UNCUYO
UNIVERSIDAD NACIONAL DE CUYO

FCE
FACULTAD DE CIENCIAS ECONÓMICAS

Carrera: Lic. en Administración.

# Bitcoin: Innovación financiera y refugio contra el estatismo

Trabajo de investigación


POR:

Alberto Conti

Profesor Tutor:

Mgtr. Alejandro Bartolomeo


Mendoza - 2017

# ÍNDICE


**I – INTRODUCCIÓN** 4

**II – CAPÍTULO I. HISTRORIA DEL DINERO** 5

- **A. Surgimiento: Del valor intrínseco al tercero de confianza.** 5
- **B. Edad Media y Edad Moderna: consolidación del monopolio de acuñación.** 8
- **C. Surgimiento de los Bancos Centrales.** 8
- **D. Crisis del ´29.** 10
- **E. El cambio de paradigma: 1971.** 10

**III – CAPÍTULO II. ASPECTOS TECNICOS DEL BITCOIN** 14

- **A. Una red descentralizada para transferencias persona a persona.** 14
- **B. Pasos para comenzar a operar en la red Bitcoin.** 15
- **C. La Blockchain: características y funcionamiento.** 17
- **D. Minería de Bitcoins.** 18
- **E. Minería hoy: Pooles y granjas.** 22

**IV – CAPÍTULO III. ECONOMÍA, HISTORIA Y FILOSOFÍA DEL BITCOIN** 25

- **A. Internet: un gran salto para la Humanidad.** 25
- **B. La antesala al Bitcoin: Predecesores y visionarios.** 27
- **C. La combinación imposible.** 29
- **D. Administrando la escasez.** 29
- **E. La máquina de generar confianza.** 30

**F. Hay confianza, pero ¿hay moneda?** **32**

**G. Bitcoin como producto y motor del cambio.** **35**

**V – CAPÍTULO IV. CONCLUSIONES, PRNOSTICOS Y RECOMENDACIONES** **37**

**A. Fortalezas** **37**

1. Poder de cómputo de toda la red Bitcoin. **37**
2. Desarrollo de las "AltCoins". **38**
3. Ritmo de emisión predecible. **39**
4. Aval de referentes: **39**

**B. Oportunidades.** **40**

1. Camino a la adopción masiva. **40**
2. Robarle al Forex. **41**
3. Más allá de la moneda: Desarrollos sobre Blockchain. **42**

**C. Amenazas.** **43**

1. Intervención gubernamental. **43**

**D. Debilidades** **44**

1. Escalabilidad. **44**

**E. Recomendaciones.** **47**

**VI – BIBLIOGRAFÍA** **48**

# INTRODUCCION

La presente investigación intentará introducir al lector en el funcionamiento de una de las tecnologías más disruptivas de los últimos tiempos, la cual apunta ni más ni menos que a generar un cambio permanente en el sistema monetario vigente, modificando el paradigma actual sobre lo que consideramos dinero. Se aspira con el presente trabajo lograr un análisis fundamentado de las razones por las que este desarrollo tecnológico podría llegar a ser exitoso en su cometido, a fin de que el lector pueda determinar la conveniencia o no de invertir recursos en el mismo durante su actual etapa de desarrollo, tratando de alguna manera cuantificar riesgos y retornos esperados de una hipotética inversión.

En el primer capítulo se llevará a cabo un repaso sobre las distintas formas de dinero que existieron a lo largo de la historia de la humanidad y las causas que nos llevaron a la adopción del dinero con el que actualmente operamos. Este abordaje resulta necesario para el presente trabajo a fin de explicitar como es que la sociedad actual llego a adoptar una forma de dinero que dista tanto de las características históricas de moneda y a su vez desnudar sus falencias a fin contrastarlas en los siguientes capítulos con las soluciones propuestas por esta nueva tecnología.

En el segundo capítulo se expondrán los procedimientos técnicos básicos mediante los cuales esta “Criptomoneda” logra funcionar junto con la forma en que el sistema es auditado y los pasos necesarios para poder operar con la misma.

Ya en el tercer capítulo, una vez explicitadas las virtudes y defectos del sistema monetario actual y aclarados los aspectos técnicos del funcionamiento del Bitcoin, iniciamos un análisis económico de esta nueva tecnología junto con los aspectos históricos y filosóficos que subyacen a su aparición.

Finalmente, en el cuarto capítulo se realizará un análisis tanto de las virtudes y defectos propios de este desarrollo tecnológico como de las variables del entorno que pueden afectarlo, a fin de poder concluir con algunas recomendaciones al respecto para los lectores.

# CAPITULO I

# HISTORIA DEL DINERO

Para el desarrollo de este capítulo las fuentes consultadas fueron la obra del historiador Yuval Harari "Sapiens. De animales a dioses: Una breve historia de la humanidad.", especialmente para la redacción de la primera sección; junto con "El origen del dinero" de Carl Menger y "La miseria del intervencionismo: 1929-2008" del Axel Kaiser, las cuales resultaron de especial utilidad para la confección de las 4 secciones siguientes, como así también el portal de la reserva federal del estado de Saint Louis "stlouisfed.org", fuente de información sobre la evolución del costo de vida en los EE.UU.

## A) SURGIMIENTO: DEL VALOR INTRINSECO AL TERCERO DE CONFIAZA

Es imposible determinar en qué fecha o territorio la humanidad comenzó a utilizar por primera vez el dinero, ya que fue creado muchas veces y en muchos lugares. Su desarrollo no requirió grandes descubrimientos tecnológicos: fue una revolución puramente mental. Implicó la creación de una nueva realidad intersubjetiva que solo existe en la imaginación compartida de la gente. El dinero no es precisamente las monedas y los billetes transados, de hecho, el dinero existió mucho antes de que se inventara la acuñación, y ha habido culturas que han prosperado empleando conchas, pieles, sal, grano, cuentas o tela como dinero. Las conchas blancas o cauris se utilizaron como moneda durante unos 4.000 años en toda África, el Sudeste Asiático, Asia oriental y Oceanía. A principios del siglo XX, en la Uganda Británica todavía podían pagarse los impuestos mediante cauris. De hecho, incluso hoy en día, desde un punto de vista macro, las monedas y billetes son una forma poco común de dinero. En el año 2008, la suma total de dinero en el mundo llegaba a unos 60 billones de dólares, pero la suma total de monedas y billetes no llegaba a los 6 billones de dólares. Más del 90% de todo el dinero (más de 50 billones de dólares que aparecen en nuestras cuentas) existe solo en los servidores informáticos.

En definitiva, el dinero es cualquier cosa que la gente esté dispuesta a utilizar para representar de manera sistemática el valor de otras cosas con el propósito de intercambiar bienes y servicios. Así es que el dinero es un sistema de confianza mutua, y no cualquier sistema de confianza mutua: El dinero es el más universal y más eficiente sistema de confianza mutua que jamás se haya inventado. Dicha confianza se fue formando muy lentamente, mediante el tejido de una red compleja de relaciones políticas, sociales y económicas.

Inicialmente, cuando surgieron las primeras versiones de dinero, no existía ese tipo de confianza entre la gente, por lo que fue necesario definir como "dinero" cosas que tenían un valor intrínseco real. El primer dinero conocido de la historia, el dinero de cebada sumerio, es un buen ejemplo. Apareció en Sumer hacia 3000 a.C., para dar respuesta a las necesidades de actividades económicas que se hacían más intensas. Cuencos normalizados con capacidad para una "sila" (840 gramos) de cebada comenzaron a utilizarse para expresar de forma estandarizada el valor del resto de los bienes de la economía. De esta forma, cualquier bien transable en Sumer tenía un precio equivalente a cierta cantidad de silas de cebada.

La cebada tiene un valor intrínseco porque la cebada tiene un valor biológico: los humanos pueden comerla. El gran avance en la historia del dinero se produjo cuando la gente llegó a confiar en dinero que carecía de valor intrínseco. Tal dinero apareció en la antigua Mesopotamia a mediados del tercer milenio a.C. Se trata del siclo de plata, el cual no era una moneda, sino una medida equivalente a 8,33 gramos de plata. Para ese entonces fue que se promulgo el célebre código de Hammurabi, el cual fijaba penas a quienes infringieran sus normas en siclos de plata, lo que implicaba abonar al rey, según el tipo de delito, determinada cantidad de gramos de plata. A diferencia de la sila de cebada, el siclo de plata era más fácil de almacenar y transportar, pero no tenía un valor intrínseco. La plata no se puede comer, beber ni hacer vestidos con ella, y es demasiado blanda para producir herramientas útiles, ya que los arados o espadas de plata se deforman casi tan fácilmente como si fuesen hechos de papel de aluminio. Cuando no era usada como medio de intercambio, la plata, y también el oro, eran transformados en joyas, coronas y otros símbolos de jerarquía: bienes de lujo que los miembros de una determinada cultura identificaban con un nivel social elevado. El valor de estos metales era, y sigue siendo, salvo por algunos usos industriales, puramente cultural.

Al siclo de plata lo siguieron diferentes tipos de pesos fijados de metales preciosos, y con el tiempo estos acabaron dando origen a las monedas. Las primeras monedas de la historia las hizo acuñar el rey Aliates de Lidia hacia el año 640 a.C., donde actualmente se encuentra Turquía. Estas monedas tenían un peso normalizado de oro o plata, y se acuñaban con una marca que testificaba cuánto metal precioso contenía la moneda y quien era la autoridad que garantizaba su contenido. Casi todas las monedas en uso en la actualidad son descendientes de las monedas de Lidia. Las monedas relegaron a los lingotes de metal sin marcas principalmente porque al contener la rúbrica de alguna autoridad política que garantizaba su valor evitaba a los vendedores tener que tomar medidas para corroborar que el metal entregado por el comprador era realmente del peso y la pureza manifestado por este. De esta forma, el surgimiento de la moneda marcó un salto en la eficiencia de las transacciones económicas al generalizar la figura del tercero de confianza, rol que ocupaba el rey o emperador que acuñaba la moneda y actuaba como garante entre las partes.

Recién más de dos milenios después, con la aparición del Bitcoin, se daría el primer caso en la historia de una moneda que logra sortear la necesidad de un “tercero de confianza”, ya que las partes intervinientes en la transacción depositan su confianza en una red descentralizada y abierta que audita la validez de las operaciones de forma fehaciente, pero este mecanismo será descripto en detalle recién en el próximo capítulo.

Al popularizarse la figura del tercero de confianza personas totalmente extrañas podían aceptar el valor de un denario romano porque creían en el poder y la integridad del emperador romano, cuyo nombre e imagen decoraban la moneda. La confianza en las monedas de Roma era tan fuerte que incluso fuera de los límites del imperio a la gente le gustaba recibir su paga en denarios. Las monedas romanas eran un medio de intercambio aceptado en los mercados de la India, aunque la legión romana más cercana se hallaba a miles de kilómetros de distancia. Los indios tenían una confianza tan fuerte en el denario y en la imagen del emperador que cuando los gobernadores locales acuñaron sus propias monedas imitaron fielmente al denario, incluso hasta el retrato del emperador romano. El nombre «denario» se convirtió en un término genérico para las monedas en casi todo el mundo, así fue que hasta los califas musulmanes arabizaron este nombre y emitieron «dinares».

## B) EDAD MEDIA Y EDAD MODERNA: CONSOLIDACION DEL MONOPOLIO DE ACUÑACION

Este privilegio con el que contaba el gobernante de disponer del monopolio de la acuñación se estableció firmemente con los emperadores romanos y fue creciendo con el paso de los siglos. Cuando, al principio de la Edad Moderna, Jean Bodin, (París, S. XVI) desarrolló el concepto de soberanía, incluyó el derecho de acuñar moneda como uno de sus componentes más importantes y esenciales. Este privilegio fue durante la Edad Media la principal fuente de ingresos de los príncipes ya que además de representar un importante instrumento del poder, comenzó a ser una tentadora fuente de ganancias, al instaurarse la práctica de acuñar monedas con menor contenido de oro y plata que el declarado en ellas.

Así vemos que el monopolio estatal de emisión de moneda ya era bastante pernicioso mientras predominaba el dinero metálico. Ahora bien, se convirtió en una terrible calamidad con el surgimiento del papel moneda, pero específicamente cuando este estuvo bajo control estatal. Ante el surgimiento de los primeros bancos, fundados en Amsterdam y luego en otras ciudades de Europa, se dio la exitosa aparición de los primeros ejemplares de papel moneda, y junto con estos se vieron experimentos privados donde crearon monedas estables y virtuosas, ya que el propio interés de los banqueros compitiendo entre sí los obligaba a satisfacer los deseos de los usuarios, controlando la oferta de dinero. Pero el creciente absolutismo pronto dinamitó estas primeras apariciones de monedas no estatales. En lugar de ello, los monarcas protegieron el crecimiento de los bancos que emitían los billetes respaldados por el estado.

## C) SURGIMIENTO DE LOS BANCOS CENTRALES

El nivel de control estatal fue creciendo al punto de que en 1694 el poderoso e influyente clan Rothschild, junto con sus socios Loeb, Lehman y otros fundaron el Banco de Inglaterra, que, si bien nació como un banco privado y comercial, tenía como función principal el servir como banco del gobierno del Reino Unido, y ya para 1844, mediante la sanción de la ley de Peel, quedó definitivamente garantizado su monopolio para la emisión de moneda.

Décadas después, en la que pasó a ser la nueva potencia económica mundial, la creación de la Reserva Federal siguió exactamente la misma lógica.

Durante gran parte del siglo XIX rigió en Estados Unidos la denominada era del “Free Banking”, que consistía en un sistema mixto donde, si bien el gobierno establecía ciertas exigencias para los bancos, como la de que al menos 1/5 de sus reservas consistieran en bonos del gobierno federal o límites sobre tasas de interés que cobraban, se les permitió a estas instituciones emitir billetes respaldados en especie (oro o plata), los cuales circulaban libremente por los diferentes estados.

Pero tras una importante crisis económica iniciada en 1907 y producto de la hábil gestión de las élites financieras, particularmente de los Morgan, los Rockefeller, los Kuhn y los Loeb, hastiados de la dura y creciente competencia que planteaban los bancos locales (pequeñas y medianas instituciones regionales con poca cantidad de sucursales), consiguieron que el Congreso y el Presidente Woodrow Wilson les otorgaran en forma de cartel el control sobre la emisión de dinero. Así fue que este grupo redactó el borrador de la ley que creó en 1913 la Reserva Federal. De ahí en adelante, sólo la FED podía imprimir dinero. Si antes de la FED los bancos estaban obligados a contener la expansión monetaria y a competir entre ellos, con la FED pudieron inflar la masa monetaria al unísono, contando además con un prestamista de última instancia que los rescataría en caso de problemas.

Como era previsible, esto derivó en la paulatina destrucción del poder adquisitivo del dólar. Tomando como referencia la evolución del índice de precios al consumidor de Estados Unidos (IPC), desde la creación de la FED en 1913, el precio a pagar por un producto que en 1913 costaba 100 dólares, en 2011 era de 2.257 dólares, lo que refleja una inflación acumulada de un 2.157,2%. Cabe destacar que con anterioridad a la creación de la FED el dólar, salvo por ciertos períodos de convulsión como la guerra civil estadounidense, mantuvo su poder adquisitivo prácticamente intacto desde 1800 ver grafico

Así mismo, el argumento para defender la existencia de los bancos centrales es que sin éstos la economía sería inestable y susceptible de repetidos pánicos financieros. Se dice que sin ellos ésta no sería lo suficientemente moderna. Al momento de fundar la FED, el contralor de la moneda en Estados Unidos incluso afirmó que gracias a la creación de la FED «los pánicos financieros y crisis comerciales con sus postraciones y miserias pasarían a ser una imposibilidad matemática», agregando que de ahora en adelante «las quiebras de bancos nacionales serían virtualmente eliminadas». La verdad, no obstante, es que el mercado nunca ha sido más inestable ni las crisis más devastadoras que desde la creación de la Reserva Federal. Según registra el National Bureau of Economic Research, desde 1913, cuando se creó la

FED, en Estados Unidos se han verificado las siguientes recesiones: 1918-1919, 1920-1921, 1923-1924,1926-1927, 1929-1933, 1937-1938, 1945, 1948-1949,1953-1954, 1957-1958,1960-1961, 1969-1970, 1973, 1975, 1980, 1981-1982, 1990-1991, 2001 y finalmente 2007. Evidentemente algo salió mal con el cálculo matemático.

## D) CRISIS DEL ´29

Los efectos de este cambio en las reglas de juego no tardaron mucho en manifestarse. En efecto, entre 1921 y 1929, la FED, coordinadamente con el Banco de Inglaterra, incrementó la masa monetaria en un 61,8%, esencialmente en forma de crédito.

El colapso llegó en octubre de 1929, seis meses después que la Reserva Federal pusiera fin a la expansión del crédito. La burbuja reventó llevando a una caída de un 89% en la bolsa durante los tres años siguientes, desplome del cual el mercado accionario no se recuperaría completamente hasta 1954.

En 1966, Alan Greenspan, atribuyó el fatídico evento a la política monetaria de la época en los siguientes términos: “El exceso de crédito que la FED inyectó a la economía entró al mercado accionario detonando una espectacular burbuja especulativa. Tardíamente, los funcionarios de la Reserva Federal intentaron extraer el exceso de reservas logrando finalmente poner fin al boom. Pero era demasiado tarde: hacia 1929 los desbalances especulativos habían alcanzado tales niveles que este intento precipitó una aguda contracción y la consecuente desmoralización en la confianza de los inversionistas. Como resultado, la economía de Estados Unidos colapso”, tal como lo cita Axel Kaiser en su obra “La miseria del intervencionismo: 1929-2008”.

## E) EL CAMBIO DE PARADIGMA: 1971

Hasta las primeras décadas del siglo pasado, todas las monedas del mundo estaban acopladas al oro. Así, un dólar era siempre convertible por 1/20 de onza de oro mientras la paridad de la libra estaba fijada a 1/4 de onza. El patrón oro implicaba que privados y gobiernos extranjeros podían convertir en cualquier momento su dinero de papel en metal, por lo que cuando los bancos centrales incrementaban

la masa monetaria en exceso se arriesgaban a generar una corrida de los tenedores de billetes en busca de sus reservas de dicho metal.

En Estados Unidos, oficialmente esto se mantuvo hasta que Franklin Roosevelt en 1934 dictara una orden ejecutiva que impuso la confiscación del oro en poder de los ciudadanos estadounidenses, castigando con multas y cárcel la posesión de cantidades del metal equivalentes a 100 dólares o más y declarando nulos todos los contratos entre privados cuyo pago estaba fijado en oro. Lo de Roosevelt fue ciertamente una expropiación abusiva al público estadounidense, al que el gobierno pagó 20,67 dólares por onza de oro para, inmediatamente después de la confiscación, devaluar el dólar fijando la nueva convertibilidad en 35 dólares la onza. Pero si bien Roosevelt le puso fin al patrón oro dentro Estados Unidos, no pudo aplicar la misma regla a otros países, razón por la cual éste continuó estando vigente internacionalmente. Es decir, los poseedores de dólares en el extranjero podían en cualquier momento exigir la conversión de sus dólares en oro en Estados Unidos al valor de 35 dólares por onza.

El sistema de convertibilidad en oro entre naciones se confirmó, bajo una fórmula menos efectiva, en el famoso acuerdo de Bretton Woods que tuvo lugar en Nueva York en 1944 y cuyo fin fue el diseño de un nuevo orden económico por parte de las potencias vencedoras en la Segunda Guerra Mundial. En ella se estableció que el dólar sería la moneda de reserva internacional, fijando las demás monedas al dólar. De este modo, por ejemplo, si Inglaterra veía caer el precio de la libra frente al dólar, su Banco Central saldría a comprar libras utilizando para ello dólares que tenía acumulados en sus reservas, de modo de aumentar el valor de la libra. Por el contrario, si el dólar se depreciaba, Inglaterra tendría que imprimir libras para comprar dólares, es decir, devaluar su moneda importando así la inflación desde Estados Unidos. Esto, a su vez, daba tranquilidad a todos los inversionistas con activos denominados en libras de que sus inversiones se mantendrían estables en términos de dólares. El dólar en tanto se mantendría fijado a un valor de 35 dólares la onza de oro, lo cual en principio tenía por objeto evitar la inflación de la masa monetaria por parte de la Reserva Federal. Bajo las nuevas reglas, sin embargo, ninguna empresa privada o individuo particular podía exigir la convertibilidad en oro, reservando el derecho para los gobiernos y bancos centrales.

Bajo este sistema entonces, cuando un país tenía superávit comercial en teoría podía convertir el exceso de dólares en su poder por oro en Estados Unidos. Así, los estadounidenses se cuidarían supuestamente de imprimir demasiados dólares para no ver desaparecer sus reservas de oro. Durante

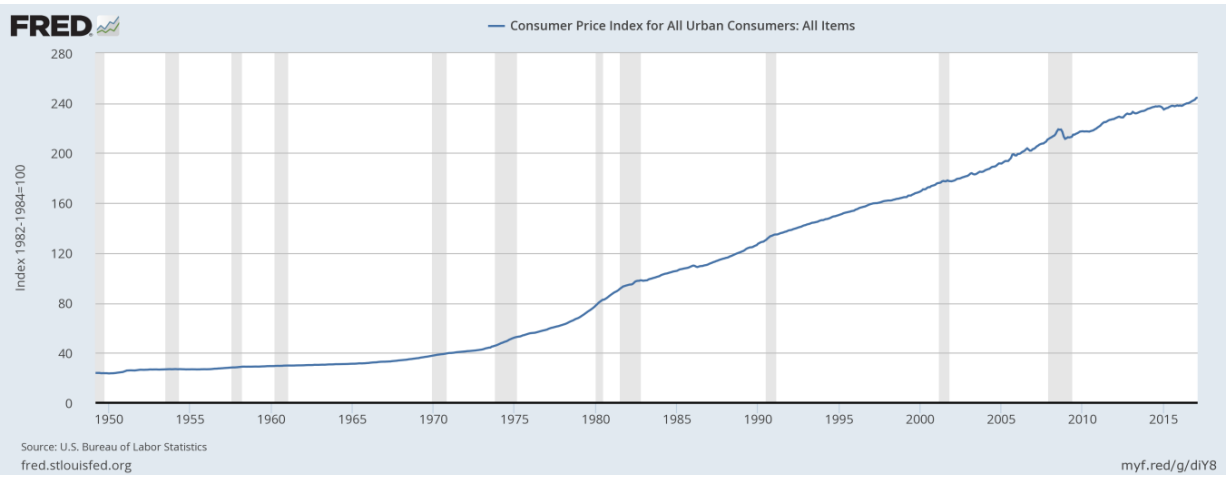
más de dos décadas el sistema funcionó, proveyendo de una clara ventaja a Estados Unidos, que vio su moneda artificialmente apreciada.

Como era de esperar, su creciente gasto fiscal debido a la Guerra Fría y a la expansión de los programas de bienestar llevó al país a imprimir cada vez más dólares. Países como Francia reaccionaron exigiendo la conversión de sus excesos de dólares en oro, provocando un drenaje del metal precioso que enfrentó a Estados Unidos a la posibilidad de perder sus reservas, lo que en la práctica significaba la quiebra.

Bajo esta presión, en 1971 Richard Nixon decidió poner fin al padrón oro llevando al mundo por primera vez a un completo estándar de dinero papel, denominado también dinero Fiat (por decreto).

El resto de la historia es imaginable. Sin el único freno que todavía existía para contener la voracidad de los políticos por imprimir moneda y dar rienda suelta a sus deseos de disparar el gasto militar, los subsidios a diversos grupos de interés, o los rescates a instituciones financieras, la cantidad de dinero creado por la Reserva Federal experimenta un incremento sostenido desde 1970, generando una pérdida de poder adquisitivo del dólar del 80% hasta 2011:

Gráfico n°1: Indice de precios al cosnumidor en EE.UU. 1950 a 2015.




*Fuente: Banco de la Reserva Federal de St. Louis. http://stlouisfed.org/*

Es importante tener presente toda esta información antes de abordar el funcionamiento del Bitcoin, ya que, al igual que el resto de las monedas de papel en la actualidad, no se encuentra respaldado por ningún bien tangible, lo cual genera ciertas suspicacias entre aquellos que comienzan a adentrarse en su lógica, olvidando o desconociendo que el resto de las monedas actuales poseen la misma característica; pero con el agregado de que el Bitcoin, como veremos más adelante en detalle, no carga con los riesgos a los que están supeditadas las monedas Fiat, derivados, por ejemplo, de manejos arbitrarios en su oferta o manipulaciones en las tasas de interés.

# CAPITULO II

# ASPECTOS TECNICOS DEL BITCOIN

Para la redacción de este capítulo debieron ser estudiadas las obras “Mastering Bitcoin”, cuya autoría corresponde a quien es probablemente el mejor divulgador de esta tecnología en la actualidad, el estadounidense Andreas Antonopoulos, además de, lógicamente, el paper académico que dio origen a esta tecnología: “Bitcoin: Un sistema de dinero electrónico entre iguales (P2P).” firmado por Satoshi Nakamoto, cuya identidad continua desconocida, como así también la completa y didáctica obra de Juan Manuel González Otero: “Bitcoin: la moneda del futuro”. De igual manera fue de gran utilidad la información obtenida en los portales especializados: “blockchain.info”, “bitcoinfundation.org”, “coindesk.com”, “wired.com” y “en.wikipedia.org/wiki/Bitcoin”.

## A) UNA RED DESCENTRLIZADA PARA TRANSFERENCIAS PERSONA A PERSONA

Este capítulo tiene como objetivo desglosar el funcionamiento de la red bitcoin, detallando, entre otras cosas, los pasos necesarios para comenzar a utilizar esta moneda, como así también la forma en que el sistema ejecuta, audita y registra las transacciones.

Hasta hace pocos años, el comercio en Internet dependía casi de forma exclusiva de las entidades financieras, que actúan como terceros de confianza en el procesamiento de los pagos electrónicos. Aunque para la mayoría de transacciones resulte lo bastante efectivo, este sistema todavía carga consigo las debilidades inherentes del modelo de confianza en el que está basado: imposibilidad de realizar

transacciones anónimas, la posibilidad de retroceder pagos, altos costos que tornan inviables las transferencias de montos pequeños de dinero y la incapacidad de evitar cierto porcentaje de operaciones fraudulentas.

En cambio, el sistema que vamos a describir es completamente descentralizado. Esto implica una importante diferencia con, por ejemplo, una transferencia electrónica de fondos desde una cuenta bancaria a otra, la cual es posible técnicamente gracias a la existencia de varios centros de cómputos de la empresa responsable de procesar las transferencias para el banco, los cuales se encuentran en lugares físicos determinados, y responden a un mando central. Con Bitcoin no existe ninguno de estos elementos, ya que su red logra sostenerse mediante el poder computacional brindado por innumerables máquinas pertenecientes a miles de usuarios conectados a la red, diseminados libremente alrededor del mundo, formando una red de pares, "peer to peer", prescindiendo así de una cede central, centro de cómputos o incluso, de una autoridad visible, ya que ni siquiera se conoce la identidad de la persona que diseño el protocolo con el cual funciona el sistema.

A lo largo del capítulo veremos cómo está diseñada la red y el modo en que están dispuestos los incentivos a fin de que los diferentes actores se comporten de forma coordinada sin la necesidad de un mando que los dirija.

## B) PASOS PARA COMENZAR A OPERAR EN LA RED BITCOIN

Lo primero que debemos hacer para empezar a operar con BTC es crear una cuenta, también llamada billetera, la cual se puede generar de forma gratuita e inmediata, ya sea descargando en una computadora o celular el programa "Cliente Oficial Bitcoin", o bien, creando una cuenta on-line entre la decena de servicios existentes a tal fin. Una vez creada la misma, lo cual puede ser de forma completamente anónima, dispondremos de dos claves o "llaves", una llamada pública y la otra privada que serán utilizadas al momento de enviar o recibir BTC.

El paso siguiente será incorporar fondos a nuestra cuenta vacía, esto se puede lograr básicamente de 3 maneras:

a) Recibiendo bitcoins desde la billetera de un tercero, como contraprestación por la entrega de dinero fiat, productos y/o servicios

b) Comprándolos a cambio de dinero fiat en alguna casa de cambio (Exchange) de Bitcoins.

c) Prestando poder de procesamiento a la red madre de Bitcoin (Minado).

Para poder recibir los bitcoins deberemos comunicarle a la contraparte nuestra clave pública, ya que es la dirección a la cual harán el envío, pero no así la clave privada, que es la que nos da el control de nuestra cuenta o "billetera". Una clave pública o dirección de bitcoins es una secuencia aleatoria de números y letras de 33 caracteres de largo, como, por ejemplo:

**1rYK1YzEGa59pI314159KUF2Za4jAYYTd**

Ahora bien, una vez fondeada nuestra cuenta, podemos hacer el camino inverso, o sea, enviar bitcoins desde nuestra cuenta a la de un tercero, o, en otras palabras, gastarlos. Para ello, necesitaremos la llave pública o dirección de la cuenta a la que vamos a transferir, a la cual le adicionaremos, ahora sí, nuestra llave privada. De esta combinación de claves o llaves genera lo que llamamos "firma", con la que estamos comunicando a toda la red nuestra voluntad de hacer la transacción. Es importante aclarar que, gracias al empleo de la criptografía asimétrica, la llave privada no puede ser deducida de la firma que de ella deriva. O sea, que es matemáticamente imposible descifrar cual fue la llave privada que, en combinación con determinada llave publica derivó en cierta "firma". Este es un punto neurálgico en el funcionamiento de la criptomoneda, ya que este procedimiento matemático permite a los usuarios (nodos) que auditan el funcionamiento de la red corroborar de forma inconfundible si la llave privada fue utilizada o no por nosotros, pero a su vez les es imposible conocerla.

Todas y cada una de las transacciones de bitcoins como las de estos ejemplos, desde la primera que se realizó hasta las que se están llevando a cabo en este mismo instante alrededor del mundo, quedan registradas como un asiento contable, en un libro mayor digital y a la vista de todos los usuarios, llamado Blockchain o cadena de bloques.

## C) LA BLOCKCHAIN: CARACTERISTICAS Y FUNCIONAMIENTO

La principal innovación que aporta el Bitcoin consiste en la posibilidad de transferir valor electrónicamente de una persona a otra sin intermediarios, lo cual se logra gracias a la tecnología subyacente a su funcionamiento: La Blockchain, o cadena de bloques.

Blockchain es básicamente un registro contable público e inalterable sostenido por una red de computadoras sin ninguna autoridad central, tan sencillo como una serie continua de asientos tipo: "N" bitcoins fueron desde la dirección "A" a la dirección "B" en el momento "X". Al tratarse de un software de código abierto es un registro totalmente transparente: cualquiera puede examinarla, en cualquier momento, para informarse acerca de cualquier transacción que se haya realizado desde el lanzamiento de Bitcoin, así como de las nuevas transacciones que se van agregando a la cadena en tiempo real:

Figura n°1: Elementos de una transacción registrada en la Blockchain.


*Fuente:* https://blockchain.info/

Aquí tenemos el ejemplo de una transacción real registrada en la Blockchain, donde vemos los diferentes elementos que la componen:

1) Código identificador (Hash) de la transacción.

2) Llave publica de la billetera remitente.

3) Llave publica de la billetera receptora.

4) Cantidad de Bitcoins transferidos.

5) Hora y fecha y número de bloque en el que fue asentada la transacción.

6) Importe abonado como Fee (comisión).

El modelo bancario tradicional logra su relativo nivel de privacidad al limitar el acceso a la información a las partes involucradas y al tercero de confianza. En la red Bitcoin la necesidad de anunciar todas las transacciones públicamente en la Blockchain se opone a este método, pero la privacidad aún puede mantenerse rompiendo el flujo de información en otro lugar: manteniendo las claves (llaves) públicas anónimas. Públicamente puede verse que alguien está enviando una cierta cantidad a otra persona, pero sin información que relacione la transacción con nadie en particular. Esto es similar al nivel de información que se muestra en las bolsas de valores, donde el tiempo y el tamaño de las transacciones individuales son públicos, pero sin decir quiénes son las partes.

Aunque, como hemos visto, ningún usuario de Bitcoin está forzado a revelar su identidad, todas las transacciones realizadas quedan grabadas en esa base de datos de libre acceso. Esta base de datos contiene el historial de posesión de todas las monedas desde la que fueron creadas hasta la dirección del actual dueño, y existe una copia de este registro actualizándose en tiempo real en cada computadora de los millones de usuarios de la Red Bitcoin conectados en el mundo. ¿Y cómo el sistema es completamente anónimo si todas las transferencias quedan plasmadas en un registro público? Esto se da porque solo figuran los números de cuentas o billeteras involucradas en cada transacción, pero nunca datos de las personas responsables de dichas cuentas.

## D) MINERIA DE BITCOINS

En los párrafos previos se describió cómo realizar una transacción y donde quedan éstas registradas, pero sin aclarar cómo y quién lleva a cabo estos registros.

Para asegurar el funcionamiento de la red de forma descentralizada, su diseño contempla la entrega de incentivos a aquellos usuarios que brinden soporte a la misma. La prestación de soporte a la red a cambio de retribuciones recibe el nombre de Minería de Bitcoins. En otras palabras, minar bitcoins es el proceso de invertir capacidad computacional para procesar transacciones y garantizar la seguridad de la red con el fin de obtener una retribución económica. Podría describirse como el centro de datos de Bitcoin, pero con la particularidad de ser completamente descentralizado con mineros operando en todos los países y sin que nadie tenga el control absoluto sobre la red.

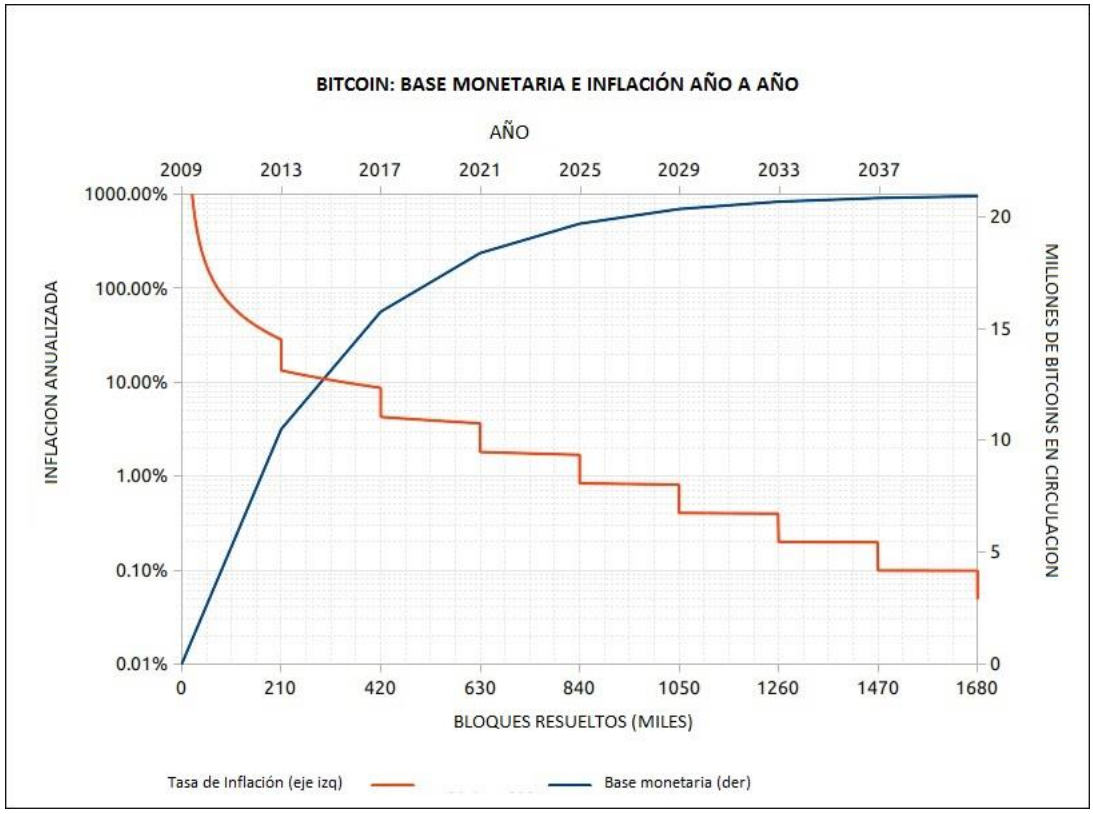
Este proceso de "minería" es a su vez el único mecanismo utilizado para emitir nuevos bitcoins. El protocolo contempla la creación (emisión) de cierta cantidad de bitcoins cada 10 minutos. Todas las transacciones que se realizan durante los 10 minutos que transcurren entre cada creación de nuevas monedas, se agrupan en lo que se llama un bloque, y entonces, el primer usuario (o grupo organizado de usuarios) que logra auditar y asentar correctamente ese bloque en la Blockchain es premiado con las monedas emitidas en ese lapso de tiempo, que a abril del 2017 son 12,5 bitcoins cada 10 minutos, los que representan ≅ U$S 7.500.

El número de bitcoins generados con cada bloque decrece geométricamente, reduciéndose en un 50% cada 210.00 bloques resueltos, o sea, cada prácticamente 4 años, ya que cada 10 minutos se genera un nuevo bloque. La cantidad de BTC emitidos durante cada “era” o etapa de 4 años (210.000 bloques) son el resultado del siguiente algoritmo, donde “i” representa cada “era”:

$$\frac{\sum_{i=0}^{32} 210000 \lfloor \frac{50.10^8}{2^i} \rfloor}{10^8}$$

Este algoritmo de emisión decreciente fija un número finito de BTC, y así es que como resultado del mismo el número de bitcoins existentes nunca superará los 21 millones, tal como podemos ver en las siguientes tablas y el siguiente gráfico que detallan la dinámica de la emisión de bitcoins desde su creación hasta que la última fracción de moneda sea emitida.

Gráfico n°2: Base monetaria e inflación año a año.




*Fuente:* https://wikipedia.com/

Tabla n°1: Cantidad de Bitcoins emitidos por bloque en cada Era.

| Bloque | Era | BTC/Bloque | BTC al comenzar | BTC incorporados | BTC al finalizar | Incremento | % BTC emitidos |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 50.00000000 | 0.00000000 | 10500000.00000000 | 10500000.00000000* | infinite | 50.00000006% |
| 210000 | 2 | 25.00000000 | 10500000.00000000 | 5250000.00000000 | 15750000.00000000 | 50.00000000% | 75.00000008% |
| 420000 | 3 | 12.50000000 | 15750000.00000000 | 2625000.00000000 | 18375000.00000000 | 16.66666667% | 87.50000010% |
| 630000 | 4 | 6.25000000 | 18375000.00000000 | 1312500.00000000 | 19687500.00000000 | 7.14285714% | 93.75000010% |
| 840000 | 5 | 3.12500000 | 19687500.00000000 | 656250.00000000 | 20343750.00000000 | 3.33333333% | 96.87500011% |
| 1050000 | 6 | 1.56250000 | 20343750.00000000 | 328125.00000000 | 20671875.00000000 | 1.61290323% | 98.43750011% |
| 1260000 | 7 | 0.78125000 | 20671875.00000000 | 164062.50000000 | 20835937.50000000 | 0.79365079% | 99.21875011% |
| 1470000 | 8 | 0.39062500 | 20835937.50000000 | 82031.25000000 | 20917968.75000000 | 0.39370079% | 99.60937511% |
| 1680000 | 9 | 0.19531250 | 20917968.75000000 | 41015.62500000 | 20958984.37500000 | 0.19607843% | 99.80468761% |
| 1890000 | 10 | 0.09765625 | 20958984.37500000 | 20507.81250000 | 20979492.18750000 | 0.09784736% | 99.90234386% |
| 2100000 | 11 | 0.04882812 | 20979492.18750000 | 10253.90520000 | 20989746.09270000 | 0.04887585% | 99.95117198% |
| 2310000 | 12 | 0.02441406 | 20989746.09270000 | 5126.95260000 | 20994873.04530000 | 0.02442599% | 99.97558604% |
| 2520000 | 13 | 0.01220703 | 20994873.04530000 | 2563.47630000 | 20997436.52160000 | 0.01221001% | 99.98779307% |
| 2730000 | 14 | 0.00610351 | 20997436.52160000 | 1281.73710000 | 20998718.25870000 | 0.00610426% | 99.99389658% |
| 2940000 | 15 | 0.00305175 | 20998718.25870000 | 640.86750000 | 20999359.12620000 | 0.00305194% | 99.99694833% |
| 3150000 | 16 | 0.00152587 | 20999359.12620000 | 320.43270000 | 20999679.55890000 | 0.00152592% | 99.99847420% |
| 3360000 | 17 | 0.00076293 | 20999679.55890000 | 160.21530000 | 20999839.77420000 | 0.00076294% | 99.99923713% |
| 3570000 | 18 | 0.00038146 | 20999839.77420000 | 80.10660000 | 20999919.88080000 | 0.00038146% | 99.99961859% |
| 3780000 | 19 | 0.00019073 | 20999919.88080000 | 40.05330000 | 20999959.93410000 | 0.00019073% | 99.99980932% |
| 3990000 | 20 | 0.00009536 | 20999959.93410000 | 20.02560000 | 20999979.95970000 | 0.00009536% | 99.99990468% |
| 4200000 | 21 | 0.00004768 | 20999979.95970000 | 10.01280000 | 20999989.97250000 | 0.00004768% | 99.99995236% |
| 4410000 | 22 | 0.00002384 | 20999989.97250000 | 5.00640000 | 20999994.97890000 | 0.00002384% | 99.99997620% |
| 4620000 | 23 | 0.00001192 | 20999994.97890000 | 2.50320000 | 20999997.48210000 | 0.00001192% | 99.99998812% |
| 4830000 | 24 | 0.00000596 | 20999997.48210000 | 1.25160000 | 20999998.73370000 | 0.00000596% | 99.99999408% |
| 5040000 | 25 | 0.00000298 | 20999998.73370000 | 0.62580000 | 20999999.35950000 | 0.00000298% | 99.99999706% |
| 5250000 | 26 | 0.00000149 | 20999999.35950000 | 0.31290000 | 20999999.67240000 | 0.00000149% | 99.99999855% |
| 5460000 | 27 | 0.00000074 | 20999999.67240000 | 0.15540000 | 20999999.82780000 | 0.00000074% | 99.99999929% |
| 5670000 | 28 | 0.00000037 | 20999999.82780000 | 0.07770000 | 20999999.90550000 | 0.00000037% | 99.99999966% |
| 5880000 | 29 | 0.00000018 | 20999999.90550000 | 0.03780000 | 20999999.94330000 | 0.00000018% | 99.99999984% |
| 6090000 | 30 | 0.00000009 | 20999999.94330000 | 0.01890000 | 20999999.96220000 | 0.00000009% | 99.99999993% |
| 6300000 | 31 | 0.00000004 | 20999999.96220000 | 0.00840000 | 20999999.97060000 | 0.00000004% | 99.99999997% |
| 6510000 | 32 | 0.00000002 | 20999999.97060000 | 0.00420000 | 20999999.97480000 | 0.00000002% | 99.99999999% |
| 6720000 | 33 | 0.00000001 | 20999999.97480000 | 0.00210000 | 20999999.97690000 | 0.00000001% | 100.00000000% |
| 6930000 | 34 | 0.00000000 | 20999999.97690000 | 0.00000000 | 20999999.97690000 | 0.00000000% | 100.00000000% |

*Fuente: [https://wikipedia.com/](https://wikipedia.com/)*

Llegará inevitablemente un momento en que cesará la emisión de Bitcoins, pero continuarán habiendo transacciones, por lo que el sistema también contempla la posibilidad de que al realizar una transacción entre dos billeteras podamos incluir una “propina” o “fee” destinado a generar un incentivo para los mineros que estén dispuestos a procesarla y la red pueda seguir funcionando. De todas formas

actualmente, más allá de que aún los mineros que primero resuelven el bloque obtienen un premio considerable, se acostumbra abonar un pequeño fee a fin de que nuestra transacción sea procesada con mayor celeridad, ya que, lógicamente, los mineros priorizan en el tiempo el procesamiento de las transacciones que mayores fee contengan, y, con el auge que ha tenido esta tecnología en los últimos años, la cantidad de usuarios ha crecido considerablemente generando demoras en las transferencias en los días y horarios donde se registra uso intensivo.

De esta forma, incontables usuarios, diseminados por todo el mundo y sin conocerse los unos a los otros, con sus computadoras o, desde años recientes, hardwares específicamente creados para este fin, controlan la legitimidad de cada transacción, agrupada a su vez en bloques, con la esperanza de ser quienes primero resuelvan el problema criptográfico con el que es encriptado cada bloque, y así obtener como premio las monedas emitidas en ese lapso de tiempo.

La probabilidad que tiene un usuario o grupo de resolver un bloque y por ende ser el beneficiario de los BTC emitidos en ese lapso de 10 minutos depende del poder de computo que aporto a la red, el cual se mide en MHash/s (Mega Hashes por segundo), sobre el poder de computo (o mejor dicho, de hasheo) total de la red. Por ende: si yo fuera el único minando, mi probabilidad de encontrar el próximo bloque sería del 100%. Pero si hubieran diez mineros (todos con igual poder de hasheo) la probabilidad de encontrar el próximo bloque, para cada uno de ellos, sería del 10%.

El sistema también contempla la posibilidad de que los usuarios (mineros) se agrupen conformando redes o pooles, de forma que complementen el poder computacional aportado por cada uno, aumentando sus probabilidades, como grupo, de ser los primeros en auditar los bloques. Una vez que un determinado pool de mineros se hace con la recompensa por la resolución del bloque podrá repartirlo entre sus integrantes en base al criterio que los miembros del grupo hayan acordado.

## E) MINERÍA HOY: POOLES Y GRANJAS

El surgimiento del Bitcoin se dio de forma silenciosa. Durante su primer año de vida la cantidad de usuarios participando de la red era muy baja, por lo que el poder total de hasheo de la red era pequeño. Así fue que en ese periodo cualquier computadora de uso personal podía minar bitcoins sin mayor

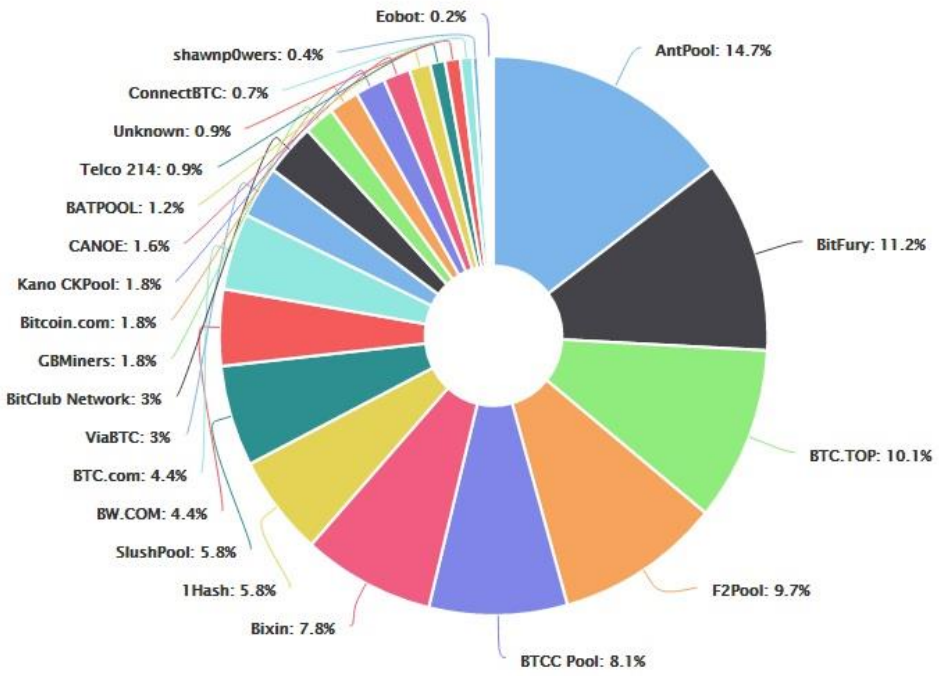
complicación. Este tipo de minería es ahora imposible, dado que el poder de hasheo total de la red ha ido creciendo de manera constante a medida que se sumaron nuevos y más poderosos mineros. Solo para hacernos una idea, con el nivel de dificultad de minado actual, una PC de escritorio de alta gama actual tardaría más de 100.000 años de promedio en resolver un bloque para obtener la recompensa por el minado.

A fines del 2010, en el afán de lograr mayores rendimientos, los incipientes mineros descubrieron que las GPUs (Graphics Processing Unit), mejor conocidas como placas de video, y que la mayoría de ordenadores modernos tienen una de estas integrada, poseían propiedades muy buenas para la minería, ya que tienen varias Unidades de Lógica Aritmética que permitían el cálculo en paralelo de diferentes hashes. Su código fue adaptado para minar bitcoins, y como además ofrecían la posibilidad de que muchas de ellas podían unirse a un único ordenador, el poder de hasheo aumentó considerablemente dando origen a la segunda generación de minado.

El constante crecimiento del universo Bitcoin derivó en la aparición a fines del 2013 de procesadores específicamente diseñados y fabricados para el minado, los ASICs (Circuito Integrado para Aplicaciones Específicas en castellano), lo cual tornó inmediatamente obsoletos a todos los mecanismos previos de minado, pero la incesante búsqueda de parte de los usuarios por lograr formas más poderosas y eficientes de minar bitcoins continuó y no solo se plasmó en los avances técnicos en los procesadores. De forma paralela, los mineros fueron intentando reducir los costos asociados al minado, los cuales son principalmente electricidad y refrigeración, ya que los equipos utilizados consumen una gran cantidad de energía y a su vez generan temperaturas tan altas (entre 80 y 120°C) que pueden comprometer su funcionamiento. Así fue que aquellas regiones donde el precio de la energía es económico y cuentan con climas templados comenzaron a contar con una ventaja competitiva determinante, lo cual repercutió en la llegada de mineros de diferentes partes que comenzaron a concentrar sus inversiones en equipos en esos lugares. Fue en estos lugares donde, en pos de generar economías de escala, edificios completos se llenaron de hardware dedicado a minar Bitcoins 24/7, incluso se construyeron nuevos galpones a tal fin. A estos edificios llenos de equipos minando se los conoce como granjas de minado, y, en este momento, y por las características previamente mencionadas, los lugares más codiciados para el establecimiento de estos emprendimientos son: en Europa, Groenlandia e Islandia, en Asía, la región del Tíbet y, dentro de los EE.UU., el estado de Washington.

Más allá de toda esta evolución en hardware, edificios y locaciones, hoy la enorme mayoría de los mineros, desde individuos en sus casas hasta grandes granjas de minado, buscan asociarse unos con otros mediante pooles que les garanticen estabilidad en el cobro de Bitcoins. Este esquema beneficia principalmente a los mineros pequeños, ya que, si tomamos como ejemplo un equipo de minado económico de los que se comercializan hoy en día, los cuales rondan valores de entre 7 mil y 10 mil dólares, el mismo demoraría, en promedio, unos 14 meses en resolver exitosamente un bloque para hacerse con los ฿ 12,5 (≅ U$S 14.000) de recompensa. Al recibir pagos más pequeños pero periódicos por su participación en un pool, el minero reduce enormemente la incertidumbre y puede proyectar mejor sus inversiones. Tal es así que al día de hoy la enorme mayoría de los bitcoins minados son obtenidos por pooles, como podemos ver en el siguiente grafico de torta que muestra cómo se distribuye el poder de hasheo a abril de 2017, donde solo el 0,9% es aportado por nodos fuera de pooles:

Gráfico n°3: Porcentaje del poder total de hasheo de la red aportado por cada pool de minado. Abril ´17.




*Fuente: https://blockchain.info/*

Es así que, resumiendo, los mineros sostienen el funcionamiento de toda la red al realizar dos tareas básicas con cada transacción que los usuarios realizan: verificar su validez y asentarlas en la Blockchain, todo esto de forma completamente anónima gracias al uso de la criptografía.

# CAPITULO III

# ECONOMIA, HISTORIA Y FILOSOFIA DEL BITCOIN

Durante la confección de este capítulo fueron consultados los libros “The internet of Money”, también de Andreas Antonopoulos, “Hactivismo”, del divulgador y activista argentino Santiago Siri y nuevamente la obra de Juan Manuel González Otero “Bitcoin: la moneda del futuro”, como así también los portales “investing.com”, fuente de información actualizada sobre la cotización de activos a nivel mundial, “coinmarketcap.com” y la página oficial del banco mundial, “worldbank.org” principalmente para la obtención de información referente al nivel de inclusión financiera en las diferentes partes del mundo.

## A) INTERNET: UN GRAN SALTO PARA LA HUMANIDAD

La historia de la humanidad esta signada por el surgimiento cada cierto tiempo de tecnologías que son varias veces superiores a las herramientas predecesoras, especialmente en los últimos siglos, generando una disrupción tecnológica tal que todo lo que se usaba antes para hacer una misma tarea queda obsoleto ante la aparición de un paradigma nuevo.

La aparición de Internet es uno de estos casos, el cual ha transformado la relación de la humanidad con el conocimiento. Uno puede comparar su impacto cultural con el que tuvo la imprenta de Gutenberg, que supo generar una nueva conciencia renacentista en la Europa medieval cambiando para siempre el rumbo de la historia. Pero si uno se limita a describir una tecnología comparándola con lo que existía antes, corre el riesgo de cegarse en percibir el verdadero potencial de lo que tiene por delante. Es así que la principal novedad respecto a Internet no es solamente cultural. Por ejemplo, un dato a considerar es que, hasta el surgimiento de internet, las instituciones que procesaban el mayor nivel de información sobre una

sociedad eran los Estados. Esto es un claro vuelco en la balanza de poder, ya que modifica el esquema de distribución de la información, la cual es un factor importantísimo de poder, llevándola desde estructuras piramidales y jerárquicas, como lo son los Gobiernos, hacia modelos más horizontales y descentralizados. La influencia de la red en nuestra concepción tanto política como económica del mundo se acrecienta cada día. Este es el proceso que genera cambios impensados hace tan solo 15 años, como el que se dio en 2012 cuando dejó de imprimirse la Enciclopedia Británica tras haber sido desbancada de su centenario reinado como principal herramienta de consulta por un competidor basado en un esquema horizontal: Wikipedia.

No casualmente el desarrollo de la tecnología digital surgió por una necesidad pública. Fue en 1879, cuando el gobierno de los Estados Unidos se transformó en el primer cliente de una joven empresa: IBM. Se usaron máquinas tabuladoras para procesar en menor tiempo la información del censo nacional y luego de las elecciones democráticas. Gracias a estas proto-computadoras se pudo reducir de 7 años el procesamiento de los datos de un censo a solamente 2. Pero hoy es imposible para cualquier Estado procesar el volumen de información que capta Internet. La red es una superestructura que responde a un grado de mayor trascendencia. Y a medida que nos adentramos en la sociedad de la información, la red empieza a ocupar roles que pertenecieron al Estado volviendo obsoletos a algunos de sus mecanismos históricos. Y uno de ellos, quizás el más importante, y que es el centro de este estudio, es el de emitir moneda.

A pesar de los avances políticos y sociales logrados en los últimos siglos, la humanidad no encuentra aún en el dinero la herramienta de completa liberación, comercio y progreso que supo ser en ciertas etapas de nuestra historia, ya que hoy funciona, quizás más que nunca, como un instrumento de control al servicio de mastodónticos y omnipresentes Estados, quienes sostienen el monopolio de la moneda por ellos impresa manteniendo a sus habitantes como rehenes sujetos a las enormes limitaciones operativas de estas divisas junto con la constante depreciación de su valor, como vimos en el capítulo 1 de este trabajo.

Como si esto no fuera poco, desde años recientes venimos presenciando como los diferentes bancos centrales alrededor del mundo comienzan a realizar importantes esfuerzos a fin de desincentivar el uso del efectivo en pos de transacciones digitales, lo cual pretende llevarnos hacia un sistema donde todas las operaciones monetarias puedan ser supervisadas por las autoridades gubernamentales, con el objetivo de evitar la evasión fiscal pero también las transacciones indeseadas, ya sean de bienes cuya

comercialización está prohibida por la legislación del país en cuestión, o el financiamiento de grupos que representen una amenaza, sean estos denominados terroristas o gobiernos enemigos. Pero la mayor amenaza que representa ese hipotético escenario es la inconmensurable concentración de poder que dicho esquema plantea, ya que sobre las autoridades políticas recaería la posibilidad de determinar qué persona es apta o no para realizar operaciones monetarias, pudiendo borrar del sistema económico a cualquier ciudadano en cualquier momento. Es estremecedor pensar el daño que una herramienta de esta magnitud podría generar en manos de, por ejemplo, regímenes como el que actualmente gobierna Venezuela, donde de no ser por la aparición de diferentes mercados negros de bienes básicos, millones de personas no lograrían subsistir ante la terrible escasez de alimentos reinante.

Es así que, en adelante, podemos seguir la senda de la centralización hasta sus últimas consecuencias, lo cual, en materia monetaria significaría un Banco Central Mundial y una moneda única, forzosa, monopólica. O podemos escoger la libertad, la descentralización y la democracia del mercado.

## B) LA ANTESALA AL BITCOIN: PREDECESORES Y VISIONARIOS

La necesidad de una moneda virtuosa ajena a los desmanejos monopólicos del estado se ha visto reflejada en décadas pasadas a través los intentos de diferentes grupos de individuos por crear una moneda privada basada en la confianza y no en la coacción. Un caso relativamente reciente, aunque no necesariamente digital, es el del Liberty Dollar, creado en 1998 en Indiana, EE.UU. por Bernard von NotHaus, quien comenzó a emitir papel moneda con su correspondiente respaldado en oro, plata, platino y cobre, rechazando la autoridad de la Reserva Federal a la cual acusaba de anticonstitucional. De acuerdo con la investigación de la justicia americana, al momento del allanamiento realizado por las fuerzas del FBI, en noviembre del 2007, existían en los EE.UU. 250.000 personas tenedoras de Liberty Dollar. Von NotHaus fue puesto tras las rejas bajo el cargo de terrorismo doméstico, siendo liberador recién en el 2015.

Simultáneamente, con el lento pero constante desarrollo de internet, comenzaron a darse los primeros casos de monedas digitales, con diferencias en su diseño e implementación, pero casi siempre destinadas al mismo final: la persecución y posterior cierre por parte de organismos gubernamentales.

Tal fue el caso de “e-Gold”, la cual fue creada en 1996 por el oncólogo Douglas Jackson, y que en su momento de mayor volumen operado llego a contar con una base monetaria aproximada de 3,5 toneladas de oro, lo que equivalía a 71 millones de dólares. Esta consistía básicamente en un certificado de depósito digital, respaldado en oro, que alcanzo un respetable nivel de aceptación y credibilidad que lo llevaron a contar al momento de su cierre, tras una demanda parte del gobierno de los EE.UU. en los tribunales de dicho país, con 5 millones de usuarios en todo el mundo.

Estos antecedentes, como algunos otros que no se incluyeron en el párrafo anterior, sentaron la pauta de que la existencia de una moneda independiente debía funcionar inevitablemente de forma descentralizada y anónima. Ya para el año 1999 el premio Nobel Milton Friedman, en otra muestra de su enorme capacidad para interpretar el comportamiento humano, se expresaba en este sentido, anticipando lo que sucedería una década después: “Yo creo que la Internet será una de las mayores fuerzas para reducir el rol del gobierno. Lo único que falta, pero que prontamente será desarrollado, es una moneda digital de confianza. Un método por el cual se pueda transferir por internet fondos de A a B, sin que A tenga que conocer a B o B a A, de la misma forma en que yo puedo entregarle un billete de 20 dólares a usted en la mano sin que quede ningún registro de donde usted lo recibió.”

Hubo que esperar hasta el año 2008 para que un ignoto, bajo el seudónimo de Satoshi Nakamoto, publicara un sencillo paper académico de 9 páginas: “Bitcoin: A Peer-to-Peer Electronic Cash System”, donde presentaba y explicaba de forma concisa el funcionamiento de esta innovación. Y ya el 3 de enero de 2009 subió a internet el software libre “Bitcoin”, creando la red del mismo nombre y emitiendo primeras unidades de la moneda.

Así fue que Bitcoin llegó para que recuperemos nuestra libertad de poder escoger que moneda utilizar, porque nos convencen sus virtudes y no porque nos obligan con una ley. Una moneda voluntaria debe intentar persuadirnos invocando a la razón para tener éxito. Debe poseer virtudes que demuestren su preponderancia sobre las alternativas. El dinero Fiat, en cambio, requiere tan sólo el uso de la fuerza del Estado. Siendo generosos y atribuyendo buenas intenciones a sus gestores (llamarlo «dinero fiduciario» ya es ser generoso), el dinero fi at requiere la confianza de todos los que lo utilizan. Confianza en que aquellos que lo controlan no se excederán en sus manipulaciones. Confianza en que los gobernantes cumplirán sus promesas y pagarán sus deudas.

## C) LA COMBINACION IMPOSIBLE

Lo que vino a proponer Nakamoto es un sistema de dinero que se comporta como "efectivo electrónico" ya que cuenta con dos características principales las cuales nunca antes habían podido armonizarse en un sistema de dinero y que son sus aristas primordiales:

- Descentralización
- Escasez digital

Este último punto se logra gracias al aprovechamiento de la criptografía, que básicamente es el arte de escribir de forma secreta usando las matemáticas, gracias a la cual podemos obtener un documento digital (una serie de ceros y unos) que no puede ser copiado, lo que parece una contradicción, ya que la esencia de la información digital es su facilidad de ser copiada casi inmediata e infinitamente.

Es en la combinación de estas dos características donde reside la revolución que plantea esta nueva moneda, ya que hasta ahora se habían podido lograr sistemas digitales que contaran con alguna de estas dos virtudes, pero nunca en simultáneo. Tal es el caso del medio de pagos digitales más popular de las últimas décadas: Visa.

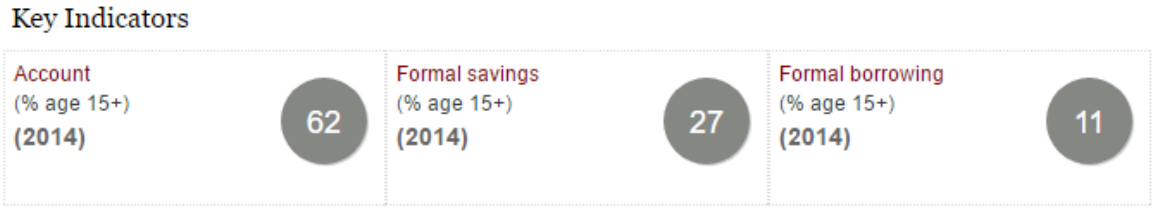
## D) ADMINISTRANDO LA ESCASEZ

"Visa" es eficiente en lograr la escasez digital, puede procesar cientos de miles de transacciones por segundo, garantizando que nadie pueda realizar "dobles gastos", o sea no permite que un usuario vaya y le compre algo al comerciante A y a continuación vaya con la misma información digital (o sea, este caso podemos hablar del mismo saldo en su cuenta) a comprar al comerciante B. Esto no sucederá con Visa, el sistema auditará el saldo en la cuenta del usuario para asegurar en todo momento de que antes de realizar una compra cuente con suficientes fondos o crédito para poder afrontarla. Este sistema funciona, pero acarrea un riesgo: es centralizado. Los usuarios deben depositar su confianza en la organización. Pero el problema no es específicamente la confianza en que hagan un buen procesamiento, ya que de hecho lo hacen, sino que con la confianza le otorgan poder, un enorme poder. Poder de rechazar una transacción,

de rechazar una solicitud de apertura de cuenta, de exigir que te identifiques o que muestres documentación que avale tu capacidad económica.

Esto es diferente a todos los sistemas monetarios previos, como vimos en el capítulo 1, ya que el efectivo, sea este papel moneda o metal precioso, puedo utilizarlo sin necesidad de tener que identificarme o demostrar capacidad financiera, puedo utilizarlo "persona a persona", sin necesidad de intermediarios. En cambio, con Visa, el esquema deja de ser persona a persona, para pasar a ser algo así como "persona a compañía a compañía a compañía a persona", donde cada corporación interviniente se lleva su tajada, dando como resultado un sistema oligopólico, con altas comisiones y limitaciones, pero principalmente que excluye a miles de millones de personas, más precisamente, entre el 40% y 50% de las personas mayores de 15 años a nivel mundial, según diferentes estimaciones, entre ella esta del Banco Mundial del 2014:

Tabla n°2: Porcentajes de la población mundial mayores de 15 años que poseen cuenta bancaria, ahorros formales y acceso al crédito.




*Fuente: Banco Mundial. http://datatopics.worldbank.org/financialinclusion/*

## E) LA MAQUINA DE GENERAR CONFIANZA

En cambio, con Bitcoin, descentralización y escasez están combinadas por primera vez en la historia, gracias a la lógica con la que opera la tecnología que subyace a su funcionamiento: La Blockchain.

Al profundizar sobre las implicancias que este salto representa podemos concluir que no estamos simplemente frente a un nuevo sistema de pagos, si no que se trata de algo macro que abarca más que solo las transacciones de valores: estamos frente a una "plataforma de confianza", o "La máquina de confianza" como denominara el semanario "The Economist" a la Blockchain en su tapa de octubre del

2015. Esta está respaldada por la matemática, más precisamente la criptografía, que básicamente es el arte de escribir de forma secreta usando las matemáticas, la cual se aplica para establecer confianza entre los participantes sin necesidad de darle a ninguno de ellos el control sobre el sistema. En definitiva, como lo define el experto informático y experto en criptomonedas Andreas Antonopoulos: “Es el concepto de descentralización aplicado al acto de transferencia de valor entre humanos”.

Ahora podemos enviar dinero a alguien sin conocerlo, sin que el otro tenga que confiar en nosotros y sin tener que confiar en nadie que intermedie ya que la confianza se deposita en el sistema y más precisamente en las reglas matemáticas en el sistema que garantizan que el valor transferido es real e imposible de duplicar. Pero la capacidad de arbitrar confianza de forma descentralizada de la Blockchain abre nuevas posibilidades más allá de solamente la transferencia de monedas, las cuales ya están comenzando a ser aprovechadas en todo el mundo.

Así como la cadena de bloques es en definitiva un enorme libro mayor descentralizado e inmutable donde se asientan todos los movimientos de bitcoins entre cuentas, ese mismo registro puede utilizarse, y de hecho lo está siendo, por ejemplo por diferentes estados para llevar de forma segura y económica el registro de bienes inmuebles, reemplazando a los antiguos registros de la propiedad, como es el caso de la República de Georgia, donde este sistema está vigente por ley desde febrero de este año, o el caso de Suecia, donde se encuentra en etapa de prueba desde marzo pasado, sumado a varios gobiernos de diferentes estados y ciudades de Estados Unidos que han informado que se encuentran testeando esta tecnología, como Chicago o Delaware. Así mismo, en el sector privado, están floreciendo de alternativas entorno a esta novedad, como empresas de notariado digital utilizando la Blockchain de Bitcoin, y gestando enormes cambios en la relación entre emprendedores y los llamados capitales ángeles, ya que actualmente una gran cantidad de startups desarrollan sus propias monedas digitales siguiendo la receta del Bitcoin y de esta forma aquellos inversores que quieran aportar capital a la empresa simplemente tienen que adquirir las monedas por estas emitidas, lo cual es mucho más sencillo y ágil y seguro para las partes que los procedimiento tradicionales. O incluso gigantes de la informática como IBM ya cuentan con su propia Blockchain con la que ofrecen a sus clientes la capacidad de mejorar la seguridad y velocidad en el flujo de información o valores.

## F) HAY CONFIANZA, PERO ¿HAY MONEDA?

Más allá de que la cadena de bloques nos garantice la descentralización y la escasez digital, esto no es suficiente para que nos refiramos al Bitcoin como moneda. Para ello debemos corroborar también su capacidad de cumplir con ciertas virtudes:

Primero que nada, debemos evaluar si cumple el rol de “refugio de valor”, lo cual podemos decir que lo cumple sobradamente ya que es el activo que más se apreció en los últimos 7 años a nivel mundial, y que además en los últimos 5 años, con excepción del 2014, fue el activo cuyo precio registro mayores incrementos año a año:

Tabla n°3: Cotización BTC/U$S. Junio 2015 – Mayo 2017.

| Fecha | Último | Apertura | Máximo | Mínimo | % var. |
|---|---|---|---|---|---|
| May 2017 | 2.360,86 | 1.362,40 | 2.389,53 | 1.332,00 | 73,29% |
| Abr 2017 | 1.362,40 | 1.079,22 | 1.368,38 | 1.068,75 | 26,24% |
| Mar 2017 | 1.079,22 | 1.191,19 | 1.316,73 | 890,80 | -9,40% |
| Feb 2017 | 1.191,19 | 970,43 | 1.215,80 | 943,89 | 22,75% |
| Ene 2017 | 970,43 | 968,62 | 1.150,00 | 752,97 | 0,19% |
| Dic 2016 | 968,62 | 742,44 | 985,33 | 742,44 | 30,54% |
| Nov 2016 | 742,00 | 697,96 | 757,64 | 675,80 | 6,31% |
| Oct 2016 | 697,96 | 609,24 | 718,00 | 608,17 | 14,55% |
| Sep 2016 | 609,28 | 572,92 | 628,95 | 568,50 | 6,35% |
| Ago 2016 | 572,92 | 635,01 | 635,73 | 482,00 | -9,78% |
| Jul 2016 | 635,00 | 671,63 | 701,40 | 611,27 | -5,50% |
| Jun 2016 | 671,98 | 531,35 | 780,00 | 526,58 | 26,42% |
| May 2016 | 531,56 | 449,96 | 547,30 | 435,30 | 18,16% |
| Abr 2016 | 449,87 | 416,37 | 469,41 | 414,41 | 8,20% |
| Mar 2016 | 415,78 | 435,55 | 436,80 | 386,00 | -4,50% |
| Feb 2016 | 435,39 | 367,67 | 446,70 | 365,88 | 18,64% |
| Ene 2016 | 366,98 | 429,97 | 463,92 | 352,11 | -14,64% |
| Dic 2015 | 429,94 | 377,03 | 469,34 | 348,15 | 14,15% |
| Nov 2015 | 376,63 | 314,06 | 500,08 | 299,17 | 20,42% |
| Oct 2015 | 312,77 | 236,28 | 334,33 | 236,13 | 32,33% |
| Sep 2015 | 236,36 | 230,13 | 245,54 | 224,49 | 2,82% |
| Ago 2015 | 229,88 | 284,98 | 285,94 | 200,00 | -19,20% |
| Jul 2015 | 284,52 | 262,65 | 313,50 | 253,00 | 8,37% |
| Jun 2015 | 262,55 | 228,82 | 268,00 | 219,99 | 14,97% |
| Máximo: 2.389,53 | Mínimo: 200,00 | Diferencia: 2.189,53 | Promedio: 674,75 | | % var.: 933,83 |

*Fuente: https://investing.com/*

Tabla n°4: Cotización BTC/U$S. Junio 2012 - Abril 2015.

| Fecha | Último | Apertura | Máximo | Mínimo | % var. |
|---|---|---|---|---|---|
| Abr 2015 | 236,00 | 243,74 | 260,87 | 215,09 | -3,33% |
| Mar 2015 | 244,13 | 252,75 | 300,10 | 233,79 | -3,72% |
| Feb 2015 | 253,57 | 217,19 | 267,10 | 213,50 | 16,63% |
| Ene 2015 | 217,41 | 317,51 | 317,51 | 164,95 | -31,42% |
| Dic 2014 | 317,00 | 376,68 | 383,11 | 303,62 | -15,85% |
| Nov 2014 | 376,72 | 337,66 | 445,00 | 321,00 | 11,79% |
| Oct 2014 | 337,00 | 387,02 | 405,80 | 285,12 | -12,95% |
| Sep 2014 | 387,14 | 487,35 | 494,28 | 367,26 | -19,91% |
| Ago 2014 | 483,37 | 578,00 | 606,10 | 100,00 | -16,52% |
| Jul 2014 | 579,04 | 650,00 | 662,00 | 550,00 | -9,53% |
| Jun 2014 | 640,01 | 638,00 | 693,89 | 545,33 | 0,69% |
| May 2014 | 635,60 | 450,81 | 635,60 | 419,77 | 41,79% |
| Abr 2014 | 448,27 | 460,32 | 522,79 | 325,00 | -0,83% |
| Mar 2014 | 452,00 | 565,00 | 685,00 | 440,35 | -20,00% |
| Feb 2014 | 565,00 | 801,93 | 814,65 | 425,00 | -29,38% |
| Ene 2014 | 800,00 | 740,00 | 950,00 | 731,00 | 9,93% |
| Dic 2013 | 727,71 | 998,06 | 1.200,00 | 408,74 | -34,58% |
| Nov 2013 | 1.112,35 | 198,51 | 1.124,36 | 198,51 | 461,14% |
| Oct 2013 | 198,23 | 125,49 | 200,62 | 99,81 | 61,03% |
| Sep 2013 | 123,10 | 128,26 | 128,26 | 116,32 | -4,91% |
| Ago 2013 | 129,46 | 96,42 | 129,46 | 93,29 | 32,22% |
| Jul 2013 | 97,91 | 84,61 | 97,91 | 66,34 | 0,41% |
| Jun 2013 | 97,51 | 129,30 | 129,30 | 94,66 | -24,31% |
| May 2013 | 128,82 | 116,38 | 133,50 | 98,10 | -7,48% |
| Abr 2013 | 139,23 | 104,00 | 230,00 | 68,36 | 49,66% |
| Mar 2013 | 93,03 | 34,50 | 93,03 | 34,25 | 178,70% |
| Feb 2013 | 33,38 | 20,50 | 33,38 | 19,63 | 63,55% |
| Ene 2013 | 20,41 | 13,30 | 20,41 | 13,28 | 51,07% |
| Dic 2012 | 13,51 | 12,56 | 13,70 | 12,50 | 7,56% |
| Nov 2012 | 12,56 | 10,57 | 12,56 | 10,47 | 12,14% |
| Oct 2012 | 11,20 | 12,40 | 12,89 | 10,17 | -9,68% |
| Sep 2012 | 12,40 | 9,97 | 12,57 | 9,97 | 22,05% |
| Ago 2012 | 10,16 | 9,55 | 13,50 | 8,00 | 8,66% |
| Jul 2012 | 9,35 | 6,63 | 9,35 | 6,45 | 39,76% |
| Jun 2012 | 6,69 | 5,27 | 6,69 | 5,21 | 29,15% |
| Máximo: **1.200,00** | Mínimo: **5,21** | Diferencia: **1.194,79** | Promedio: **284,26** | | % var.: **4.455,98** |

*Fuente: https://investing.com/*

Segundo debemos determinar si es un “medio de cambio”, y, si bien no es un medio de pago completamente masivo, ya es aceptada por más de 100 mil comercios y empresas en el mundo, entras las que se encuentran Microsoft, Dell, Amazon y PayPal, sumado a que financieras ofrecen desde hace años

tarjetas de débito o crédito Visa, o de otras grandes empresas, las cuales debitan saldos en bitcoin de la cuenta del cliente para realizar pagos en moneda local a comerciantes.

Y finalmente, aún no podemos decir que sea unidad de medida debido a su volatilidad, pero podrá serlo eventualmente, ya que esta característica la adquiere gradualmente. Mientras más gente la adopte, irá creciendo la economía generada en torno a ella, con lo que se verá un aumento en la circulación, generando mayor liquidez y por ende reduciendo la volatilidad.

Para que esto ocurra debe darse una adopción masiva, pasando de los entre 2 y 20 millones de usuarios actuales (debido a su carácter anónimo es imposible saber con certeza el número de personas que poseen Bitcoins, solo la cantidad de carteras activas) a los cientos de millones. ¿Y tenemos alguna forma de estimar cuándo se dará este salto? Un análisis que podemos hacer es revisar la velocidad con que se dieron las adopciones en los últimos dos grandes cambios en la concepción de moneda. Tenemos por un lado el papel moneda, que fue insertado en Europa por Marco Polo en el siglo XIII, pero no fue hasta 400 años después que se lo adoptó masivamente. Suena lógico pensar que más allá de las ventajas que representaba el uso del papel moneda fue muy difícil para la gente de la época aceptar el nivel de abstracción que implicaba asignar el mismo valor a las monedas de metal precioso con las que habían convivido por milenios que a un trozo de papel. El siguiente cambio tecnológico de envergadura se dio con la aparición de la tarjeta de crédito, la cual también debió enfrentar una serie de prejuicios y romper paradigmas fuertemente instalados, por lo cual su adopción masiva recién se dio 50 años después. Finalmente, desde 2009 tenemos el Bitcoin, la última gran disrupción en el concepto de moneda, y que, en base al ritmo de crecimiento presente más los antecedentes previamente mencionados, sumados a la velocidad exponencial con que crece el flujo de información gracias a internet, debería demandar un periodo relativamente menor que el que le demandó a la tarjeta de crédito, o sea, entre 10 y 20 años, según diferentes expertos.

## G) BITCOIN COMO PRODCUTO Y MOTOR DEL CAMBIO

Con el surgimiento de internet vimos como por primera vez en la historia de la humanidad la información pudo fluir libremente por todo el mundo, incomodando a aquellas elites acostumbradas a regular su circulación ya que consideran una idea aterradora que cualquier persona hable de cualquier

tema que le plazca y lo comunique a sus semejantes. Bitcoin recrea las mimas circunstancias para el dinero, permitiendo un flujo libre del dinero y la confianza, lo cual también es una idea aterradora para algunos. Es por esto que es erróneo pensar que Bitcoin es simplemente “dinero para internet”, si no que se trata más bien de “La internet del dinero”.

Desde el surgimiento de Bitcoin es posible enviar valor desde cualquier lugar en cualquier momento sin restricciones hacia donde uno desee. Este es un cambio que llegó para quedarse, incluso sea o no con Bitcoin, porque por más allá de la suerte que este experimento corra en el futuro, su “receta” puede ser replicada infinidad de veces, como de hecho ya está sucediendo con la aparición de nuevas criptomonedas, de menor envergadura y diseminación, pero cada una con su identidad propia fruto de diferentes modificaciones en el diseño, las cuales se encuentran en permanente crecimiento.

Probablemente una de las principales razones por la que mucha gente encuentre complicado comprender al Bitcoin es que nos resulta bizarro el concepto de un sistema de confianza sin autoridad, sin jerarquía, ya que todos los sistemas de confianza de nuestra sociedad siempre fueron jerárquicos, donde la autoridad recae, ya sea mediante elección, por herencia o incluso por la fuerza, en una persona o un grupo, o sea que siempre hay una pirámide y en la punta de la misma hay alguien que concentra poder. Bitcoin es un sistema plano, donde algunas personas parecen tener un rol más importante, como pueden ser los mineros o los desarrolladores de softwares aplicados, pero básicamente ninguno de estos tiene capacidad de gobernar a los otros.

Esta es, en definitiva, su gran fortaleza, ya que su filosofía se encuentra en consonancia con la tendencia que sigue la humanidad desde el cambio que significó el Renacimiento: una lenta pero constante erosión del poder concentrado. Y el Bitcoin seguramente con el paso de los años irá ocupando un rol cada vez más importante, no solo como producto de ese cambio, si no también como motor central del mismo.

# CAPITULO IV

# CONCLUSIONES, PRONOSTICOS Y RECOMENDACIONES

A modo de cierre, y como para englobar de forma ordenada los conceptos vertidos en capítulos anteriores, resulta conveniente tratar de explicitar un cuadro situacional con las fortalezas y debilidades que posee este desarrollo tecnológico, junto con las oportunidades y amenazas que plantea su entorno. Esto no permitirá bosquejar un pronóstico sobre lo que le depara el futuro a este desarrollo tecnológico, y en base a este podremos determinar si es recomendable o no involucrarse en el desarrollo de esta innovación financiera, ya sea adquiriendo Bitcoins a modo de inversión y a la espera de que continúe creciendo su precio, o incluso sumarse a la ola de desarrollos entorno a esta red.

## A) FORTALEZAS

### 1) PODER DE CÓMPUTO DE TODA LA RED BITCOIN:

Como ya mencionamos previamente, el diseño de la Blockchain, mediante la correcta disposición de incentivos, logra que miles de mineros diseminados por el mundo y sin conocerse unos con otros inviertan enromes recursos para dar soporte a la red en pos de obtener una recompensa. Pero, además, podemos agregar que esa cantidad de enorme de recursos pueden medirse en cualquier momento, y de hecho se hace un seguimiento permanente del mismo, el cual, a mayo de 2017 asciende a 672 Petaflops, lo que equivale a 64.000 veces el poder de cálculo de las 500 supercomputadoras más potentes del mundo, y continúa en ascenso. Esto nos marca la pauta de que, a aquellos interesados en destinar recursos informáticos a fin de infiltrar la red para procesar fraudulentamente operaciones falsas, sean estos particulares u organismos gubernamentales, les resultaría prácticamente inviable la tarea dado que la inversión a realizar es infinitamente superior a cualquier beneficio que pueda extraerse. Esta virtud del

sistema es su escudo ante los intentos de ataques que puede recibir de parte de detractores o simples delincuentes, y es la principal garantía de que más allá de lo que puedan determinar las legislaciones que se vayan aprobando sobre Bitcoin en los diferentes países, es prácticamente imposible detenerlo.

## 2) DESARROLLO DE LAS "ALTCOINS":

El hecho de que el software de Bitcoin sea de código abierto implica (y probablemente busca) que cualquier persona puede copiarlo a fin de incorporar las modificaciones que crea útiles, lo cual, de hecho, está sucediendo, y en gran medida. Es así que desde el surgimiento de bitcoin en 2009 diferentes desarrolladores han puesto en funcionamiento sus propias Criptomonedas, algunas descentralizadas y otras no, totalizando más de 830 criptomonedas diferentes y en funcionamiento a mayo de 2017, cada una con sus particularidades de diseño basadas en las necesidades que cada grupo de desarrolladores busca atender, como por ejemplo mecanismos para garantizar de forma aún más fehaciente el anonimato de las transacciones, o, para intensificar la descentralización del funcionamiento en otras.

Tal es el grado de desarrollo y adopción que están alcanzando estas monedas que las más importantes cuentan ya con capitalizaciones de mercado (el valor de una unidad monetaria por la cantidad emitida) de mil seiscientos millones de dólares (USD 1.600.000.000) en el caso del "Litecoin", lanzada en 2011, o de hasta de dieciséis mil millones de dólares (USD 16.000.000.000) como sucede con "Ethereum", creada en 2013, la cual ha ganado popularidad gracias a su plataforma que facilita la celebración de contratos inteligentes. Estos contratos consisten básicamente en un programa informático que asegura, hace cumplir acuerdos registrados entre personas y/o organizaciones, ya que cuando se dispara una condición pre-programada, el contrato inteligente ejecuta la cláusula contractual correspondiente.

Este importante nivel de desarrollo que vienen alcanzando estas criptomonedas alternativas al Bitcoin, también conocidas como "Altcoins" (del inglés Alternative coins, o monedas alternativas), generan un considerable desincentivo para los gobiernos que pretenda atentar contra el desarrollo del Bitcoin, ya que muestran que incluso en caso de que lograran la tarea casi imposible de acabar con la red Bitcoin, de poco servirían sus esfuerzos ya que existen una gran cantidad de alternativas que permiten a sus ciudadanos continuar transfiriendo valor entre pares, de forma segura y descentralizada. Están ante un "monstruo "de mil cabezas. Esto es una prueba más de que el cambio que representa Bitcoin para la humanidad es irreversible.

Tabla n°5: Ranking de las principales criptomonedas según su capitalización de mercado a mayo 2017.

| # | Name | Symbol | Market Cap | Price | Circulating Supply | Volume (24h) |
|---|---|---|---|---|---|---|
| 1 | Bitcoin | BTC | $38,430,571,718 | $2350.81 | 16,347,800 | $1,393,210,000 |
| 2 | Ethereum | ETH | $16,932,011,313 | $184.31 | 91,869,517 | $517,115,000 |
| 3 | Ripple | XRP | $12,435,490,439 | $0.322727 | 38,532,538,149 * | $154,585,000 |
| 4 | NEM | XEM | $2,348,064,000 | $0.260896 | 8,999,999,999 * | $19,665,500 |
| 5 | Litecoin | LTC | $1,629,324,717 | $31.80 | 51,240,332 | $218,759,000 |
| 6 | Ethereum Classic | ETC | $1,189,470,388 | $12.95 | 91,862,345 | $146,998,000 |
| 7 | Dash | DASH | $1,078,646,764 | $147.47 | 7,314,198 | $54,943,800 |
| 8 | Monero | XMR | $813,269,670 | $56.05 | 14,510,520 | $73,687,200 |

*. Fuente: https://coinmarketcap.com/*

3) RITMO DE EMISION PREDECIBLE:

El hecho de que la generación de Bitcoins está determinada exclusivamente por el algoritmo que fija su ritmo de emisión finita es la garantía de que el valor de esta moneda, a diferencia del resto de las monedas tradicionales del mundo, está exenta del riesgo asociado a los cambios de política monetaria de los bancos centrales, los cuales cuentan, como vimos en el capítulo 1, con un importante historial de manipulación del valor de las divisas que emiten. Como afirma Andreas Antonopoulos: “Bitcoin no está desregulado, está regulado, pero por un algoritmo en vez de por un gobierno. Es In-corrupto “.

4) AVAL DE REFERENTES:

Al tratarse de un desarrollo tecnológico complejo en el que para comprender a fondo algunas de sus funciones se requiere un profundo entendimiento de programación y desarrollo de softwares es importante saber que relevantes referentes de la industria tecnológica, como también de la política y la economía, han expresado sus consideraciones positivas sobre el Bitcoin. A continuación, tenemos una serie de declaraciones de reconocidas figuras mundiales donde explicitan sus evaluaciones positivas sobre este desarrollo e incluso sus expectativas sobre la evolución futura de esta tecnología:

“Creo que el hecho de que en el universo Bitcoin un algoritmo remplace funciones del gobierno me parece muy atractivo. Soy un gran fan de Bitcoin.” Al Gore, 45to vicepresidente de los Estados Unidos.

“Realmente creo que Bitcoin es la primera criptomoneda que tiene el potencial de hacer algo como cambiar el mundo.” Peter Thiel, Co-Fundador de Paypal.

“Bitcoin es un logro criptográfico destacable y la posibilidad de crear algo que no es duplicable en el mundo digital tiene enorme valor” Eric Schmidt, CEO de Google 2001-2011.

“Bitcoin es una proeza tecnológica, es mejor que el dinero tradicional para realizar transacciones internacionales” Bill Gates, Fundador de Microsoft.

“No puedes detener cosas como el Bitcoin. Estará en todas partes y el mundo deberá reajustarse. Los gobiernos del mundo deberán reajustarse. “John McAfee, Fundador de McAfee Seguridad Informática.

“Bitcoin puede ser la internet del dinero” Paul Buchheit, Creador de Gmail.

“Bitcoin es un desarrollo muy excitante, probablemente llegue a ser una divisa mundial. Creo que durante la próxima década va a crecer para volverse una de las formas más importantes para pagar cosas y transferir valores.” Kim Dotcom, CEO de MegaUpload.

“Bitcoin tiene el balance y los incentivos correctos, es por eso que esta comenzado a despegar” Julian Assange, fundador de WikiLeaks.

## B) OPORTUNIDADES

### 1) CAMINO A LA ADOPCION MASIVA

La principal oportunidad entorno a este desarrollo radica en el hecho de que, no obstante, las fortalezas de su diseño y funcionamiento, el crecimiento en el precio, desde menos de un centavo de dólar

en 2010 hasta los más de dos mil dólares en mayo de 2017, y la gran cantidad de nuevos emprendimientos gestándose a su alrededor, se estima que la cantidad de usuarios a nivel mundial, “apenas” ronda los 20 millones de personas.

Es difícil anticipar en que segmentos de la población mundial se dará el próximo salto en la aceptación de esta invención, puede ser entre los miles de millones de habitantes que se encuentran fuera del sistema bancario actual, como se mencionó en el capítulo 4, o quizás entre los ciudadanos de naciones desarrolladas, con mayor acceso a la información y el aval, o al menos sin el impedimento, del gobierno local.

En este sentido, la novedad más relevante de los últimos tiempos se dio el pasado 1ro de Abril con una pronunciación respecto a Bitcoin de parte del gobierno de Japón, 4ta potencia económica del mundo, mediante la promulgación de un decreto con el que reconoce a las diferentes criptomonedas digitales como “medio de pago reconocido”. Si bien no significa que el estado las considere, por ahora, como divisas, de todos modos, esta categorización ha desatado una serie de cambios positivos para el Bitcoin, que se encuentran en pleno desarrollo, y que está disparando el número de comercios donde es recibido como medio de pagos, desde los 4.500 existentes a comienzo de año hasta 260.000 estimados para fin de año. Esto nos marca la pauta que a pesar de los inconvenientes que este tipo de monedas anónimas puedan acarrear a los gobiernos, estos van tomando noción de que no hay forma de detener su avance, por lo que es más conveniente ir tomando medidas que acompañen su desarrollo antes que interponerse, y además, que a medida que este tipo de legislaciones vayan profundizándose y replicándose en otros puntos del globo la adopción podrá ir masificándose en un periodo no tan distante.

## 2) ROBARLE AL FOREX

El mercado de divisas, también conocido como Forex (abreviatura del término inglés Foreing Exchange) es un mercado mundial descentralizado en el que se negocian divisas.

Este mercado nació con el objetivo de facilitar el flujo monetario que se deriva del comercio internacional. Es, por gran margen, el mercado financiero más grande del mundo, llegando a mover un volumen diario de transacciones de alrededor de cinco billones de dólares, según el Bank for International Settlements, más que todos los demás mercados bursátiles del planeta combinados.

El mercado de divisas es un mercado mundial que, aunque cuenta con acceso las 24 horas, en la práctica se ve limitado por el paréntesis de las operaciones en el fin de semana. Como vimos anteriormente en este trabajo, una de las tantas virtudes del Bitcoin es su posibilidad de transferirse de forma casi inmediata desde cualquier lugar del mundo, en cualquier momento y por un costo muy bajo. Estas ventajas resultan claramente atractivas para los operadores del mercado Forex. Y al tratarse este de un mercado con un volumen operado tan alto, basta con que tan solo entre el 1% y 10% de su volumen operado diario comience a moverse en Bitcoins para que el precio de la criptomoneda se dispare a valores entre USD 100.000 y USD 1.000.000, según cálculos del especialista financiero americano Max Keiser. Y este salto en el precio no implica necesariamente una adopción masiva por parte de la población en general, si no, simplemente, que comience a ser tomado más en cuenta por quienes operan en estos mercados, que por lo general se trata de personas con acceso a información de calidad y con formación en matemáticas y economía.

## 3) MAS ALLA DE LA MONEDA: DESARROLLOS SOBRE LA BLOCKCHAIN

De forma paralela al desarrollo de bitcoin como divisa, la tecnología Blockchain, al tratarse de un registro abierto, inmutable, y descentralizado admite el funcionamiento de otras aplicaciones sobre ella diferentes a la moneda y que poco a poco despiertan el interés de distintas industrias, siendo la de las aseguradoras de riesgo una de las más involucradas en este momento, con casos concretos como las empresas Allianz, MetLife y Liberty Mutual que anunciaron estar trabajando en desarrollos con esta tecnología.

La posibilidad registrar contratos inteligentes en la Blockchain acelerarán la tramitación de siniestros en los seguros de Salud, Autos, Multirriesgos y Asistencia en Viaje, por ejemplo, con menos formularios que cumplimentar, menor necesidad de interacción entre reclamantes y aseguradoras y con menos posibilidades de error. Un sistema de contratos inteligentes reuniría en una misma infraestructura abierta a todos los participantes en la cadena de valor del seguro: consumidores, aseguradoras, tramitadores de siniestros e intermediarios. Se conseguiría así un proceso más rápido y cómodo de tramitación, gracias a la reducción de la documentación requerida, una menor dependencia de las comprobaciones manuales y mayor rapidez en la ejecución de los pagos. Solo en el segmento del seguro de Automóviles de uso personal, la consultora francesa Capgemini estima que los contratos inteligentes tienen un potencial de ahorro anual para las aseguradoras británicas cercano a 21.000 millones de dólares

en concepto de reducción de costes de tramitación a nivel mundial. Un ejemplo de esto sería una aplicación para smartphones que brinde la posibilidad a los clientes de la aseguradora de adquirir un seguro para un viaje específico que desee realizar con su vehículo de improviso, en el acto, registrando con un par de clicks la operación en la blockchain, por lo que informa de inmediato a toda la cadena de valor.

## C) AMENAZAS

### 1) INTERVENCION GUBERNAMENTAL

Hoy quizás la mayor amenaza que enfrenta el desarrollo del Bitcoin pasa por la hipotética posibilidad de que un gobierno, más precisamente el de la República Popular de China, que cuenta con un vasto historial de abierta censura e intervención sobre compañías que prestan o intentaron prestar servicios on-line en su territorio (Google, Facebook, Twitter), perpetre un ataque al funcionamiento de la red Bitcoin basándose en una particularidad demográfica de la que podrían sacar provecho: a diciembre del 2016, el 70% de todo el poder de procesamiento de la red Bitcoin proviene de mineros radicados en China (ver gráfico en página 23) , mientras que un porcentaje similar de los exchanges (casas de cambio) de Bitcoin a nivel global se encuentran también en ese país.

Según analistas, son variadas las causas por las que esta nación cuenta actualmente en su territorio con tal nivel de concentración de desarrollos en torno a esta criptomoneda (controles de capital sobre el Yuan - precio de la energía - características culturales de la población), pero el hecho es que este nivel de aglutinamiento existe y justo en una nación con los tristes antecedentes mencionados. De todas formas, al tratarse de una red descentralizada, un intento bloqueo al funcionamiento no sería tan sencillo como en los casos de las compañías nombradas, de hecho, les resultaría imposible detener el funcionamiento de toda la red, pero si es cierto que ante un asedio a grupos de mineros y/o traders podrían generar un daño importante a la comunidad Bitcoin, con serias repercusiones, momentáneas, pero serias al fin, en la cotización a nivel global de la criptomoneda.

Al comportarse Bitcoin como “efectivo digital”, gran parte de actividades consideradas ilícitas por los gobiernos, como la comercialización de drogas prohibidas, el tráfico de armas, la financiación a grupos

terroristas, la comercialización pornografía infantil o el tráfico de órganos humanos se concretan utilizando esta u otras criptomonedas. Esto atenta contra intereses, a veces honestos y otras veces no tanto, de los gobernantes, y al ser todas actividades repudiadas por la mayoría de la sociedad, seguramente representarán los argumentos que los enemigos de las criptomonedas utilizarán para intentar sumar el apoyo de la ciudadanía durante un hipotético ataque de parte de los gobiernos contra el Bitcoin.

## D) DEBILIDADES

### 1) ESCALABILDAD:

Es un tema crucial actualmente dentro de la comunidad Bitcoin. La creciente cantidad de usuarios vino acompañada naturalmente de un número cada vez mayor de transacciones diarias, que ahora son contadas por cientos de miles. La desafortunada realidad es que la red de Bitcoin, desde hace unos meses, es incapaz de procesar todas esas transacciones lo suficientemente rápido.

El problema reside en el límite que el software Bitcoin establece para el tamaño de cada bloque de transacciones procesado por los mineros, el cual continúa en un megabyte (1MB), sin que se haya modificado desde que Nakamoto lanzara el paper original. Cada transacción consta de datos importantes: el remitente, el destinatario, la cantidad de Bitcoins en la transferencia, etc. Estos datos ocupan un espacio, lo cual es bastante insignificante cuando se habla de una sola transacción. Pero suma cuando hay cientos de transacciones que tienen lugar cada minuto.

El límite de tamaño actual de 1 MB por bloque puede soportar como máximo de tres a cuatro transacciones por segundo, lo que equivale a unas 300.000 transacciones diarias. El problema aquí es que para una red con proporciones como las actuales esto ya no es suficiente. A continuación, veremos en un gráfico el crecimiento en el último año de las transacciones por día y de cómo desde hace pocas semanas, la red ha comenzado a operar al límite de su capacidad de 300.000 trans/día:

Gráfico n°4: Número de transacciones confirmadas por día en toda la red Bitcoin. Junio ´15 – Mayo ´17.


. *Fuente: https://blockchain.info/*

Cuando la red comienza a operar por encima del límite de su capacidad se ve a obligada a dejar transacciones pendientes de procesar, pero como vimos en el capítulo 2, la velocidad a la que los mineros de Bitcoin procesarán cualquier transacción en particular depende directamente del fee o comisión establecida por el remitente para cada transacción, por lo que las transacciones que quedarán demoradas serán aquellas con los menores fees abonados. Tal es así que en los primeros años las comisiones se medían en simples fracciones de un centavo, mientras que hoy en día, a mayo de 2017, ante la gran cantidad de transacciones que quedan por horas a la espera de ser procesadas, se ha generado una competencia entre los usuarios por lograr que los mineros prioricen sus pedidos, llevando el fee promedio abonado por transacción desde los U$S 0,05 hace un año hasta aproximadamente U$S 2,50. Vale aclarar que el importe abonado como fee es independiente de la cantidad de bitcoins transferidos, por lo que torna prácticamente inviable las transacciones de importes pequeños que pretendan ser inmediatas.

Gráfico n°5: Promedio en USD de los fee abonados desde Junio ´16 a Mayo ´17.


*Fuente: https://bitinfocharts.com/*

Esto nos marca la pauta de que una solución a este inconveniente debe ser implementada a la brevedad, por lo que desde hace un tiempo existen dos alternativas principales en disputa dentro de la comunidad sobre cómo resolver este inconveniente, sin que aún la mayoría de los involucrados se haya decidido por una u otra. Estas son: “Segregated Witness” (SegWit) y “Bitcoin Unlimited”.

La propuesta denominada SegWit no se ocupa del límite de tamaño de bloque, si no que propone eliminar los datos no críticos de las transacciones, disminuyendo el tamaño de cada transacción individual, haciendo posible empaquetar más transacciones en un bloque del mismo tamaño. Puede conducir a un aumento del 60–70 por ciento en el rendimiento de la red, es decir, basta para resolver el problema de la escala solamente en el mediano plazo, mientras se espera que la evolución de las tecnologías que se están desarrollando alrededor de Bitcoin maduren como para brindar una solución más estable.

Bitcoin Unlimited, por otro lado, propone directamente abolir el límite de 1MB en el tamaño del bloque, lo cual permitiría transacciones inmediatas y a un costo casi nulo, pero en contrapartida conduciría a una mayor centralización de Bitcoin, ya que sólo las grandes empresas podrían permitirse el espacio de almacenamiento, la potencia de cálculo y el ancho de banda necesarios para procesar los bloques de tamaño tan grande, eliminando a los operadores de pequeña escala de la red. Eso va en contra de la idea misma de Bitcoin como el dinero gobernado por cada uno de sus usuarios, socavando el espíritu descentralizador de la moneda.

Para que una de las dos propuestas sea adoptada debe ser implementada por una mayoría considerable de los usuarios, y si bien aún no se ha definido, por el momento SegWit cuenta con una ventaja en cantidad de apoyos.

## E) RECOMENDACIONES

En base a toda la información vertida en este trabajo, podemos concluir que esta tecnología, si bien cuenta con todas las condiciones necesarias para serlo, aún dista de constituirse en una moneda de cambio masivamente aceptada, ya que la cantidad de usuarios y de comercios dispuestos a recibirla representa un porcentaje absolutamente ínfimo del comercio mundial.

Pero para un inversor dispuesto a asumir cierta cuota de riesgo esto está lejos de ser una mala noticia, por el contrario, representa una oportunidad más que interesante para obtener una rentabilidad muy por encima de la media al constituirse como inversor temprano de una tecnología que a todas luces está destinada a cuanto menos alcanzar un grado de adopción considerablemente superior al actual, lo cual, lógicamente, impulsará el precio al incrementarse la demanda vía crecimiento en el número de usuarios, cosa que ha ido ocurriendo sistemáticamente desde su lanzamiento, y no debería sorprendernos que así continúe dadas las enormes ventajas, descriptas en este trabajo, con las que cuenta este activo, y, principalmente, por las virtudes técnicas que la hacen prácticamente imposible de desmantelar.

# BIBLIOGRAFÍA


ANTONOPOULOS, Andreas: “Mastering Bitcoin.”, EE.UU., O’Reilly Media, segunda edición. (2017).

ANTONOPOULOS, Andreas: “The Internet of Money.” Merkle Bloom LLC; primera edición (2016).

GONZALEZ OTERO, Juan Manuel: “Bitcoin: la moneda del futuro.” Amazon Media. (2013).

HARARI, Yuval Noahl: “Sapiens. De animales a dioses: Una breve historia de la humanidad.”; Editorial Harper, Israel. segunda edición (2011).

KAISER, Axel: “La miseria del intervencionismo: 1929-2008.”. Penguin Random House, primera edición, Chile (2012).

MENGER, Carl: “El origen del dinero.” Austria, Economic Journal, primera edición. (1892).

NAKAMOTO, Satoshi: “Bitcoin: Un sistema de dinero electrónico entre iguales (P2P).” Bitcoin Fundation. (2008).

SIRI, Santiago: “Hacktivismo.” Argentina. Sudamericana, primera edición (2015).

## SITIOS WEB CONSULTADOS

- http://blockchain.info/
- http://coindesk.com/
- http://investing.com/
- http://stlouisfed.org/
- http://elbitcoin.org/
- http://wikipedia.com
- http://wired.com
- https://coinmarketcap.com/
- http://datos.bancomundial.org/
- https://bitcoinfoundation.org/

**Declaración Jurada Resolución 212/99-CD**

"El autor de este trabajo declara que fue elaborado sin utilizar ningún otro material que no haya dado a conocer en las referencias, que nunca fue presentado para su evaluación en carreras universitarias y que no transgredí o afecta derecho de terceros"

Mendoza,

Apellido y Nombre: Conti, Alberto

N° Registro: 23.728

Firma