta el 13 de noviembre del 2017:

Gráfica 6: Datos obtenidos de (Blockchain Luxembourg S.A.R.L, 2017b)

Una vez viendo esto podemos observar como es que existe una diferencia significativa de los primeros años a los últimos años. Al 19 de julio del 2010 tenemos los siguientes precios de acuerdo a 3 páginas diferentes: XE.com estaba en 0.08181 dólares un bitcoin (XE.com, 2017a), en Coindesk a 0.08 (coindesk, 2017c) y por último Bitcoin.com en 0.08 (Bitcoin.com, 2017e). Por lo tanto si alguien hubiera comprado 1,000 dólares en bitcoin en ese momento tendría en promedio unas 80 bitcoins, que hoy en día equivalen a 793,361.6 dólares (XE.com, 2017b). Es verdad que bitcoin sube y está subiendo mucho de precio, al igual que ha tenido sus bajas de precios y crisis, sin embargo al ver esta gráfica y reflexionar sobre las monedas de Satoshi Nakamoto surge la pregunta de quiénes son los beneficiados principales al invertir o comprar o usar bitcoin. Dada la anonimidad de bitcoin y su creador, no sabemos a la inversión de quien estamos contribuyendo, a diferencia de un Banco o institución centralizada en la que se tiene un claro Presidente o Vice-Presidente y personas a las que “damos” nuestro dinero el comprar bitcoin o invertir en esta moneda.

Esto abre la discusión a qué es bitcoin o si se puede ver como un nuevo tipo de empresa o modelo de ganancia, la cual funciona como una casa de cambio pero mucho más rentable. Con esta reflexión es pertinente ahora abordar el tercer capítulo en el cual se habla de mi experiencia de trabajo de campo y se ve con más cercanía el uso y sus consecuencias.

Aventuras en el De Fe[30]:

Experiencias, usos y consecuencias de bitcoin

Al proponerme investigar sobre los usos de bitcoin me encontré en una situación en el trabajo de campo que pensaba no me iría a suceder. Se puede entender como una pequeña defensa a la etnografía digital y sucedió al buscar el uso físico de esta moneda. Se dice como crítica a la etnografía digital que tiene poco que ver con la etnografía clásica. Sin embargo, en mi caso me sentí como un antropólogo haciendo ese último tipo de etnografía. Buscando dentro de la Ciudad de México la afamada moneda en cuestión, tuve que ir a lugares que de acuerdo a un mapa ("coinmap.org, 2017), son establecimientos donde se acepta bitcoin, pero en muchos de los casos no existían esos lugares, habían cambiado de dueños o habían cerrado. Es de este modo que encuentro una similitud en el trabajo de campo clásico y mi experiencia en la realidad aquí presentada; para mí fue tomar un mapa virtual y explorar la Ciudad de México en busca de una moneda digital, que por momentos dudé que llegaría a encontrarla por el poco número de lugares en donde se acepta.

Tal vez no sea comparable mi situación a la de un antropólogo en busca de una sociedad perdida en la selva del Amazonas, pero por momentos me llegué a sentir de ese modo buscando en el "DeFe" (ahora Ciudad de México) una moneda que se usa en contados lugares, por lo menos en el intervalo de mi trabajo de campo. Es así que elaboro una pequeña defensa para la etnografía digital donde una experiencia de esta índole, me llevó, a mi modo de verlo, a buscar algo igual de efímero que un antropólogo en una tribu aislada, y al final de cuentas una experiencia etnográfica en la realidad. Llevándome a experiencias en concreto un tanto extrañas a mi realidad como se verá en unos párrafos.

Otro punto que ayuda para argumentar el acercamiento a la etnografía clásica es lo excluyente que fue la situación de intentar encontrar los lugares en donde se usaba esta moneda. Como ya se mencionó, mí mapa no fue del todo exacto para encontrar los lugares en donde podría haber un uso potencial, y en los establecimientos donde sí se maneja la divisa se creó un punto de contacto reducido para poder interactuar con mi meta-sujeto[31] de estudio. Teniendo de esta manera un trabajo de campo, que aunque

[30]Juego de palabras de la canción de Rockdrigo González llamada "Aventuras en el DeFe", en mi caso fueron aventuras en el De Fe pues como se verá fue difícil encontrar bitcoin en el ex Distrito Federal, ahora Ciudad de México

[31]Se usa la palabra de meta-sujeto de estudio simplemente para hacer una diferencia entre mis sujetos de estudio quienes son las personas que manejan bitcoin, del bitcoin como tal.

fue en Internet y en la Ciudad de México, así como en Acapulco Guerrero, hubo que hacerlo en lugares selectos que crearon a mi manera de verlo un aislamiento, o un lugar exclusivo al interactuar con bitcoin.

Profundizando en lo excluyente que puede ser la experiencia etnográfica, el investigar y hacer trabajo de campo en Internet entra bien en este apartado. Significa estar frente a un teclado, un ratón y una pantalla horas para hacernos una mejor idea de aquello que estamos investigando, ya sea con información cualitativa o cuantitativa estamos abstraídos de la realidad, conectados al Internet, interactuando, obteniendo y/o generando datos. Todo esto sin perder de vista que estamos frente a objetos inanimados, como lo es la computadora que, aunque tenga animaciones y un modo de interacción con el usuario en su pantalla, esto es sólo la representación de los mecanismos internos de la computadora y de su sistema operativo.

Comparativamente me parece ahora relevante profundizar un poco sobre lo digital y el peso que tiene la etnografía virtual, pues ya se ha hablado de la clásica. Como se mencionó anteriormente, bitcoin puede ser visto como un meta-sujeto de estudio, y si nos ponemos un poco creativos podemos decir que el lugar donde este meta-sujeto de estudio "habita" o "vive" es en Internet. Al entrar entonces a su hábitat natural y estudiar la divisa de este modo podemos ver que ahí se encuentra mucha información; desde datos de la red, el historial de sus precios, noticias sobre la moneda, la red, diferentes repercusiones en los diferentes países del mundo y la característica más importante, la cadena de bloques, que se encuentra distribuida y sincronizada gracias a Internet. Teniendo entonces cualitativa y cuantitativamente muchas características en el Internet, o su "hogar".

Ya se habló de la etnografía en sus dos ámbitos, considero ahora relevante dar información precisa de cuándo es que salí a tener estas experiencias. Esto es porque podría suceder que para el lector en el momento en que lee esta tesis, bitcoin tenga un incremento en los lugares donde se puede usar no sólo en lo virtual, sino que en la realidad, así como una diferencia de precio significativa. Para ejemplificar lo que quiero decir, al viernes 26 de Mayo del 2017 a las 5:42 pm el precio de una bitcoin se encuentra en 2,214.68 dólares (coindesk, 2017d) y el equivalente a pesos es de 41,635.98 ("Tipo de Cambio del Dólar y Divisas | Banamex.com," 2017) a diferencia de cuando compré mis primeras milésimas[32] de bitcoin en el cual el precio estaba en: 612.4 dólares (coindesk, 2017e), que equivalió en ese momento a 11,819.32 pesos (Banxico, 2017b), es decir que se ha multiplicado su valor casi cuatro veces, en un

[32] Es decir 1 dividido entre mil, es lo que conforma una milésima, en números: 0.001

lapso de unos cuantos meses octubre de 2016 a mayo de 2017.

Vamos acercándonos en forma al tema del capítulo, que es la aventura que viví en el ya extinto Distrito Federal con la fe de encontrarme con bitcoin. Sin embargo, antes de comenzar de lleno a hablar sobre ello, los usos y las consecuencias de los usos, quiero plantear una reflexión creativa relacionando bitcoin con la mitología grecorromana.

Esta reflexión nos sirve para entender la moneda de un modo no tan formal y pensar en ella de otra manera. El mito grecorromano que tengo en mente es el Rey Midas. Si vemos a bitcoin, entendido como un meta-sujeto de estudio como ya se ha venido planteando, y pensamos en él como Rey Midas, si recordamos que el deseo que Dionisio le cumplió a Midas fue que todo objeto que tocara se convertiría en oro, en este caso tenemos un Rey Midas contemporáneo extrañamente vivo en nuestra realidad. Verificando con fechas: al primero de Junio del 2017 el precio de una onza de oro está en 23,476.90 pesos (XE.com, 2017c) a diferencia del "oro" de nuestro Rey Midas que al "tocar" las monedas gubernamentales logra convertir un solo bitcoin en algo 1.9 veces más valioso que una onza de oro, es decir 45,365.33[33] pesos (coindesk, 2017f).

Es decir, bitcoin convierte a cualquier moneda fiduciaria en algo más valioso que el oro, y ha tenido históricamente una tendencia a la alta, es decir que no se ha devaluado, más que en algunos momentos y en espacios de tiempo breves. Si vemos toda su historia hasta ahora, ha tenido siempre un aumento de valor, aunque no se garantice que esto vaya a continuar, e incluso una de las advertencias al usar y empezar a usarla es que la moneda es altamente volátil y que no tiene ningún respaldo como tal. Dado como verdadero entonces que a bitcoin, Dionisio le concedió un deseo, y su deseo fue crear un sistema de par a par digital de efectivo, donde toda aquella moneda que toque se convierta en oro o en algo más valioso que el oro tenemos entonces que preguntarnos que pasará con el futuro de bitcoin, pues bien sabemos que le pasó al Rey Midas. Si bien estoy haciendo este ejercicio puramente para imaginar y ayudar a plantear cuestiones diversas de bitcoin, es también una manera interesante de acercarnos a pensar en las consecuencias de que tenga tanta popularidad y un uso cada vez más grande, al igual que es un modo de generar reflexiones introductorias para el capítulo en cuestión.

Para cerrar con el mito y la personificación de bitcoin como Rey Midas podemos vislumbrar dos salidas o maneras de resolver el mito. La primera es decir que así como el Rey Midas perdió esa

[33] En este caso estuvo en 2,452.18 dólares un bitcoin, y el precio del dólar en ese momento estaba en 18.5 de acuerdo a Banxico ("Mercado cambiario, tipo de cambio, Banco de México - 1 Junio,")

capacidad que lo hacía humano en ultima instancia, que era comer, obtener energía y vivir, pues toda la comida que tocaba también se convertía en oro, entonces nuestro meta-sujeto de estudio perderá su capacidad vital. La segunda manera de resolver esto es aquello que hizo el Rey Midas, que fue pedirle a Dionisio que lo regresara a la normalidad, éste accedió y le indico al Rey Midas bañarse en donde nace el río Pactolo en el monte Tmolo en lo que ahora es Turquía, regresándolo de ese modo a la normalidad. Éste hecho hizo que la arena del río tuviera una abundancia de oro. (THEOI, 2017)

Tenemos por lo tanto en la primera opción de bitcoin una situación en la que se perderá su "vitalidad", las comillas son porque no debemos olvidar que es un ente electrónico. Al obtener tanta importancia a nivel mundial y al tener un bitcoin un valor de casi el doble de una onza de oro, se puede dar una posible situación en la que bitcoin por su misma "avaricia" deje de ser aquello en lo que se fundó y nació. Por otro lado en la segunda opción, que es con la reflexión que me gustaría entrar al capítulo, nuestro meta-sujeto reconoce que su don en verdad se asemeja más a una maldición, termina por perder esa capacidad de convertir cualquier moneda fiduciaria en oro o algo más valioso tras bañarse en un río en lo que hoy es Turquía, después de pedir clemencia al Dios que le otorgó ese don. Pero aquello que nuestro meta-sujeto deja en el río en este caso no sería oro, sino que sería en mi opinión la cadena de bloques, blockchain en inglés. Es decir, la capacidad de convertir todo en oro o de más valor es en mi opinión la cadena de bloques, y es el verdadero oro de Midas que tiene bitcoin, en mi opinión.

Comenzando ahora con el capítulo podemos citar la conocida frase o pregunta clásica que le hacemos a nuestros profesores o maestros o a nosotros mismo en algún punto de nuestras vidas: ¿Y eso de que me sirve? Dentro de bitcoin es una pregunta relevante que intentaré aclarar en este capítulo. La pregunta la he escuchado mucho al explicar lo que es bitcoin en general; a familiares, personas cercanas o incluso desconocidos. Al explicar la utilidad de algo no estamos explicando directamente como se usa, pero al acercarnos al tema de este modo nos daremos una idea de sus diferentes usos, y respondiendo de manera un poco creativa a la pregunta anterior, puedo decir que de no ser por bitcoin no estaríamos leyendo esto ni tendríamos motivo de una investigación.

Siguiendo con la respuesta del párrafo anterior en mi caso, la utilidad que le he encontrado a bitcoin se ve reflejada en muchos diferentes aspectos. Desde los aspectos más personales de salir a lugares que no conozco y encontrarme en situaciones nuevas como lo fue un congreso en Acapulco de anarquistas, un nuevo modo de ahorrar y ver mi dinero crecer con el tiempo sin una institución bancaria, hasta pagar en un restaurante usando mi celular con la conexión de Internet en la red de bitcoin, es decir una red sin

institución central mantenida globalmente en pleno auge capitalista.

Adentrándome en las experiencias nuevas que me ha hecho vivir bitcoin tenemos mi primera compra de la moneda, así como mi primera experiencia formal en el trabajo de campo. Esta fue el lunes 3 de octubre del 2016, cuando decidí ir a un Cibercafé en Ixtapaluca después de salir de clases de la UAM Iztapalapa. La crónica es la siguiente:

Habiendo checado el mapa de cómo llegar y después de un largo trayecto llegué. El trayecto fue en automóvil y existen dos maneras de llegar, por la carretera "México-Pachuca" o la libre. Yo tenía la idea de que en verdad la carretera que tomé era México-Pachuca pero mi nerviosismo o prisa me hizo leer mal. Describiendo como había llegado con César Lemus, Ingeniero en Cómputo que es el dueño del ciber y quién me atendió, me di cuenta de mi error y que en verdad es la carretera México-Puebla.

Al llegar saludé, había una mujer barriendo el lugar y limpiando, misma que estuvo aseando el interior y el exterior del lugar durante toda mi estancia. Al pedir 50 pesos en bitcoin, después de una breve plática con César de como había encontrado el lugar y sobre una nota del periódico *Reforma* que hablaba sobre su Cibercafé, hubo un error en el sistema por la venta en cuestión, y tuve que esperar un poco más de la cuenta. La manera en la que me enteré del cibercafé de César fue en la nota del Reforma del 28 de Mayo del 2016 (Reforma, 2016), en donde mencionaban que se podía adquirir de forma similar a una recarga, y el precio al momento de la nota por bitcoin era de aproximadamente 610 dólares (coindesk, 2017d), que en pesos a ese momento eran aproximadamente 11,773 pesos (Banxico, 2017c). Gracias a la nota yo no era el único que había ido con Cesar, además de que varias personas lo habían contactado para obtener más información sobre como recibir o vender cosas en bitcoin.

Me ofreció una silla, pero antes de eso le comenté que era antropólogo social y estaba interesado en hacer una investigación sobre esta nueva moneda digital. Respondí esto ante la pregunta de César, de: ¿Y esto para que te sirve? Es decir, ¿en qué gastaría mis bitcoins? No supe darle una respuesta concreta, pues en ese momento no sabía donde era que podía gastarlas, por lo menos físicamente. La plática con César fue agradable e interrumpida por unas dos o tres llamadas con las cuales aclaró el problema de la venta, y para desgracia mía llegaron tres clientes al cibercafé a hacer impresiones, comprar un folder y cosas del diario, no para comprar bitcoin como yo.

Al momento en que me ofreció César la silla me dio también una hoja impresa con información que me pareció tenía ya preparada para la venta de bitcoin. La plática tomó más forma con esta hoja, pues había lugares y páginas en Internet en donde se puede comprar usándola. Hablando de gastarlas y hacer

un intercambio físico, César comentó de las únicas personas que conoce en México que la aceptan de ese modo es una empresa llamada Neubox que proporciona servidores y hospedaje de páginas web.

De ese modo fui comenzando a imaginar y darme una idea real del alcance de bitcoin en México por lo menos al 3 de octubre del 2016. Era un panorama no tan esperanzador, pero había algo ya tangible en donde indagar y lo más importante, estaba por recibir mis primeras unidades, aunque fueran milésimas de esta moneda (0.001 BTC). Como mencioné anteriormente, Cesar dijo que muchos negocios y personas lo habían contactado después de la nota del *Reforma*, para ver la posibilidad de recibirlas como método de pago, y proporcionar algún bien o servicio. No indagué en qué personas habían sido aquellas que lo contactaron, pero tenemos un punto muy relevante al hablar del uso y de la investigación.

A lo largo de toda mi investigación yo he "comprado" o "cambiado" de pesos mexicanos a bitcoin, pero no logré recibir bitcoin a cambio de algún bien o servicio que yo he proporcionado. Este es otro método de obtener y por desgracia no fue abordado en la investigación, en el sentido de que no intenté vender nada en bitcoin, pero espero esclarecer el tema y mi opinión al respecto a continuación.

El recibir directamente lo que se hace es ver el tipo de cambio al momento de la venta, si nos ponemos en los zapatos de la persona que está vendiendo algo, hacemos la conversión y cobramos directamente nuestro bien y/o servicio para recibir bitcoin. En la investigación llegué a hacer simplemente la transferencia a personas interesadas en usarlas o tenerlas, y por cantidades modestas, sin embargo no efectué nunca una venta o servicio de algún bien. Una vez entendido esto podemos profundizar en los beneficios de recibir bitcoin de este modo por parte de las personas que contactaron a César.

La nota del *Reforma* menciona solamente que bitcoin permite realizar compras en línea y es una forma de ahorro. Si tomamos en cuenta que las personas no sabían mucho más de la moneda y solamente estaban interesados en los beneficios de los que la nota del *Reforma* hablaba, se muestra un interés por parte de las personas de un modo de ahorro alternativo al de los pesos y obviamente en un interés por tener liquidez virtual, si le podemos llamar así, o simplemente de poder ganar en bitcoin y gastarlo en línea.

Esto es viendo las conclusiones más obvias y directas, pero haciendo una búsqueda con la ayuda de Google con la pregunta "¿Qué es bitcoin?", e introduciendo un intervalo de tiempo correspondiente a la nota del *Reforma* del 28 de mayo del 2016 y como límite el 28 de agosto del 2016 (Google, 2017) podemos observar que existe suficiente información indicando su funcionamiento básico así como los

beneficios económicos de usar esta moneda, como puede ser cero cobro de comisiones, poder cambiarlo a cualquier divisa en el mundo, gratis para empezar a usarlo; las carteras o wallets son gratis de usar y descargar, el que no tenga una institución central implica que nadie puede congelar tu cuenta, bajas comisiones por hacer un movimiento en la red, entre otros beneficios. (BTC Fácil, 2016) Coincidentemente, no se menciona con precisión en los videos y en los resultados de la búsqueda una aplicación o cartera para empezar a usarlos y su obtención tampoco queda clara. Indicándonos posiblemente el interés de recibirlos directamente por parte de las personas que contactaron a César, en lugar de ellos invertir o comprarlas en algún lugar.

Regresando a la crónica tenemos que en la hoja que me entregó César, venía la información relevante y enlaces de Internet sobre bitcoin. Desde el costo de una, el costo mínimo de compra, el monto máximo de compra diaria, cada cuánto se puede comprar, dónde se puede comprar e incluso una invitación para venderla en la localidad de uno si es que cuenta con un negocio. Aquí estamos tocando otro punto importante relacionado al uso, y es la manera en la que se refieren a las transacciones de bitcoin. Yo en lo personal lo veo como un cambio de divisa, pero en la hoja que me entregó César, así como en la entrevista y la plática que tuve con él, un binomio de palabras fue recurrente; vender y comprar.

Es así que podemos decir que para César y la empresa que habilitó a César para vender bitcoin vemos una inclinación para ver bitcoin como un producto o algo similar. Concretamente en la entrevista con él, menciona que es un distribuidor, no obstante también menciona y entiende que es una moneda, que tiene un valor y puede servir como tal. Si vemos un pequeño fragmento de la entrevista esto se podrá aclarar:

Rodrigo: ¿Bueno cuál sería o cuál fue tu experiencia comprando bitcoins? O ¿Ya has comprado o intentado comprar?

Cesar: Pues yo he intentado mas bien investigar como se compran, yo los vendo pero realmente nunca lo he comprado, sé cómo se maneja, pues la compra de los bitcoins y a (una) transacción, ¿no? Bueno en el caso de nosotros a diferencia de todos en el mundo, lo manejamos como una transacción directa a un número celular. Y en los otros es como cotizar la bolsa de valores, ver en cuanto está el precio del bitcoin y posteriormente transferirlo a lo que se le llama un wallet, que es como el monedero electrónico, aquí no. Tú llegas a cualquier tienda, y como si hicieras una recarga a un teléfono compras el saldo, e inmediatamente lo transfieres al wallet. No es necesario ver en cuanto está, ni cómo lo vas a

> transferir, ni cómo lo vas a transformar, es decir, cuánto equivale, no sé, 100 pesos en bitcoin ¿no? Inmediatamente la máquina te hace esa conversión sin necesidad de que tú lo hagas.

No indagué en la manera interna en la que opera César para enviar bitcoins, pero después de investigar un poco y al ver la plataforma que usé puedo inferir y esbozar la manera en la que opera. La aplicación de interfaz con el usuario es MaxSaldo, aplicación que le pertenece al grupo Mexicano Zmart, mismo que en el 2013 tuvo un crecimiento del doble del año anterior, con un millón de operaciones mensuales, 16,000 puntos de venta con un crecimiento mensual de 1,000 a 1,200 (memonius, 2014). Sin embargo es gracias a la unión que hicieron Zmart y Bitso, anunciada el 17 de mayo del 2016 en el blog oficial de Bitso, que me fue posible adquirir mis primeras milésimas con César. En esta fecha en que se anunció la integración de Bitso en la aplicación de MaxSaldo para la venta de bitcoins, el número de localidades de venta se declaró alrededor de las 29,000 en el 2016 (Forbes, 2016). Como se verá en el apartado de Las Casas de Cambio estas fechas fueron muy importantes para Bitso pues se expandió con Zmart al igual que Unisend y en abril del 2016 logró recaudar 45 millones de pesos, en el portal de Bank To The Future.(Bitso, 2017)

Una vez planteado todo esto podemos observar cómo entonces Bitso adquirió una gran potencialidad de clientes gracias a su alianza con Zmart, dándole al exchange más liquidez y capacidad de cambio, al igual que un obvio incremento de usuarios. Al momento en que hice mis compras con César, no era consciente de que Bitso estaba detrás de la transacción, este hecho fue algo importante de descubrir, pues César tampoco sabía de su existencia o influencia en la transacción. De tal modo que lo que se hace es usar la plataforma de MaxSaldo, como si fuera una recarga o un servicio usual de MaxSaldo, pero en este caso es un servicio nuevo o extra implementado por Bitso. Es por esto que César menciona una preocupación por investigar cómo se compran, y también ve las monedas como algo que él distribuye, pero no ha tenido la oportunidad de comprarlas o tenerlas como tal, pues es una adición a los servicios de la plataforma de MaxSaldo. Es decir no se tiene ninguna apropiación directa de aquello que está vendiendo; es verdad que es un activo digital, pero es una diferencia notable tener el control de él al venderlo y solamente tratarlo como una recarga más. Es así que podemos decir, como menciona Pablo Gonzalez, CEO de Bitso, en una entrevista en las Conferencias Internacionales de Transferencia de Dinero y Pagos (IMTC en inglés), que bitcoin fue *algo invisible* para César y para mí: “Lo que nosotros estamos haciendo para darle más confianza al consumidor ahorita, es que estamos haciendo a

bitcoin invisible.” (Youtube, 2015)

La compra de bitcoins entonces, volviendo de nuevo a la crónica, con mis 50 pesos iniciales, sucedió después de un par de llamadas que hizo con lo que me pareció eran las personas de sistemas de MaxSaldo, o incluso de Bitso, para aclarar el proceso de venta de bitcoin. Como podemos ver en el fragmento de entrevista con Cesar, el sistema hace todo automático para facilitar la venta, uno proporciona su número celular y el monto que quiere recibir, paga la cantidad acordada, y en unos minutos, en mi caso fueron más de unos, llega un SMS con una dirección de una página de Internet. Es importante aclarar que en este momento aún no había recibido mis milésimas de bitcoin, solamente había recibido el enlace a una página en donde más tarde podría “cobrar” o recibirlas. Tal vez un ejemplo comparable para que se entienda la transacción que intento describir es un cheque. Llego, pago a César 50 pesos, el emite un “cheque” al portador, mi número celular, y yo más tarde lo “cobro”.

El cobrar el cheque en este ejemplo sería entonces abrir la página que recibí por SMS e introducir la dirección a dónde quiero recibir mis diezmilésimas de bitcoin. La dirección es una generada por la wallet o cartera. En este caso específico al terminar el día y regresar de LEMUSOFT desde Ixtapaluca, generé mi dirección en una cartera que tengo dentro de una computadora fija en mi casa, y recibí exitosamente mis primeras bitcoins. A continuación dos imágenes del trámite en cuestión:

Imagen 4: Imagen que ilustra el primer paso para recibir BTC

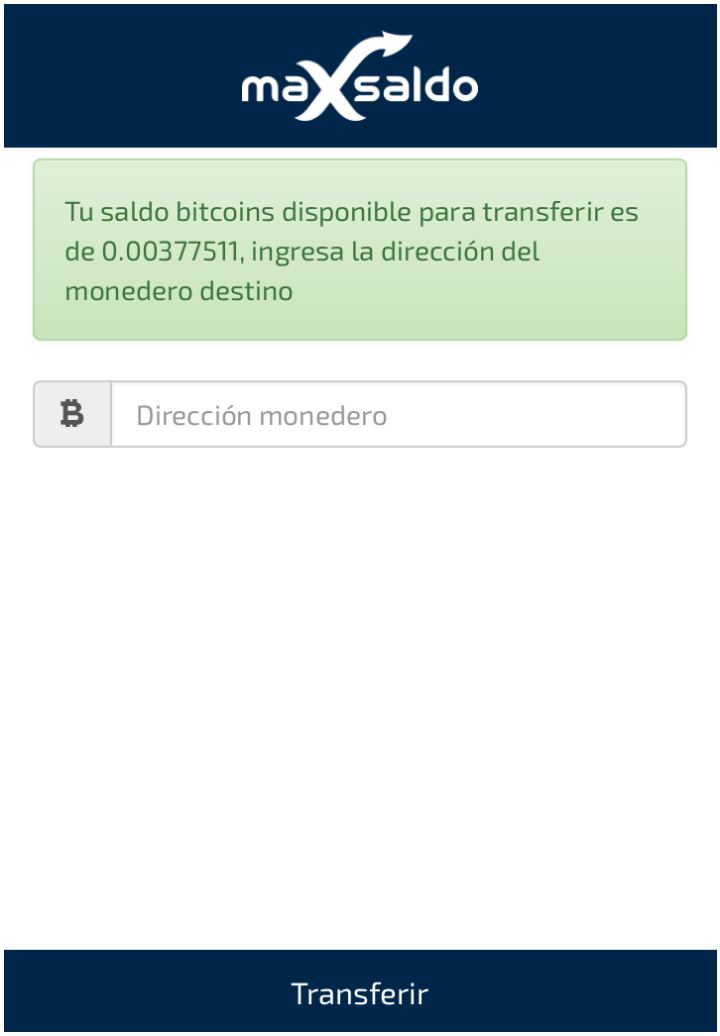


Imagen 3:Imagen que ilustra el segundo paso donde debemos introducir nuestra dirección.

Como se puede observar en la primera imagen, son requeridos tres campos, que siguiendo con la analogía del cheque se pueden entender teléfono, transacción y token como: el beneficiario, lugar y fecha de emisión y número de cheque, respectivamente. La segunda imagen sería cuando ya se verificó con el banco el cheque y procedemos a cobrarlo finalmente, hablando en términos de bitcoin es cuando generamos una dirección con nuestra cartera, y se nos transfieren los fondos. Es en este momento que recibí mis primeras milésimas de bitcoin; para ser exactos: 0.00377511 a las 6:11 PM de la Ciudad de México, que de acuerdo a mis cálculos[34] aproximadamente fueron 44.5 Pesos mexicanos, lo que nos indica que entre MaxSaldo y Bitso se quedan con un 11% aproximado de la venta de mis 50 pesos por el tipo de cambio. Dato que se podrá corroborar con las demás compras que hice de bitcoin con César.

Cuando se habló de la búsqueda en retrospectiva en Google, para observar los resultados a la pregunta de: ¿Qué es bitcoin? en el intervalo de mayo del 2016 a agosto del mismo año, se dijo que no había un cobro de comisiones. Como se vio ya en el capítulo de la explicación de bitcoin, existen comisiones que los mismos mineros cobran, como incentivo para el minado. Sin embargo esta es la única comisión cobrada internamente, y por desgracia como podemos observar, existen servicios ofrecidos por Casas de Cambio o vendedores independientes como Cesar, que cuentan con el respaldo de una empresa, quienes cobran una comisión también. Por lo tanto aquí se pone en tela de juicio la afirmación que se tiene, como un punto de venta de bitcoin, en el que se dice que no se cobran comisiones. La afirmación correcta en este caso sería, un cobro muy bajo de comisiones al usarla sin intermediarios, al usarla con intermediarios tenemos un cobro por el servicio que nos proporcionan con comisiones de hasta 11% como mi caso. Sin embargo si comparamos las comisiones que se cobran en las instituciones centrales, como los bancos, tenemos una clara diferencia, pero esto no borra el hecho de que por el uso de bitcoin exista una comisión.

Si hacemos una división, de la comisión que reciben los mineros (Blockchain Luxembourg S.A.R.L, 2017c) entre el número de transacciones confirmadas por día (Blockchain Luxembourg S.A.R.L, 2017d), obtenemos una estimación de cuánto reciben por confirmar una transacción. Después de obtener ese resultado, si calculamos esto mismo para todos los días que se tienen registrados y seguido de ello promediamos todos los resultados, llegamos a la cifra de 0.0005 bitcoins[35]. Por ende históricamente tenemos un promedio, del estimado de la comisión que reciben los mineros, en 0.0005

[34] El precio de bitcoin al 3 de Ocutbre del 2016 de 23:10 – 23:11 fue de 610.29 dólares (coindesk, 2017e) y el precio del dólar en pesos fue de 19.3 (Banxico, 2017b) es por esto que nos da 44.5 pesos 0.00377511 bitcoins.
[35] Lo que serían 66 pesos de acuerdo a XE.com, al 6 de noviembre del 2017 (XE.com, 2017d)

bitcoins por cada transacción procesada, en el lapso del 3 de enero del 2009 al 4 de junio del 2017. Concretamente en mi compra de bitcoins anteriormente mencionada la comisión fue de 0.0003 bitcoins que equivalía en pesos al tipo de cambio del 3 de Octubre a 3.5 pesos[36].

Este sería el análisis de las comisiones internas que tiene bitcoin, sin embargo hablando de las comisiones externas podemos ver como se divide ese 11% que ya se mencionó. El modelo bajo el cual MaxSaldo opera es aquel de un intermediario financiero el que obtiene comisiones o ganancias por hacer o procesar transacciones, con bonos por el uso de sus servicios y un porcentaje de comisión de las ganancias de las personas a las que uno invita a usar la aplicación. (MaxSaldo, 2017) Por lo tanto, gracias a mi compra de 50 pesos a César le abonaron en la aplicación de MaxSaldo, 7% de mis 50 pesos que son 3 pesos con 50, mientras que MaxSaldo y Bitso obtuvieron 5 pesos con 50 centavos de mi compra. Por lo tanto, podríamos considerar una ganancia neta por parte de MaxSaldo y Bitso de 2 pesos que representa el 4% de mis 50 pesos después de restar el saldo abonado a César por su "recarga" de bitcoin. piramidal

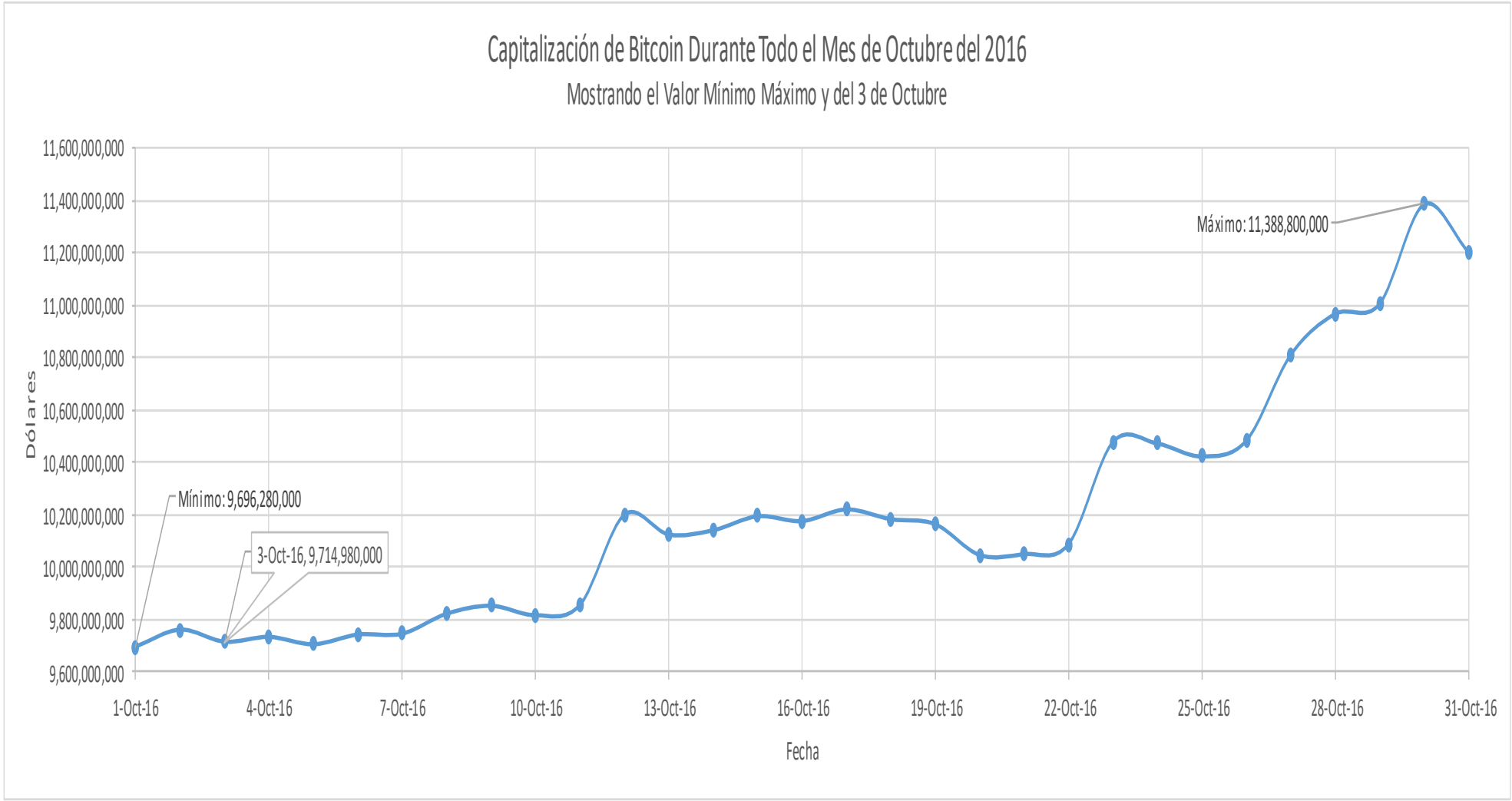
Un punto para la reflexión de lo que se acaba de comentar anteriormente es que, lo que se abona a César es saldo para la aplicación. No podemos olvidar que este es un bono dentro de la aplicación, y representa dinero a favor pero la aplicación no permite extraer ese saldo a manera de efectivo. En tal caso podemos entonces decir que el 11% de la comisión cobrada por MaxSaldo y Bitso es recibida por ellos, mientras que el sistema de bonos por invitación y uso de sus servicios sirve para, no solo incentivar a las personas a buscar conocidos o invitar a más gente a usar la aplicación, pero también para poder solventar el bono que reciben como tal, pues cada persona que yo invito a usar MaxSaldo gana también 7% de cada venta o servicio pero yo gano 10% de lo que ellos ganan.

Un último apunte sobre la crónica de mi primera experiencia de trabajo de campo es sobre las demás personas que habían ido a comprar bitcoin con Cesar a LEMUSOFT. Pregunté si era yo el primero o si habían venido más personas a visitarlo para comprar bitcoins, a lo que respondió César que solamente había venido una persona más antes de mí. No me dio muchos más detalles, pero la información como tal cuenta mucho pues tenemos un primer indicador que en un mínimo de 6 meses después de la nota en el *Reforma* no han ido más de dos personas por bitcoins con César.

Para complejizar más la situación, en la cual tenemos muy poco uso presencial y un uso virtual en

[36] El precio de bitcoin al 3 de Ocutbre del 2016 de 23:10 – 23:11 fue de 610.29 dólares (coindesk, 2017e) y el precio del dólar en pesos fue de 19.3 (Banxico, 2017b) lo que nos da 3.5 pesos.

donde se llegan a hacer transacciones cuyos totales llegan a millones de dólares, considero relevante agregar cuatro gráficas en total, que muestran información que nos ayuda a ver la situación que se acaba de plantear. Son gráficas de Octubre del 2016, que muestran el volumen de intercambio de Bitso y de 100 exchanges diferentes a lo largo del mundo, al igual que su capitalización.



Gráfica 7: Datos obtenidos de (“Bitcoin (BTC) historical data | CoinMarketCap - octubre 2016,”)

Como podemos ver en la primera gráfica; el máximo valor de capitalización de los bitcoins es 11,388,800,000 de dólares y ocurre el 30 de octubre, del mismo modo el mínimo que ocurre el primero de octubre es de 9,696,280,000 dólares. En particular, si restamos estos números, podemos ver una diferencia aproximada de 1,700 millones de dólares[37] lo que nos da una clara idea de la volatilidad de la red, característica que ya se mencionó anteriormente, y de lo rápido que puede cambiar el precio dentro de un plazo de 30 días; en promedio tenemos un incremento de 56 millones de dólares diarios en el valor de las bitcoins.

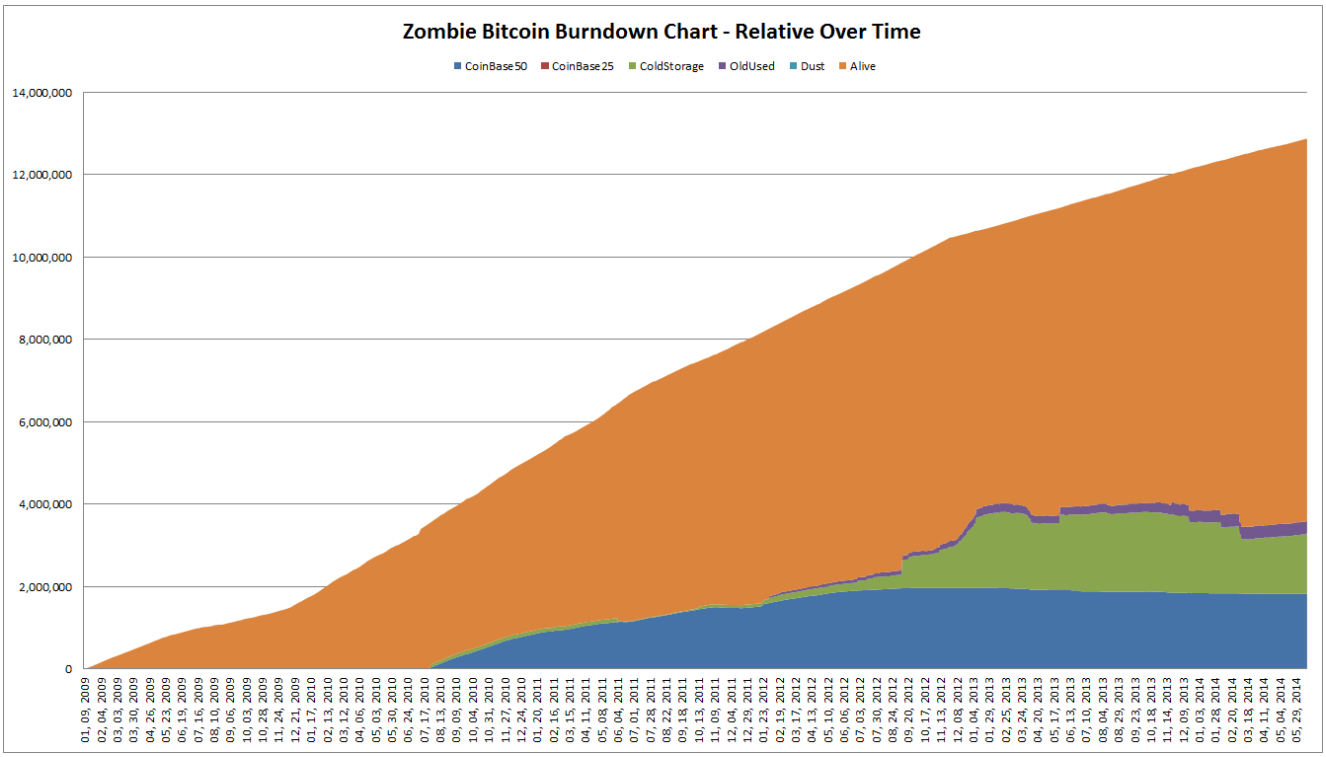
Sin embargo, esta cifra puede ser cuestionada pues es una simple multiplicación del número de monedas en *circulación* por el precio al momento ("CoinMarketCap FAQ,"). He incluido las cursivas pues existe la posibilidad de que no todas las monedas en la red puedan circular. Me ayudo para declarar esto gracias a un meta-análisis que John W. Ratcliff hizo el 22 de junio del 2014 (Ratcliff, 2014) de la cadena de bloques, nuestro libro mayor Público. El hizo su análisis con el fin de comprender que monedas estén probablemente fuera de circulación y sirvan como base, sustento o estabilidad para bitcoin, o visto de otro modo la potencialidad que estas monedas tienen para causar alteraciones o rupturas en el dado caso que exista algún movimiento de ellas.

En el 2014 entonces, de acuerdo a Ratcliff el 30% de todas las bitcoins en existencia eran "monedas zombi"[38], de las cuales 10% pertenecían en ese entonces a Satoshi Nakamoto. Como menciona el autor, entre más suba el precio es más difícil que las personas no muevan ni toquen sus monedas, concluyendo que si hay posibles movimientos son por cuestiones de seguridad son para: transferirlas a una cartera más segura, para hacer alguna compra o simplemente para verificar que su PIN privado, sigue funcional. De este modo analiza y vigila aquellas direcciones que experimentaron este tipo de ganancia, dependiendo si han efectuado algún movimiento no para descartar de ese modo las que están completamente "muertas" a las monedas que todavía tienen dueño y su dueño puede controlar dichas monedas. Escogió año y medio pues las personas que adquirieron bitcoin anterior a esta fecha, del 2009 al 2012, adquirieron bitcoin a un costo promedio de 3.66 dólares.

Es así que Ratcliff nos proporciona con la siguiente gráfica:

[37]La diferencia exacta es de: 1,692,520,000 dólares

[38] A lo que se refiere Ratcliff con monedas zombie son: todas las bitcoins asociadas con una dirección pública, PIN público, que no han enviado ninguna transacción por más de año y medio. Escogió año y medio pues las personas que adquirieron bitcoin anterior a esta fecha, considerando el 2014 como base, adquirieron bitcoin a un costo promedio de menos de un dólar.



Gráfica 8: Imagen obtenida de (Ratcliff, 2014)

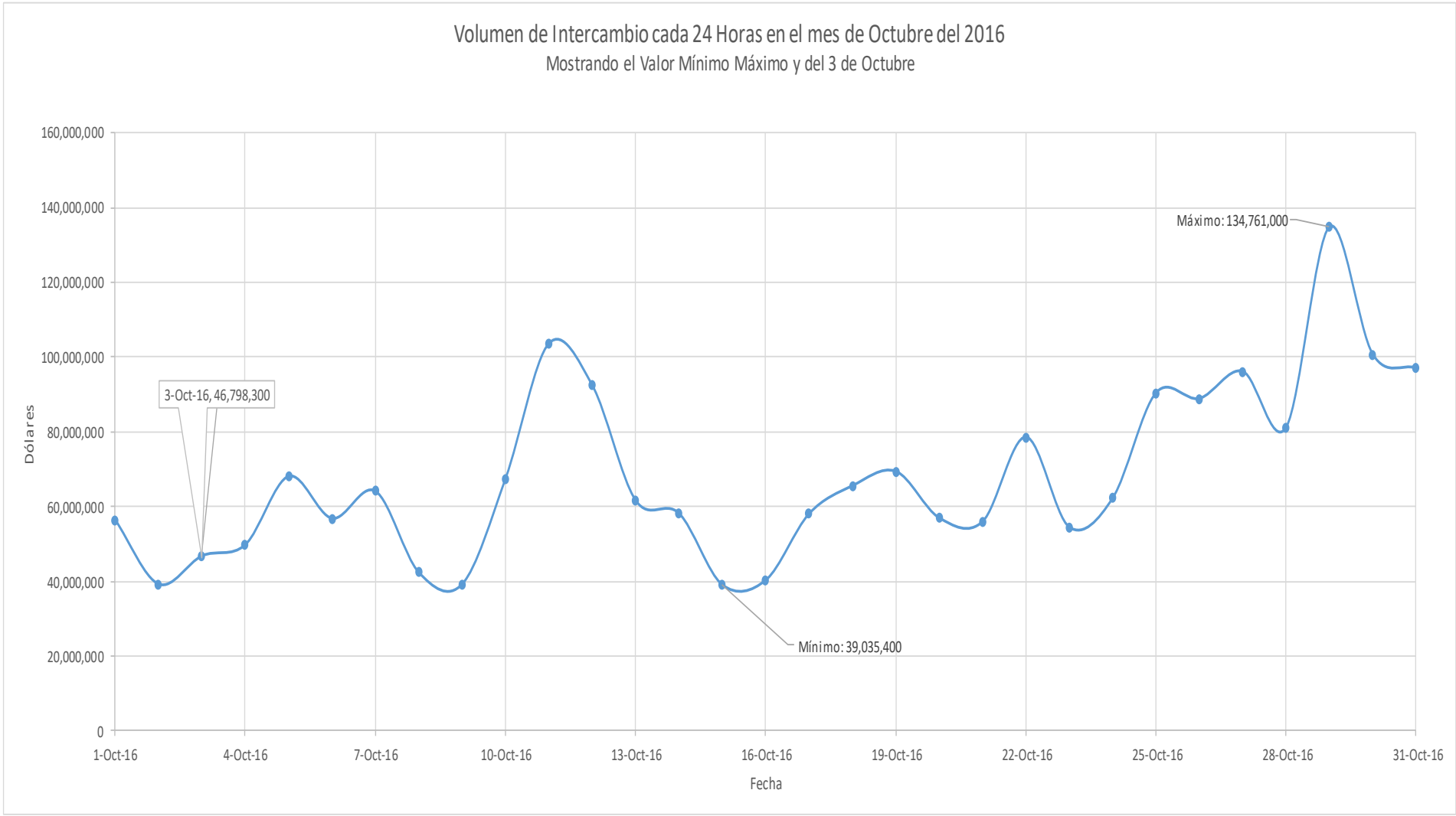
Para entender la siguiente gráfica es necesario explicar la llave de colores: CoinBase50 son las direcciones que recibieron la recompensa de la *Zona* 1 de la mina, la porción azul inferior de la gráfica y el grupo más propenso a ser "monedas zombi", es aquí donde se encuentran las monedas de Satoshi Nakamoto. CoinBase25 es demasiado pequeño para ser observado, esta es la *Zona* 2, y es difícil ver las direcciones que tienen estas monedas pues la gran mayoría fueron redistribuidas y pocas fueron las direcciones que no hicieron ningún movimiento. ColdStorage son las direcciones que no están relacionadas con ninguna *Zona* de la "mina", son direcciones que han recibido bitcoin pero no han gastado ninguna, no han hecho ningún envió por más de año y medio, y son probablemente carteras físicas. OldUsed son direcciones que han recibido y enviado bitcoin, sin embargo se encuentran inactivas por más de año y medio. Dust son las direcciones que contienen menos de 0.001 bitcoin que aunque existan millones de este tipo de direcciones, en total no agregan valor alguno como para ser registradas en la gráfica. Alive son las direcciones que han hecho transacciones dentro de un año y medio. (Ratcliff, 2014)

Por desgracia el código que implemento Ratcliff no está actualizado para analizar la cadena de bloques del 2017, esto por una cuestión técnica del tamaño de los bloques. Sin embargo esto nos da una idea de

cómo acercarnos a las cifras de bitcoin de una manera más crítica, de igual manera si personas que experimentaron una ganancia de un promedio de 3.5 dólares a 600, y como dice Ratcliff no han hecho movimiento, puede ser por que esperan todavía más ganancias, no son conscientes que son dueños de dichas monedas o el caso negativo es la perdida de su PIN privado.

Regresando al 2017 y con esto en mente, si vemos cifras más recientes podemos ver la capitalización al 22 de junio, es decir al momento en que se escriben estas líneas, tenemos que es de 44,352 mdd[39] o casi 4 veces más que en octubre del 2016. ("Bitcoin (BTC) price, charts, market cap, and other metrics | CryptoCurrency Market Capitalizations,") Este número nos puede dar una cierta idea del potencial que tiene, así como una idea general de la riqueza de la red, entendida en términos de una capitalización similar a la que se hace en el mercado de valores. Retomando brevemente lo que se dijo en la introducción del capítulo si observamos a nuestro Rey Midas y vemos que lugar toma en la lista de Forbes de personas más ricas del mundo, entonces ocupa el número 11 de la lista, con sus 44,352 mdd. ("Éstos son los 20 billionaires más ricos del mundo en 2017," 2017)

[39]Millones de dólares

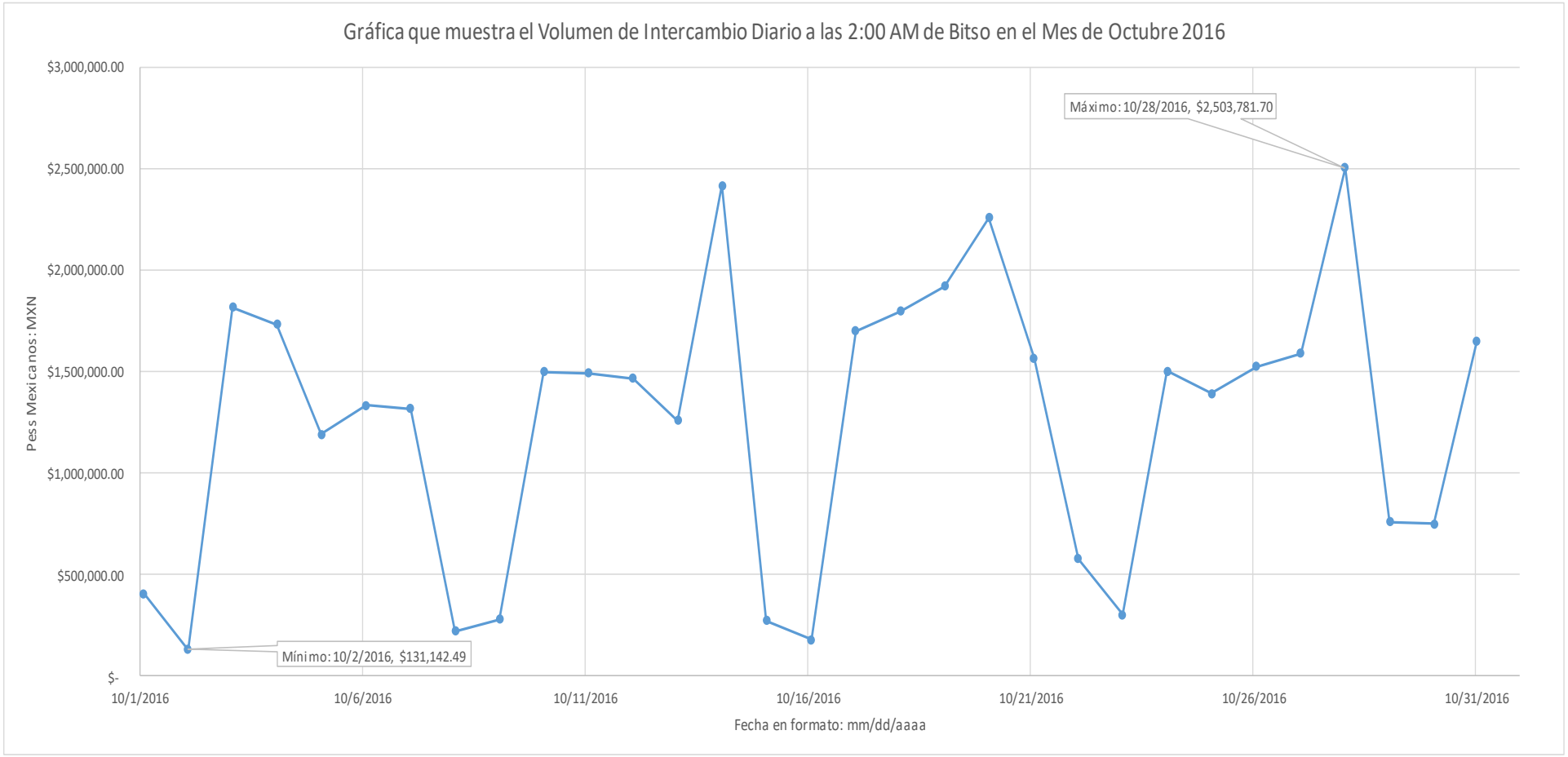


Gráfica 9: Datos obtenidos de ("Bitcoin (BTC) historical data | CoinMarketCap - octubre 2016,")

Analizando la segunda gráfica y dejando de lado las comparaciones mitológicas tenemos el *volumen de 24 horas de transacciones*, "*24h Vol*", misma que es mucho más relevante para nuestro análisis y lo que se quiere reflexionar en relación a la disparidad que observamos entre los usos de bitcoin. Antes de profundizar en la reflexión es pertinente explicar algunas definiciones; lo que significa por *volumen de transacciones*, es el valor total de todas las bitcoins que fueron compradas o vendidas en un periodo de 24 horas. Los datos son recolectados de diversos exchanges; recordando brevemente, los exchanges son páginas web o aplicaciones digitales en las cuales se intercambia bitcoin por cualquier otra divisa, y en ocasiones no sólo se intercambia bitcoin, sino que se intercambia más de una criptomoneda o más de una divisa. Bitso es el principal exchange Mexicano que ocupa el lugar 122 de 400 en el volumen diario de bitcoin con 1,280,320 dólares[40] y colaborando con 0.11% del volumen total de transacciones diarias al 22 de junio del 2017 (CoinMarketCap, 2017b)

Veamos de nuevo la segunda gráfica, al 3 de octubre del 2016 tenemos un volumen diario total de 46,798,300 dólares, que equivale a 904,194,634.13[41] pesos, cifra que casi llega a mil millones de pesos. No podemos olvidar que esta cifra considera las transacciones presenciales y virtuales que se hacen a través de exchanges, y se obtiene de todos los movimientos y transacciones de 100 de ellos[42] a lo largo de todo el mundo. Estas "Casas de Cambio", se ubican desde Estados Unidos de América, Gran Bretaña, China, India, Seychelles, Singapur, Polonia hasta Rusia, es decir en todo el mundo. Sin embargo, es relevante ver la gráfica número nueve en donde tenemos el volumen de intercambio de todo octubre para Bitso, pues es el caso específico a México.

[40] 23,173,792 de pesos con el dólar a 18.1 de acuerdo a Banxico ("Mercado cambiario, tipo de cambio, Banco de México,")
[41] El precio del dólar en pesos el 3 de octubre fue de: 19.3211
[42] Al 22 de junio se tenían en consideración 400 exchanges diferentes como ya se mencionó, sin embargo el número de exchanges no es constante y ha venido de menos a más cómo se verá, de octubre del 2016 a junio del 2017.



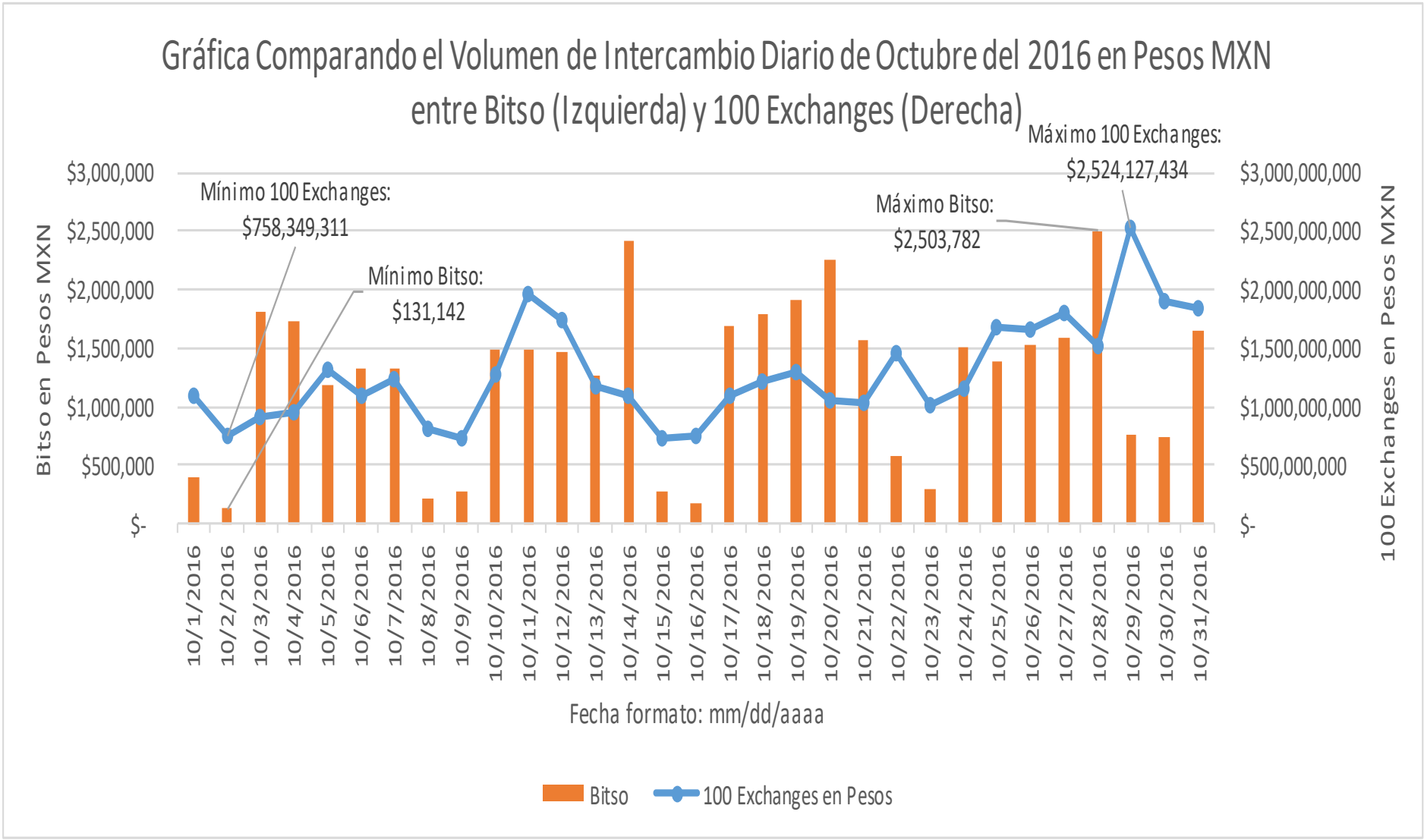
Gráfica 10: Información obtenida de: (Bitcoinity, 2017)

Una vez dicho esto podemos ver la tercera gráfica con otros ojos; al poder comparar la gráfica 2 con la gráfica 3, tenemos una comparación directa del principal exchange mexicano en contra de la suma de exchanges mencionados antes. También nos permite observar el carácter mundial o internacional de bitcoin, pues se dice que es Global, pero una de las maneras de ver esto es viendo la tendencia en México y observar qué tanto se asemeja a la tendencia mundial y poder ver una posible conexión entre ambas gráficas.

Un punto necesario de aclarar es que puede haber personas alrededor de todo el mundo con cuentas dentro de Bitso, haciendo inversiones y uso de la aplicación fuera de México; pero como menciona Pablo González hablando de las Remesas "las cuales son prácticamente nuestra misión principal en Bitso" en una entrevista en Coin Summit[43] (Money & Tech, 2014), y Daniel Vogel, presidente de dicho exchange, en otra entrevista: "mucha gente utiliza bitcoin en México como su primera manera para hacer inversiones" (Bitso, 2016) podemos ver una tendencia en sus usuarios. Es así que podemos concluir: la mayoría de sus usuarios representan de manera general a México y a su población, pues se reciben las remesas en México, al igual que tienen un número amplio de usuarios para invertir su dinero. De ese modo, aunque la gráfica 3 no representa en su totalidad la actividad en México, son las cifras que más se acercan a la realidad mexicana.

Si comparamos entonces las dos gráficas en cuestión tenemos que en efecto es visible hasta cierto punto una tendencia que corresponde con el resto de los exchanges alrededor del mundo. Si observamos los mínimos o las bajas tenemos una similitud en los 100 exchanges y en Bitso, como por ejemplo en los días 2, 8, 10 y 23 de octubre. Observando los máximos tenemos que ocurren con una diferencia de días entre ambos, ejemplificando: el 10 de octubre tenemos un máximo en los 100 exchanges que ocurre en Bitso el 14, a diferencia del segundo máximo que ocurre el 28 para Bitso y el 29 para los 100 exchanges. Con fines de ilustrar lo que se ha dicho he incluido una gráfica en la que se pueden observar ambos datos, pero es importante no perder de vista que en una escala tenemos miles de millones de pesos y en otra escala solamente millones de pesos.

[43] Una conferencia en Londres de dos días en la cual se conectan emprendedores de bitcoin con inversores, al igual que hay pláticas de directores de empresas que usan bitcoin y de Informática.



Gráfica 11: Información obtenida de (Bitcoinity, 2017)

Tabla que muestra el porcentaje que ocupa Bitso en el volumen de intercambio diario en octubre 2016										
Día de octubre 2016	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
Bitso (%)	0.04	0.02	0.20	0.18	0.09	0.12	0.11	0.03	0.04	0.12
100 Exchanges (%)	99.96	99.98	99.80	99.82	99.91	99.88	99.89	99.97	99.96	99.88
Día de octubre 2016	***11***	***12***	***13***	***14***	***15***	***16***	***17***	***18***	***19***	***20***
Bitso (%)	0.08	0.08	0.11	0.22	0.04	0.02	0.16	0.15	0.15	0.21
100 Exchanges (%)	99.92	99.92	99.89	99.78	99.96	99.98	99.84	99.85	99.85	99.79
Día de octubre 2016	***21***	***22***	***23***	***24***	***25***	***26***	***27***	***28***	***29***	***30***
Bitso (%)	0.15	0.04	0.03	0.13	0.08	0.09	0.09	0.16	0.03	0.04
100 Exchanges (%)	99.85	99.96	99.97	99.87	99.92	99.91	99.91	99.84	99.97	99.96
Día de octubre 2016	***31***									
Bitso (%)	0.09		Promedio Bitso		0.10					
100 Exchanges (%)	99.91									

Tabla 3: Información obtenida de (Bitcoinity, 2017)

Como podemos observar existe una tendencia en el mercado en la cual México sigue en sus máximos y mínimos a los demás exchanges, pero si observamos la tabla anterior tenemos información contrastante en la cual vemos la poca colaboración que México tiene al mercado mundial. He subrayado en rojo la colaboración mínima y en verde la máxima, estas son, 0.02% y 0.22% respectivamente. Es decir la colaboración máxima de Bitso comparada con el mercado global fue de 0.22. He incluido también el promedio que es de una décima, 0.1, lo cual nos habla de que no hubo una gran incidencia en octubre del 2016 en el resto del mundo. Como último punto tenemos una coincidencia en ambos mínimos el 2 de Octubre la incidencia de Bitso fue mínima al igual que hubo un mínimo el volumen de intercambio diario.

Regresando al punto inicial de la discusión tenemos que se tienen en México un número reducido de transacciones físicas y como las gráficas nos indican se llegan a mover millones de pesos en la plataforma de Bitso. Al 3 de octubre que fue mi primera compra de bitcoin, en donde era el segundo en ir a comprar con César, tras haberse anunciado en el *Reforma* por 6 meses, tenemos un volumen de transacción por parte de Bitso en casi 2 millones de pesos, 1,815,949 para ser exactos, de los cuales 50 pesos fueron de una transacción o compra física mía.

Otra advertencia es que estoy tomando mi primera transacción y la baja actividad que César me comentó que ha tenido, al igual que las pocas transacciones físicas que logré tener a lo largo de mi investigación como una constante. Es verdad que debido a lo grande que es la Ciudad de México no sería la única transacción física, pero es difícil que con dos puntos de venta de bitcoin

y 3 localidades que aceptan, que son los sitios que encontré durante mi trabajo de campo, se muevan cifras en los millones de pesos.

Una de las localidades mencionadas que aceptan bitcoin es Fantástico Comics S de RL de CV. Este fue el único lugar que encontré durante mi trabajo de campo que aceptaba bitcoin fuera de la plataforma de Bitso. Es una tienda de comics, manga y curiosidades de ese tipo, que inteligentemente dentro de la misma tienda se hace un 10% de descuento al pagar con bitcoin.

En esta tienda tienen también un cajero donde se puede comprar bitcoin, imprimir una cartera de papel, cambiar pesos por bitcoin y vice versa. El cajero tiene un lector de códigos QR que son los que contienen la dirección de bitcoin, una pantalla táctil, una ranura para depositar dinero y otra para extraerlo. Hablando sobre la tasa de cambio y el descuento de la tienda tenemos una relación como ya se mencionó interesante, pues el cajero nos da una conversión de pesos a bitcoin en la que ellos se quedan con aproximadamente 10% de los pesos que uno cambia a bitcoin. Es decir que de 200 pesos, realmente se obtienen 180 pesos usando el cambio de bitcoin de páginas reconocidas en internet con la tasa de cambio del mercado.

Cuando se hace el cobro entonces en la tienda de fantástico con bitcoin se nos hace un descuento del 10% como ya se dijo, y al comprar bitcoin en su cajero tenemos que se quedan con un 10% de lo que cambiamos el tipo de cambio. Es asi que el beneficio aparente de pagar con bitcoin realmente no está ahí y lo que se proporciona en la tienda es más la experiencia de usar bitcoin, si es que no se consigue otro tipo de cambio de bitcoin o se llega con bitcoins con otro tipo de cambio.

Con esto tenemos un panorama mucho mejor ilustrado de la situación mexicana: el volumen del principal exchange mexicano, un bajo uso presencial ya sea adquiriendo o usando, y una cercanía a la tendencia mundial en las transacciones virtuales. Esto nos genera un punto para comenzar a concluir con la disparidad observada inicialmente que era: un mínimo uso presencial y un uso virtual muy alto. Podemos ahora después de observar las gráficas plantearlo como un uso *efectivo* presencial muy bajo y un volumen de intercambio alto. Lo que nos indica que las personas que lo usan principalmente es en un entorno virtual, como se menciona, con objetivo de conseguir un beneficio o una inversión, al igual de una nueva manera para enviar remesas en el caso de México, y en una perspectiva general de lo que se puede concluir de las entrevistas que

Bitso tiene al público. He incluido la palabra *efectivo* solamente para diferenciar entre usos que impliquen una combinación de usos virtuales con físicos como pueden ser las remesas y de los que son puramente físicos como lo podría ser comprar algo o vender algo al igual que con efectivo, como mi compra con César.

Por lo tanto bitcoin es principalmente una moneda digital con un volumen de intercambio elevado, en donde los usuarios pueden tener inversiones o usarla como alternativa para transferir remesas en el caso mexicano, por mencionar los ejemplos que he encontrado analizando a Bitso. Pero lo más importante es lo que ya se mencionó, es en la mayoría de su uso una divisa o moneda *digital*, con la cual existe un movimiento total diario que oscila en los millones de pesos. Este es un hecho que se venía esbozando poco a poco, pero aquí es donde finalmente podemos observar concretamente la gran cantidad de dinero que bitcoin logra circular y todo esto dentro de un entorno primordialmente virtual.

¿Cómo se puede entender entonces esta diferencia notable en los dos tipos de usos, presencial y virtual?

Hablando ahora conclusivamente de lo que podemos observar ante la diferencia de ambos tipos de uso, y reduciendo la reflexión a México, que es en donde se desarrolló mi investigación, estamos frente a una moneda cuyo volumen de intercambio diario sobrepasa a su volumen de uso físico por un aproximado de 30 mil veces[44], si es que se toma como cierto que hay un poco volumen de intercambio físico, que en el tiempo de mi investigación fue una constante.

Como es evidente tengo también una entrevista transcrita con César, sin embargo la entrevista la hice la segunda vez que lo visité y fui por más bitcoins. No fue la primera ocasión que conocí a César. A continuación me gustaría comentar los puntos más interesantes de la entrevista así como hablar de sus consecuencias y relaciones al uso de bitcoin, que es lo que nos compete en este capítulo. La entrevista ocurrió el martes 22 de noviembre de 2016, y fue cuando regresé con César para comprar 500 pesos en bitcoin así como para entrevistarlo. A continuación los fragmentos de la entrevista:

[44] Si se divide el volumen de intercambio diario del 3 de octubre del 2016, que es 1,815,949 de pesos entre los 50 pesos de mi primera compra con bitcoin tenemos una diferencia de 36,319. Aun si tomáramos un promedio de 50 pesos en las otras 4 localidades en donde se acepta y procesa bitcoin físicamente, tendríamos una diferencia de 7,264 veces. Cifra hipotética pero que sigue estando dentro de los diez miles.

Rodrigo: La otra pregunta o reflexión es sobre la antigüedad ¿Qué opinas? Bueno yo tengo entendido que llevan desde el 2008, 2009 más o menos, ¿Tu desde cuándo te enteraste? Bueno me dijiste que en lo de CNN ¿No? ¿Pero hace cuánto fue más o menos? y ¿Qué opinas también de que sean tan antiguas o que implica que tengan esa antigüedad? ¿No? ¿Qué opinas más bien de la antigüedad?

Cesar: Mira yo tengo hace como dos años que supe de los bitcoins, en cambio, como tú lo indicas pues tienen más años de existencia. El primer problema o la primer incertidumbre en este tipo de moneda es que como no hay una institución bancaria que te respalde se puede dar a casos fraudulentos, de que hoy puedo generar, no sé, como programador o como hacker, cracker, no sé cómo se le pueda decir; crear una moneda de tal que sea efectiva en su momento, pero igual que como en las tarjetas de crédito pues, sabes que este pago, o este tipo de moneda no existe en realidad, es cancelado entonces como comercio o como comprador te vez afectado ¿no? Es grave la incertidumbre en cuanto a esta moneda, por eso también a pesar de los años que tiene no ha sido como que aceptada en todos los lugares por el tipo de riesgo que existe, en que realmente exista o no exista, o más bien ¿Quién te respalda esa moneda electrónica? ¿No?

Rodrigo: He visto también o siempre que leo la información dicen que es muy volátil ¿No? Que puede de un día para otro variar, bueno con las elecciones de Trump creo que saltó, como con el Dólar, creo que saltó muchísimo estuvo en... no sé en cuántos pesos la moneda (bitcoin)[45].

Cesar: Ajá la ventaja por ejemplo del bitcoin es que hasta al momento no se ha visto que se devalúe ni nada por el estilo sino que todo lo contrario hoy lo compras y te sale no sé, un bitcoin en 8 mil, y esos 8 mil que tú compraste hoy, bueno en pesos mexicanos, 8 mil pesos, ponle que sean 8 mil un bitcoin ahora, el día de mañana o pasado mañana, tu bitcoin que compraste ahora ya es de 1.2 por ejemplo, 1.3, entonces ahí podríamos decir que ya no son 8 mil, sino ya son 8 mil por ejemplo 30 pesos 8 mil 40 ¿no? Entonces sí es una ventaja utilizar los bitcoin o por ejemplo cuando compras algo virtualmente si te sale un artículo en quinientos pesos y lo compras con bitcoin te sale no sé en 460 y tú dices, ah pues, me ahorro 40 pesos ¿No? He he

[45] Concretamente el precio aumentó un 5%, con la presidencia de Trump, de 702 dólares a 737 (CoinTelegraph.com, 2017)

Rodrigo: 40 pesos y también la velocidad, ¿no? La velocidad de la transacción

Cesar: Y es una transacción en automático a diferencia de que aunque digan que el SPEI (Sistema de Pagos Electrónicos Interbancarios) es una manera rápida automática de transacción no lo es, porque cuando lo haces entre bancos que sean diferentes el SPEI, se lo pone siempre y cuando sea el mismo horario del banco. Es decir si tú mandas no sé una transacción de Bancomer a las 5 de la tarde, que cuando ellos cierran a las 4 y tú se lo mandas a Banorte que cierra a las 6, aunque tú pagues el cobro de SPEI de casi, no sé 8 pesos, 18 pesos dependiendo de la institución bancaria, para que sea el mismo día, no se transacciona porque el banco cerró antes desde donde lo enviaste, que del que lo recibió, o viceversa ¿no?

Comentando la primera respuesta tenemos que Cesar ya sabía de la existencia de bitcoin desde 2014 aproximadamente, y la respuesta que nos da a continuación es muy sugerente para el tema del capítulo. De lo que nos habla Cesar es de la incertidumbre que rodea a bitcoin por el hecho de no tener una institución que la respalda. Nos da el ejemplo en el que él llegara a programar o construir una criptomoneda que se use y se da el caso de una cancelación o se llega a identificar que esa moneda es inexistente como tal y solamente es una estafa, generando una afectación por ambas partes, los que la dan así como de los que la reciben. Es de este modo que César relaciona la antigüedad que ya tiene, el riesgo y la falta de respaldo en consecuencia de que han afectado la aceptación y su uso a lo largo de los años.

Independiente de la seguridad que pueda tener o no bitcoin, pues no ha habido noticias recientes ni en su historia de hackeo o crackeo, y como ya se explicó en el primer capítulo, se tendría que tener mas de la mitad de todo el poder computacional para poder hacer satisfactoriamente algún tipo de hackeo o crackeo, hecho que es poco práctico y difícil de realizar. Sin embargo de lo que sí ha habido fallas son de los llamados exchanges, el caso más famosos es de uno llamado Mt.Gox y se explicará más tarde.

Regresando a la entrevista, Cesar tocó un punto sensible en lo que concierne a bitcoin y esto es, si bitcoin es algo real y si tiene certidumbre. Es evidente y más en las fechas

posteriores de mi trabajo de campo el gran auge que está teniendo bitcoin, pero esto no significa necesariamente certeza. Es decir que muchas personas estén de acuerdo en algo o usen algo no significa que eso inmediatamente será algo bueno, o que tengamos la certeza de que no es una estafa o algo que podría no es real como nos sugiere Cesar. De este modo podemos tomar, por cuestiones de la investigación, una postura completamente negativa, posicionarnos en el peor caso de bitcoin y analizarlo de ese modo, como un fraude.

Profundizar en esta postura surge como un ejercicio hipotético en el que analizaré los casos y la situación de que pasaría si fuera un fraude o un negocio piramidal, no necesariamente estamos concluyendo o diciendo que bitcoin es de este modo, pero nos sirve para explorar las diferentes posturas que se podrían tener. Esto también se tratará brevemente para no salirnos de la discusión de la entrevista de Cesar y será también tratado en entrevistas posteriores en donde surjan por igual aspectos negativos o en su caso positivos de otras entrevistas y experiencias de campo.

Dicho entonces esto, visto bitcoin como un negocio piramidal, tenemos en nuestras manos un negocio piramidal global, es decir el primero que tiene a una red en Internet a su servicio, así como muy eficiente, empleando creativamente y un poco oximorónicamente los términos de bitcoin, un negocio piramidal descentralizado. Primeramente hablando de la adopción del esquema o como se unen las personas tenemos que las personas se unen voluntariamente, por recomendación de un amigo, conocido o familiar, interés propio o tal vez por iniciativa propia, pero lo importante del unirse a la red es que, el sacar una cuenta, si usamos la analogía de un banco, no tiene ningún costo extra. Es decir usar y descargar una cartera digital ya sea en computadora o móvil no tiene ningún costo adicional. Existen carteras a las que se les llama de almacenamiento físico que tienen un costo elevado dependiendo de su seguridad, pero se usan para almacenar un número considerable de bitcoins.

Por lo tanto aquella inversión que queramos hacer para obtener nuestras primeras bitcoins, es en lo primero en lo que gastamos, a diferencia de los bancos que cobran una comisión a la cuenta por usar su servicio, en bitcoin no existe dicha comisión por tener una cuenta. Se podría ver reflejada la comisión de uso de cartera en la comisión que se les

paga a los mineros, pero aún así esta comisión sigue siendo mínima, pues tenemos una comisión que, de ser así, tomaría en cuenta el uso de la cartera y la transacción. Por ende nuestro paquete para iniciar en este negocio piramidal consiste en una cuenta bancaría que no cobra comisiones por apertura ni uso, no caduca, pues nuestras bitcoins siguen siendo bitcoins por el tiempo que siga activa la red y en última instancia puede verse como una aplicación gratuita y/o un programa de código abierto.

En segundo lugar tenemos el beneficio por "reclutar", si es que lo podemos ver de este modo. El reclutar a una persona que en este caso sería que aquella persona o un grupo de personas usen bitcoin y esto es, que con dinero Fiat[46] o fiduciario compren o hagan la conversión de su dinero a bitcoin, tenemos varias consecuencias. La primera es que esto es un usuario más a la red de bitcoin con toda la potencialidad que eso lleva (desde convencer a más personas, a invertir grandes o pequeñas cantidades de dinero o incluso a perder la llave privada que controla su cartera, y volverse parte de las monedas "muertas" o "zombi" de Ratcliff). La segunda consecuencia es que su primera transacción representa trabajo para los mineros, es decir que por introducir a una persona a este "esquema" genera una moneda o una fracción de moneda[47] como tal por el diseño de la red y los beneficios del minado. La tercera consecuencia es un tanto obvia y es un aumento a la cantidad de personas que están dentro de la red de bitcoin, aumentando de ese modo la demanda de bitcoin, con una escasez determinada por las reglas definidas de bitcoin, y generando por lo tanto un aumento en su precio.

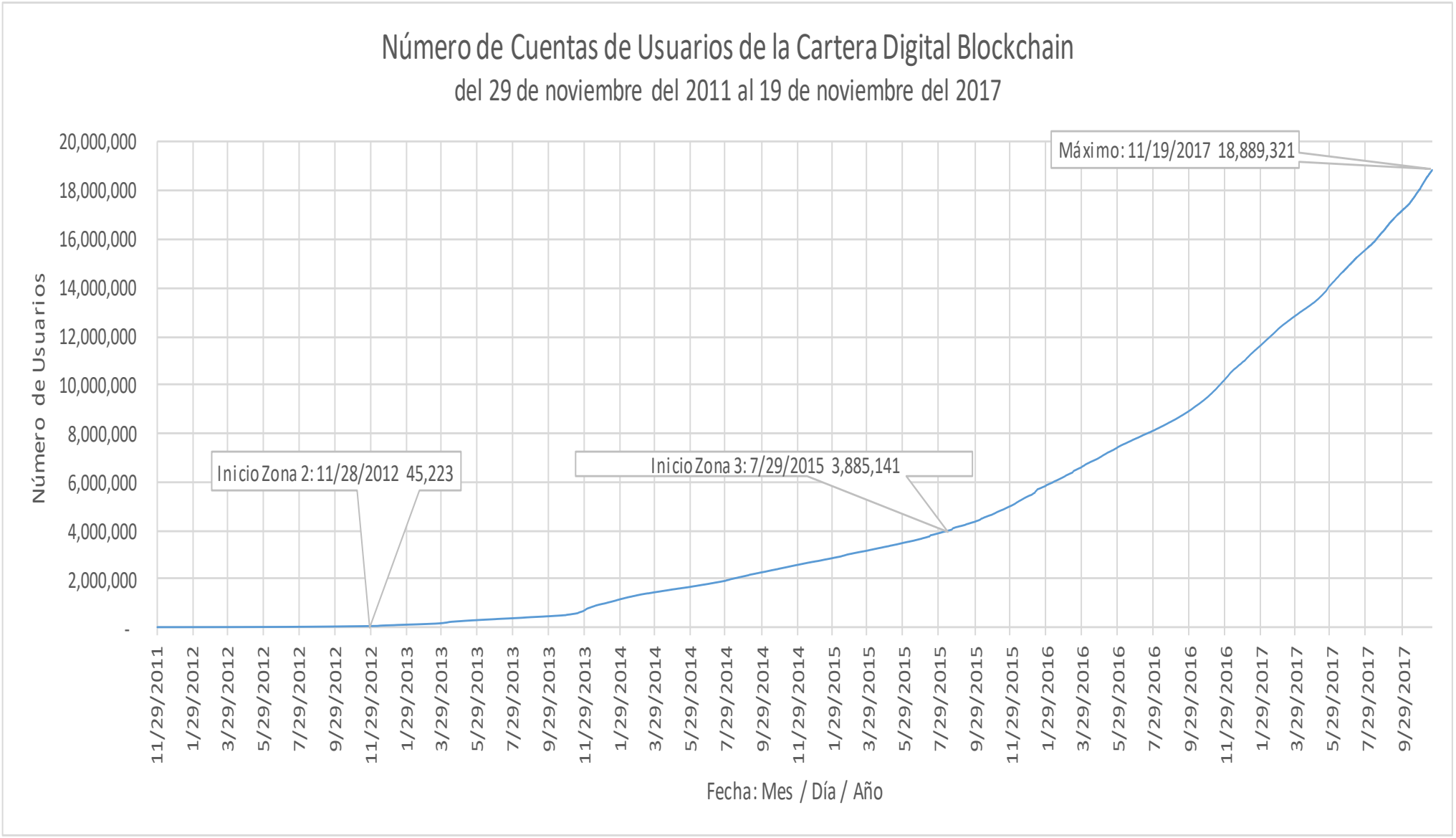
Para respaldar lo anterior podemos ver las siguientes gráficas que nos proporcionan una idea general de lo que se quiere decir, la primera gráfica es de la cantidad de usuarios que la cartera digital llamada blockchain tiene. Coincidentalmente esta página es de donde he sacado muchas de las otras gráficas y cifras de la investigación, y si bien no es la cartera más popular de todas, y no es de software libre nos da una idea general de una cartera promedio cuantos usuarios tiene. De acuerdo a un artículo en el 2015 se posiciona en la

[46] Fiat es un término usado mucho en la jerga de bitcoin como se verá posteriormente cuando hable de mi experiencia etnográfica en Acapulco, Guerrero en el congreso de Anarquistas Capitalistas.
[47] Pues como ya se explicó los Fondos de mineros son un conjunto de personas dedicadas a procesar transacciones y al momento de verificar satisfactoriamente la recompensa es dividida entre todas las personas del Fondo (Pool).

cartera número 6 de 8 posibles, y se nos dice que nuestro PIN privado se almacena en internet, así como su código no está abierto al público. (Mark, 2015)

Es necesario subrayar con precisión que el nombre de la cartera digital en este caso se llama del mismo modo de aquello que explicamos en el primer capítulo que es el libro mayor o la cadena de bloques, la tecnología detrás de bitcoin. En este caso son dos cosas completamente diferentes pero que se relacionan.

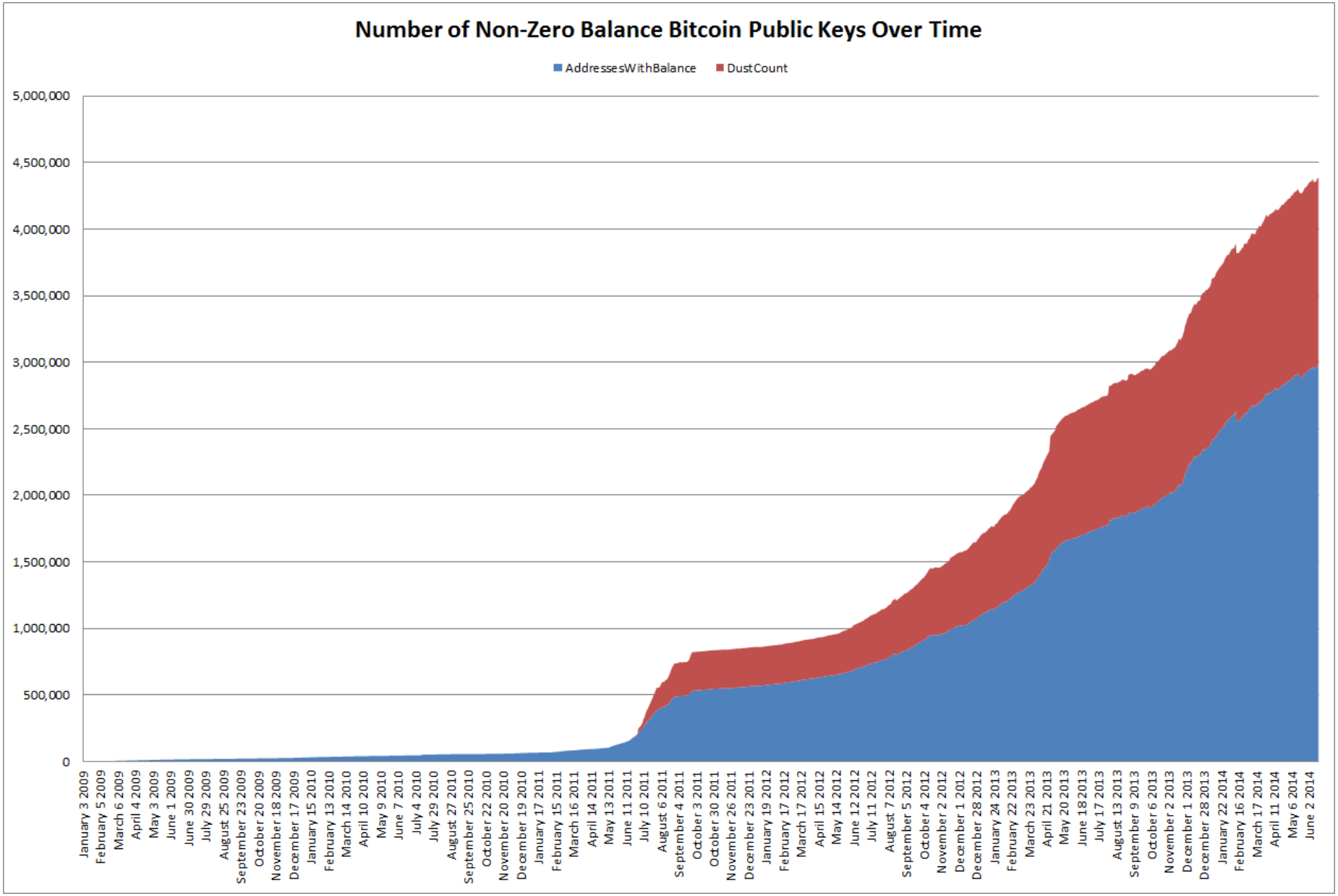
La gráfica a continuación:



Gráfica 12: Datos obtenidos de (Blockchain Luxembourg S.A.R.L, 2017d)

Un primer comentario de la gráfica y de la estadística que se nos proporciona es que, no necesariamente un usuario nuevo implica ser una persona diferente, pues una persona puede tener hasta 10 carteras diferentes o más. Sin embargo pienso que es un caso límite y no es necesario tener más de una cartera, en especial para personas que comienzan a usar bitcoin, si es suficientemente difícil entender la moneda, es aún más difícil tener más de una cuenta o cuentas diferentes para manejar nuestras monedas. Comparativamente para usuarios más avanzados, se podría dar la situación en la que tuvieran más de una cartera.

En la gráfica resalté las diferentes "*Zonas*" de la mina, es decir las diferentes etapas de las recompensas que reciben los mineros por procesar transacciones. En total de la "*Zona* 2" tenemos un incremento de 3,839,918 usuarios a diferencia de lo que va de la "*Zona* 3", 19 de noviembre del 2017, en la cual se han unido 15,004,180 usuarios. Respectivamente el precio de bitcoin al inicio de la "*Zona* 2" fue de 12.5 dólares, del inicio de la "*Zona* 3" de 293 dólares, y al 19 de noviembre del 2017 fue de 8,036 dólares (coindesk, 2017g). El deseo de hacer la conclusión y relacionar un incremento de 3.8 millones de usuarios con un aumento de precio de un 2,344%, del mismo modo podemos relacionar un incremento de 15 millones de usuarios con un aumento al precio de 293 a 8,036 dólares, 2,742%%, pero antes de hacer ese tipo de conclusiones es relevante ver la siguiente gráfica:



Gráfica 13: Información obtenida de (Ratcliff, 2014)

La gráfica anterior es de un análisis que ya se ha citado anteriormente, y lo que representa es el número de Public Keys, es decir PINs Públicos, direcciones donde recibimos monedas, que tienen un balance significativo en comparación a las que tienen Dust, es decir polvo, menos de 0.001 bitcoin que al 2014 no eran significativas.

Por lo que muestra esta gráfica no podemos hacer la conclusión anterior, pues de ese incremento de 3.8 millones de usuarios, no sabemos realmente cuáles tienen un balance dentro de sus carteras y cuáles fueron usadas como intermediarias en una transacción y ya no tienen fondos o un balance.

Así que siendo conscientes de las limitaciones de las gráficas podemos proceder a una conclusión no tan ambiciosa. Con por lo menos un incremento de 3.8 millones de usuarios tenemos un incremento en el precio de 2,344% con una distribución de 25 bitcoins por bloque minado. En lo que va de la "*Zona* 3" existe por lo menos un incremento de 15 millones de usuarios relacionado a un incremento del 2,742% al precio con una distribución de 12.5 bitcoins por bloque de transacciones procesado.

Por lo tanto, si no podemos establecer una correlación directa entre más usuarios más sube el valor de bitcoin, lo que si podemos hacer y se está haciendo con las cifras anteriores es vincular cómo se obtiene una moneda, con las personas que la usan y su incremento de precio. Otra conclusión o cuestión que podemos plantear a favor del argumento de bitcoin como una pirámide es la frase común de cuánto se ha enriquecido una persona a lo largo del tiempo, pues existe un incremento significativo en el precio de bitcoin. Que podría verse relacionado al incremento de los usuarios de la cartera.

Antes de concluir sobre bitcoin como un negocio piramidal estamos evitando u olvidando mencionar algo muy importante de los negocios piramidales, y es aquella persona u organización que se encuentra en la cima de la pirámide y quien obtiene la mayoría de los beneficios. En este caso nuestro afamado Satoshi Nakamoto, quien de acuerdo a cálculos hechos por Sergio Lerner (que se autodenomina en su blog como Cryptofan, Investigador de Seguridad Independiente y especialista en bitcoin desde el 2011 (Lerner, 2011)) tiene aproximadamente 1 millón de bitcoins que representan al momento de escribir estas

líneas (6 de junio del 2017) aproximadamente 7% de todas las bitcoins minadas, y en dólares a 2,957,950,000 dólares al 6 de junio del 2017.

De acuerdo a Sergio Lerner, él no puede garantizar con certeza que todas las primeras bitcoins minadas le pertenezcan a Satoshi Nakamoto, pero algo de lo que sí puede estar seguro es de que la actividad de minado de las primeras monedas fue hecha por una sola entidad, misma que empezó a minar desde el primer bloque, el *Bloque Génesis*. (Lerner, 2013) De este modo no sabemos con certeza si Satoshi Nakamoto es dueño de todas esas monedas pero dada la situación en la que la moneda "nació", en un contexto muy cerrado en la cual las primeras monedas y pruebas del programa eran hechas por contadas personas, podemos concluir que el hecho más probable es que en verdad pertenezcan a Satoshi o a una entidad o grupo de personas relacionados con él.

Es así que la persona con posiblemente más bitcoins es la que se ve beneficiada en mayor grado, pero esto es por la cantidad de bitcoins que tiene, pues el valor de cada moneda o fracción es equivalente a lo largo de toda la red. Si seguimos con la metáfora o el oxímoron de pirámide descentralizada podríamos imaginarnos algo así como una pirámide, pero en lugar de tener solamente una cumbre o punto cúspide, tenemos varios, siendo entonces de este modo algo mucho más cercano a una montaña en donde se tienen varios picos de una forma un tanto irregular, o incluso podríamos extender la imaginación a un volcán el cual está durmiente y puede en cualquier momento hacer erupción.

Antes de ser conclusivos sobre este tema es necesario hablar de Mt. Gox un exchange que se mencionó brevemente cuando se explicaba la diferencia entre la seguridad de la cadena de bloques y la seguridad de plataformas, como exchanges que usan dicha tecnología. En el caso de dicho exchange se declaró en quiebra junto con la pérdida de 650,000 bitcoins a finales del 2013 inicios del 2014. Se dice que las bitcoins que manejaba el exchange fueron robadas o se encontraban desaparecidas, sin embargo en un estudio hecho en colaboración con la Universidad de Tulsa y Tel Aviv (Gandal *et al*., 2017) analizan la actividad de dicho exchange antes de que se declarara en banca rota.

En el estudio se encuentran movimientos fraudulentos por parte de dos entidades, Markus y Willy, que afectaron el precio de bitcoin aumentándolo. Estamos hablando de un

aumento de aproximadamente 150 dólares a 1,000 en dos meses, y de alrededor de 600,000 bitcoins. La situación en concreto fue la adquisición fraudulenta de estas monedas por parte de Markus y Willy[48], sin que aquellos gastaran algo por dicha adquisición, es decir las cuentas de dichos usuarios no estaban respaldadas con dinero del exchange. Dichas bitcoins fueron transacciones duplicadas y por ello mismo ningún cliente de Mt. Gox recibió el dinero con el cual se adquirieron aquellas bitcoins. Suena como una situación improbable por lo que ya se mencionó de la tecnología del libro mayor, pero nos habla y pone en juicio las instituciones que rodean a la moneda como tal. En donde la cadena de bloques nunca ha sido modificada por hackers o crackers pero sí las instituciones construidas alrededor de ella.

Concluyendo entonces sobre el tema de si bitcoin es un negocio piramidal tenemos algunos puntos a favor que pueden hacernos pensar que es un esquema piramidal, pero me gustaría pensar más bien en los temas expuestos aquí, esos puntos a favor de un esquema piramidal, como características que podemos ir esbozando, agregando a bitcoin para poder hacer y complejizar verdaderamente esta moneda o ente virtual económico que, como mencioné en la introducción, podría ser un Rey Midas moderno.

Tenemos entonces dos características concretas. Nulo cobró de comisiones por apertura o por mantener la cuenta inactiva o con un bajo saldo. Beneficio generalizado de reclutamiento, que en este caso se ve reflejado en la tendencia de bitcoin de estar siempre subiendo, pero con oscilaciones que pueden ser volátiles.

Finalmente tenemos un primer análisis de un caso negativo de bitcoin como negocio piramidal que surge de la entrevista de César. Es necesario recalcar que no estoy implicando que César piense todo esto, sino que fue un ejercicio creativo para analizar una de las muchas posibilidades de bitcoin que se pueden dar, y es una reflexión gracias a la entrevista que tuve con él y mi conversación con él.

Otra de las experiencias etnográficas que tuve fue pagando tacos de guisado tradicionales de Morelos, México llamados acorazados en el restaurante llamado Los Acorazados del

[48] En el análisis citado se habla que el usuario Willy era una persona interna del exchange pues tenía actividad cuando este se encontraba sin conexión al Internet.

Golden Braun al igual que pizzas de maíz azul en un restaurante llamado Pixza. En ambos restaurantes el encargado de procesar mi pago fue Bitso SAPI de CV con su plataforma. La otra compra que logre hacer en la Ciudad de Mexico fue en Fantástico Comics S de RL de CV, en dónde compre 3 libros de comics diferentes, sin embargo esta fue usando una plataforma propia de la tienda no con la plataforma de Bitso.

A continuación retomaré un poco más la discusión sobre mi experiencia etnográfica en el campo, está ya se mencionó en la Introducción, y es el congreso de Anarquistas Capitalistas en Acapulco llamado "Anarchapulco". Será en un formato narrativo y se retomarán las discusiones que surjan sobre el tema de bitcoin como se ha estado haciendo.

Cryptopulco es un día dedicado a pláticas sobre criptomonedas y todo lo relacionado a ellas. Este día sucede dentro de una conferencia anual, la cual va en su tercer año consecutivo, llamada Anarchapulco. Ella trata todo lo relacionado a la Anarquía Capitalista y vienen varias personas a hablar desde cómo ser emprendedores, inversiones, política, filosofía, salud hasta relaciones personales. Yo atendí a la edición del 2017 y solamente al día de Cryptopulco.

Una persona que no he introducido es Juan S. Galt, quien fue la segunda persona que entrevisté en mi trabajo de campo, y gracias a él me enteré de Anarchapulco. Se denomina como: "Deep Thinker, blockchain Journalist/ Consultant. Voluntarist, Social Connector"("Juan S. Galt (@JuanSGalt) | Twitter," 2016). Es entonces que después de regresar de comprar mi boleto de vuelta a la ciudad en la estación de camiones en Acapulco, me encontré con él. Antes de la última conferencia de Cryptopulco en la que habló Roger Ver, también conocido como bitcoin Jesus.

Para ese entonces había bebido ya mi segunda taza de café orgánico de *Verde Vegan*, un restaurante vegano en Acapulco que tenía un módulo en el hotel, el café fuerte, yo estaba un poco alterado, también un poco emocionado y nervioso pues era ya la última conferencia del día. Subiendo hacia el salón de conferencias para mi sorpresa ahí estaba Juan. Hablando con otras personas y vendiendo ledgers, que son carteras físicas de bitcoin que garantizan seguridad más avanzada a una cartera en un celular o teniendo bitcoin en una cuenta de un exchange. Los ledgers que vendía Juan costaban 40 dólares en bitcoin y 45 dólares en Fiat. Es decir el dólar es

la moneda común que se estaba manejando y es algo que aún no comento, pero es relevante pues muchas de las personas que atienden Anarchapulco son estadounidenses, aunque también, en esta edición hubo europeos y más mexicanos como yo, pero la mayoría era estadounidense, de acuerdo a lo que Amparo me comentó, empleada de *Verde Vegan*.

Me gustaría hacer un pequeño comentario sobre esta palabra Fiat que la escuché muchas veces a lo largo de todo Cryptopulco. En lugar de referirse a una moneda específica como pesos o dólares usan esta palabra Fiat, y con ella su contraparte Crypto como abreviado de criptomonedas o simplemente usan la criptomoneda a la que se refieren, como puede ser bitcoin, dash o cualquier otra criptomoneda.

Mientras estuve con Juan vendió aproximadamente de 3 a 4 Ledgers a personas que atendían al congreso, de las cuales solamente una pagó en bitcoin. Yo por mi parte hubiera comprado un Ledger, pero gasté todas mis bitcoins que tenía acumuladas al momento para pagar el boleto del congreso y tenía solamente 100 pesos aproximadamente en ese momento en bitcoin.[49] Hablando de Fiat no contaba con suficiente para poder pagar uno. Otro punto importante es que esta inversión se recomienda hacer por dos razones principalmente, o por lo que yo sé lo haría en dos casos particulares, y esto es por tener extra seguridad al almacenar las bitcoins y otro caso particular sería en el dado caso que llegara a tener una cantidad considerable de bitcoins.

Esperé a que terminara y lo saludé, no me reconoció, pero al decir mi nombre y quien era me ubicó. Le pregunté si podíamos seguir con la plática/entrevista que habíamos estado teniendo a través de Internet y que quería finalizarla con algunos aspectos más personales y cuestiones de finanzas, que me parecía mejor hablarlas en persona. Él accedió y comenzamos a platicar mientras nos paseábamos por los diferentes cuartos de la sala de exposición. Algo recurrente que me pasó con Juan es que cada vez que mencionaba que estaba haciendo una entrevista él se veía un poco perplejo y me sirve esto para hacer un hincapié sobre la metodología empleada para la investigación; si bien a mi parecer estaba teniendo una entrevista con Juan y tenía un guión con preguntas como guía, lo que llegué a tener con él fue una conversación muy interesante de diversas preguntas y discusiones entretenidas. Que aunque no pareciera una entrevista formal de pregunta y respuesta sí tenía una estructura como tal.

[49] Si observamos mi pago en febrero que fue de 900 pesos en bitcoin en febrero del 2017 y lo comparamos con el tipo de cambio de noviembre del 2017, tenemos una diferencia notable en la que esos mismos 900 pesos ahora son, 6867.91 pesos al 28 de noviembre del 2017.

La primer pregunta y fue algo que me surgió al intentar poner todo en perspectiva sobre las criptomonedas y bitcoin, un tanto para ubicar a Juan, y a todas las personas de la conferencia que tienen una visión más libertaria de bitcoin. La pregunta o pauta con la que empezó la conversación fue sobre el uso diverso que bitcoin puede tener, es decir; desde ser un vehículo y el medio con el cual se pueden dar prácticas anarquistas capitalistas o libertarianas y también aquellas prácticas opuestas a Anarchapulco.

Si se ve bitcoin como un universo muy grande, no todas las personas que la usan se adhieren automáticamente a un pensamiento libertariano o de anarquismo capitalista. A esto Juan comentó que las tecnologías y bitcoin se pueden considerar como armas de dos filos y ciertamente se pueden usar de ambas maneras. Adicional a esto en donde reconoció que se puede usar bitcoin de modos diversos, Juan comentó que para él, bitcoin se puede ver como un modo de propagar obligaciones. Son obligaciones a un modo de contrato en el que dos personas se ponen de acuerdo para hacer cualquier tipo de transacción, movimiento o trato. Ejemplificando esto me comentó que existen muchos mini mercados en el que se conectan y se hacen este tipo de obligaciones como puede ser Amazon o eBay.

La siguiente pregunta fue para que Juan me esclareciera una cuestión que yo había escuchado como una de las ventajas de usar bitcoin y es algo que me parece que tiene un potencial muy grande hablando de bitcoin como una tecnología, y esto es que bitcoin es programable, es decir es dinero programable. Así que le hice una pregunta pidiendo que me clarificara como es que las transacciones pueden ser programadas. Comentó que un modo de hacer esto es que una transacción no avance hasta que pasen cierto número de confirmaciones, lo que en este caso agregaría seguridad en la transacción. Es decir, mi pago no se hará hasta que yo sepa que se han validado por lo menos cinco pagos antes en la cadena de bloques y de ese modo yo tengo certeza de que mi transacción es segura.

Seguida de esta pregunta le comenté de una idea que me ha surgido al estar estudiando y entendiendo todo lo relacionado a bitcoin, y que sería un tipo de sistema con votos programables para cualquier tipo de elección democrática. Estos “votos programables” serían aquellos en el que se programan a modo de un lenguaje de programación y al momento en que una persona da un voto a otra, el voto ya tiene ciertas características en donde si no se usa para aquello para lo que fue programado no se pueda usar el voto como tal. Es por esto que me parece que la idea de

dinero programable o tener la ventaja de poder programar algo usando la cadena de bloques tiene un potencial muy grande.

Este comentario lo hice pues antes de ir al congreso vi un video en donde dos personas reconocidas de la comunidad de bitcoin, llamadas Roger Ver y Tone Vays, discuten sobre el futuro de bitcoin, pues se está llegando a un punto en el cual el tamaño de los bloques en la cadena de bloques está siendo muy grande y esto genera repercusiones en el tiempo de validación de transacciones y en el minado. En el video estas dos personas discuten dos diferentes soluciones y hoy en día aún no se soluciona el problema de qué hacer.

Si llegara a haber votos programables podría la comunidad votar y darle una solución a este problema usando las mismas tecnologías de bitcoin, pero es más complicado que mi propuesta. Lo que Juan me comentó es de un tipo de validación que existe que se llama Proof of Stake, y es un método que ya existe para votar en donde un determinado valor es un voto, y es un sistema que se puede proteger de alguien que compra mucho queriendo obtener una mayoría de los votos, pues si una persona llegara a comprar una gran cantidad de valor en votos, todo el demás valor de las personas subiría.

Regresando al congreso y a mi conversación con Juan, antes de que termináramos le pedí un estimado de qué tan seguido usa bitcoin, a lo cual me respondió que unas 10 veces al mes. Le pregunté también sobre montos, pero me dijo que prefería no dar esa información. Al momento en el que hice este último comentario estaba ya la clausura y la conferencia de Roger Ver, quien es el dueño del dominio de www.bitcoin.com patrocinador grado platino del evento, y decidimos hablar y buscarnos al terminar la conferencia.

La conferencia de Roger Ver fue principalmente anecdótica, en la que contó mucho de su vida personal, en el sentido de por qué él usa bitcoin. Su historia es la de un expatriado, él reside en Japón y no se le tiene permitida la entrada a los Estados Unidos de Norte América. El tono de la plática y de las pláticas en general era muy relajado, por lo mismo hacía preguntas al público para que levantáramos las manos y era un ambiente muy incluyente. De igual manera había frases que el público gritaba o seguida de alguna frase de Ver algunas personas en el publico alzaban la voz en acuerdo.

En la ceremonia de clausura salí de la sala de conferencias, con el fin de encontrar el café llamado *Verde Vegan* con menos actividad y para entrevistar a una empleada. Ella se llama Amparo Manzanares y atiende lo que es el único lugar en Acapulco que acepta bitcoin, este café era uno de los principales comedores o lugares en donde la mayoría de los conferencistas y personas que atendían comían o tomaban un almuerzo.

Ella conoció bitcoin desde el 2016 cuando estaba una en 3,000 pesos, conocía ya los torrents[50] y las redes descentralizadas de par a par. Curiosamente la persona que los introdujo como negocio a bitcoin, fue Juan S. Galt mediante el exchange de Bitso, él les puso su cuenta y les explicó como debían de hacer todo. Hablando de las ventajas por usar bitcoin mencionó que se tiene mucho más rendimiento en los ahorros personales a diferencia del banco y que es más cómodo. Hablando del rendimiento me dijo que en Anarchapulco de 2016 muchas personas pagaron todo en bitcoin y que recibieron muchas bitcoins, por desgracia tuvieron que pagar bastantes deudas y no lograron conservar muchas. De haber conservado todas las bitcoins que tenían me mencionó que hubieran multiplicado por 7 esas ganancias que tuvieron en el 2016. Comparando el 2016 contra el 2017 tenemos que en el segundo recibieron muchísimos menos pagos en bitcoin a diferencia del 2016.

Hablando por ultimo de la seguridad mencionó que es una moneda in-hackeable y que solamente puede caer si todo el Internet cae como tal. Mencionó también que la generación de hoy en día es una que no confía tanto en los bancos y en las instituciones, pues solamente mantiene seguro su dinero, pero no genera buen rendimiento como sucede en bitcoin. Similarmente mencionó que es una inversión de ahorro a largo plazo como lo puede ser con el oro y la plata. Comentó también sobre la identidad de Satoshi Nakamoto, que nadie sabe quién es a ciencia cierta y era consciente también que en un futuro habrá más monedas.

Después de haber terminado la entrevista con Amparo, yo esperaba ver a todas las personas de la conferencia salir por el pasillo que daba al restaurante donde se encontraba *Verde Vegan*, pero por desgracia no sucedió así y me encontraba solo después de mi entrevista, sin poder conversar más con Juan y las personas de la conferencia. Busqué brevemente a Juan y a las demás personas pero ya se encontraba sola la sala de conferencias, dado que solamente fui un día y no todo el

[50] Los torrents son archivos que se usan en Internet para transmitir y compartir todo tipo de cosas, desde películas, libros, música e incluso programas.

congreso, no sabía los puntos de reunión usuales. Un poco desilusionado y algo preocupado decidí tomar mi bicicleta e irme a mi hotel cuando a unos 10 minutos después de mi trayecto me habló por teléfono Juan.

Contesté mientras andaba en la bicicleta y acordamos vernos en el Bar del Hotel, me preguntó si quería ir a una fiesta. Me tomó un poco de tiempo llegar a dicho lugar y una vez ahí intenté establecer una conversación con las personas que estaban tomando y platicando, mi tema para empezar la conversación era si habían visto a Juan S. Galt, pero no logré desarrollar una plática con nadie de los que estaban presentes. Tal vez fue mi acento en inglés o mi cara de preocupación al no encontrar a Juan, pero tampoco noté mucha apertura de las personas al hablar.

Decidí tomarme una cerveza y esperar, Juan no contestaba su teléfono ni los mensajes, así que después de que me confundiera la mesera con un americano y una breve conversación me senté a escribir en mi libreta notas y reflexiones que aún no quedaban registradas. Finalmente Juan llegó un poco más tarde de lo acordado, no le pregunté por qué se retrasó, él al llegar saludó a todas las personas a las que les pregunté si lo habían visto y pidió un trago. Se sentó conmigo, platicamos del congreso, le comenté cómo me perdí al entrevistar a Amparo de *Verde Vegan*. Le pregunté de donde, era a lo que respondió que era de Colombia y después de platicar de algunas cosas terminamos por dirigirnos a la fiesta.

Del hotel salían combies a la fiesta, con cupo aproximadamente de unas 6-7 personas, el costo por el viaje era de 250 pesos en total, mi bicicleta viajó gratis en una combie en la cual no cupimos Juan y yo, por lo que tuvimos que esperar por la siguiente. En lo que esperábamos platiqué brevemente con el conductor y me comentó que él poco a poco se estaba adhiriendo al pensamiento libertariano anarquista capitalista. También intenté indagar por dónde era la casa de Micheal donde sería la fiesta, el lugar me sonaba conocido. Esperamos a las últimas personas que dieron un curso en el congreso, un instructor de Yoga y una pareja de Relajación con Percusiones y otras más personas se nos unieron y salimos rumbo a la fiesta.

Al llegar mi bicicleta se encontraba ahí en buen estado, cosa que me dio confianza y ubicaba relativamente bien dónde estábamos, era una zona residencial en la parte alta de Acapulco con casas grandes, si recuerdo bien, llegue a ver un letrero que decía El Márquez o algo similar. Al

llegar se notó un ambiente relajado y estuve persiguiendo a Juan por todos lados, la primera parada fue el bar, en donde muy generosamente me invitó una cerveza y tomó otra para él. Después de esto me introdujo a sus amigos que hablaban español; Rodolfo y su pareja, y el Vicepresidente de Pagos de Bitso José Rodríguez. Me introdujo así como lo que estaba estudiando y me dejó platicando con ellos y él se fue por la fiesta.

Platicamos entre los cuatro de varias cosas, desde los orígenes de bitcoin y cómo se relacionaba al movimiento cypherpunk, en donde Rodolfo me comentó sobre las referencias del White Paper de Satoshi Nakamoto, una de ellas es un artículo sobre e-cash, una propuesta desde una perspectiva un tanto cypherpunk para la adopción de efectivo electrónico, escrita por Wei Dai. También mencionó que me ayudaría a entender la creación de bitcoin leyendo a economistas de la escuela de Austria en especial a Von Mises y Hayek. Es decir que bitcoin surge y el por qué se puede considerar como la escuela austriaca de economía de acuerdo a Rodolfo. Otra de las cosas que le pregunté era de donde conocía a Juan, a lo que me mencionó que lo conocía de bastante tiempo y que ayudó colaborando para el congreso de Anarchapulco.

Lo que platiqué con José Rodríguez fue breve, le pregunté desde unas precisiones de su plática en el congreso en donde mencionó que Trump removería todas las fábricas de Ford en México, el precio de bitcoin subió considerablemente. Otra cosa que me dijo José fue que metiera todo mi dinero en bitcoin cada que pudiera hacerlo, que el peso no era realmente estable o que no tenía un rendimiento o valor bueno, por lo que entendí. Al intentar obtener información de primera mano de las personas de Bitso no tuve ninguna respuesta. Envié un cuestionario al soporte técnico, al igual que contacté por teléfono y correo a su CEO, después de recibir su tarjeta. Por esta razón hice el tipo de análisis indirecto de su información y declaraciones en internet, pues no conté con ningún contacto de ellos, más que el anteriormente mencionado con José Rodríguez, vicepresidente de pagos en Bisto, pero fue uno casual y en un ambiente relajado, no académico o formal.

Después de un tiempo de estar hablando entre nosotros se nos acercó un panelista del congreso a darnos su opinión sobre unos de los temas que se estaban discutiendo en ese entonces, que era sobre los ETF exchange Transfer Fund en inglés o Fondo de Inversión Cotizado. En ese momento existían dos Fondos diferentes que estaban esperando aprobación por el SEC (Security and exchange Comision en inglés) o la Comisión de Bolsa y Valores de Estados Unidos. El

primer fondo era una propuesta de los gemelos Winkelvoss[51] y la otra propuesta era por parte de SolidX, una empresa de tecnología financiera. Este panelista que se acercó a conversar con nosotros, se llama Trace Mayer, es una persona influyente en bitcoin, lleva desde el 2010 en la escena, al igual que tiene un podcast llamado bitcoin Knowledge, donde ha entrevistado al CEO de Bitso Pablo González.

En relación al espacio la apertura y la convivencia podemos resumirlo en palabras de Juan S. Galt: "Sí pues en cuanto a las relaciones y vínculos en la comunidad, es una comunidad muy concentrada en negocios, y en el capitalismo pues en su forma pura, no en el *crapitalismo* que vemos en el mundo ahorita.

Pero más como el capitalismo de la clase media, o clase baja media, y hasta clase más alta pero que no son necesariamente tan políticos o tan, *you know*, malignos pues en la forma en que invierten su dinero, tan apáticos pues, como cosas que vemos en estos días. Pero, si o sea yo la verdad llevo viviendo de bitcoin varios años y prácticamente todas las personas con las que paso tiempo están bien entendidas en cuanto que es el bitcoin y para qué sirve y todo esto y lo usan regularmente o tienen, están esperando para que suba de precio y todo eso, entonces... Si me preguntaras a mí cual es mi nación cual es mi cultura yo te puedo decir de dónde nací o de dónde fue, de dónde aprendí inglés, pero en cuanto a mi cultura yo diría que mi cultura en este momento es gente que son como anarcocapitalistas libertarios que se meten en el espacio de bitcoin.

O sea no hay nombre para esta cultura en este momento, pero, *you know*, es una sub-cultura de gente que está metida muy en la tecnología, y no es difícil conectarse con la gente, con los líderes más visibles en este espacio, es lo hermoso, no es difícil conectarse con ellos, si tienes algo que ofrecer y si tienes unas buenas ideas. Si eres efectivo en tus comunicaciones puedes llegar a bastantes personas en este espacio y eso. Mucha de la gente en este espacio tiene buenas intenciones. Siempre hay sangre nueva que entra o los banqueros se están tratando de meter y pues hay problemas ahí, pero yo creo que el crecimiento de los *grassroots* de bitcoin es bastante

[51] Los gemelos Winkelvoss son entre otras cosas, quienes demandaron al creador de Facebook, Mark Zuckerberg por robarles la idea de detrás de Facebook. (Wikipedia, 2017b)

fuerte y pues vamos, tenemos nuestros problemas que resolver, en cuanto a governance y todo eso pero pues, sí o sea hay bastantes oportunidades, si hablas inglés en particular, es un movimiento bastante dominado por el inglés y por el chino también"

Esto último sobre los banqueros intentando entrar se puede ver reflejado en la diferencia con la que logré contactar a Juan y tener la apertura con él, a diferencia de Bitso, que incluso después de que Juan S. Galt me recomendó hablar con ellos y me comentó que ellos estaban trabajando de primera mano con el gobierno para regular el uso y la aceptación, no logré entablar una conversación con ellos, más allá de la que tuve con José Rodríguez en Acapulco.

Por último quedan las reflexiones finales de la investigación para cerrar con todo lo que se ha comentado.

Conclusiones

Para las conclusiones considero importante primero hablar sobre los temas tocados a lo largo de la investigación, ya que gracias a ellos vemos matices notables de bitcoin. Más tarde, una vez comprendidos estos temas, abordaré los temas más cercanos a la antropología como es la tipología de los usuarios de bitcoin y las conclusiones menos evidentes o más personales a las que me llevó el estudio de dicha moneda.

El primer tema a reflexionar es la seguridad, no solo de nuestras monedas, así como de nuestra wallet o cartera, sino que también la seguridad como tal de bitcoin. Si comenzamos a hablar por la seguridad que tenemos con las carteras y el almacenamiento de las monedas, tenemos que es un tema principalmente vinculado a la iniciativa propia. Es decir si empleamos y decidimos usar una wallet en lugar de un exhange o casa de cambio para almacenar nuestras monedas, depende del usuario generar una contraseña lo suficientemente buena, segura y aleatoria para que nuestras monedas se encuentren protegidas. En cuestión de criptografía elegir una contraseña con estas características resulta fundamental, pues si tomamos a la ligera este punto, o hacemos una contraseña demasiado fácil de adivinar o de obtener para un hacker, ponemos en riesgo todas nuestras monedas.

Resulta un tema de iniciativa propia, por lo menos en lo que observé de mi experiencia, pues al comenzar a usar la cartera donde obtuve mis primeras fracciones de bitcoin, tuve que informarme sobre las medidas de seguridad de bitcoin; donde se almacenaba mi llave privada, como respaldar aquella llave y por último como generar una contraseña la cual sea lo suficientemente buena como para no poner en riesgo mis bitcoins. Similarmente cuando descargué mi cartera en el teléfono celular tuve que generar una contraseña suficientemente buena. Ambas contraseñas de mis carteras fueron usando el método de Reinhold, que ya se explicó en el primer capítulo.

Una analogía que se hace al explicar y hacer entender lo importante que es esto es: tú eres tu propio banco, es decir tú eres el encargado de poner las capas de seguridad que creas necesarias para tus monedas, claro que es proporcional a la cantidad de monedas y al uso que le daremos. Es decir si tenemos una cartera con un límite bajo de bitcoins, tal vez consideremos no usar tanta

seguridad en comparación a una cuenta de ahorros en donde hemos invertido una cantidad mucho más grande.

Los puntos que se desprenden de que la seguridad dependa de las personas, y no de una institución central, son en mi opinión tres. El primero y más directo es que las monedas pueden perderse muy fácilmente, si no comprendemos en su totalidad qué es una llave privada, dónde se guarda, cómo se guarda y cómo se genera una buena llave privada. Dándose el caso, posible o real, de personas que extravían de manera irreversible sus bitcoins, por las cuestiones anteriormente mencionadas. El segundo punto es que se necesita tener cierto grado de familiaridad con cuestiones de cómputo para poder saber con precisión qué y cómo necesitamos proceder para lograr la seguridad apropiada, limitando considerablemente los usuarios. El tercer punto nos lleva a los exchanges y casas de cambio, al ser un tema en el cual no todas las personas que emplean bitcoin quieren adentrarse, los exchanges nos ofrecen ser el intermediario entre nuestras monedas y nuestras carteras. Por lo cual tenemos una solución atractiva para no tener que preocuparnos por estos tecnicismos y comenzar a usar bitcoin rápidamente. Creando una transferencia de responsabilidad, es decir la seguridad, en este caso, depende de las casas de cambio y no de los particulares.

Los exchanges lo que hacen, recordando brevemente pues se desarrolló ya este tema en el primer capítulo, es, similar a un banco, darle la opción a un usuario de crear una cuenta dentro de su plataforma en la que puede vender y comprar bitcoin pero, en última instancia el usuario es dueño de su cuenta en el exchange y no de sus monedas directamente. Es decir la casa de cambio actúa como un tercero o intermediario entre nuestras bitcoins y nuestra cartera en una transacción. Hoy en día los exchanges tienen sistemas de seguridad avanzados y están en constante desarrollo para darle un buen servicio a sus clientes, sin embargo, existen casos muy famosos como el que se vio en el tercer capítulo del exchange llamado Mt.Gox, en el cual se perdieron 650,000 bitcoins al declarase en banca rota en el 2013[52].

Por lo tanto, la seguridad es un punto muy importante al hablar de bitcoin, pues uno no sólo es su propio banco sino que, al no estar regulado por alguna institución central o gobierno, cualquier persona puede llegar a crear un "banco" como tal, es decir un exchange, teniendo los

[52] "Este punto se retomará y profundizará en el apartado de tipologías de usuarios.

conocimientos apropiados, la seguridad y confianza de sus usuarios. Esto nos lleva a esbozar una primera conclusión, vinculada a la regulación. Aunque no exista un órgano que regule directamente a bitcoin, podemos observar que con las casas de cambio se puede comenzar a esbozar un tipo de regulación, pues es a través de estas casas de cambio que uno compra y vende al precio que ellos establecen. Del mismo modo que uno es su propio banco o podemos llegar a formar nuestro propio banco, nosotros podemos fijar el tipo de cambio, dentro de las variaciones aceptadas que se tienen, al vender o comprar bitcoin.

Un punto derivado del anterior, en el sentido de la iniciativa personal es aquel de la anonimidad. La anonimidad depende del uso en general que tengamos y las prácticas que tengamos con bitcoin y en Internet. Es decir, si decidimos tener una dirección con la que no queremos que nos relacionen, pero al navegar en internet no usamos ningún tipo de seguridad en cuanto a la privacidad y el anonimato, resulta mucho más fácil que vinculen nuestra dirección de bitcoins a nuestra identidad. Lo mismo se da para el caso contrario, en el que tenemos un uso de Internet al igual que de nuestra computadora y en general buena consciencia para ser anónimos, pero no tenemos buenas prácticas al usar bitcoin, como por ejemplo usar una dirección más de una vez, entonces nuestra anonimidad se vería comprometida.

Por lo tanto con estos dos puntos podemos comenzar a esbozar dos conclusiones. La primera es que sí llega a existir un tipo de regulación. La segunda es la iniciativa personal y el interés propio que uno debe de tener para entender a fondo la moneda, para que, de ese modo uno comprenda que pasa al usar un exchange o los riesgos que conlleva no respaldar nuestras llaves privadas, o como ser verdaderamente anónimos. Característica que, comparada con las monedas nacionales o fiduciarias no tiene tanta relevancia, pues uno no necesita saber cómo funciona el peso, y las instituciones que resguardan los pesos mexicanos, para poder conservar sus monedas y ahorros como tal, e incluso emplearlas.

En otras palabras, podemos decir que existe una barrera tecnológica con bitcoin, que no existe con las monedas fiduciarias, pues para ganar un peso mexicano y gastarlo no es necesario, ser o saber cuestiones de computo que garanticen la seguridad y pertenencia de nuestros pesos. O visto de otro modo, podemos declarar que a algunos de los usuarios de bitcoins requieren una serie de conocimientos adicionales al que tendríamos que tener en comparación con una moneda fiduciaria. Se dice que algunos de los usuarios, pues no todas las personas que usan bitcoin saben

a profundidad cómo funciona internamente al igual que los mecanismos necesarios para hacer uso pleno, seguro y anónimo, de la moneda.

Esto nos lleva a una reflexión, en la cual con bitcoin tenemos la posibilidad de saber cómo es que se crea, se procesa y se pueden almacenar nuestras monedas, así como otras características que no pueden ser comparables con las monedas fiduciarias, de instituciones centralizadas como los bancos. Si bien puede parecer una comparación injusta, ésta deja de serlo en la medida en que entendamos que existe una regulación en ambas, aunque por más pequeña que sea, en bitcoin se comienza a esbozar y de igual modo se ocupa y está en contacto directo con el dinero fiduciario.

El segundo tema a tratar es la centralización, hay dos ámbitos en los que podemos hablar de centralización. El primero es con los mineros, y el segundo es con el uso en sí de la moneda. Desarrollando el primer ámbito; se dice que la red de bitcoin es una descentralizada, en la cual cualquier persona tiene la misma oportunidad, nivel de jerarquía e importancia en general. Sin embargo, como se habló ya en el apartado de los fondos de mineros en el capítulo primero, existen unos en los cuales participan muchas personas en conjunto para hacer el minado. Es por esto que podemos hablar de cierto grado de centralidad en la minería. Pues en los momentos críticos en los que se tiene que tomar una decisión, ya sea que afecte a toda la cadena de bloques o simplemente en cómo se procesan transacciones o nuevas reglas, así como posibles mejoras, los fondos más grandes tienen un voto más significativo que los más pequeños.

El segundo ámbito en el cual podemos hablar de centralización es en el uso que se tiene de bitcoin, es decir tenemos una mayoría de uso virtual, una centralización en su uso. Esto es una conclusión clara pues con bitcoin no podemos comprar algo tan fácilmente como con los pesos mexicanos, como por ejemplo unos chicles en un puesto en la calle, una revista o periódico.

Es decir, aunque sea una red descentralizada podemos observar dentro de su uso una centralización notable, en la cual se mueve una cantidad muy grande de dinero. Vista en dólares tenemos que se mueven miles de millones de dólares. Por lo tanto podemos esbozar también una conclusión en la que comenzamos a ver centralización, por parte de los mineros y los fondos de minería quienes tienen un gran poder de voto para las decisiones del futuro de bitcoin. Al igual que centralización en el uso, es decir no existe una diversidad de las maneras en que se emplea la moneda. La principal es entonces el uso en Internet.

Es importante comprender los puntos que se han desarrollado hasta este momento, pues de no ser así sería fácil pensar en bitcoin como una moneda con una administración o manejo un tanto democrático por la red de par a par. Similarmente si observamos que no existe ningún órgano o institución central que regule y que nos de algún tipo de garantía es fácil otorgarle cualidades a bitcoin que no tiene o que parecería que tuviera.

Es una moneda que aunque no tenga claras instituciones centrales, podemos observar a los mineros, quienes son los que tienen una inversión muy grande de dinero y recursos para hacer que la red funcione como tal, al igual que su voto para decidir en qué dirección se desarrolla. Paralelamente es verdad que se tiene un manejo de la moneda con una red descentralizada de par a par, como ya se explicó en el primer capítulo, sin embargo esto no garantiza que un minero individual con mucho menos poder de cómputo en comparación al de todo un fondo tenga el mismo peso en la toma de decisiones para implementar una mejora o una diferente manera de procesar un transacción.

Un breve comentario para terminar de redondear la reflexión sobre la centralidad y unirlo con el que ya se explicó de la regulación es sobre los desarrolladores. Estas personas son las encargadas en estar modificando, mejorando y sugiriendo mejoras para el código interno de bitcoin, como se expuso en el capítulo segundo. Estas personas están familiarizadas con la computación, así como con la programación y al paralelo con los mineros serían los encargados o lo más cercano que tendríamos en bitcoin en cuanto a una regulación como tal.

Una vez que se ha dicho cuales son las dos entidades que tienen más peso en la regulación podemos entonces ver en quien está depositada la confianza, directa o indirectamente. Hablo de depositar confianza directa o indirectamente pues en las instituciones centrales, como por ejemplo un banco, al tener una cuenta en él, estamos de un modo u otro aceptando los términos de uso, al igual que tenemos cierto grado de confianza en la institución para manejar nuestros ahorros y finanzas. Entendida la confianza al usar bitcoin, del mismo modo en el que las personas confían su dinero a un banco observamos algo muy sugerente. En otras palabras al comprar bitcoin lo que estamos haciendo es invertir en última instancia, si omitimos el tema de la confianza, en un bien digital con una comunidad abierta en la cual todos podemos acceder, siempre y cuando tengamos los conocimientos, propuestas adecuadas y demás características que ya se mencionaron. Una comunidad hecha por criptógrafos, matemáticos, mineros y

desarrolladores, que como se mencionó en el capítulo dos, tiene ventajas claras frente a una institución privada cerrada al público.

Se ha dicho que se puede omitir el tema de la confianza pues no necesariamente por usar bitcoin confiamos en el sistema y las personas que lo respaldan así como sus mecanismos internos. Se puede dar el caso de alguien que sin entender las cuestiones de fondo y de seguridad criptográfica, quiera tener una pequeña inversión para ver empíricamente cómo funciona. Paralelamente confiemos o no en el sistema si llegamos a comprar bitcoins lo que estamos haciendo es, en términos básicos, invertir, dar dinero y trabajo a los mineros. Esto nos lleva a una reflexión profunda sobre que significa invertir o comprar fracciones o una bitcoin entera, puesto que hacer una transacción implica no sólo una ganancia y trabajo para los mineros, sino que aumentamos la cantidad de bitcoin que hay[53] y en última instancia hacemos que alguien que tenía bitcoin tenga ahora dinero fiduciario. Es decir se puede ver como una compra de acciones de un activo digital, en este caso efectivo de internet, en el cual nosotros gastamos dinero fiduciario, desde la perspectiva del comprador, para recibir una fracción de este activo.

Si hablamos por lo tanto de un activo digital o bien nos encontramos con uno con muchas características. Es un activo que ha demostrado ser muy popular, tiene un aumento de precio constante, así como todas las características técnicas que se han mencionado ya de la moneda en el primer capítulo. Sin embargo, si observamos los inicios de bitcoin en el 2009 cuando no había personas que lo compraran, o un mercado como tal, entonces podemos considerar a Satoshi Nakamoto o la entidad responsable de minar el primer millón de bitcoins, como uno de los accionistas más grandes, o acumuladores más grandes de este activo.

Es atractiva la idea de plantear bitcoin como una acción de una empresa, pues como hemos observado en el tercer capítulo de uso, no se puede emplear tan fácilmente como moneda. Si exploramos la idea de bitcoin como una acción, entonces tenemos que describir primero qué tipo de empresa sería bitcoin. La empresa de la cual estamos hablando sería una que estaría administrada globalmente, ya que los mineros están distribuidos por muchas partes del mundo, paralelamente existen computadoras con el libro mayor de la empresa en el cual podemos ver qué acción le pertenece a quién y todos los movimientos que han ocurrido con dichas acciones.

[53] Por cuestiones de practicidad no se explicará nuevamente los detalles de la creación de bitcoin, pues esto se desarrolló en el primer capítulo.

Hablando de los socios mayoritarios tenemos muchas personas que compraron bitcoin cuando su precio era muy reducido como Trace Mayer, con quien tuve la suerte de platicar en el congreso de anarquistas capitalistas en Acapulco, o alternativamente Satoshi Nakamoto quién al momento de que se minen todas las 21 millones de monedas tendrá aproximadamente el 5% de la totalidad.

Un punto en donde se consolida la idea de comparar a bitcoin con las acciones de una empresa es el de las ganancias. Podemos relacionar la gran subida de precio que ha demostrado bitcoin a lo largo del tiempo como una demanda y compra, alta y constante de acciones respectivamente. Si hablamos de la volatilidad que tiene bitcoin se puede relacionar a una acción de alto riesgo o una inversión riesgosa. Alternativamente la volatilidad de la moneda puede verse como una empresa que no tiene ninguna garantía o respaldo y que podría caerse o quebrar de un momento a otro. Si consideramos las bitcoins como acciones de una empresa, entonces las acciones de nuestra empresa están limitadas a 21 millones, como se explicó en el primer capítulo, esto es cuando los mineros no puedan producir más bitcoins, o en su caso en donde las acciones de la empresa se terminen por el mismo diseño de la empresa. De este modo es en el que tenemos dinero como tal entrando a la empresa, si hablamos de las ganancias que una empresa tiene por vender acciones. Cuando estas acciones se acaben y no se puedan producir más, entonces me atrevería a decir que podríamos observar realmente a bitcoin como una moneda. Ya que se acabaron de distribuir todas las acciones de la empresa y se conformó como tal, sería posiblemente en ese momento que bitcoin se convertiría en algo más que una acción o un bien digital.

La “venta de acciones” se puede ver entonces como el simple hecho de que alguien compre bitcoin. De tal forma que si yo compro 50 pesos en bitcoin y obtengo 0.05 bitcoins al tipo de cambio de ese momento, entonces yo doy a la empresa 50 pesos a cambio de 0.05 “acciones” de bitcoin. Se habla mucho del precio en el que está y que ha estado subiendo constantemente, sin embargo hablando de cálculos, el que nos corresponde es aquel de la venta que hacen los mineros de sus bitcoins al minar las monedas que obtienen. Esas serían las acciones directas o las que más se asemejarían a las acciones, pues se puede dar el caso de una transacción de una bitcoin pero que ya pasó de una mano a otra y no necesariamente vino del trabajo de un minero.

Tener bitcoin implicaría entonces formar parte de una empresa la cual, no tiene un gobierno ni una institución central, pero que está limitada a internet como tal, es decir con los matices que ya

se han estado mencionando sobre la regulación y la centralidad. La idea de bitcoin como una acción de una empresa no se encuentra tan alejada a la realidad, pues en la fecha del congreso de Anarchapulco, estaba en discusión la inclusión de bitcoin como un fondo de inversión cotizado en la Bolsa de Valores de Nueva York.[54]

Si regresamos a los matices de bitcoin, el tercer tema que nos ayuda a matizarlo es la internacionalidad. Es verdad que es una moneda internacional y que podemos hacer transacciones muy rápidas e incluso instantáneas de un país a otro pero todo esto depende del Internet. Es necesario tener una conexión a Internet para poder usar bitcoin y hacer una transacción, esto es entonces una internacionalidad condicionada. Suena un tanto confuso plantearlo de este modo, pero la frontera, a modo de país, que tiene bitcoin entonces es internet. En lugar de que sea o no aceptada o posible de usar en tal o cual país, lo que limita y posibilita el uso de bitcoin es Internet como tal.

El último y cuarto tema a tratar en la misma línea de estos matices de bitcoin es la cadena de bloques como tal. Se habló ya a lo largo de toda la investigación, específicamente en el primer capítulo, de qué es y cómo funciona la blockchain. Recordando unas cifras y para refrescar la memoria del lector tenemos que al 16 de noviembre del 2017 la cadena de bloques tiene un tamaño electrónico de 133.2 GB (Bitcoin.com, 2017b). Para poner en perspectiva dicho número si tomamos la información del Directorio Estadístico Nacional de Unidades Económicas (DENUE)[55], el Banco de Indicadores, el Inventario Nacional de Viviendas, Microdatos y la Sala de prensa por área geográfica, proyectos, años de la información, temas y formatos del Instituto Nacional de Estadística y Geografía (INEGI) para todo México, de los años 2015 a 2017 (Geografía (INEGI), 2017) el tamaño de dicha base de datos es de 6.21 GB. Por lo tanto el libro mayor es 21.4 veces mayor que las bases de datos antes mencionadas de 3 años diferentes para todo México.

Si hablamos en número de páginas tendríamos un libro mayor a la misma fecha con 494,544 páginas, tomando en cuenta que una página contiene toda la información de un bloque, donde

[54] Al 10 de diciembre del 2017, fecha que no corresponde a mi trabajo de campo, tenemos que se aceptó bitcoin en el Chicago Board Options exchange CBOE en ingles que es un mercado de opciones financieras. (coindesk, 2017h)
[55] El DENUE es una base de datos en donde se ofrecen la identificación, ubicación, actividad económica y tamaño de los negocios en todo el territorio mexicano, en el cual se tienen contabilizados a 5,053,130 negocios diferentes. (Geografía (INEGI), 2014)

cada bloque tiene aproximadamente 263,000 transacciones en promedio, esto de lo que hemos definido como la *Zona* 3. Se hace hincapié en el tamaño de la cadena de bloques porque se nos plantea como algo abierto al público y algo que todos podemos ver y analizar, cosa que es cierta. Al igual que existen páginas en las cuales podemos revisar qué transacciones ha recibido y enviado qué dirección; pero si queremos hacer un análisis a fondo, en la práctica es muy difícil pues, no sólo cada día crece la cadena sino que es necesario saber obtener la información que queremos[56] de la cadena de bloques y más tarde analizarla a detalle. Uno de estos análisis lo he citado en la investigación, en el tercer capítulo, es el que habla sobre el polvo y las monedas "zombi" de John W. Ratcliff (LetsTalkBitcoin.com, 2014).

Paradójicamente habría que hacer minería de datos, a la cadena de bloques, para obtener información que va más allá de lo que las páginas nos permiten ver a simple vista. La cadena de bloques se nos presenta entonces como un registro abierto al público en dónde se encuentran todas las direcciones en toda la historia de bitcoin, pero para poder hacer un análisis cualitativo de la información que se nos presenta ahí es necesario no sólo saber y escribir un programa sino que tener un poder de computo o el tiempo disponible para analizar 20 veces más la información de todo México de 3 años diferentes, del DENUE y de las diferentes bases de datos de las que se habló en los párrafos anteriores.

Una vez que ya se han tocado los varios matices que podemos observar de bitcoin, ahora considero necesario hablar de la tipología de usuarios de bitcoin. En esta sección de las conclusiones no se hablará de usuarios específicos, sino que se intentará exponer las razones más generales que las personas tienen para usar bitcoin y definir ciertas diferencias entre uno y otro.

Los primeros usuarios que me parecen los más adecuados para comenzar a describir son los mineros. De ellos ya se ha hablado en abundancia y de la labor que hacen, sin embargo la manera en la que emplean bitcoin a diferencia de todas las personas que lo compramos, es trabajando para obtenerlo. Se le llama trabajo a la actividad que hacen de mantener muchos procesadores y súper computadoras activas y en buen estado, al igual que estar al día de todas las mejoras tecnológicas y de cualquier posible falla en sus sistemas. Como existe la minería de muchas posibles monedas también existe la posibilidad de solventar otros costos, como la luz por

[56] Es decir usar código que ya está programado o programar uno su propio código para extraer de la cadena de bloques la información que tiene. Pues toda la información está en lenguaje de computadora, y son ellas las que lo procesan.

ejemplo, minando altcoins mencionadas en el segundo capítulo. También se menciona el estimado de ganancias si nos uniéramos a la minería en noviembre del 2017 en el primer capítulo, pero lo más importante es que este grupo de usuarios son los que hacen, producen o imprimen como tal bitcoin.

De aquellas monedas que crean o el mismo sistema les otorga, reinvierten algunas de esas monedas pues es necesario pagar la cuenta de luz y estar al corriente de toda la tecnología detrás de bitcoin. De igual manera necesitan tener los procesadores en buen estado, y actualizados para las necesidades y crecimiento de la red.

Los segundos usuarios de los que podemos hablar son unos que se pudieron haber visualizado en lo que se mencionó en las primeras páginas de las conclusiones, donde se habló sobre las 650,000 monedas extraviadas de Mt. Gox. Es decir, éstos son los usuarios que hacen uso de bitcoin de forma ilegal y buscan una ganancia de este modo. Dentro de este apartado podemos incluir a todas las personas que usan bitcoin con cualquier tipo o forma de ilegalidad, como puede ser por ejemplo el lavado de dinero, compra de artículos ilegales en la llamada deep web[57], los ataques de ransomware,[58] y el hecho por el cual surgió este tema, que son fraudes y robo a las personas en los exchanges. Esto no quiere decir que todos los exchanges sean fraudulentos, pero sí se han llegado a dar por lo menos 7 otros casos en los que los hackers han ingresado a otros exchanges o se han declarado en banca rota por hackeo. (Lee, 2017) Gracias a este punto podemos tocar un tema de bitcoin que se menciona indirectamente, que es, al ser una moneda sin regulación, con posible anonimidad las personas lo han usado para enriquecerse de manera ilegal.

Otro punto importante es que no por este tipo de uso tenemos que dotar de negatividad a bitcoin y a la deep web, pues son simplemente tecnologías que nos permiten hacer cosas en anonimato.

[57] Deep Web es simplemente un internet anónimo. Es un modo de navegar en Internet en el cual nadie sabe quién es quién. Para explicarla pensemos en la analogía en la cual el Internet actual o de la Superficie sería lo equivalente a salir a la calle y que todo mundo supiera quién eres, de dónde eres, dónde has ido, un historial de lugares que has querido ir, así como quiénes son tus amigos y cómo te relacionas con las personas con las que tienes amistades. En comparación, la Deep Web es aquella en la que sales a la calle y nadie sabe quién eres, qué amigos tienes, cuáles son tus preferencias y en general se es anónimo al "salir a la calle", que en este caso sería el navegar.

[58] Ransomware es un nuevo tipo de ataque cibernético en el cual se encripta el disco duro de una computadora con un programa y se le pide al usuario de la computadora un pago con bitcoins para que el programa desbloqueé el disco duro y con ello toda la información de la computadora.

Si hubiera otro tipo de red y moneda con mayor seguridad y anonimidad es seguro que la deep web y bitcoin serían remplazadas muy fácilmente. Al igual que anonimidad no implica directamente ilegalidad, pues se puede también usar la anonimidad, de la deep web, por ejemplo para ejercer libertad de expresión o de prensa y tener algún tipo de remuneración con donaciones de bitcoin por dicho ejercicio.

Tenemos entonces un segundo tipo de usuarios que son aquellos que emplean o han empleado bitcoin con fines ilegales para hacerse ricos. Recordando brevemente, el volumen diario de intercambio de bitcoin es muy grande, existe una alta volatilidad en la moneda, se puede hacer en cualquier lugar del mundo que cuenta con una conexión a Internet y sobre todo existe la posibilidad de que esto sea anónimo. Se podría ver, así como se menciona que existen paraísos fiscales, en este caso tenemos en nuestras manos una lavandería paradisiaca.

Un tercer tipo de usuarios son aquellos que compran bitcoin como inversión, ya sea a corto o largo plazo. Estos usuarios se pueden caracterizar como aquellos que están en atención constante del precio, cuando baja o creen que esté suficientemente bajo compran bitcoin, de igual modo cuando piensen que esté en su máximo o antes de que una burbuja explote venden para obtener una ganancia notable de su inversión. Dentro de estos tipos de usuarios puede estar también los que compraron una vez bitcoin, como se mencionó a manera de acción, y no han hecho más movimientos, esperando que bitcoin llegue a algún valor deseado o extremadamente alto.

Un cuarto tipo de usuarios que es muy similar al que se acaba de mencionar antes es aquel que compró bitcoin cuando estas costaban muy poco, un ejemplo de alguien así, es Trace Mayer con quién tuve el privilegio de platicar en Anarchapulco, que compró bitcoin en 2010 a centavos de dólar. Se les conoce como “early adopters” y son personas que tienen mucho peso en la comunidad de bitcoin, pues en general se les considera como líderes de opinión y son consultados en las cuestiones y debates sobre el futuro de bitcoin. Otro rol que cumplen los “early adopters” es que están promoviendo el uso de bitcoin, ya sea en conferencias, en videos en Internet, en sus cuentas de las redes sociales. Se les puede considerar como promotores de la moneda.

El quinto tipo de usuarios son los que venden bitcoin como tal, es decir los distribuidores. Estos usuarios se distinguen de los mineros y de los inversionistas que venden bitcoin, porque su

actividad principal es actuar como intermediario o punto de venta de bitcoin. Dentro de estos usuarios se encuentran todas las personas afiliadas a MaxSaldo, como César Lemus por ejemplo, al igual que todas las tiendas de conveniencia Oxxo y 7-Eleven que eran aproximadamente 29,000 en el 2016 (Forbes, 2016). En estos usuarios también podemos observar a las personas que usan la página de LocalBitcoins (LocalBitcoins, 2017), así como los exchanges que dentro de México tenemos a Bitso e ISBIT (ISBIT, 2017), al igual que Volabit que no es concretamente un exchange sino que es una empresa dedicada a la venta de bitcoin. (Volabit, 2017)

El sexto tipo de usuarios que podemos esbozar son aquellos que usan bitcoin por cuestiones de ideología, como por ejemplo todos aquellos que forman parte de Anarchapulco. Es decir anarcocapitalistas libertarios, que usan bitcoin por cuestión de principios al igual que tienen un uso regular de la moneda y se puede decir que viven o sobreviven intentando usar solamente criptomonedas lo más que puedan.

El séptimo y último tipo de usuarios, un tanto contrario al anterior mencionado, son aquellos quienes aceptan bitcoin ya sea por cuestiones de practicidad en sus negocios, por los beneficios en el uso al cobrar en bitcoin, por darle algo adicional a su negocio como puede ser recibir y aceptar bitcoin. Se mencionan los beneficios al cobrar en bitcoin pues como no está regulada y en México se comienza a esbozar una ley de criptodivisas y bienes digitales resulta fácil la evasión de impuestos, pues se paga directamente en efectivo electrónico a través de Internet el bien o servicio ofrecido.

En el caso de que bitcoin en verdad fuera un tipo de esquema piramidal, o como fue planteado en el capítulo 3, si fuera un volcán durmiente con varias cumbres o picos los cuales podrían explotar en cualquier momento, podemos hablar de un octavo tipo de usuario. Este usuario sería aquel que participa en el esquema y es convencido, a manera de pirámide, que el invertir en este producto lo volverá rico en la medida que convenza a 10 personas o más en usar e invertir en bitcoin. La adopción de bitcoin por este tipo de usuario puede ser puramente pasional o el rendimiento de la inversión de bitcoin, y una prueba de que funciona y de cómo funciona, pueden ser incentivos suficientes para comprar dicha moneda.

Tal vez podríamos hablar de un noveno tipo de usuario y este seríamos las personas quienes estamos estudiando bitcoin. Yo participé en la compra de bitcoin, al igual que la usé como

moneda para comprar tacos, pizzas y comics, sin embargo nunca participé en la venta más que en pequeñas cantidades a personas cercanas y amigos. Por lo tanto se podría decir que la actividad principal de este tipo de usuarios son los que la estudian como tal, y efectúan algunas de las prácticas de la moneda para entenderla y comprender su uso y alcance.

Es con esta última tipología que procedo ahora a hablar de las reflexiones y conclusiones que me ha dado bitcoin, en el ámbito personal y posteriormente en un ámbito más general: el antropológico.

Antes de comenzar me parece relevante hablar un poco del contexto en el que me parece que está situado bitcoin. Este es un contexto el cual está condicionado altamente por Internet, pero es en esencia una red que ha estado activa desde el 2009 hasta el 2018, y no parece que vaya a tener días de descanso. Si hacemos una analogía del mundo físico y la tierra como tal vemos que tarda 24 horas para cumplir un ciclo, comparativamente, en el mundo digital tenemos que lo que podríamos llamar un día ocurre más rápidamente en este entorno.

Respectivamente con los bancos, ellos tienen un horario fijo de funcionamiento así como no están conectados de la misma manera como lo está conectado bitcoin. Por ello podemos entonces decir que el mundo digital es un mundo más rápido o alternativamente sin ciclos, o sin descanso en el cual están constantemente haciéndose transacciones en todas partes del mundo sin ningún horario de atención o fijo como tal.

Esta idea se podría desarrollar todavía más en varios ámbitos, desde la creación de lo “social” en las redes sociales, la información transmitida, “minada” y en general el movimiento de información del Internet. Al ser una red usada a lo largo de todo el mundo tenemos siempre creación y movimiento de datos. Lo que ahora nos queda sería plantear o encontrar un modo o lugar donde comparar el mundo virtual al mundo real, para de este modo ver cual transcurre más rápido o para simplemente hacer un ejercicio mental de la diferencia de ambos mundos.

El espacio que tengo en mente es un casino de Las Vegas, o cualquier tipo de casino que está aclimatado para que parezca que el tiempo no transcurre, o como si pareciera que fuera de día todo el tiempo. Esto nos lleva a un dato interesante que es: las direcciones más usadas en la red de bitcoin son aquellas de casas de apuestas en línea usando bitcoin (Blockchain Luxembourg

S.A.R.L, 2017e)[59]. Siguiendo con los casinos tenemos entonces que se puede cambiar con dólares por poner un ejemplo, a las fichas del casino que en este caso serían las criptomonedas o bitcoin en el mundo virtual. Es entonces que todo el conjunto que se tiene de diferentes juegos e interacciones, como las máquinas que otorgan a uno un beneficio o pérdida dependiendo de las habilidades o de la suerte de uno, serían las fluctuaciones de bitcoin o la perdida repentina o fallo de cualquier sistema que usamos para almacenar nuestras monedas.

Aquí podemos relacionar lo que se dice de bitcoin, que es muy volátil y es también de este modo que uno puede obtener, en un casino, ganancias muy rápidamente o perderlo todo en un instante. Esta es una buena analogía, pues representa la atemporalidad de bitcoin; es decir que la red no se detiene nunca y se está minando, "están abiertas las puertas del casino", a quien sea que quiera entrar o usar la red y validar una transacción o hacerla, "cambiar dólares por fichas de casino y apostar".

Una vez planteado este casino como el contexto en el cual bitcoin se desarrolla podemos plantear situaciones un tanto imaginarias para poder llegar a algunas reflexiones. La primera es aquella en la que un empresario como Jamie Dimon jefe del banco JP Morgan, entre a uno de estos casinos, compre muchas fichas y tenga una pérdida considerable en alguna de las máquinas o apostando. Es así que se podrían ver desencantados los banqueros al tener este tipo introducción o acercamiento a la moneda y dar la siguiente declaración: "La divisa no va a funcionar. No puedes tener un negocio en donde las personas inventen una moneda de la nada y pensar que las personas que la están comprando son muy listas." (Monaghan, 2017)

Esto puede hacernos ver bitcoin como una "lección" a los banqueros o especuladores en donde desacreditan públicamente la moneda, y ésta llega a un precio y un aumento en su valor, un rendimiento nunca antes visto siendo completamente virtual, sin ningún gobierno y ningún tipo de regulación. La lección sería, una en la cual sin ningún tipo de regulación y centralización, el aumento de precio de un bien o valor económico, que es virtual, adquiere un crecimiento nunca antes visto. Puede verse o bien como una lección o una oportunidad, que estoy seguro que los especuladores más grandes, o notables desaprovecharon.

[59] Al 21 de diciembre del 2017 la dirección más usada de bitcoin es una con 3192185 entradas y le corresponde a una página llamada SatoshiDICE que es una casa de apuestas en Internet.

Tal es el caso de Tidjane Thiam director general de Credit Suisse, Warren Buffet inversionista multimillonario y Ray Dalio, quien es fundador de uno de los fondos de inversión de alto riesgo más grandes del mundo. Donde declaran que: "De lo que podemos identificar, la única razón hoy en día para comprar o vender bitcoin es para hacer dinero, que es la definición misma de especulación y la definición misma de una burbuja"(De, 2017a), "No se puede valuar bitcoin porque no es un bien que produzca valor" (De, 2017b) y por último "(bitcoin) No es almacenamiento efectivo de riqueza porque tiene volatilidad a ella. bitcoin es un mercado altamente especulativo. bitcoin es una burbuja" (De, 2017c) respectivamente.

Esto nos habla de un descrédito público por parte de autoridades financieras como lo son, directores generales de bancos con una influencia considerable a nivel mundial, un inversionista multimillonario y el fundador de uno de los fondos de inversión de alto riesgo más grandes del mundo. Al igual, nos habla también de cómo consideran, públicamente, la divisa estos actores financieros. Curiosamente si analizamos el precio de bitcoin unos días después de sus declaraciones vemos una tendencia a la baja. Al momento en que Jamie Dimon hizo su declaración, el 12 de septiembre del 2017, se encontraba en 4,143.18 dólares y después de 3 días el precio bajó a 2,976.56 dólares un bitcoin (coindesk, 2018). Con la declaración de Ray Dalio tenemos un movimiento de 3,901.35 dólares el 19 de septiembre a 3,527.79, 3 días después (coindesk, 2018b). Similarmente con la declaración de Tidjane Thiam observamos un movimiento de 7,029.98 dólares el 2 de noviembre a 10 días después en 5,617.69 dólares un bitcoin (coindesk, 2018c).

En palabras del mismo Tidjane Thiam, "la única razón hoy en día para comprar o vender bitcoin es para hacer dinero" (De, 2017a) y si bien no nos consta que él haya comprado bitcoin o el motivo último de su declaración haya sido ganar dinero, su declaración generó la oportunidad de comprar bitcoin aproximadamente 2 mil dólares abajo del precio de diciembre, o al precio promedio de octubre del 2017[60]. Esta es una situación similar en todas las demás declaraciones, pero solamente se analizó la más significativa, que es la declaración de Thiam. De la misma manera aunque sean declaraciones negativas hacia bitcoin, éstas hacen que el tema adquiera

[60] El costo promedio de en todo el mes de octubre del 2017 fue de 5,275.23 dóalres un bitcoin. Dato obtenido con el precio diario de octubre del 2017 de: (Bitcoin.com, 2017e)

mucha más popularidad, pues es un tema digno de mencionar de las personas anteriormente mencionadas que tienen un peso considerable en el sector financiero.

En una escala más grande y en otro sector que puede mostrar también cierto descredito, es decir los países, tenemos que en los siguientes la moneda es ilegal: Argelia, Marruecos, Bolivia, Ecuador, Kirguistán, Bangladesh, Nepal e Islandia. Esto es al 9 de enero del 2018 de acuerdo a Wikipedia. (Wikipedia, 2018) Sin embargo esta lista puede ser engañosa, pues de acuerdo a ésta existen países como Portugal en donde se menciona que es legal pero también se dice que no existe ningún marco jurídico específico para bitcoin. Por lo tanto podemos agregar dos términos más, el primero es aquel donde bitcoin no tiene un marco legal y tiene muy pocas regulaciones, el segundo es donde sí existe un marco legal o bien está regulado de un modo u otro. Si contamos el primer conjunto de países el total es de 44 países[61], por el contrario si vemos el segundo conjunto tenemos solamente 17 países[62]. Es decir, tenemos a lo largo del mundo 8 países en el cual el casino que se ha planteado unos párrafos antes es ilegal, 44 países en donde no está regulado y 17 en los cuales existe por lo menos algún tipo de regulación hacia ellos. Datos obtenidos de (Wikipedia, 2018) y corroborados con (Staff, 2016) y (Bitconnect.co, 2018).

Si regresamos a las palabras de Tidjane Thiam, especular entra en contacto directo con la compra y venta de bitcoin para obtener una ganancia y a lo que llama una burbuja. Es verdad que bitcoin se presta para la especulación como cualquier otro instrumento financiero, bien o activo, al igual que para la formación de burbujas. Sin embargo nos podemos preguntar: ¿cómo es que una moneda inventada de la nada, como dice Jamie Dimon, puede tener un rendimiento y un crecimiento mayor al oro, al igual que prestarse para la especulación, para la posible adquisición de personas en el sector financiero norte americano o simplemente para hacer una declaración oficial y al público de dicha moneda?

[61] Nigeria, Sudáfrica, Namibia, Zimbabue, México, Nicaragua, Jamaica, Trinidad y Tobago, Brasil, Chile, Colombia, Chipre, Arabia Saudita, Jordania, Líbano, Turquía, India, Pakistán, Hong Kong, Corea del Sur, Taiwán, Indonesia, Malasia, Vietnam, Croacia, Polonia, Romania, Eslovaquia, Ucrania, Dinamarca, Estonia, Lituania, Rusia, Bosnia Herzegovina, Grecia, Italia, Malta, Portugal, Bélgica, Irlanda, Países Bajos, Reino Unido, Australia y Nueva Zelanda.

[62] Argentina, Israel, Japón, Filipinas, Singapur, Tailandia, República Checa, Alemania, Eslovenia, Suiza, Finlandia, Noruega, Suecia, Bulgaria, España, Francia y Luxemburgo.

La respuesta que yo encuentro más relevante, con todas sus críticas, es aquella en la cual las personas y todo el entorno de bitcoin, que incluye un mercado y los que lo mantienen, son capaces de convertir un sistema digital de efectivo, que en el 2009 no tenía valor de mercado alguno, en un bien virtual. Un bien con alta demanda o demanda en aumento, un bien con alto rendimiento de ahorro, transacciones rápidas, pero bajo uso monetario. Un bien que aumentó su precio por su demanda, entre otros factores, en toda su historia un 18,611,600%[63]. Tal vez es una conclusión un tanto precipitada y existen muchos otros factores más que influencian el crecimiento, pero un hecho que no podemos negar es que un bien digital pasó de no tener ningún tipo de valor a valer algo, y es en ese momento que existe un aumento de precio sin igual, de 0, es decir nada, a 0.05. Se puede ver equiparable al nacimiento de un bien o moneda de intercambio para una sociedad digital o basada en Internet.

Regresando a la situación imaginaria del casino una reflexión importante de abordar es la velocidad de las transferencias, la practicidad de las mismas y lo rápido que cambia de valor bitcoin. Esto es equivalente a lo rápido que sería intercambiar nuestras fichas de casino una vez que tengamos una ganancia, o simplemente recibir nuestras ganancias una vez que se nos son dadas, pero con un factor adicional que sería que los juegos y mecanismos de apuesta estén fluctuando muy rápido su valor. Esta situación hace que resulte un tanto secundario hacer cuentas en la vida real, es algo que pasa a segundo plano por la rapidez de cambio en bitcoin. Es de este modo que perdí la cuenta muy fácilmente de cuanto había y he comprado, aunque se puede checar fácilmente todo en la cadena de bloques.

Es decir que las bitcoins que uno tiene fluctúan tan rápido en el día y en general suben su valor así que “10” pesos iniciales, si tomamos ese ejemplo y aceptamos que esos pesos ya son bitcoin como tal, entonces para saber cuántas tenemos, es necesario checar la tasa de cambio, hacer la conversión y ver en cuánto están al día. Adicionalmente si esos 10 pesos iniciales son 0.1 bitcoin por ejemplo, gastamos en una compra 4 pesos que equivalen al momento 0.4 bitcoins, nos restan 0.06 bitcoins. Pero supongamos que la tasa de cambio es ahora de 15 pesos por 0.1 bitcoins tendríamos que hacer nuevamente una conversión para saber cuánto valen nuestros 6 pesos restantes de inversión al tipo de cambio de 15 pesos, por 0.1 bitcoins, (que nos daría 9 pesos al

[63] Esto si tomamos el precio más bajo de bitcoin es decir 0.05 dólares al 18 de julio del 2010 y tomamos el precio al 27 de noviembre del 2017: 9305.8 dólares.

nuevo tipo de cambio). Puede parecer una situación simple, y un tanto confusa, pero en la realidad se tienen muchos decimales más, y aunque es posible calcular la tasa de cambio y llevar una cuenta de cuanto uno ha gastado es difícil tener un balance de cuanto fue nuestra inversión inicial y cuanto equivale esa inversión inicial en bitcoin, para más tarde tener los cálculos de los mismos balances, después de haber hecho una transacción.

Antes de abordar los últimos puntos conclusivos de la tesis, considero necesario hablar sobre las limitaciones de la investigación, algunos puntos críticos en donde pudo haber fallado y por último los temas pendientes para investigar en un futuro.

Una primera limitación fue el no lograr una entrevista propiamente con los mineros y tener de ese modo un acercamiento más allá de los datos para entender su actividad, y tener de primera mano información etnográfica de estas personas que ayudan a mantener en lo más básico a la red de bitcoin. Otra limitación ya se ha señalado un par de veces a lo largo de toda la investigación es la cadena de bloques. Aunque se llegó a algunas conclusiones no fue posible hacer un análisis cuantitativo o económico de la distribución entre las bitcoins y las direcciones, u obtener el coeficiente de Gini o datos similares.

Un punto crítico en el que pudo haber fallado la investigación fue en no haber sido un promotor de bitcoin, en el sentido de explicar qué es e invitar a las personas a que conocieran la moneda, la usaran e incluso vender algunas fracciones a conocidos o personas. En relación a los temas pendientes por investigar u otros que se podrían desarrollar en investigaciones posteriores tenemos dos. El primero es uno no tan cercano a bitcoin, pero que influye como contexto en la creación de lo social en Internet y es la cuestión de la velocidad con la que se crean u obtienen datos, pues tenemos una mina de información, abierta las 24 horas, si estamos constantemente monitoreando los patrones de uso de todos los usuarios que se conectan a Internet. Desde la misma navegación que hace un usuario hasta los patrones con los que hace uso de sus aplicaciones se pueden obtener estos datos las 24 horas del día pues en todo momento existe gente conectada al Internet.

El segundo punto en el cual se podría profundizar la investigación es en los diversos usos que se le ha dado a la cadena de bloques y la tecnología de bitcoin. Hablando concretamente de uno de ellos, y recordando la conversación que se tuvo con Juan S. Galt en Anarchapulco, él me

mencionó un sistema de validación similar al de bitcoin llamado Proof of Stake para implementar un sistema de votación (el sistema de validación de bitcoin es llamado Proof of Work y es el problema que resuelven los mineros). En este tipo de variación de la cadena de bloques en lugar de tener cierto número de bitcoins y que eso nos haga tener cierta cantidad de riqueza, lo que se acumula en lugar de riqueza es poder de voto para tomar alguna decisión. Es así que se podría plantear una investigación analizando los diversos usos que se le puede dar a la cadena de bloques, e incluso llegar a plantear una implementación, o una criptomoneda con fines antropológicos como una moneda comunitaria por ejemplo.

Dejando de lado la situación imaginaria del casino y los puntos evaluativos de la investigación, quiero retomar la analogía que introduje en el tercer capítulo. En él se menciona la idea de ver bitcoin como si fuera el rey Midas. Una vez planteado todo el análisis que ya se ha hecho podemos hacer algunas preguntas, retomando la idea de bitcoin como rey Midas. Esto con él fin de abordar las conclusiones finales y algunas cuestiones antropológicas. Abordar de este modo bitcoin tiene sus beneficios y desventajas, pero usado como punto de partida nos permite llegar a conclusiones profundas sobre la moneda.

Las cuestiones que quiero plantear son las siguientes: ¿Qué implica que el "rey Midas toque" monedas fiduciarias y las convierta en algo que sea más valioso que una onza de oro?, ¿Cuáles son las consecuencias de que el rey Midas tenga cada vez más monedas y bienes convertidos en oro?, ¿Perderá su humanidad el rey Midas debido a su avaricia cada vez mayor,? Y tal vez la pregunta más relevante: ¿Qué podemos aprender del mito del rey Midas?

La primera pregunta nos revela algo esencial de la comparación de bitcoin con el Rey Midas, y esto es que no estamos tan lejos de aquella situación mitológica, en la que un ente o sujeto convierte todo aquello que toca en oro. En este caso el tocar, sería convertir de moneda fiduciaria a bitcoin, donde lo que está siendo convertido por el Rey Midas tiene más valor, incluso al doble de una onza de oro, como se vio en el tercer capítulo. Adicionalmente podemos decir que el valor de bitcoin se puede entender como el precio que el mercado o las personas en su totalidad le dan en última instancia a bitcoin.

Respondiendo la segunda pregunta podemos afirmar que nuestro rey Midas al tener cada vez más ganancias y más oro, está más cerca de darse cuenta que su don no es más que una maldición o

una desgracia pues no le es posible desarrollar las funciones que lo hacen humano. La misma pregunta en términos puramente de bitcoin sería: ¿Cuáles son las consecuencias del uso cada vez más popular de bitcoin? A lo que podemos responder, al tener más demanda entonces sube más el precio de bitcoin, pero esto tiene sus consecuencias.

Consecuencias no solamente en el ámbito técnico, pues esto implica más trabajo para los mineros, mayor número de transacciones que procesar y hace en última instancia que se sature la red cada vez más. Más allá del ámbito técnico tenemos mayor interés como puede ser aquel de los países y de figuras importantes en el sector financiero, como también su posible inclusión en un fondo de inversión cotizado o lo que ya se ha dicho del 10 de diciembre del 2017 en el que bitcoin entró en un mercado de opciones financieras de Chicago. (coindesk, 2017h) Es verdad que crece y está creciendo, pero el crecimiento que está teniendo es áquel de un bien que se vincula con burbujas financieras, con la especulación y la riqueza en última instancia, no está teniendo un crecimiento como una moneda con la cual se puede comprar agua por ejemplo en una tienda de abarrotes, pero sí se pueden comprar bitcoins en una tienda de abarrotes o de autoservicio.

Con esto podemos proceder a la tercera pregunta, que es aquella en la cual la humanidad del rey Midas entra en juego por su avaricia. Dicho de otro modo la capacidad de bitcoin como un sistema descentralizado de efectivo basado en Internet entra en tela de juicio por el uso y el crecimiento que está teniendo. Es decir se mide el crecimiento de bitcoin en cuestión de valor que tiene, pero no se mide de acuerdo al impacto que esta moneda podría tener o tiene como tal. En lugar de ver el número de personas que beneficia en el día a día[64], la noticia que tenemos de bitcoin es aquella en la cual dos personas se convierten en los primeros multimillonarios de bitcoin (The Guardian, 2017), o se dan noticias constantes del precio en el que la moneda está, o su inclusión en los mercados financieros.

Es de este modo que una moneda o un bien que logra generar un valor dentro del internet termina por servir, en términos del rey Midas, su propia avaricia y en convertirse en la persona más rica del mundo, y en términos de bitcoin termina por servir y enriquecer a las personas que en última instancia lo usan. De esto podemos obtener dos reflexiones, la primera es la limitación que tiene

[64] Como podría ser la inclusión financiera para todas aquellas personas a las que se les niega un préstamo, cuenta bancaria o servicios financieros básicos. Mismos que tienen un rendimiento menor al crecimiento de bitcoin.

internet hoy en día como tal para crear una moneda de uso práctico, y la segunda es el acierto que bitcoin tuvo y ha tenido para lograr tener hoy en día un bien sin fronteras ni instituciones centrales, con todas las limitaciones ya mencionadas.

Si hablamos de la limitación de internet como medio para una moneda, se puede ver realmente como un indicador de cuantas personas están realmente conectadas a los beneficios que se tienen del Internet como tal. Es decir, beneficios no solamente en el ámbito de acceder a uno de los buscadores más grandes del mundo y a las aclamadas redes sociales, sino que a los beneficios como lo puede ser bitcoin y toda la gama de criptomonedas asociadas con Internet. Si vemos el Internet como un medio para una moneda internacional sin fronteras bancos ni países podemos ver a bitcoin como el primer paso o el primer ejemplo para lograr este cometido. Es posible tener una moneda internacional de internet, sin embargo bitcoin es el primer esbozo o prueba de esta moneda y a lo que ha sido llevada es a ganancias multimillonarias, inclusión en mercados financieros, ganancias y pérdidas en los miles o millones de pesos y posibles burbujas.

Antes de responder la última pregunta de qué enseñanzas podemos obtener del mito del rey Midas, es relevante hacer un recuento de todas las pequeñas conclusiones que se han mencionado a lo largo de toda la conclusión. Es decir, se debe tener iniciativa personal e interés propio para entender y comprender el uso de bitcoin a fondo. Existe centralización y regulación en la moneda por parte de los mineros, fondos de mineros y desarrolladores. Es imperativo tener una conexión a internet, pues la única frontera que existe con bitcoin es Internet como tal. A lo largo del mundo existe el doble de aceptación y desregulación en comparación a los países que lo regulan o prohíben. Por lo menos 4 personas de peso en el sector financiero han descreditado la moneda causando bajas considerables a su precio, creando a su vez una oportunidad de compra. Se puede entender bitcoin como una empresa o la acción de una empresa con todas las características antes mencionadas.

Ahora bien podemos responder la última pregunta sobre el rey Midas de las enseñanzas que podemos obtener sobre el mito del rey Midas. En el tercer capítulo se mencionó que el verdadero oro de Midas es la cadena de bloques, es decir aquello que hace posible el toque del rey Midas. Sin embargo se puede considerar bitcoin como un modo o una forma en la cual una gran parte de la sociedad actual o moderna, o si nos vemos más específicos, la sociedad de Internet, gasta en bitcoin, le da valor a bitcoin, e invierte su dinero como tal.

Dentro de esta línea de reflexión podemos en el ámbito personal decir que bitcoin me ayudó a ver las monedas como tal, no como algo único, sino que he adquirido, lo que se podría decir, una dimensión más para entender las monedas. En lugar de verlas como algo único, relacionadas a un país, una nación e incluso a una tradición, llega bitcoin que no tiene país ni fronteras, ni gobiernos, ayuda a poner en perspectiva las monedas como algo que pueden, incluso en nuestra época, cambiar o ser reemplazables, rediseñadas o repensadas como divisa.

Esto es ayudarme a ver las monedas como lo que son, pues muy fácilmente se olvida esto. Hoy en día se pueden llegar a ver como algo absoluto, cuando a lo largo de la historia es algo que se ha desarrollado y se sigue desarrollando. bitcoin ha hecho que me dé cuenta que no son algo absoluto, no son algo que no pueda ser repensado, ni rediseñado, sino que con el fundamento y seguridad adecuados incluso algo virtual como lo puede ser bitcoin, llega a adquirir un valor no antes pensado dentro de la sociedad en la que vivimos. Al igual que un suma muy grande de dinero invertida a esta moneda.

La última conclusión o enseñanza que podemos obtener está relacionada a algo que se menciona en el primer capítulo de la investigación. Esto es el vínculo muy estrecho que existe en bitcoin entre la cantidad de monedas totales y la recompensa del minado. Si la cantidad de monedas fuera ilimitada, entonces garantizar la rentabilidad del minado se vuelve un tema o cuestión difícil de resolver. Esto nos puede hablar de una falla en el diseño de bitcoin, o visto de un modo más positivo y global no sólo de bitcoin sino también de las monedas. En bitcoin tenemos una limitación sobre la cantidad total de bitcoins que serán minadas, concepto que se puede tal vez extrapolar al dinero fiduciario. Curiosamente Satoshi nos sugiere directa o indirectamente que puede existir una moneda que pueda caducar[65], que no sea infinita y que tenga límites en su producción, un hecho que en mi experiencia no veo reflejado en la realidad. Se habla de riqueza ilimitada y nos plantean como si no hubiera un límite en la producción del dinero, o la riqueza que alguien puede acaparar. Ya sea aumentando la cantidad de monedas y ganancias que uno tiene o haciendo que las ganancias y acciones que uno tenga suban de valor. Sin embargo con bitcoin, una moneda digital, una moneda de internet, podemos esbozar la situación hipotética de que pasaría con una moneda con un número fijo de unidades.

[65] Caduca en el sentido de que se deje de usar la moneda dentro de 20 años como sugiere Satoshi, ya sea por una recompensa muy pequeña, o que las comisiones para procesar transacciones sean demasiado costosas para el usuario.

Es decir estamos hablando de una moneda cuya producción total está limitada, y si bien puede considerarse un tanto radical plantear una moneda gubernamental con un número fijo de unidades, así como es un planteamiento que tiene que considerarse con muchos más factores, lo que sí nos permite comenzar a pensar es plantear un límite en la riqueza. No es que Satoshi esté planteando un límite en la distribución de las monedas actuales pero nos permite imaginar y repensar la idea de una moneda con una distribución limitada y tal vez por consiguiente, una limitación en la riqueza acumulable.

Con esta reflexión es que podemos comenzar a esbozar la conclusión final de la tesis y esta es que gracias a bitcoin se está generando una ruptura o una manera diferente de entender las monedas. bitcoin sirve solamente para los usos que las personas que ya caracterizamos anteriormente le dan, pero para todo lo demás que sirve una moneda, bitcoin no sirve. Es entonces solamente un bien y una mercancía, un activo digital. En mi opinión todas estas características, limitaciones y situaciones comienzan a generar una ruptura de lo que se considera dinero/moneda como tal, o tal vez podemos plantear una conclusión no tan ambiciosa. Esta sería que bitcoin es una moneda construida sobre preceptos completamente diferentes a los que se tienen en la sociedad actual de cómo y quiénes deben de ser los que controlan y administran las monedas. Lo que nos lleva a una manera nueva de ver aquello que consideramos como una moneda o dinero como tal.

Esto se puede ver reflejado incluso en las primeras reacciones que tenemos de las personas a las que se les explica o ven el tema por primera ocasión. Esto es un impacto, pues es difícil comprender que pueda existir una moneda, con todas las limitaciones que ya se han mencionado y discutido, la cual no tenga gobierno ni instituciones centrales, con la cual podemos comprar, aunque sean pocos, bienes y alimentos preparados.

Anexo Técnico

Para lograr describir las actividades que se desarrollan en la red, que son propiamente las transacciones y la validación de transacciones es necesario antes, comprender como funciona internamente. Estas actividades son las que se desarrollan virtualmente pero en la realidad tenemos el uso de bitcoin a modo de moneda o a modo de bien digital entendido como un activo digital.

La criptografía asimétrica fue propuesta en 1976 por Whitfield Diffe y Martin Hellman ("Understanding Public Key Cryptography,") Este tipo de criptografía consiste en usar dos llaves, una llave privada y otra pública. Para el caso de las bitcoins estas dos llaves son usadas para garantizar la seguridad de las direcciones usadas para recibir y enviar bitcoins, así como de la seguridad de las transacciones, cabe mencionar que la criptografía usual es empleada para transferir un mensaje.

Adicional a las dos llaves (privada y pública) tenemos en el uso de las bitcoins una firma o signature en inglés y por último una dirección que depende de la llave pública y será usada para las transacciones. Estos 3 mecanismos son usados para lograr procesar una transacción dentro de la red de bitcoins, y son almacenadas en los programas conocidos como carteras o wallets. Es importante resaltar que no se toma como cuarto mecanismo la dirección pues ella se puede generar de la llave pública.

De acuerdo a la entrevista con Juan tenemos como él lo entiende y hablando sobre llaves privadas y públicas podemos ver que nos da un panorama global: "En cuanto a la cuestión de las llaves públicas y privadas tiene que ver con el tipo de criptografía que utilizan, creo que se llama ECDSA o algo así, criptografía de curva elíptica, entonces la cuestión es ésta, yo no soy criptógrafo, te puedo explicar más o menos el concepto, pero pues es mejor que vayas y lo leas en Wiki o algo así cómo funciona la criptografía de las llaves públicas de bitcoin, pero esto es criptografía, usada popularmente en tecnología como PGP o creo que SSL también usa tecnología por el estilo, no estoy seguro. Pero pues es criptografía vetada con 20 años de prueba pues, básicamente requiere la llave pública y la llave privada para poder hacer la matemática especial para que sirva.

Básicamente tú conoces mi llave pública y tu llave privada, y haces las encriptaciones en un mensaje con tu llave privada y mi llave pública, y luego cuando mandas el mensaje encriptado, yo cojo tu llave pública y mi llave privada y la matemática funciona de una forma que yo puedo entonces, des-encriptar, esa información, pero sólo si yo tengo la llave privada que corresponde a mi llave pública y sólo si tu llave pública corresponde a tu llave privada, es magia y matemática, pero es el pedo, y la firma es una forma de autenticar que el mensaje viene de ti, se compara contra la llave pública. Es un modo, método de autentificación digital que es bastante poderoso, pues, importante."

Hablando ahora de las carteras tenemos que es entonces un programa que en su más básica etapa almacena una o varias llaves privadas y genera con la llave privada diferentes llaves públicas, firmas digitales y direcciones para enviar y recibir bitcoins. En su forma más compleja es además de un almacenamiento de lo mencionado anteriormente, es un cliente con el cual se pueden enviar pagos, ver el estado de la red de bitcoins y encriptar o codificar las llaves para un almacenamiento más seguro, entre otras cosas. ("Clients - bitcoin Wiki,") Hoy en día hay una variedad muy grande de carteras, existen desde aplicaciones de celular como lo es el caso de la aplicación de Copay a incluso carteras hechas de papel ("Paper wallet - bitcoin Wiki,")

Profundizando con la cartera tenemos que la llave privada es lo primero que se genera, y este es un número generado al azar, entre el 1 y el 2^{256}. (Antonopoulos, 2015, p. 63) Que sin abreviar es el número:

115792089237316195423570985008687907853269984665640564039457584007913129639936 ("2**256 - Wolfram|Alpha,")

El número que uno elija generar como llave privada se puede crear con papel pluma y una moneda, hasta usando complejos algoritmos de computadora, el número es almacenado en un formato comprimido y fácil de procesar.

Una vez que se tiene la llave privada, se genera la llave pública con la multiplicación criptográfica asimétrica de curva elíptica que ya se mencionó antes (ECDSA). Que en términos más simples se puede considerar como una multiplicación. Lo que se hace en los términos más sencillos que puedo explicar es trazar una curva (elíptica) en un plano cartesiano, que es similar a una Omega griega horizontal, sobre esta curva se toma la llave privada como el punto inicial

"G". Desde el punto inicial "G", se desplaza en una línea, sobre la curva, y después de cierto número de movimientos, se termina en otro punto, siempre dentro de esta misma curva. Ese nuevo punto que tiene dos coordenadas es la llave pública. Para ver una explicación un poco más detallada y con cierto rigor matemático y computacional sobre la multiplicación de curva elíptica se puede ver en el enlace: https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

Y a continuación una imagen que espero ayude a aclararlo:

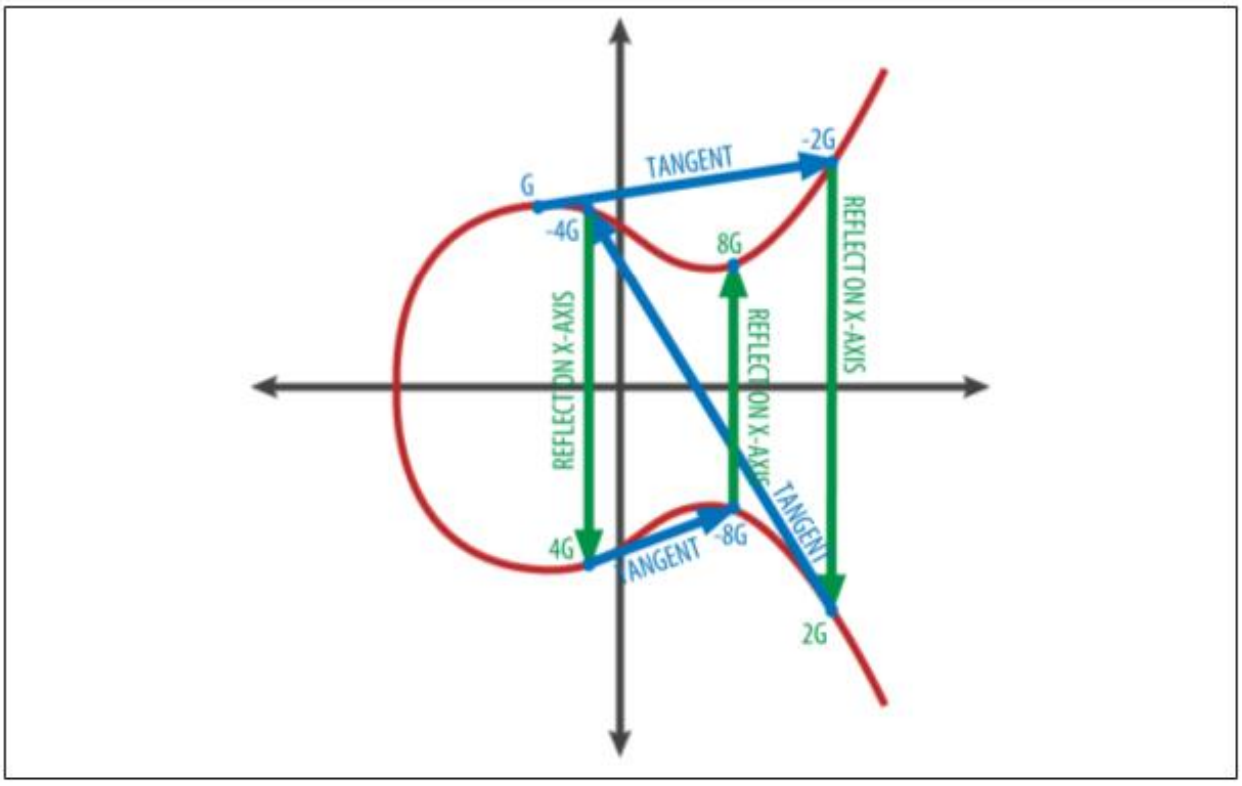


Figure 4-4. Elliptic curve cryptography: Visualizing the multiplication of a point G by an integer k on an elliptic curve

(Antonopoulos, 2015, p. 70)

Donde G es el punto inicial y lo que podemos considerar como la llave privada, y -2G, 2G, -4G, 4G, -8G Y 8G son los movimientos que se hacen sobre la curva para llegar a la llave pública 8G. Cabe mencionar que a lo que yo estoy llamando "movimientos" dentro de la gráfica son en realidad operaciones matemáticas bien definidas sobre un conjunto de números, que en este caso

son números primos. Y cada punto de la gráfica es un número primo como tal.

Una vez que se llega del punto G al punto 8G, tenemos como se podrá imaginar dos coordenadas, la coordenada en el plano X y en el plano Y. Dependiendo de si la coordenada en Y es par o impar tenemos el inicio de la llave pública y lo que sigue a continuación es la coordenada en el plano X. Este número como tal es ya considerado como la llave pública.

Solamente falta por explicar las direcciones. Si se recuerda bien se dijo que las direcciones eran generadas a partir de la llave pública. Se generan comprimiendo la llave pública usando dos algoritmos de hash, llamados RIPEMD-160 y SHA-256, estos dos algoritmos usados en conjunto se conocen como HASH-160. Lo que los algoritmos de hash hacen es básicamente tomar una cadena de cualquier número de entradas y transformarla en otra cadena con ciertas características y un número fijo de entradas. La nueva cadena generada es mucho menor en tamaño y esto ayuda para hacer más eficiente el procesamiento en la red.

Lo más importante de todos estos procesos que involucran, los algoritmos de hash y la multiplicación de curva elíptica es que son matemáticamente y computacionalmente muy difíciles de revertir, sino es que prácticamente imposible con la tecnología e investigación que se tiene hoy en día. Concretamente para hacer el proceso inverso de la multiplicación elíptica el problema es conocido como el logaritmo discreto (“Elliptic Curve Cryptography: ECDH and ECDSA - Andrea Corbellini,”), y hasta hoy en día no se tiene una solución eficaz para resolverlo. Aqui es donde tal vez se encuentra la magia y matemática de la cual nos habla Juan.

Una vez explicado cómo se crean las llaves que son en mi opinión la base de las bitcoins, explicaré ahora su uso y como se dan las transacciones dentro de la red.

Tomando en cuenta que una persona ya hizo todos los pasos necesarios, y con la seguridad apropiada para tener una fuerte llave privada, y tener ya una cartera como tal voy a describir, y explicar como son las transacciones. Con esta llave privada se crea la llave pública la cual ya se explicó antes y después esa llave pública se usa con los algoritmos de HASH-160 (SHA-256 y RIPEM-160 en conjunto).

Se recomienda crear para cada nueva transacción una llave pública nueva por cuestiones de seguridad y de privacidad. Esto es por razones diversas, pero la principal y más funcional, es que se crea al momento con algoritmos que se mencionaron antes una dirección nueva usando la

llave privada del usuario que desea recibir sus bitcoins, y se garantiza de este modo que se está usando una dirección válida para recibir las moneda. Otra razón para usar una dirección nueva para cada transacción es que, si uno emplea para la totalidad de sus transacciones la misma dirección existe una posibilidad muy alta de que vinculen a una persona o identidad con la dirección siendo usada. (“Address reuse - bitcoin Wiki,”).

Una vez que tenemos entonces nuestra llave privada; que sólo nosotros y la cartera dentro de la computadora sabemos cuál es, y recordando el proceso brevemente, se genera la dirección pública “multiplicando” la llave privada. El resultado es la llave pública que con el algoritmo HASH-160, (que es el algoritmo SHA-256 combinado con el RIPEMD-160) calcula nuestra dirección. En este punto tenemos nuestra llave privada, pública y la dirección ahora sólo falta hacer la transacción y para eso se usa la firma.

Se inicia la transacción y se crea entonces una firma, o “firmamos” digitalmente la transacción en cuestión. Es importante mencionar que la firma digital se crea también usando la multiplicación criptográfica de curva elíptica, y se valida usando un algoritmo o ecuación que tiene que cumplir con una dirección valida, el “resultado anterior” y la firma digital.(Preshing, 2014) Lo que ésta firma representa es que la transacción en curso fue autorizada por la persona a la cual le pertenece y creó la dirección, y simultáneamente que la cantidad de bitcoins llamada “resultado anterior” en la transacción nos “pertenecen” o están vinculadas a nuestra llave pública. Como “resultado anterior” se entiende el “haber”, como es comprendido en contabilidad. Para ver la relación que existe entre las llaves publicas privadas firmas y los usuarios que mandan y reciben es muy relevante la siguiente imagen:

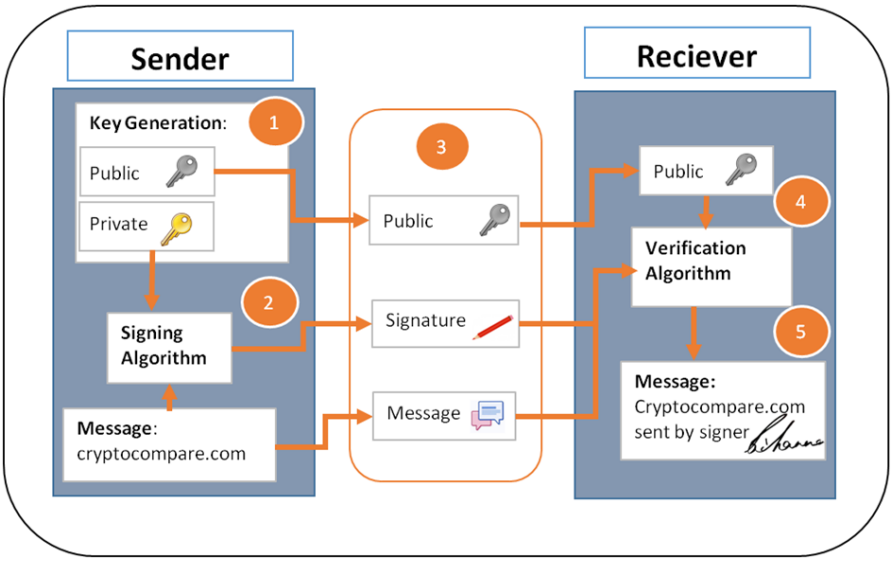


Imagen 5: Imagen obtenida de *(“How do digital signatures in bitcoin work?,” 2016)*

El paso tres en la imagen es lo que sería la transacción propiamente hablando, y los procesos que ya se han descrito sobre criptografía elíptica creación de llaves y verificación las hacen los usuarios que mandan (Sender en la imagen) y reciben (Reciever en la imagen).

Una vez explicado el proceso y los elementos que componen una transferencia podemos observar la siguiente transacción que justamente fue mi primera compra de bitcoins, y sus elementos. Nota: esto no es recomendable hacerlo público, pues estoy indicando o haciendo fácil la asociación de una dirección a una que se puede relacionar a mí, sin embargo usé para esta transacción una dirección y una cartera que ya están en desuso.

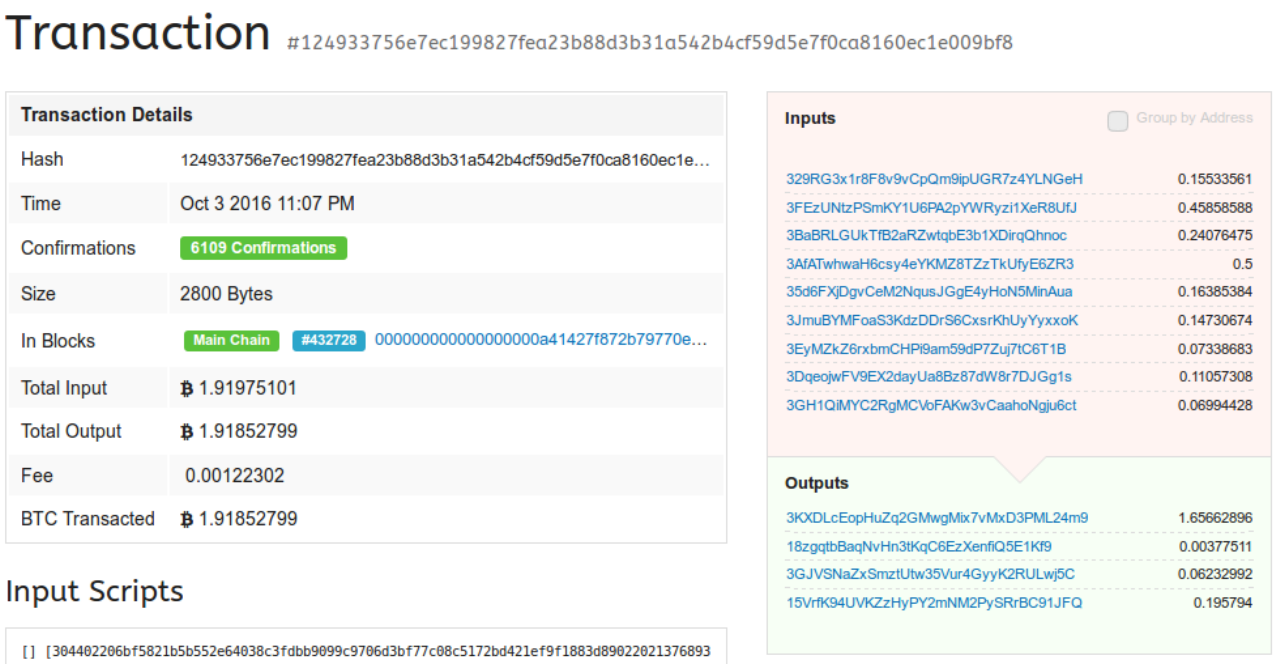


Imagen 6: Obtenida de ("Bitcoin Transaction 124933756e7ec199827fea23b88d3b31a542b4cf59d5e7f0ca8160ec1e009bf8 | Block Explorer | Biteasy.com,")

Los elementos que componen internamente y son usados en la red en una transacción son: la versión, que indica que reglas tiene que seguir la transacción; un contador de "entradas", que indica cuántas entradas tiene la transacción; las "entradas", que indica una o más "entradas" de la transacción; un contador de "resultados anteriores", así como los "resultados anteriores", que son respectivamente cuantos resultados anteriores tiene y los resultados anteriores como tal, y, por

último, el número de bloque (Antonopoulos, 2015, p. 111). Por “entradas” estoy refiriéndome al equivalente al “debe”, usado en la contabilidad.

Todos estos elementos internos se pueden ver en la imagen, excepto la versión de la transacción. Por parte del contador de las “entradas” (Inputs o “debe” de contabilidad) tenemos 9, el contador de los “resultados anteriores” (Outputs o el “haber” de contabilidad) son 4. El número de bloque es el número #432728. Ésta es una transacción básica y todas las transacciones que se hacen dentro de la red de bitcoins quedan registradas en un libro mayor Público llamado cadena de bloques o comúnmente conocido en inglés como blockchain.

Este nombre no es accidental y representa como su nombre lo indica una cadena de bloques, cada bloque está formado por más de una transacción, es decir una agrupación de transacciones forman lo que se llama un bloque. Para definir un bloque tenemos un “valor definido o código” que representa el conjunto de transacciones que más tarde se usará en el minado de las bitcoins.

La manera en la que un minero recibe su comisión y valida un bloque de transacciones es la siguiente. Se emplea el “código o valor definido”, se le agregan unos valores adicionales para que pueda ser usado con el algoritmo de criptografía de SHA-256. El resultado de usar el algoritmo nos tiene que dar un valor acordado por la comunidad, este valor acordado por la comunidad se entiende como la “solución”.

Ya se ha explicado qué tan difícil es revertir el proceso que llevan los métodos de criptografía como lo son el método de SHA-256 y el RIPEMD-160. Esto es uno de los pilares de la seguridad de las llaves, al igual que de la validación de las transacciones. Así como estos métodos de encriptado son difíciles de revertir son también difíciles de predecir sus resultados, y es una característica deseada de la encriptación moderna y en general. Es entonces que no existe un proceso de pasos definido para obtener el valor deseado acordado por la comunidad, la “solución”, para estas funciones criptográficas y se tiene que estar intentando a mucha velocidad con muchas variantes y modificaciones usando el algoritmo de SHA-256 para obtener el valor deseado.

Al obtener esta solución se tiene la validación correcta de un bloque definido de cierto número de transacciones, los mineros obtienen una recompensa por obtener la solución. Pero no podemos perder de vista que la solución representa la validación de un número específico de

transacciones, misma como de la imagen anterior de mi primera compra de bitcoin.

La red en la que están planteadas estas monedas es una descentralizada llamada de par a par o peer to peer en inglés y hay muchas personas haciendo este proceso de validación de bloques y de transacciones, los ya introducidos mineros. Existen hoy dos tipos de mineros, individuales y Fondos o Mining Pools. Ambos tienen computadoras corriendo las 24 horas intentando encontrar la "solución" a un bloque de transacciones.

Un detalle que no se ha mencionado es que los mineros al encontrar la solución acordada del código que definieron para describir un grupo de transacciones, es decir un bloque, tienen que distribuirla por esta red descentralizada de par-a-par. Ellos propagan su solución a la red y las demás personas, pueden validar de manera muy rápida la solución que se obtuvo como correcta, pues como ya se dijo es difícil de predecir y revertir, pero muy fácil de verificar. Si la solución es correcta, entonces las transacciones del bloque definido por el minero que proporcionó la solución se agregan a la cadena de bloques como definitiva y se actualiza la cadena de bloques para toda la red. Siempre se agrega a la cadena de bloques la solución encontrada primero y la Cadena de bloques más larga será siempre la correcta, con estos dos principios se garantiza la integridad de nuestro libro mayor o blockchain. Similarmente esta es la manera en la que se genera un flujo de transacciones, se mantiene sincronizada la red y correcto el libro mayor o la cadena de bloques.

En la siguiente página podemos observar una explicación con procesos que podemos hacer con una calculadora científica demostrando las llaves, el firmar una transacción y en general el funcionamiento interno: https://www.coindesk.com/math-behind-bitcoin/.

Referencias y Bibliografía

Banking consortium awards Digital Trade Chain contract to IBM [WWW Document], 2017. . Finextra Res. URL https://www.finextra.com/newsarticle/30747/banking-consortium-awards-digital-trade-chain-contract-to-ibm (accessed 9.1.17).

Banxico, 2017a. Mercado cambiario, tipo de cambio, Banco de México - 9 Nov [WWW Document]. URL http://www.banxico.org.mx/portal-mercado-cambiario/index.html (accessed 11.10.17).

Banxico, 2017b. Mercado cambiario, tipo de cambio, Banco de México - 3 de octubre [WWW Document]. URL http://www.banxico.org.mx/portal-mercado-cambiario/ (accessed 6.28.17).

Banxico, 2017c. Mercado cambiario, tipo de cambio, Banco de México - 26 de Mayo [WWW Document]. URL http://www.banxico.org.mx/portal-mercado-cambiario/ (accessed 6.21.17).

Bitcoin ATM Mexico – find bitcoin machine locations [WWW Document], 2014. URL https://coinatmradar.com/country/138/bitcoin-atm-mexico/ (accessed 10.13.17).

Bitcoin Project, 2017a. Descargar - Bitcoin [WWW Document]. URL https://bitcoin.org/es/descargar (accessed 8.26.17).

Bitcoin Project, 2017b. Development - Bitcoin [WWW Document]. URL https://bitcoin.org/en/development (accessed 8.26.17).

Bitcoin Project, 2017c. Download - Bitcoin [WWW Document]. URL https://bitcoin.org/en/download (accessed 8.26.17).

Bitcoin Wiki, 2017. Genesis block - Bitcoin Wiki [WWW Document]. URL https://en.bitcoin.it/wiki/Genesis_block (accessed 10.18.17).

Bitcoin.com, 2017a. Miner Revenue | Bitcoin.com Charts [WWW Document]. URL https://charts.bitcoin.com/chart/miner-revenue#0 (accessed 11.9.17).

Bitcoin.com, 2017b. Blockchain Size | Bitcoin.com Charts | Consulta 17 Nov 2017 [WWW Document]. URL https://charts.bitcoin.com/chart/blockchain-size#0 (accessed 11.17.17).

Bitcoin.com, 2017c. Daily Blocks | Bitcoin.com Charts | Consulta 17 Nov [WWW Document]. URL https://charts.bitcoin.com/chart/blocks-daily#0 (accessed 11.17.17).

Bitcoin.com, 2017d. Daily Transactions | Bitcoin.com Charts | Consulta 17 Nov [WWW Document]. URL https://charts.bitcoin.com/chart/daily-transactions#0 (accessed 11.29.17).

Bitcoin.com, 2017e. Bitcoin Price | Bitcoin.com Charts | Consulta 19 de julio [WWW Document]. URL https://charts.bitcoin.com/chart/price#0 (accessed 11.28.17).

Bitconnect.co, 2018. Legality of Bitcoin & cryptocurrency | Bitconnect [WWW Document]. Bitconnect.co. URL https://bitconnect.co/bitcoin-information/8/legality-of-bitcoin-cryptocurrency (accessed 1.16.18).

Bitso, 2017. Bitso - The Bridge to Mexico's New Digital Economy [WWW Document]. URL https://webcache.googleusercontent.com/search?q=cache:76aOnq_WXAQJ:https://bnktothefuture.com/pitches/bitso/business_page+&cd=2&hl=en&ct=clnk (accessed 8.2.17).

Bitso, 2016. Daniel Vogel de Bitso en El Financiero Bloomberg.

Bitso, 2015. BitPay y Bitso anuncian alianza [WWW Document]. Bitso. URL https://blog.bitso.com/bitpay-y-bitso-anuncian-alianza-e3f9ff66f6aa (accessed 2.2.18).

Blockchain Luxembourg S.A.R.L, 2017a. Bitcoins in circulation [WWW Document]. Blockchain.info. URL https://blockchain.info/total-bitcoins (accessed 10.12.17).

Blockchain Luxembourg S.A.R.L, 2017b. Bitcoin currency statistics - 9 enero a 13 nov [WWW Document]. Blockchain.info. URL https://blockchain.info/stats (accessed 6.1.17).

Blockchain Luxembourg S.A.R.L, 2017c. Total Transaction Fees - BTC [WWW Document]. Blockchain.info. URL https://blockchain.info/transaction-fees (accessed 11.6.17).

Blockchain Luxembourg S.A.R.L, 2017d. Confirmed Transactions Per Day [WWW Document]. Blockchain.info. URL https://blockchain.info/n-transactions (accessed 11.6.17).

Blockchain Luxembourg S.A.R.L, 2017e. 100 Most Popular Bitcoin Addresses - Blockchain.info [WWW Document]. URL https://blockchain.info/popular-addresses (accessed 12.21.17).

Bradbury, D., 2014. How Dangerous is Satoshi Nakamoto? [WWW Document]. CoinDesk. URL http://www.coindesk.com/dangerous-satoshi-nakamoto/ (accessed 11.8.16).

BTC Fácil, 2016. Introducción al Bitcoin.

coindesk, 2018a. Bitcoin Price Index - Real-time Bitcoin Price Charts | Cambio de precio 12 sep 2017 [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 1.10.18).

coindesk, 2018b. Bitcoin Price Index - Real-time Bitcoin Price Charts | Cambio de precio 19 sep 2017 [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 1.10.18).

coindesk, 2018c. Bitcoin Price Index - Real-time Bitcoin Price Charts | Cambio de precio 2 nov 2017 [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 1.10.18).

coindesk, 2017a. Bitcoin Price Index - Real-time Bitcoin Price Charts - Precio Mineros [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 11.9.17).

coindesk, 2017b. Bitcoin Price Index - Real-time Bitcoin Price Charts | 15 Nov 12 [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 11.16.17).

coindesk, 2017c. Bitcoin Price Index - Real-time Bitcoin Price Charts | 19 de julio [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 11.28.17).

coindesk, 2017d. Bitcoin Price Index - Real-time Bitcoin Price Charts - Mayo [WWW Document]. CoinDesk. URL http://www.coindesk.com/price/ (accessed 5.26.17).

coindesk, 2017e. Bitcoin Price Index - Real-time Bitcoin Price Charts - 3 de octubre [WWW Document]. CoinDesk. URL http://www.coindesk.com/price/ (accessed 6.28.17).

coindesk, 2017f. Bitcoin Price Index - Real-time Bitcoin Price Charts - 1 de Junio [WWW Document]. CoinDesk. URL http://www.coindesk.com/price/ (accessed 6.27.17).

coindesk, 2017g. Bitcoin Price Index - Real-time Bitcoin Price Charts - Consulta Zona 2 [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 11.21.17).

coindesk, 2017h. CBOE to Begin Bitcoin Futures Trading December 10 [WWW Document]. CoinDesk. URL https://www.coindesk.com/cboe-begin-bitcoin-futures-trading-december-10/ (accessed 12.17.17).

coinmap.org - Bitcoin accepting shops, ATM's & venues. [WWW Document], 2017. . Coinmaporg - Map Bitcoin Accept. Venues. URL https://coinmap.org/ (accessed 6.16.17).

CoinMarketCap, 2017a. All Cryptocurrencies | CoinMarketCap | Total de Criptomonedas [WWW Document]. URL https://coinmarketcap.com/all/views/all/ (accessed 11.14.17).

CoinMarketCap, 2017b. Bitcoin (BTC) price, charts, market cap, and other metrics | Bitcoin Markets [WWW Document]. URL http://coinmarketcap.com/currencies/bitcoin/#markets (accessed 6.22.17).

CoinTelegraph.com, 2017. World Markets in Selloff, Trump Presidency Spikes Bitcoin Price [WWW Document]. Cointelegraph. URL https://cointelegraph.com/news/world-markets-in-selloff-trump-presidency-spikes-bitcoin-price (accessed 11.19.17).

CoinWarz, 2017. Bitcoin Mining Calculator and Profitability Calculator - CoinWarz - SHA-256 Hash Rate 14,000.00 GH/s [WWW Document]. URL https://www.coinwarz.com/calculators/bitcoin-mining-calculator/?h=14000.00&p=1375.00&pc=0.15&pf=0.00&d=1452839779145.92000000&r=12.50000000&er=7369.30000000&hc=2000.00 (accessed 11.10.17).

De, N., 2017a. Credit Suisse CEO: Bitcoin the "Very Definition of a Bubble" [WWW Document]. CoinDesk. URL https://www.coindesk.com/credit-suisse-ceo-bitcoin-definition-bubble/ (accessed 1.10.18).

De, N., 2017b. "A Real Bubble": Billionaire Warren Buffett Doubles Down on Bitcoin Doubt [WWW Document]. CoinDesk. URL https://www.coindesk.com/real-bubble-billionaire-warren-buffett-doubles-bitcoin-doubt/ (accessed 1.10.18).

De, N., 2017c. World's Largest Hedge Fund Founder: Bitcoin is a "Bubble" [WWW Document]. CoinDesk. URL https://www.coindesk.com/bridgewater-associates-head-says-bitcoin-bubble/ (accessed 1.10.18).

Finney, H., 2013. Bitcoin and me (Hal Finney) [WWW Document]. URL https://bitcointalk.org/index.php?topic=155054.0 (accessed 8.23.17).

Forbes, M., 2016. La startup mexicana que venderá Bitcoins en las tienditas de la esquina [WWW Document]. Forbes Mex. URL https://www.forbes.com.mx/la-startup-mexicana-que-vendera-bitcoins-en-las-tienditas-de-la-esquina/ (accessed 7.11.17).

Gandal, N., Hamrick, J.T., Moore, T., Oberman, T., 2017. Price Manipulation in the Bitcoin Ecosystem. Workshop Econ. Inf. Secur. WEIS 2017.

Geografía (INEGI), 2017. Descarga masiva [WWW Document]. URL http://www.beta.inegi.org.mx/app/descarga/# (accessed 12.19.17).

Geografía (INEGI), I.N. de E. y, 2014. Directorio Nacional de Unidades Económicas. DENUE [WWW Document]. Censos Económicos 2014. URL http://www.beta.inegi.org.mx/app/mapa/denue/default.aspx (accessed 12.19.17).

Goodin, D., 2012. 25-GPU cluster cracks every standard Windows password in <6 hours [WWW Document]. Ars Tech. URL https://arstechnica.com/information-technology/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/ (accessed 10.11.17).

Google, 2017. ¿qué es bitcoin? - Google Search [WWW Document]. URL https://encrypted.google.com/search?q=que+es+bitcoin&hl=en&biw=1366&bih=602&source=lnt&tbs=cdr%3A1%2Ccd_min%3A5%2F28%2F2016%2Ccd_max%3A8%2F28%2F2016&tbm=#safe=off&hl=en&tbs=cdr:1,cd_min:5/28/2016,cd_max:8/28/2016&q=%C2%BFqu%C3%A9+es+bitcoin? (accessed 6.21.17).

Graham, G., 2017. The White Paper FAQ (Frequently Asked Questions). White Pap. Guy - Gordon Graham.

Hern, A., 2015. Bitcoin creator Satoshi Nakamoto denies being Craig Wright (maybe).

How did Satoshi register bitcoin.org? [WWW Document], 2016. URL https://bitcointalk.org/index.php?topic=103369.msg1134000 (accessed 11.7.16).

ISBIT, 2017. Plataforma de Intercambio de Activos Digitales Líder en México - ISBIT [WWW Document]. URL https://www.isbit.co/ (accessed 12.21.17).

Juan S. Galt (@JuanSGalt) | Twitter [WWW Document], 2016. URL https://twitter.com/JuanSGalt (accessed 11.15.16).

Lee, T.B., 2017. A brief history of Bitcoin hacks and frauds [WWW Document]. Ars Tech. URL https://arstechnica.com/tech-policy/2017/12/a-brief-history-of-bitcoin-hacks-and-frauds/ (accessed 12.21.17).

Lerner, S.D., 2013. The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius. Bitslog.

Lerner, S.D., 2011. About. Bitslog.

LetsTalkBitcoin.com, 2014. User Info - jratcliff63367 | Lets Talk Bitcoin [WWW Document]. URL https://letstalkbitcoin.com/profile/user/jratcliff63367 (accessed 11.17.17).

Licencia MIT, 2017. . Wikipedia Encicl. Libre.

LocalBitcoins, 2017. About LocalBitcoins.com [WWW Document]. URL https://secure.livechatinc.com/licence/5492471/open_chat.cgi?groups=0&embedded=1&newWebserv=undefined&__lc_vv=2&session_id=S1504052906.06db9c0ddc&server=secure.livechatinc.com#https://localbitcoins.com/about (accessed 10.13.17).

Malmi, M., 2015. I'm Martti Malmi, early bitcoin developer and the original founder of the Bitcointalk.org forums, AMA! [WWW Document]. Bitcoin Forum. URL https://forum.bitcoin.com/ama-ask-me-anything/i-m-martti-malmi-early-bitcoin-developer-and-the-original-founder-of-the-bitcointalk-org-forums-ama-t2770.html (accessed 9.8.17).

Mark, 2015. Bitcoin Wallets Comparison Chart and Reviews. The Merkle.

MaxSaldo, 2017. Como funciona Maxsaldo - Recargas Electrónicas Pago de Servicios [WWW Document]. URL https://www.maxsaldomexico.com/como-ganar/ (accessed 7.14.17).

McGrath Goodman, L., 2014. The Face Behind Bitcoin [WWW Document]. Newsweek. URL http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html (accessed 11.8.16).

memonius, 2014. Zmart Group 4 min.

Metzdowd - cryptography Info Page [WWW Document], n.d. URL http://www.metzdowd.com/mailman/listinfo/cryptography (accessed 8.23.17).

Mifiel, 2017. Preguntas Frecuentes [WWW Document]. Mifiel. URL https://www.mifiel.com/es/preguntas (accessed 10.4.17).

Monaghan, A., 2017. Bitcoin is a fraud that will blow up, says JP Morgan boss. The Guardian.

Money & Tech, 2014. Pablo Gonzalez & Ben Peters of Bitso @ CoinSummit.

Nakamoto, S., 2017. bitcoin: Bitcoin Core integration/staging tree. Bitcoin.

Nakamoto, S., 2010a. What's with this odd generation? [WWW Document]. URL https://bitcointalk.org/index.php?topic=48.msg329#msg329 (accessed 9.7.17).

Nakamoto, S., 2010b. How divisible are bitcoins and other market/economic questions [WWW Document]. URL https://bitcointalk.org/index.php?topic=44.msg267#msg267 (accessed 9.7.17).

Nakamoto, S., 2009. Bitcoin v0.1 released [WWW Document]. URL https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html (accessed 10.12.17).

Nakamoto, S., 2008a. Bitcoin P2P e-cash paper - PDF.

Nakamoto, S., 2008b. Bitcoin P2P e-cash paper | Primera Publicación [WWW Document]. URL https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html (accessed 10.25.17).

Nakamoto, S., 2008c. Re: Bitcoin P2P e-cash paper [WWW Document]. URL https://www.mail-archive.com/cryptography@metzdowd.com/msg09980.html (accessed 8.23.17).

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27, Discussions, V., 2014a. Bitcoin open source implementation of P2P currency | Mar [WWW Document]. URL http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A52186 (accessed 9.6.17).

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27, Discussions, V., 2014b. Bitcoin open source implementation of P2P currency | Sept [WWW Document]. URL http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?xg_source=activity&id=2003008%3ATopic%3A9402&page=4 (accessed 10.26.17).

Prahalad, B., 2016. Should I keep my Bitcoin on an exchange or in a wallet? - Quora [WWW Document]. URL https://www.quora.com/Should-I-keep-my-Bitcoin-on-an-exchange-or-in-a-wallet (accessed 10.27.17).

Ratcliff, J.W., 2014. Rise of the Zombie Bitcoins [WWW Document]. Lets Talk Bitcoin. URL https://letstalkbitcoin.com/blog/post/rise-of-the-zombie-bitcoins (accessed 11.17.17).

Reforma, 2016. Hay Bitcoins... ¡en Ixtapaluca! [WWW Document]. URL http://www.reforma.com/aplicacioneslibre/articulo/default.aspx?id=855153&md5=cb704d14c0ab6149345890a85040acc8&ta=0dfdbac11765226904c16cb9ad1b2efe&lcmd5=1ce3a794c9b4222932b16999aacbad57 (accessed 6.21.17).

Reinhold, A.G., 2017. Diceware Passphrase Home [WWW Document]. URL http://world.std.com/~reinhold/diceware.html (accessed 10.10.17).

satoshin@gmx.com is compromised [WWW Document], 2016. URL https://bitcointalk.org/index.php?topic=775174.0 (accessed 11.7.16).

Simmel, G., 2016. Philosophie des Geldes, Primera Edición. ed. Ediciones Culturales Paidos S. A. de C. V.

StackExchange, 2013. password cracking - What is the entropy of just 1 Diceware passphrase like my passphrase? - Information Security Stack Exchange [WWW Document]. URL https://security.stackexchange.com/questions/36246/what-is-the-entropy-of-just-1-diceware-passphrase-like-my-passphrase (accessed 10.11.17).

Staff, G.L.R.D., 2016. Bitcoin Survey [WWW Document]. URL https://www.loc.gov/law/help/bitcoin-survey/ (accessed 1.19.18).

The Guardian, 2017. How the Winklevoss twins became the world's first bitcoin billionaires [WWW Document]. the Guardian. URL http://www.theguardian.com/technology/shortcuts/2017/dec/04/winklevoss-twins-bitcoin-billionaires-mark-zuckerberg (accessed 1.19.18).

THEOI, 2017. MIDAS - Phrygian King of Greek Mythology [WWW Document]. URL http://www.theoi.com/Heros/Midas.html (accessed 6.16.17).

Tipo de Cambio del Dólar y Divisas | Banamex.com [WWW Document], 2017. URL https://www.banamex.com/economia_finanzas/es/divisas_metales/resumen.htm (accessed 5.26.17).

Top Open Source Licenses [WWW Document], n.d. . Black Duck Softw. URL https://www.blackducksoftware.com/top-open-source-licenses (accessed 8.29.17).

Volabit, 2017. ¿Qué es Volabit? - Preguntas Frecuentes | Volabit [WWW Document]. URL http://ayuda.volabit.com/article/75-que-es-volabit (accessed 12.21.17).

Wikipedia, 2018. Legality of bitcoin by country or territory. Wikipedia.

Wikipedia, 2017a. Solicitud de información. Wikipedia Encicl. Libre.

Wikipedia, 2017b. Winklevoss twins. Wikipedia.

XE.com, 2017a. XE: XBT / USD Currency Chart. Bitcoin to US Dollar Rates | Consulta 19 de julio 2010 [WWW Document]. URL http://www.xe.com/currencycharts/?from=XBT&to=USD&view=10Y (accessed 11.28.17).

XE.com, 2017b. XE: XBT / USD Currency Chart. Bitcoin to US Dollar Rates | precio al 28 de noviembre [WWW Document]. URL https://www.xe.com/currencycharts/?from=XBT&to=USD (accessed 11.28.17).

XE.com, 2017c. XE: XAU / MXN Currency Chart. Gold Ounce to Mexican Peso Rates [WWW Document]. URL https://www.xe.com/currencycharts/?from=XAU&to=MXN (accessed 6.16.17).

XE.com, 2017d. XE: Convert XBT/MXN. BTC to Mexico Peso [WWW Document]. URL http://www.xe.com/currencyconverter/convert/?Amount=0.0005&From=XBT&To=MXN (accessed 11.7.17).

Yeow, A., 2017. Global Bitcoin nodes distribution [WWW Document]. URL https://bitnodes.21.co/ (accessed 10.13.17).

Youtube, 2015. #IMTCWORLD 2015 Entrevista - Pablo Gonzales (BITSO) - YouTube [WWW Document]. URL https://www.youtube.com/watch?v=3beakMIHGos&list=PLrou7z4TGqLPoEYAhqaC4iufoW2qynQJF&index=6 (accessed 7.13.17).

Banking consortium awards Digital Trade Chain contract to IBM [WWW Document], 2017. . Finextra Res. URL https://www.finextra.com/newsarticle/30747/banking-consortium-awards-digital-trade-chain-contract-to-ibm (accessed 9.1.17).

Banxico, 2017a. Mercado cambiario, tipo de cambio, Banco de México - 9 Nov [WWW Document]. URL http://www.banxico.org.mx/portal-mercado-cambiario/index.html (accessed 11.10.17).

Banxico, 2017b. Mercado cambiario, tipo de cambio, Banco de México - 3 de octubre [WWW Document]. URL http://www.banxico.org.mx/portal-mercado-cambiario/ (accessed 6.28.17).

Banxico, 2017c. Mercado cambiario, tipo de cambio, Banco de México - 26 de Mayo [WWW Document]. URL http://www.banxico.org.mx/portal-mercado-cambiario/ (accessed 6.21.17).

Bitcoin ATM Mexico – find bitcoin machine locations [WWW Document], 2014. URL https://coinatmradar.com/country/138/bitcoin-atm-mexico/ (accessed 10.13.17).

Bitcoin Project, 2017a. Descargar - Bitcoin [WWW Document]. URL https://bitcoin.org/es/descargar (accessed 8.26.17).

Bitcoin Project, 2017b. Development - Bitcoin [WWW Document]. URL https://bitcoin.org/en/development (accessed 8.26.17).

Bitcoin Project, 2017c. Download - Bitcoin [WWW Document]. URL https://bitcoin.org/en/download (accessed 8.26.17).

Bitcoin Wiki, 2017. Genesis block - Bitcoin Wiki [WWW Document]. URL https://en.bitcoin.it/wiki/Genesis_block (accessed 10.18.17).

Bitcoin.com, 2017a. Miner Revenue | Bitcoin.com Charts [WWW Document]. URL https://charts.bitcoin.com/chart/miner-revenue#0 (accessed 11.9.17).

Bitcoin.com, 2017b. Blockchain Size | Bitcoin.com Charts | Consulta 17 Nov 2017 [WWW Document]. URL https://charts.bitcoin.com/chart/blockchain-size#0 (accessed 11.17.17).

Bitcoin.com, 2017c. Daily Blocks | Bitcoin.com Charts | Consulta 17 Nov [WWW Document]. URL https://charts.bitcoin.com/chart/blocks-daily#0 (accessed 11.17.17).

Bitcoin.com, 2017d. Daily Transactions | Bitcoin.com Charts | Consulta 17 Nov [WWW Document]. URL https://charts.bitcoin.com/chart/daily-transactions#0 (accessed 11.29.17).

Bitcoin.com, 2017e. Bitcoin Price | Bitcoin.com Charts | Consulta 19 de julio [WWW Document]. URL https://charts.bitcoin.com/chart/price#0 (accessed 11.28.17).

Bitconnect.co, 2018. Legality of Bitcoin & cryptocurrency | Bitconnect [WWW Document]. Bitconnect.co. URL https://bitconnect.co/bitcoin-information/8/legality-of-bitcoin-cryptocurrency (accessed 1.16.18).

Bitso, 2017. Bitso - The Bridge to Mexico's New Digital Economy [WWW Document]. URL https://webcache.googleusercontent.com/search?q=cache:76aOnq_WXAQJ:https://bnktothefuture.com/pitches/bitso/business_page+&cd=2&hl=en&ct=clnk (accessed 8.2.17).

Bitso, 2016. Daniel Vogel de Bitso en El Financiero Bloomberg.

Bitso, 2015. BitPay y Bitso anuncian alianza [WWW Document]. Bitso. URL https://blog.bitso.com/bitpay-y-bitso-anuncian-alianza-e3f9ff66f6aa (accessed 2.2.18).

Blockchain Luxembourg S.A.R.L, 2017a. Bitcoins in circulation [WWW Document]. Blockchain.info. URL https://blockchain.info/total-bitcoins (accessed 10.12.17).

Blockchain Luxembourg S.A.R.L, 2017b. Bitcoin currency statistics - 9 enero a 13 nov [WWW Document]. Blockchain.info. URL https://blockchain.info/stats (accessed 6.1.17).

Blockchain Luxembourg S.A.R.L, 2017c. Total Transaction Fees - BTC [WWW Document]. Blockchain.info. URL https://blockchain.info/transaction-fees (accessed 11.6.17).

Blockchain Luxembourg S.A.R.L, 2017d. Confirmed Transactions Per Day [WWW Document]. Blockchain.info. URL https://blockchain.info/n-transactions (accessed 11.6.17).

Blockchain Luxembourg S.A.R.L, 2017e. 100 Most Popular Bitcoin Addresses - Blockchain.info [WWW Document]. URL https://blockchain.info/popular-addresses (accessed 12.21.17).

Bradbury, D., 2014. How Dangerous is Satoshi Nakamoto? [WWW Document]. CoinDesk. URL http://www.coindesk.com/dangerous-satoshi-nakamoto/ (accessed 11.8.16).

BTC Fácil, 2016. Introducción al Bitcoin.

coindesk, 2018a. Bitcoin Price Index - Real-time Bitcoin Price Charts | Cambio de precio 12 sep 2017 [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 1.10.18).

coindesk, 2018b. Bitcoin Price Index - Real-time Bitcoin Price Charts | Cambio de precio 19 sep 2017 [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 1.10.18).

coindesk, 2018c. Bitcoin Price Index - Real-time Bitcoin Price Charts | Cambio de precio 2 nov 2017 [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 1.10.18).

coindesk, 2017a. Bitcoin Price Index - Real-time Bitcoin Price Charts - Precio Mineros [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 11.9.17).

coindesk, 2017b. Bitcoin Price Index - Real-time Bitcoin Price Charts | 15 Nov 12 [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 11.16.17).

coindesk, 2017c. Bitcoin Price Index - Real-time Bitcoin Price Charts | 19 de julio [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 11.28.17).

coindesk, 2017d. Bitcoin Price Index - Real-time Bitcoin Price Charts - Mayo [WWW Document]. CoinDesk. URL http://www.coindesk.com/price/ (accessed 5.26.17).

coindesk, 2017e. Bitcoin Price Index - Real-time Bitcoin Price Charts - 3 de octubre [WWW Document]. CoinDesk. URL http://www.coindesk.com/price/ (accessed 6.28.17).

coindesk, 2017f. Bitcoin Price Index - Real-time Bitcoin Price Charts - 1 de Junio [WWW Document]. CoinDesk. URL http://www.coindesk.com/price/ (accessed 6.27.17).

coindesk, 2017g. Bitcoin Price Index - Real-time Bitcoin Price Charts - Consulta Zona 2 [WWW Document]. CoinDesk. URL https://www.coindesk.com/price/ (accessed 11.21.17).

coindesk, 2017h. CBOE to Begin Bitcoin Futures Trading December 10 [WWW Document]. CoinDesk. URL https://www.coindesk.com/cboe-begin-bitcoin-futures-trading-december-10/ (accessed 12.17.17).

coinmap.org - Bitcoin accepting shops, ATM's & venues. [WWW Document], 2017. . Coinmaporg - Map Bitcoin Accept. Venues. URL https://coinmap.org/ (accessed 6.16.17).

CoinMarketCap, 2017a. All Cryptocurrencies | CoinMarketCap | Total de Criptomonedas [WWW Document]. URL https://coinmarketcap.com/all/views/all/ (accessed 11.14.17).

CoinMarketCap, 2017b. Bitcoin (BTC) price, charts, market cap, and other metrics | Bitcoin Markets [WWW Document]. URL http://coinmarketcap.com/currencies/bitcoin/#markets (accessed 6.22.17).

CoinTelegraph.com, 2017. World Markets in Selloff, Trump Presidency Spikes Bitcoin Price [WWW Document]. Cointelegraph. URL https://cointelegraph.com/news/world-markets-in-selloff-trump-presidency-spikes-bitcoin-price (accessed 11.19.17).

CoinWarz, 2017. Bitcoin Mining Calculator and Profitability Calculator - CoinWarz - SHA-256 Hash Rate 14,000.00 GH/s [WWW Document]. URL https://www.coinwarz.com/calculators/bitcoin-mining-calculator/?h=14000.00&p=1375.00&pc=0.15&pf=0.00&d=1452839779145.92000000&r=12.50000000&er=7369.30000000&hc=2000.00 (accessed 11.10.17).

De, N., 2017a. Credit Suisse CEO: Bitcoin the "Very Definition of a Bubble" [WWW Document]. CoinDesk. URL https://www.coindesk.com/credit-suisse-ceo-bitcoin-definition-bubble/ (accessed 1.10.18).

De, N., 2017b. "A Real Bubble": Billionaire Warren Buffett Doubles Down on Bitcoin Doubt [WWW Document]. CoinDesk. URL https://www.coindesk.com/real-bubble-billionaire-warren-buffett-doubles-bitcoin-doubt/ (accessed 1.10.18).

De, N., 2017c. World's Largest Hedge Fund Founder: Bitcoin is a "Bubble" [WWW Document]. CoinDesk. URL https://www.coindesk.com/bridgewater-associates-head-says-bitcoin-bubble/ (accessed 1.10.18).

Finney, H., 2013. Bitcoin and me (Hal Finney) [WWW Document]. URL https://bitcointalk.org/index.php?topic=155054.0 (accessed 8.23.17).

Forbes, M., 2016. La startup mexicana que venderá Bitcoins en las tienditas de la esquina [WWW Document]. Forbes Mex. URL https://www.forbes.com.mx/la-startup-mexicana-que-vendera-bitcoins-en-las-tienditas-de-la-esquina/ (accessed 7.11.17).

Gandal, N., Hamrick, J.T., Moore, T., Oberman, T., 2017. Price Manipulation in the Bitcoin Ecosystem. Workshop Econ. Inf. Secur. WEIS 2017.

Geografía (INEGI), 2017. Descarga masiva [WWW Document]. URL http://www.beta.inegi.org.mx/app/descarga/# (accessed 12.19.17).

Geografía (INEGI), I.N. de E. y, 2014. Directorio Nacional de Unidades Económicas. DENUE [WWW Document]. Censos Económicos 2014. URL http://www.beta.inegi.org.mx/app/mapa/denue/default.aspx (accessed 12.19.17).

Goodin, D., 2012. 25-GPU cluster cracks every standard Windows password in <6 hours [WWW Document]. Ars Tech. URL https://arstechnica.com/information-technology/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/ (accessed 10.11.17).

Google, 2017. ¿qué es bitcoin? - Google Search [WWW Document]. URL https://encrypted.google.com/search?q=que+es+bitcoin&hl=en&biw=1366&bih=602&source=lnt&tbs=cdr%3A1%2Ccd_min%3A5%2F28%2F2016%2Ccd_max%3A8%2F28%2F2016&tbm=#safe=off&hl=en&tbs=cdr:1,cd_min:5/28/2016,cd_max:8/28/2016&q=%C2%BFqu%C3%A9+es+bitcoin? (accessed 6.21.17).

Graham, G., 2017. The White Paper FAQ (Frequently Asked Questions). White Pap. Guy - Gordon Graham.

Hern, A., 2015. Bitcoin creator Satoshi Nakamoto denies being Craig Wright (maybe).

How did Satoshi register bitcoin.org? [WWW Document], 2016. URL https://bitcointalk.org/index.php?topic=103369.msg1134000 (accessed 11.7.16).

ISBIT, 2017. Plataforma de Intercambio de Activos Digitales Líder en México - ISBIT [WWW Document]. URL https://www.isbit.co/ (accessed 12.21.17).

Juan S. Galt (@JuanSGalt) | Twitter [WWW Document], 2016. URL https://twitter.com/JuanSGalt (accessed 11.15.16).

Lee, T.B., 2017. A brief history of Bitcoin hacks and frauds [WWW Document]. Ars Tech. URL https://arstechnica.com/tech-policy/2017/12/a-brief-history-of-bitcoin-hacks-and-frauds/ (accessed 12.21.17).

Lerner, S.D., 2013. The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius. Bitslog.

Lerner, S.D., 2011. About. Bitslog.

LetsTalkBitcoin.com, 2014. User Info - jratcliff63367 | Lets Talk Bitcoin [WWW Document]. URL https://letstalkbitcoin.com/profile/user/jratcliff63367 (accessed 11.17.17).

Licencia MIT, 2017. . Wikipedia Encicl. Libre.

LocalBitcoins, 2017. About LocalBitcoins.com [WWW Document]. URL https://secure.livechatinc.com/licence/5492471/open_chat.cgi?groups=0&embedded=1&newWebserv=undefined&__lc_vv=2&session_id=S1504052906.06db9c0ddc&server=secure.livechatinc.com#https://localbitcoins.com/about (accessed 10.13.17).

Malmi, M., 2015. I'm Martti Malmi, early bitcoin developer and the original founder of the Bitcointalk.org forums, AMA! [WWW Document]. Bitcoin Forum. URL https://forum.bitcoin.com/ama-ask-me-anything/i-m-martti-malmi-early-bitcoin-developer-and-the-original-founder-of-the-bitcointalk-org-forums-ama-t2770.html (accessed 9.8.17).

Mark, 2015. Bitcoin Wallets Comparison Chart and Reviews. The Merkle.

MaxSaldo, 2017. Como funciona Maxsaldo - Recargas Electrónicas Pago de Servicios [WWW Document]. URL https://www.maxsaldomexico.com/como-ganar/ (accessed 7.14.17).

McGrath Goodman, L., 2014. The Face Behind Bitcoin [WWW Document]. Newsweek. URL http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html (accessed 11.8.16).

memonius, 2014. Zmart Group 4 min.

Metzdowd - cryptography Info Page [WWW Document], n.d. URL http://www.metzdowd.com/mailman/listinfo/cryptography (accessed 8.23.17).

Mifiel, 2017. Preguntas Frecuentes [WWW Document]. Mifiel. URL https://www.mifiel.com/es/preguntas (accessed 10.4.17).

Monaghan, A., 2017. Bitcoin is a fraud that will blow up, says JP Morgan boss. The Guardian.

Money & Tech, 2014. Pablo Gonzalez & Ben Peters of Bitso @ CoinSummit.

Nakamoto, S., 2017. bitcoin: Bitcoin Core integration/staging tree. Bitcoin.

Nakamoto, S., 2010a. What's with this odd generation? [WWW Document]. URL https://bitcointalk.org/index.php?topic=48.msg329#msg329 (accessed 9.7.17).

Nakamoto, S., 2010b. How divisible are bitcoins and other market/economic questions [WWW Document]. URL https://bitcointalk.org/index.php?topic=44.msg267#msg267 (accessed 9.7.17).

Nakamoto, S., 2009. Bitcoin v0.1 released [WWW Document]. URL https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html (accessed 10.12.17).

Nakamoto, S., 2008a. Bitcoin P2P e-cash paper - PDF.

Nakamoto, S., 2008b. Bitcoin P2P e-cash paper | Primera Publicación [WWW Document]. URL https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html (accessed 10.25.17).

Nakamoto, S., 2008c. Re: Bitcoin P2P e-cash paper [WWW Document]. URL https://www.mail-archive.com/cryptography@metzdowd.com/msg09980.html (accessed 8.23.17).

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27, Discussions, V., 2014a. Bitcoin open source implementation of P2P currency | Mar [WWW Document]. URL http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A52186 (accessed 9.6.17).

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27, Discussions, V., 2014b. Bitcoin open source implementation of P2P currency | Sept [WWW Document]. URL http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?xg_source=activity&id=2003008%3ATopic%3A9402&page=4 (accessed 10.26.17).

Prahalad, B., 2016. Should I keep my Bitcoin on an exchange or in a wallet? - Quora [WWW Document]. URL https://www.quora.com/Should-I-keep-my-Bitcoin-on-an-exchange-or-in-a-wallet (accessed 10.27.17).

Ratcliff, J.W., 2014. Rise of the Zombie Bitcoins [WWW Document]. Lets Talk Bitcoin. URL https://letstalkbitcoin.com/blog/post/rise-of-the-zombie-bitcoins (accessed 11.17.17).

Reforma, 2016. Hay Bitcoins... ¡en Ixtapaluca! [WWW Document]. URL http://www.reforma.com/aplicacioneslibre/articulo/default.aspx?id=855153&md5=cb704d14c0ab6149345890a85040acc8&ta=0dfdbac11765226904c16cb9ad1b2efe&lcmd5=1ce3a794c9b4222932b16999aacbad57 (accessed 6.21.17).

Reinhold, A.G., 2017. Diceware Passphrase Home [WWW Document]. URL http://world.std.com/~reinhold/diceware.html (accessed 10.10.17).

satoshin@gmx.com is compromised [WWW Document], 2016. URL https://bitcointalk.org/index.php?topic=775174.0 (accessed 11.7.16).

Simmel, G., 2016. Philosophie des Geldes, Primera Edición. ed. Ediciones Culturales Paidos S. A. de C. V.

StackExchange, 2013. password cracking - What is the entropy of just 1 Diceware passphrase like my passphrase? - Information Security Stack Exchange [WWW Document]. URL https://security.stackexchange.com/questions/36246/what-is-the-entropy-of-just-1-diceware-passphrase-like-my-passphrase (accessed 10.11.17).

Staff, G.L.R.D., 2016. Bitcoin Survey [WWW Document]. URL https://www.loc.gov/law/help/bitcoin-survey/ (accessed 1.19.18).

The Guardian, 2017. How the Winklevoss twins became the world's first bitcoin billionaires [WWW Document]. the Guardian. URL

http://www.theguardian.com/technology/shortcuts/2017/dec/04/winklevoss-twins-bitcoin-billionaires-mark-zuckerberg (accessed 1.19.18).

THEOI, 2017. MIDAS - Phrygian King of Greek Mythology [WWW Document]. URL http://www.theoi.com/Heros/Midas.html (accessed 6.16.17).

Tipo de Cambio del Dólar y Divisas | Banamex.com [WWW Document], 2017. URL https://www.banamex.com/economia_finanzas/es/divisas_metales/resumen.htm (accessed 5.26.17).

Top Open Source Licenses [WWW Document], n.d. . Black Duck Softw. URL https://www.blackducksoftware.com/top-open-source-licenses (accessed 8.29.17).

Volabit, 2017. ¿Qué es Volabit? - Preguntas Frecuentes | Volabit [WWW Document]. URL http://ayuda.volabit.com/article/75-que-es-volabit (accessed 12.21.17).

Wikipedia, 2018. Legality of bitcoin by country or territory. Wikipedia.

Wikipedia, 2017a. Solicitud de información. Wikipedia Encicl. Libre.

Wikipedia, 2017b. Winklevoss twins. Wikipedia.

XE.com, 2017a. XE: XBT / USD Currency Chart. Bitcoin to US Dollar Rates | Consulta 19 de julio 2010 [WWW Document]. URL http://www.xe.com/currencycharts/?from=XBT&to=USD&view=10Y (accessed 11.28.17).

XE.com, 2017b. XE: XBT / USD Currency Chart. Bitcoin to US Dollar Rates | precio al 28 de noviembre [WWW Document]. URL https://www.xe.com/currencycharts/?from=XBT&to=USD (accessed 11.28.17).

XE.com, 2017c. XE: XAU / MXN Currency Chart. Gold Ounce to Mexican Peso Rates [WWW Document]. URL https://www.xe.com/currencycharts/?from=XAU&to=MXN (accessed 6.16.17).

XE.com, 2017d. XE: Convert XBT/MXN. BTC to Mexico Peso [WWW Document]. URL http://www.xe.com/currencyconverter/convert/?Amount=0.0005&From=XBT&To=MXN (accessed 11.7.17).

Yeow, A., 2017. Global Bitcoin nodes distribution [WWW Document]. URL https://bitnodes.21.co/ (accessed 10.13.17).

Youtube, 2015. #IMTCWORLD 2015 Entrevista - Pablo Gonzales (BITSO) - YouTube [WWW Document]. URL https://www.youtube.com/watch?v=3beakMIHGos&list=PLrou7z4TGqLPoEYAhqaC4iufoW2qynQJF&index=6 (accessed 7.13.17).