Universidad Zaragoza
1542

Trabajo Fin de Grado

ASPECTOS TÉCNICOS Y ECONÓMICOS DE BITCOIN FRENTE AL DINERO FIDUCIARIO

BLOCKCHAIN

Autor/es

Javier Martínez Morales

Director/es

Patricia Bachiller Baroja

Facultad de Economía y Empresa/ Campus río Ebro

Año 2019

Contenido

CAPITULO I: INTRODUCCION Y OBJETIVOS

1.1 PRESENTACIÓN Y JUSTIFICACIÓN DEL ESTUDIO

Bitcoin y las criptomonedas en general, han tenido una gran repercusión mediática por su carácter especulativo. El espectacular crecimiento que tuvo la moneda Bitcoin durante 2018 llamó la atención al mundo.

Esto es conocido por todos, el hecho de que el tipo de cambio de un Bitcoin llegará a ser de 20.000 dólares es más que suficiente para aparecer en las noticias. Pero no todo el mundo conoce lo que hay detrás de esta moneda.

Este trabajo se centra entonces en llegar a sus características innovadoras, y de una comparativa en un contexto económico. La intención ha sido, primeramente, mostrar mediante un marco simplificado el cómo están estructurados los mercados financieros para luego hablar profundamente del Bitcoin en sus aspectos más técnicos y explicar debidamente las revoluciones que destacan de la misma, con el objetivo de examinar si las criptomonedas son válidas como método de intercambio de valor y superar el velo mediático en el que únicamente han sido nombradas por su carácter especulativo.

El trabajo se desarrolla de la siguiente manera, se debiera comenzar con el apéndice 1, que es un breve comentario histórico sobre el cómo surge el concepto de dinero, ya que cuando hablamos de una criptomoneda, es necesario hacer una previa definición de lo que realmente es el dinero y si las criptomonedas pueden ejercer esta función. Además, también es importante situar el cómo nacen diversos agentes y conceptos que rigen nuestra economía actual. El capítulo II se centra en crear un marco del modelo económico actual y describir las herramientas del banco central direccionado a la política monetaria de éste. Los apéndices 2 y 3, tratan los temas de la crisis económica de 2007 que fue un gran motor para la expansión de Bitcoin como alternativa de reserva de valor y cómo se puede desarrollar un pánico bancario, respectivamente.

Seguidamente se habla del cómo nace el concepto de criptomoneda, y cuáles son las ideas que llevan a esta alternativa de un sistema descentralizado y un breve acercamiento al creador de la moneda Bitcoin, Satoshi Nakamoto.

En el siguiente capítulo, se presenta la tecnología Blockchain, la red que soporta la criptomoneda, tipos y aplicaciones de ésta al mundo moderno. Para luego explicar técnicamente los aspectos del ejemplo más conocido de la Blockhain o cadena de bloques, Bitcoin.

Además, el apéndice 4 es una cronología que muestra el exponencial crecimiento de la moneda.

Y por último un capítulo de conclusión, donde se reflexiona todo lo explicado durante el trabajo y propongo mi opinión.

CAPITULO II: SISTEMA DE EMISION CENTRALIZADA

2.1. PAPEL Y FUNCIONES DE UN BANCO CENTRAL

Los mercados financieros[1] desempeñan un papel esencial en la economía. Determinan el coste de los fondos que captan las empresas, los hogares y el Estado y, a su vez, afectan a las decisiones de gasto.

Primeramente, nos centramos en la influencia que tiene el banco central en los tipos de interés, para simplificar la realidad, consideraremos que solo existen dos activos financieros, a saber, el dinero que no rinde intereses, y los bonos, que sí. Esto nos permite entender cómo se determina el tipo de interés de los bonos y el papel que desempeña el banco central.

En la actualidad, la mayoría de los países cuentan con un sistema financiero similar en donde existe un banco central encargado de regular la oferta monetaria de su economía.

Un Banco Central[2] es entonces: –"Una Institución que tiene como misión la definición y ejecución de la política monetaria dentro de un área determinada, incluyendo la emisión de su moneda de curso legal. Esta misión normalmente va asociada al objetivo de mantener la estabilidad de los precios. Los bancos centrales, dependiendo de las competencias que les hayan sido asignadas, pueden ejercer también otras funciones, como la supervisión de los sistemas de pago, la supervisión de las entidades de crédito, servir de agente financiero del Estado, etc."–

En Europa, es el Banco Central Europeo (BCE) y, en Estados Unidos, la Reserva Federal (FED). A la definición anterior, habría que añadir que es un organismo independiente del poder político, del gobierno. En el caso de la FED se trata de un organismo privado. El marco económico sobre el que funciona el banco central evoluciona. Estudios ulteriores apuntan, que el Banco Central, para su mejor funcionamiento, no debe estar influenciado por el poder político de su mismo país, sino que debe regir con independencia las herramientas que tiene a su alcance para lograr sus objetivos. Aunque en determinados casos, deberá articular simultáneamente con el gobierno central acciones para evitar crisis económicas.

Los Bancos Centrales, en términos generales, tienen dos objetivos: lograr la estabilidad macroeconómica y la estabilidad financiera del país los Bancos Centrales.

1.- Lograr la estabilidad macroeconómica[3]:

Uno de los objetivos del banco central es entonces lograr un crecimiento estable sin grandes oscilaciones de los precios. En resumidas cuentas, el objetivo es tener una inflación controlada.

---

[1] Oliver Blanchard, Macroeconomía (2017), 7ªedición, capítulo 4

[2] Banco Central, definición propuesta por https://www.eleconomista.es/diccionario-de-economia/banco-central

[3]Objetivo Banco Central: https://economipedia.com/definiciones/funciones-y-objetivos-bancos-centrales.html

El objetivo fundamental del Banco Central Europeo (BCE) es mantener la estabilidad de precios en la zona euro. Es decir, controlar la inflación para que los precios no se disparen o se contraigan demasiado. Actualmente, la cifra de referencia para "controlar" la inflación se sitúa entre un 2% y un 3%, por lo que el BCE intenta asegurar que se cumpla ese objetivo de inflación a través de los instrumentos de la política monetaria.

2.- Mantener la estabilidad financiera [4]del país.

Este objetivo no tiene una finalidad tan concreta como el anterior. Mantener la estabilidad financiera reúne varios determinantes cómo: lograr una estabilidad del tipo de cambio con respecto a otras divisas, conseguir el pleno empleo, moderar los tipos de interés en el largo plazo, y prevenir o mitigar los pánicos o crisis financieras. El proceso de creación del dinero bancario hace a la economía susceptible a estos pánicos, lo explicaremos más adelante en el siguiente capítulo junto con el apéndice 2.

Para cómo lograr sus objetivos el banco central dispone de 3 herramientas fundamentales:

A. La política monetaria
B. Prestamista de última instancia
C. Regulación y supervisión financiera

La política monetaria será la herramienta que nos ocupe el resto de la primera parte del estudio, ya que es directamente controlada por el banco central y es prácticamente la razón de su existencia.

El papel como prestamista de última instancia se tratará en el apéndice 2 ejemplificando un pánico bancario y cuál es el papel que debe tomar el banco central para mitigarlo.

2.2. INTERMDIARIOS FINANCIEROS Y DINERO BANCARIO

Antes de hablar de las herramientas de que dispone el banco central para influir en la oferta monetaria, referida al total de dinero de una economía de un país determinado, cabría distinguir entre el dinero legal y el dinero bancario, y como se crea este último.

En añadido al apéndice 1, en el que tratábamos el tema de la evolución del dinero hasta nuestros días, ahora pues, con el dinero fiduciario, es conveniente añadir esta distinción entre estas dos "clases" de dinero.

[4] Objetivo Banco central: https://economipedia.com/definiciones/funciones-y-objetivos-bancos-centrales.html

- El dinero legal[5], constituido por los billetes y monedas emitidos por el banco central, es el que circula por una economía. En la actualidad, España es uno de los países de la Unión Europea (UE) integrado en la denominada zona euro, es decir, que han adoptado el euro como moneda, por lo que el organismo encargado de emitir y controlar la cantidad de dinero circulante es el Banco Central Europeo (BCE).

- El dinero bancario[6], sería aquel creado por los bancos a partir de los depósitos que hacen los ahorradores, que se convierten en nuevos depósitos, es decir, nuevo dinero. Se distingue entre los depósitos a la vista (cuenta corriente o de ahorro), de disposición inmediata y sin remuneración, y los depósitos a plazo, cuya disponibilidad no es inmediata, sino una vez finalizado el plazo de tiempo comprometido, y que obtienen una remuneración, un interés, durante ese tiempo.

Las economías modernas se caracterizan por la existencia de muchos tipos de intermediarios financieros, es decir, de instituciones que reciben fondos de los individuos y de las empresas, y los utilizan para comprar bonos o acciones, o para hacer préstamos a otras personas o empresas.

Los bancos son uno de los tipos de intermediario financiero. Lo que hace que sean especiales (y la razón por la que aquí centramos la atención en ellos y no en los intermediarios financiero en general) es que su pasivo es dinero.

Los bancos reciben fondos de las personas y las empresas, que los depositan directamente o los envían a sus depósitos a la vista (por ejemplo, depositando directamente su nómina). En cualquier momento pueden extender cheques, utilizar una tarjeta de débito o retirar fondos, hasta agotar el total de sus depósitos a la vista. El pasivo de los bancos es, pues, igual al valor de estos depósitos a la vista.

[Podemos distinguir entre depósitos a la vista – con los que no conseguimos remuneración, pero su disponibilidad es inmediata – y los depósitos a plazo – que nos permiten obtener las ganancias derivadas del rendimiento del dinero a un tipo de interés pactado, pero con la salvedad de que no podremos disponer del mismo hasta la fecha de vigencia que haya sido estipulada-. Como es bien sabido, los depósitos de los ahorradores son prestados a los inversores. Por lo tanto, la cantidad total de dinero en la economía es siempre mucho mayor que el dinero legal que hay, por lo que no se puede respaldar todo el dinero de la economía sólo con los billetes y monedas que han sido emitidos.]

Los Bancos mantienen como reservas algunos de los fondos que reciben. Los mantienen parte en efectivo, y en parte, en una cuenta que tienen los bancos en el banco central, a la

[5]Dinero legal: https://www.vivus.es/blog/prestamopedia/tipos-dinero/
[6] Dinero bancario: https://sites.google.com/site/economia20parabachillerato/temario/tema-7-el-mercado-de-dinero/2-el-mercado-monetario

que pueden recurrir cuando los necesitan. Los bancos mantienen reservas por varias razones:

Un día cualquiera, las personas que tienen cuentas en el banco extienden cheques a otras personas que tienen cuentas en otros bancos, mientras que otras depositan dinero. No hay razón por las que las entradas de dinero y las salidas sean iguales, por lo que el banco debe tener algún efectivo disponible.

Esto implica que los bancos quieran tener alguna cantidad de reservas, aunque no se les obligara. Pero, además, suelen estar sujetos a coeficientes de reservas obligatorias, que les exigen mantener unas reservas proporcionales a sus depósitos a la vista. En Estados Unidos, la Fed establece las reservas obligatorias en un 10% del valor de los depósitos a la vista. Los bancos pueden utilizar el resto para conceder préstamos o comprar activos financieros.

En estados unidos los prestamos representan alrededor de un 70% de los activos de los bancos que no son reservas.

Los bancos, entonces, reciben dinero de los ahorradores. Este dinero, una vez es ingresado en el banco por el individuo o empresa que lo deposita, pasa a formar parte de su cuenta de resultados, es el pasivo del banco. Los bancos, entonces prestan (o compran activos financieros) ese dinero a empresas e individuos que precisan de financiación, el proceso de creación de dinero bancario podría ejemplificarse de la siguiente manera:

Imaginemos una economía con un solo banco y un coeficiente de reserva legal del 3% (es decir, el banco tiene que guardar como reservas un 3% del total). Una persona A deposita 100 euros en el banco, el banco entonces se queda con 3euros y presta 97 euros a otra persona B para que se compre algo.

En los ordenadores del banco, la persona A sigue teniendo los 100 euros, pero además la persona B tiene 97 euros de nuevo dinero bancario en su cuenta. Son solo dígitos en una pantalla de ordenador, no hay dinero en efectivo u oro que respalde los nuevos números de la cuenta de B. Esto es dinero nuevo creado como deuda. Cuando la persona B gasta esos 97 euros, digamos en una tienda, el dueño de la tienda los deposita en el banco, que los vuelve a prestar (salvo el 3% de reserva legal) una y otra vez. Nuestros 100 euros originales, se han multiplicado y ahora hay más de 3.333 euros en el sistema. Este proceso por el que los bancos prestan mucho más dinero del que tienen en sus cajas fuertes, se llama reserva fraccionaria.

La oferta monetaria, contiene entonces el total de dinero en circulación de una economía de un país determinado. Este total, de dinero en circulación, será el conjunto del dinero legal y dinero bancario.

Como ya hemos mencionado, una de las funciones principales del banco central es controlar la oferta monetaria, para exponerlo, explicaremos brevemente de manera algebraica de cómo se compone la oferta y demanda monetaria.

2.3. OFERTA Y DEMANDA DE DINERO

Demanda de dinero[7]

La oferta monetaria, se puede formular a raíz de la igualdad de equilibrio de los mercados financieros, en donde la oferta monetaria debe ser igual a la demanda de dinero.

La demanda de dinero, en su conjunto, no es más que la suma de las demandas de dinero de todas las personas y las empresas de la economía. Ésta depende del nivel total de transacciones que se realizan en la economía y del tipo de interés. Es lógico pensar que cuantas más transacciones realice un individuo, mayor cantidad de dinero en efectivo necesitara para satisfacerlas (mayor demanda de dinero), y de la misma manera cuanto más alto sea el interés al que puede prestar su dinero, más le interesara comprar bonos o realizar depósitos a plazo (menor demanda de dinero).

La demanda de dinero se formula entonces:

$$M^{\mathrm{d}} = \underset{(-)}{YL(i)} \in$$

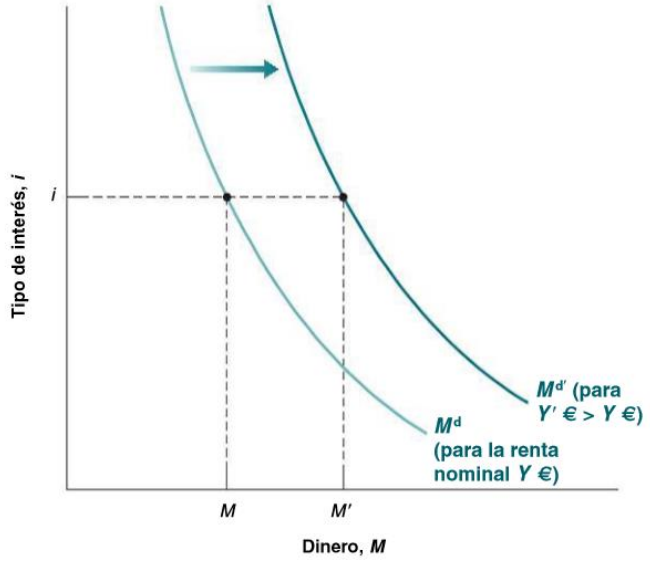
Esta ecuación la debemos entender de la siguiente manera; la demanda de dinero, M^d , es igual a la renta nominal, Y, multiplicada por una función decreciente del tipo de interés.

- El signo negativo situado debajo de *i,* en *L(i),* refleja el hecho de que el tipo de interés produce un efecto negativo en la demanda de dinero, ya que la gente coloca mayor parte de su dinero en bonos. Cuanto más bajo es el tipo de interés (menor i), mayor es la cantidad de dinero que quieren mantener los individuos (mayor M).
- La demanda de dinero aumenta en proporción a la renta nominal. Si la renta nominal se duplica, la demanda de dinero también se duplica. Pues es lógico pensar que, si la renta de un individuo aumenta, también aumentará su número de transacciones y en resumen su demanda de dinero.

Estas dos conjeturas, pretenden explicar el comportamiento de un individuo, que se puede extrapolar además al total de la economía en este plano simplificado en donde solo pudiéramos elegir entre invertir en bonos o mantener efectivo para realizar nuestras transacciones.

Podemos representar entonces la curva de demanda de dinero M^d :

[7] Oliver Blanchard, Macroeconomía (2017), 7ªedición, capitulo 4



Esta gráfica muestra visualmente, la relación entre la demanda de dinero, la renta nominal y el tipo de interés. El tipo de interés, i, se mide en el eje de ordenadas y el dinero, M, en el de abscisas.

A la vista del grafico, la curva M^d representa la relación entre la demanda de dinero y el tipo de interés correspondiente a un determinado nivel de renta nominal, €Y. Como hemos dicho, tiene pendiente negativa, cuanto mayor es el tipo de interés, menor es la demanda de dinero.

Además, dado el tipo de interés, i, un aumento de la renta nominal desplaza la demanda de dinero hacia la derecha, desde M^d a $M^{d'}$, es decir, eleva la demanda de dinero.

Una vez analizada la demanda de dinero, ahora prestaremos atención a la oferta de dinero del Banco Central.

Oferta de dinero[8]

En el mundo real hay dos tipos de dinero: los depósitos a la vista, que son ofrecidos por los bancos, y el efectivo, que es suministrado por el banco central. Supondremos que el único dinero que hay es el efectivo, el dinero del banco central. El algebra será más sencilla y las conclusiones básicas serán las mismas.

Supongamos que el banco central decide ofrecer una cantidad igual a M, por lo que:

$$M^s = M$$

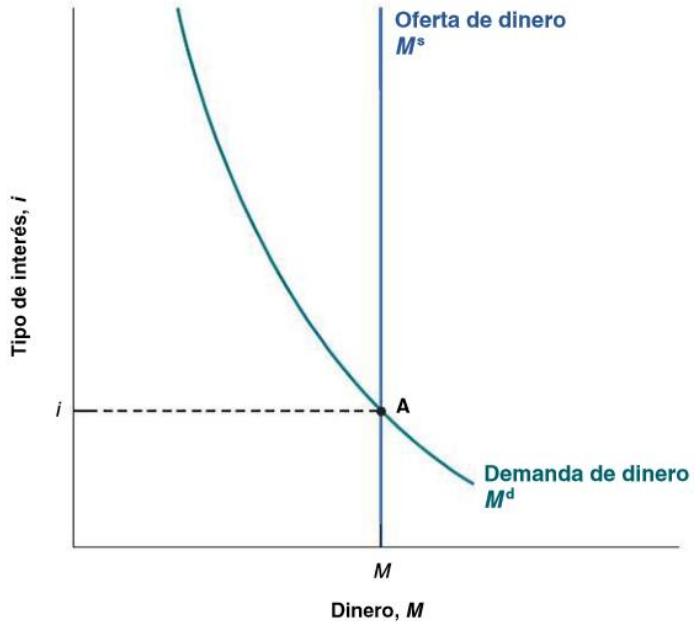
Para que los mercados financieros estén en equilibrio, la oferta monetaria debe ser igual a la demanda de dinero, es decir, $M^s = M^d$

[8] Oliver Blanchard, Macroeconomía (2017), 7ªedición, capítulo 4

Oferta de dinero = demanda de dinero

$$M = YL(i)\ €$$

Esta ecuación nos dice que el tipo de interés *i* debe ser tal que los individuos, dada su renta nominal *Y €,* estén dispuestos a tener una cantidad de dinero igual a la oferta monetaria existente, *M*. Esta relación de equilibrio se denomina relación LM.



La demanda de dinero, M^d, que corresponde a un determinado nivel de renta nominal, Y €, tiene pendiente negativa: cuando sube el tipo de interés, la demanda de dinero disminuye. Como hemos dicho, cuanto más interés recibiéramos por prestar nuestro dinero, más nos interesa esa opción, en vez de mantener efectivo.

La oferta monetaria es una línea recta vertical representada por M^s: la oferta monetaria es igual a M e independiente del tipo de interés. El equilibrio se encuentra en el punto A y el tipo de interés de equilibrio es i.

Esto implica que la oferta monetaria es fijada por el banco central y por lo tanto se muestra en el grafico como una línea recta. Mediante ella, pueden influir en la demanda de dinero, intentando fijar un tipo de interés que se adecue a los objetivos de las políticas monetarias.

Ahora una vez sabemos cómo está estructurado el mercado financiero y cuáles son los factores que lo modifican podemos hacer hincapié en las herramientas de las que este dispone para modificar la oferta monetaria y afectar al equilibrio.

2.4. LA POLITICA MONETARIA Y LAS OPERACIONES DE MERCADO ABIERTO

En las economías modernas, los bancos centrales suelen modificar la oferta monetaria comprando o vendiendo bonos en el mercado de bonos. Si un banco central quiere aumentar la cantidad de dinero en la economía, compra bonos y lo hace creando dinero nuevo. Si quiere reducirla, vende bonos y retira de la circulación el dinero que recibe a cambio. Estas actividades se denominan operaciones de mercado abierto, porque se realizan en el mercado abierto de bonos.

El activo de un banco central está formado por los bonos y activos financieros que tiene en su cartera y su pasivo por la cantidad de dinero que hay en la economía. Las operaciones de mercado abierto[9] provocan un cambio de igual magnitud del activo y del pasivo del banco central. Es decir, si aumenta el dinero en la economía por valor de 1000 millones (su pasivo aumenta), lo hace comprando bonos por valor de 1000 millones (su activo aumenta), a eso se refiere el cambio de igual magnitud entre activo y pasivo, ocurriría de la misma forma, pero a la inversa, en el caso de que retirara dinero de la economía.

Ahora explicamos brevemente la relación entre el precio de los bonos y el tipo de interés, puesto que, lo que se determina realmente en los mercados de bonos es el precio de éstos y no el tipo de interés.

Supongamos que los bonos de nuestra economía son bonos a un año, es decir, bonos que prometen pagar una determinada cantidad de euros, por ejemplo, 100 €, dentro de un año. Supongamos que su precio actual es P_B €, donde B se refiere a bono. Si compramos el bono hoy y lo conservamos durante un año, su tasa anual de rendimiento es igual a (100 € - P_B €)/P_B €. Por lo tanto, el tipo de interés del bono es:

$$i = \frac{100\ € - P_B\ €}{P_B\ €}$$

Si P_B € es igual a 95 €, el tipo de interés es igual a (100-95) €/95 € = 0,053, o sea, 5,3 %. Si es igual a 90 €, el tipo de interés es del 11,1 %. Cuanto más alto es el precio del bono, más bajo es el tipo de interés.

Dicho esto, consideremos primero el caso de una operación de mercado abierto expansiva, en la que el banco central compra bonos en el mercado de bonos y los paga creando dinero. Al comprar bonos, la demanda de bonos aumenta y, por lo tanto, su precio sube. Y a la inversa, el tipo de interés de los bonos baja. Consideremos, por el contrario, una operación de mercado abierto contractiva, en la que el banco central reduce la oferta monetaria. Vende bonos en el mercado abierto (bonos de su activo). Eso provoca una bajada de su precio y una subida del tipo de interés.

[9] Operaciones mercado de mercado abierto: Oliver Blanchard, Macroeconomía (2017), 7ªedición, capítulo 5

Resumamos:

- El tipo de interés es determinado por la igualdad de la oferta y la demanda de dinero.
- Modificando la oferta monetaria, el banco central puede influir en el tipo de interés.
- El banco central altera la oferta monetaria realizando operaciones de mercado abierto, que son compras o ventas de bonos por dinero.
- Las operaciones de mercado abierto en las que el banco central eleva la oferta monetaria comprando bonos provocan una subida de su precio y una bajada del tipo de interés.
- Las operaciones de mercado abierto en las que el banco central reduce la oferta monetaria vendiendo bonos provocan un descenso del precio de los bonos y una subida del tipo de interés.
- La demanda de dinero está influenciada por dos factores, la renta nominal, que ejerce una variación positiva, y el tipo de interés, que ejerce una variación negativa en la demanda de dinero.
- Los Bancos Centrales piensan que tipos de interés quieren alcanzar y después modifican la oferta monetaria mediante las operaciones de mercado abierto.
- La política monetaria, que es la herramienta más importante del Banco Central, implica entonces que pueden variar el tipo de interés modificando así la oferta monetaria.

Dicho esto, es preciso añadir, que la realidad dista sustancialmente de ser tan sencilla. Hemos supuesto que sólo había una clase de bonos, sin embargo, los bonos difieren en varios aspectos.

Ni usted ni yo podemos endeudarnos al tipo de los fondos fijado por la Fed y hay un motivo para ello. Cualquier prestamista sabe que existe probabilidad de que no fuéramos capaces de hacer frente a los pagos. Lo mismo ocurre con las empresas que emiten bonos. Algunas presentan poco riesgo y otras más. Para compensar la existencia de riesgo, los tenedores de bonos exigen una prima de riesgo.

El enfoque práctico [10]de esto se podría ejemplificar con lo ocurrido durante la crisis financiera de 2007.

Para ello reflexionaremos sobre lo ocurrido, prestando atención a tres clases de bonos y teniendo en cuenta el intervalo de tiempo del año 2000 a 2014. Dichas clases presentan los tipos de interés de tres clases de bonos desde el año 2000: Bonos del Estado estadounidense, considerados casi sin riesgo, junto a bonos corporativos calificados como

[10] Comentario informativo sobre las limitaciones de la Fed para influir en el tipo de interés real de la captación de recursos por empresas; Oliver Blanchard, Macroeconomía (017), 7ªedición

seguros (AAA), y menos seguros (BBB), respectivamente, por las agencias de calificación crediticia. Podemos llegar a tres conclusiones.

En primer lugar, históricamente, el tipo de los bonos corporativos incluso de la máxima calificación crediticia (AAA) supera en EE. UU. al tipo de los bonos del Estado en una prima de alrededor del 2%, en promedio. Es decir, el Gobierno de Estados Unidos puede endeudarse a tipos más bajos que las empresas estadounidenses. En segundo lugar, y de la misma manera, el tipo de los bonos corporativos de menor calificación (BBB) supera al tipo de los bonos de máxima calificación (AAA) en una prima que suele exceder el 5%. En tercer lugar, lo que realmente ocurrió durante 2008 y 2009 conforme se desarrollaba la crisis financiera, fue que, aunque el tipo de los bonos del Estado cayó, reflejando la decisión de la Fed de reducir el tipo oficial, el tipo de interés de los bonos de menor calificación aumentó bruscamente, alcanzando el 10% en los momentos álgidos de la crisis. Es decir, pese a que la Fed estaba reduciendo el tipo oficial hasta situarlo casi en cero, el tipo al que las empresas de menor calificación crediticia podían endeudarse aumentó sustancialmente, por la que la inversión pasó a ser una opción extremadamente poco atractiva para ellas.

Este hecho nos muestra ciertas limitaciones del gobierno central para fomentar la inversión mediante políticas monetarias expansivas.

2.5. RESULTADOS DEL SISTEMA

Hasta ahora hemos hablado del sistema financiero actual, de los agentes que intervienen en él, y de las políticas que toma el Banco Central para intentar lograr sus objetivos o paliar las recesiones que pudiera sufrir un país. Pero como en cualquier proceso surgen residuos, podríamos nombrar como el principal resultado indirecto de las políticas monetarias expansivas la inflación.

Su concepción es desde luego sencilla, se trata del aumento continuado y generalizado de los precios. Es fácil entender que, si de forma continuada aumenta el total de dinero en la economía sin un acompañamiento acorde de la producción, el resultado sería un aumento del precio de los bienes. La inflación es entonces una pérdida del poder adquisitivo de la moneda.

Para medir el crecimiento de la inflación se utilizan índices que reflejan el crecimiento porcentual de una 'cesta de bienes' ponderada. El índice de medición de la inflación es el Índice de Precios al Consumidor (IPC). El IPC[11] refleja el coste monetario de una lista especifica de bienes y servicios a lo largo del tiempo. Esta lista, que se basa en un minucioso estudio del gasto de los consumidores, intenta recoger la cesta de consumo de un consumidor urbano representativo y se actualiza cada dos años.

En Estados Unidos, esta cesta recoge los precios de 211 artículos en 38 ciudades. Al igual que el deflactor del PIB (el nivel de precios correspondiente a la producción agregada o PIB), es un índice. Es igual a 100 en el periodo elegido como base y su nivel no tiene ningún significado especial. El periodo base actual es 1982-1984, por lo que la media en

[11] Descripción del IPC Oliver Blanchard, Macroeconomía (2017), 7ªedición

ese año es igual a 100. En 2014, el IPC fue 236´7, por lo que comprar la misma cesta de consumo valía más del doble en dólares que en 1982-1984.

Pero ¿por qué preocupa la inflación?

Si un aumento de la tasa de inflación significara simplemente una subida más rápida, pero proporcional, de todos los precios y los salarios (caso que se conoce como inflación pura), la inflación sólo sería un pequeño inconveniente, ya que no afectaría a los precios relativos.

Preocupa precisamente porque la inflación pura no existe:

Durante los periodos de inflación, no todos los precios y salarios suben de la misma manera, por lo que la inflación afecta a la distribución de la renta, lo cual significa que, por ejemplo, en algunos países los jubilados reciben prestaciones que no suben al mismo ritmo que los precios y, por lo tanto, pierden en relación con otros grupos cuando la inflación es alta. Esto ocurrió en Rusia durante la elevadísima inflación que padeció en 1990, las pensiones no subieron al mismo ritmo que la inflación y eso llevó a muchos jubilados al borde de la inanición.

La inflación introduce otras distorsiones. Las variaciones de los precios relativos también crean incertidumbre, dificultando a las empresas tomar decisiones sobre el futuro, por ejemplo, de inversión. Algunos precios, que se fijan por ley o que están regulados, se quedan rezagados con respecto a otros, lo que altera los precios relativos. Los impuestos interactúan con la inflación y crean más distorsiones. Por ejemplo, si los tramos impositivos no se ajustan para tener en cuenta la inflación, los contribuyentes pasan a tramos cada vez más altos a medida que aumenta su renta nominal, aunque su renta real no varíe.

Otro añadido como resultado del sistema financiero actual son los altos costes de intermediación para verificar las transacciones monetarias entre las partes, cuando se utiliza cualquier otra forma de dinero que no sea el dinero en efectivo (tarjetas, cheques, etc…)

Esto queda en evidencia sobre todo al mostrar el modelo de intercambio de valor de bitcoin. Podemos hacernos mil cuestiones sobre su validez o si pudiera reemplazar nuestro sistema, mejorarlo, o fusionarse. Pero lo que sí que hace evidente es que, si entendemos el dinero como un método de intercambio de valor, las criptomonedas tienen voz en este debate.

CAPITULO III: ORIGEN DE BITCOIN

3.1. CREADOR Y ORIGEN DEL BITCOIN

El origen y las influencias desde las que nace Bitcoin no es exacto, pero se podría considerar como punto de partida la segunda mitad del siglo XX, con el inicio de la criptografía de clave pública y la sucesiva aparición de importantes avances tecnológicos de la época, con internet como principal protagonista.

A raíz de este mundo de posibilidades que ofrece internet, nacen distintas corrientes de pensamiento, emanadas sobre el cómo actuar en este nuevo mundo digital, entre otras "*el Hacktivismo*[12]*"* un acrónimo de hacker y activismo que hace referencia a la utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos. De éste surge a principios de los 90 el movimiento *cypherpunk*, que tiene especial importancia en el origen de Bitcoin. El termino *cypherpunk* hace referencia a la nueva vulnerabilidad de la información que se deposita en la red y a la imposibilidad en muchas ocasiones del anonimato.

Las ideas básicas del movimiento **se pueden encontrar en *A Cypherpunk's Manifesto***, escrito por Eric Hughes en 1993:

> *La privacidad es necesaria para una sociedad abierta en la era electrónica. [...] No podemos esperar que los gobiernos, las empresas u otras grandes organizaciones sin rostro nos la proporcionen. [...] Debemos defender nuestra propia privacidad si esperamos tener alguna. [...] Los cypherpunks escriben código. Sabemos que alguien tiene que hacerlo para defender la privacidad, y nosotros vamos a escribirlo.*

Fuente: https://www.genbeta.com/a-fondo/que-son-los-cypherpunks-y-por-que-son-tan-importanes-en-la-lucha-por-la-privacidad

Pero no es finalmente hasta 1998, en la lista de correos Cypherpunk, cuando aparece por primera vez el concepto de ``moneda criptográfica´´, el cual fue definido por Wei Dai[13], un ingeniero informático que describió un sistema descentralizado, que por medio de la criptografía permite a los usuarios el intercambio de valor mediante una moneda electrónica. Ésta moneda a la que llamo ``B-money´´, estaría fuera del control de los gobiernos y demás instituciones reguladoras. Este trabajo es completado posteriormente por otros expertos en criptografía como Nick Szabo y Hal Finney.

Para poder realizar las transacciones que describía Wei Dai, cada usuario dispone de una cuenta propia en donde almacena el dinero y desde la cual, podemos realizar las mismas

[12] Corrientes de pensamiento del que emanan las criptomonedas https://www.genbeta.com/a-fondo/que-son-los-cypherpunks-y-por-que-son-tan-importanes-en-la-lucha-por-la-privacidad

[13] Wei Dai como precursor: *http://www.weidai.com/bmoney.txt*

acciones que con nuestra cuenta bancaria, desde cualquier parte del mundo, a través de un dispositivo electrónico.

A diferencia de lo que sucede en la actualidad, la red base de las criptomonedas, más conocido como Blockchain, es completamente descentralizado ya que no interviene ningún órgano normalizador, evitando de esta forma las barreras y limitaciones (largos procesos administrativos, comisiones, retrasos en las transacciones, seguridad…) propias de un mercado regulado.

El mensaje de Wei Dai en dicha lista de correos, llamó la atención de otro usuario, Satoshi Nakamoto, quien más tarde, en noviembre de 2008, anunciaría en el foro de la P2P Foundation el nacimiento del Bitcoin, publicando un documento titulado "Bitcoin: A Peer-to-Peer Electronic Cash System[14]", en donde se establecen las bases del proyecto.

La identidad de Satoshi es un misterio desde entonces.

La propuesta de Wei Dai no despertó en su momento mayor interés, pero más adelante – nadie sabe a ciencia cierta cuánto tiempo después – fue rescatada silenciosamente, desarrollada y perfeccionada por Satoshi Nakamoto, quien decidió incluirla como referencia en su ya célebre *paper ("Bitcoin: A Peer-to-Peer Electronic Cash System")*, publicado en el año 2008.

He aquí un fragmento del texto que inspiró a Satoshi Nakamoto, traducido al español:

> *Me fascina la idea de Tim May de una sociedad completamente voluntaria y protegida por medio de la criptografía. A diferencia del tipo de comunidad tradicionalmente asociado con la palabra "anarquía", en una cripto-anarquía el gobierno no es eliminado, pero es incapaz de imponerse. En este tipo de comunidad, la amenaza de la violencia resulta impotente, dado que no es posible ejercer la violencia sobre miembros de una comunidad que no pueden ser identificados en contra de su voluntad.*
>
> *Hasta ahora no está claro, ni siquiera en teoría, cómo podría funcionar semejante comunidad. Una comunidad se define por el nivel de cooperación entre sus miembros, y para que esa cooperación sea eficiente, es necesario contar con un medio de intercambio (dinero) y determinar la manera en que se harán cumplir los contratos. Tradicionalmente, estos servicios han sido proporcionados por los gobiernos (o por instituciones patrocinadas por los gobiernos) a personas físicas o jurídicas definidas por ellos. En este artículo describiré un protocolo en virtud del cual dichos servicios pueden ser suministrados a entidades irrastreables y por entidades irrastreables.*

El reciente éxito de Bitcoin ha llevado a Satoshi Nakamoto [15]a estar dentro de lista Forbes. Dicha lista, reúne a las personas más ricas del planeta, ya que se estima que debe tener alrededor de 980.000 bitcoins en su haber. Pero ¿Qué sabemos realmente de Satoshi Nakamoto? Nakamoto no es una persona conocida, sigue en el anonimato, y de hecho ni siquiera se puede confirmar si es una persona o un grupo de personas, ya que actualmente se considera que el nombre de Satoshi Nakamoto es un seudónimo. Lo único que se sabe

[14] "Bitcoin: A Peer-to-Peer Electronic Cash System": https://bitcoin.org/bitcoin.pdf
[15] Información provista de Satoshi Nakamoto en el Instituto de Estudios Fiscales, http://campus.ief.es/

es que está relacionado con el ámbito universitario, puesto que dónde publicó el documento en el que establecía las normas de la propia moneda y de la cadena de bloques, fue en este ámbito universitario.

CAPITULO IV: CADENA DE BLOQUES O BLOCKCHAIN

4.1. INTRODUCCION A BLOCKCHAIN

La cadena de bloques o Blockchain se considera una tecnología disruptiva con el potencial de cambiar la forma de llevar a cabo las transacciones y el intercambio de bienes tal y como se desarrolla en la actualidad.

Blockchain es una tecnología construida sobre la estructura de internet la cual permite que, transacciones y sistemas de información complejos se ejecuten de manera transparente y segura sobre un modelo de interacción distribuido, que desplaza a numerosos intermediarios asentados y erradica el control de una autoridad central.

La gran diferencia con las monedas fiat o fiduciaria (aquellas emitidas y respaldadas por un banco central) es que es una moneda digital, no existe un equivalente físico de la moneda Bitcoin y la otra gran peculiaridad es el sistema que la soporta, la cadena de bloques (Blockchain). Se trata entonces de un sistema descentralizado, es una tecnología basada en las redes P2P[16], lo que quiere decir que su funcionamiento no depende de ningún servidor central, sino que son los propios usuarios (nodos) de la red, los que hacen funcionar el sistema con aplicaciones instaladas en sus ordenadores personales. Estos ordenadores que forman parten de la red, llamados nodos, se encargan de verificar todos los procesos relacionados con la moneda, lo que tiene grandes beneficios en cuanto a seguridad.

Blockchain[17], es fundamentalmente la base de datos en donde se anotan todas las transacciones que realizan los usuarios, formada por una sucesión de bloques. Cada uno de estos bloques está compuesto de transacciones, de manera que el saldo de cualquier cuenta (monedero) se calcula de manera sencilla a partir de la sucesión de bloques que conforman la cadena. Es decir, la cadena está formada por bloques, los bloques están formados por transacciones, el saldo de una cuenta se obtiene de manera sencilla a raíz de la sucesión de las operaciones contenidas en los bloques.

Por lo tanto, tiene vital importancia que se respete el orden de los bloques en el tiempo (veremos cómo se protege esta sucesión de los bloques en el apartado del hash).

La forma más sencilla de entender la Blockchain es como un gran libro contable.

Una de las principales características de la cadena de bloques o Blockchain, es que está diseñada para evitar su modificación una vez que un dato ha sido publicado. Para ello, se usa un sellado de tiempo confiable y se enlaza a un bloque anterior, de esta manera una

[16] Redes P2P: https://tecnologia-facil.com/que-es/que-es-p2p/
[17] Blockain aspectos técnicos: curso de criptomonedas http://campus.ief.es/

vez que un bloque se valida y pasa a formar parte de la cadena de bloques, cualquier cambio que se pretendiera hacer en cualquier bloque de la cadena crearía una irregularidad en la cadena. Por esta razón, es especialmente adecuada para almacenar datos de forma creciente, ordenados en el tiempo y sin posibilidad de modificación. En el siguiente capítulo explicaremos claramente cómo funciona.

Este gran libro de contabilidad tiene además la peculiaridad de que se encuentra repartido entre una gran cantidad de personas, utilizando las redes P2P para distribuir este gran libro de cuentas. De manera que, cada uno de estos nodos pueden verificar cada transacción que se une al mismo libro, comprobando que ésta sea correcta y consistente con los datos que se tienen de la misma.

Antes de seguir, no imaginemos a una persona comprobando cada transacción, sino que, al formar parte de la red, estás trabajando para ella.

Cuando se produce una transacción, lo que sucede es que esta transacción pasa a formar parte de un concepto que se denomina bloque, este bloque tiene actualmente alrededor de un mega de información y dentro de él se encuentran unas 2000-2500 transacciones como máximo, todas estas transacciones son verificadas previamente por los nodos antes de entrar a un bloque, o como popularmente se les llama, mineros.

En resumen, la red bitcoin es a la vez, un banco (de bitcoins), un banco central (que emite bitcoins) y un procesador de pagos totalmente automatizado y que funciona 24 horas al día, 7 días a la semana.

Los cuatro principios básicos que sigue la moneda y la cadena de bloques son los siguientes:

- La criptografía asimétrica: básica para poder firmar las transacciones y poder corroborar quien ha realizado la transacción. Es el método criptográfico que usa un par de claves para el envío de mensajes.
- Redes P2P: básicas para poder distribuir el libro de cuentas de manera que todos los nodos tengan la posibilidad de verificar las transacciones.
- Mecanismos de consenso: Es necesario que estos nodos que forman la red Bitcoin, tengan unos mecanismos para poder verificar que las transacciones están bien realizadas.
- Funciones Hash: un concepto matemático que veremos más adelante que nos permite resumir cualquier tipo de entrada, ya sea un texto, un archivo… en una cadena alfanumérica de longitud fija.

4.1.1 ASPECTOS DESTACADOS DE LA BLOCKCHAIN:

1. Almacenamiento de datos: se logra mediante la replicación de la información de la cadena de bloques en cada uno de los nodos que operan en la red.
2. Transmisión de datos: se logra mediante redes de pares (red P2P).
3. Confirmación de datos: se logra mediante un proceso de consenso entre los nodos participantes. El tipo de algoritmo más utilizado es el de prueba de trabajo (PoW) en el que hay un proceso abierto competitivo y transparente de validación de las nuevas entradas llamada minería que veremos más a delante en el apartado 4.3.

4.1.2 CLASIFICACION DE BLOCKCHAIN:

Según el acceso a los datos[18]:

1. Cadena de bloques pública: es aquella en la que no hay restricciones ni para leer los datos de la cadena de bloques (los cuales pueden haber sido cifrados) ni para enviar transacciones para que sean incluidas en la cadena de bloques. En ellas es fácil entrar y salir, son transparentes, están construidas con precaución para la operación en un entorno no confidencial. Son ideales para uso en aplicaciones totalmente descentralizadas como por ejemplo para Internet.

2. Cadena de bloques privada: es aquella en la que tanto los accesos a los datos de la cadena de bloque como el envío de transacciones para ser incluidas, están limitadas a una lista predefinida de entidades.

[18] Clasificación según el acceso a los datos:
https://es.bitcoinwiki.org/wiki/Clasificaci%C3%B3n_de_blockchains

Según los permisos[19]:

1. Cadena de bloques con permisos: son aquellas en las que la tarea de procesar transacciones es llevada a cabo por una lista de participantes conocidos. Por ello generalmente no necesitan tokens nativos. Es típico que usen como protocolo de consenso prueba de participación (PoS) en lugar de pruebas de trabajo (PoW).

2. Cadena de bloques sin permisos: son aquellas en las que no existen restricciones a la hora de procesar transacciones y crear bloques. Este tipo de cadena de bloques necesitan tokens nativos para proveer incentivos a los usuarios y que éstos mantengan en sistema. Ejemplos de tókens nativos son los nuevos bitcoins que se obtienen al construir un bloque y las comisiones de las transacciones. La cantidad recompensada por crear nuevos bloques es una buena medida de la seguridad de una cadena de bloques sin permisos.

4.1.3 APLICACIONES DE BLOCKCHAIN

1. Contratos Inteligentes: Digitalización y ejecución automática de contratos.
2. Industria Financiera: Monedas digitales, operaciones financieras, ventas en línea, etc.
3. Contenido Digital: Propiedad intelectual
4. Internet de las cosas: transacciones entre dispositivos electrónicos y actualización del software
5. Servicios Médicos: Descentralización y administración de los registros médicos
6. Bienes Raíces: Reducción en la posibilidad de fraude, rastrear operaciones, transparencia, etc.

Para ver el funcionamiento de una cadena de bloques vamos a examinar el ejemplo más reconocido que es el de Satoshi Nakamoto, es decir, el del funcionamiento del bitcoin. En este caso el contenido de los bloques serán transacciones.

[19]Clasificación según los permisos: https://www.miethereum.com/blockchain/#toc15

CAPITULO V: RED BITCOIN

5.1. GENERACION DE BITCOINS

Para empezar a entrar más detalle sobre la red bitcoin, comenzaremos con cómo se genera la moneda.

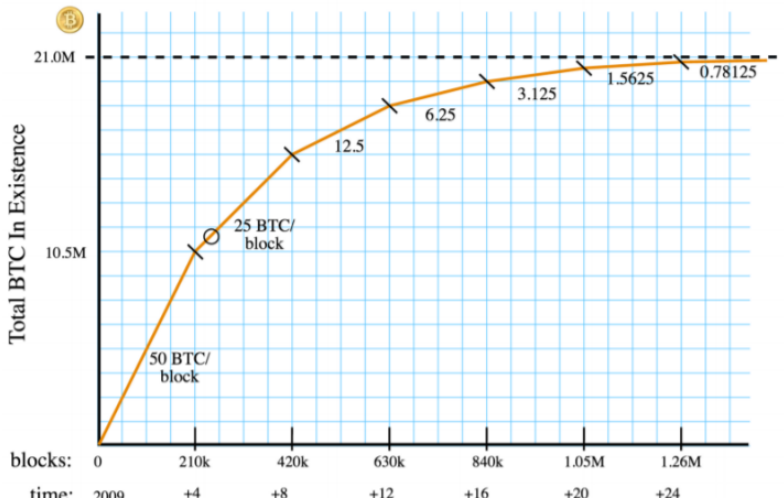
Del mismo modo que un banco central emite su moneda, la red bitcoin emite su moneda a través de un procedimiento conocido como minar, en donde el minero que resuelve el bloque es recompensado con una cantidad de Bitcoins de nueva emisión. Se denomina "minería de Bitcoins[20]" al proceso de generación de bloques, los cuales son incorporados en la cadena de bloques y de esta manera se procesan y verifican las transacciones.

Aproximadamente cada 10 minutos se genera un bloque y cada generación de bloque lleva consigo una recompensa de bitcoins para el nodo (minero) que haya resuelto dicho bloque. Resolver un bloque para que pase a formar parte de la cadena de bloques es el resultado de encontrar el hash de dicho bloque, que veremos en el apartado 4.3.

La recompensa atribuida a la resolución de un bloque varia con el tiempo, como sabemos, una de las grandes peculiaridades de Bitcoin es que la emisión de los mismos está limitada a 20.999.999 BTC, la fecha en la que se calcula alcanzar el total de Bitcoins a emitir es en torno al año 2040, por lo que llegará un momento en el que la emisión finalice. La red Bitcoin lleva recompensando el minado con Bitcoins desde su creación en 2009, dicha recompensa empezó siendo de 50 BTC por bloque minado y esta recompensa se divide a la mitad cada 4 años (en un proceso llamado halving) como vemos en el siguiente gráfico.

Actualmente, la recompensa que recibe un minero al minar un bloque es de 12,5 BTC.

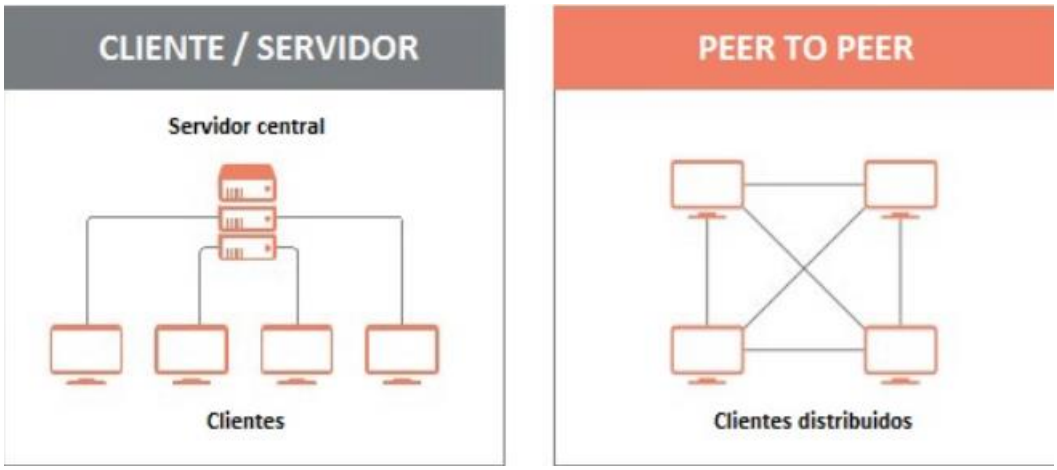
[20] Minería de Bitcoin aspectos técnicos: curso de criptomonedas http://campus.ief.es/



En materia de generación de bitcoins, es importante entender que, la solución de los bloques o el tiempo que tarda en minarse un bloque no está fijado en 10 minutos de manera programada, sino que, el hash, es decir, el problema a resolver en cada minado se configura con una dificultad, haciendo que su resolución le sea al total de la red (los nodos que operan) de 10 minutos. Para ello, cada dos semanas se revisa la dificultad o grados de dificultad del hash, midiendo el número de bloques que se han resuelto contra los que deberían haberse resuelto, veremos esto más en profundidad en el capítulo de hash y minería.

5.2. RED P2P

En informática existen las llamadas redes P2P [21](peer to peer) o redes entre pares. Estas redes están formadas por un conjunto de ordenadores conectados entre sí, llamados "nodos" en los que se permite el intercambio directo de información, sin necesidad de que esa información pase por un servidor central.



Fuente: https://www.miethereum.com/blockchain/#toc4

[21] Descripción red P2P: https://www.miethereum.com/blockchain/#toc4

La primera aplicación con uso de red P2P, que se tiene como referencia, fue Napster en 1999[22]. Desde entonces la tecnología P2P no ha parado de crecer y actualmente es una de las formas más populares y eficientes de transmitir todo tipo de material entre usuarios de internet.

Las redes P2P se describen entonces como una red de computadoras que funciona sin necesidad de contar con servidores fijos, lo que le otorga una flexibilidad que de otro modo sería imposible de lograr. Los nodos que trabajan en la red son los propios clientes, es decir, funcionan tanto como de clientes, como de servidores, soportando la red.

La principal ventaja de las redes P2P es que son mejores en cuanto la eficiencia en el uso del ancho de banda entre los usuarios para el intercambio de archivos, lo que se traduce en una mejor velocidad de transferencias.

Esta mejora de la eficiencia de la red P2P respecto a una red centralizada se origina en la configuración misma de la red, ya que en definitiva el número de servidores que pueden llegar a operar es mucho mayor.

Las redes P2P son útiles para todo lo relacionado con compartir información entre usuarios y es muy utilizada en la actualidad. También muchas empresas hacen uso de esta tecnología peer to peer para proveer de servicios a sus clientes. Un caso típico de ello es Skype y su exitoso servicio de telefonía VoIP. También otras compañías que usan las redes P2P para montar sus servicios son Netflix, con su streaming de películas a la carta, Spotify y muchos más.

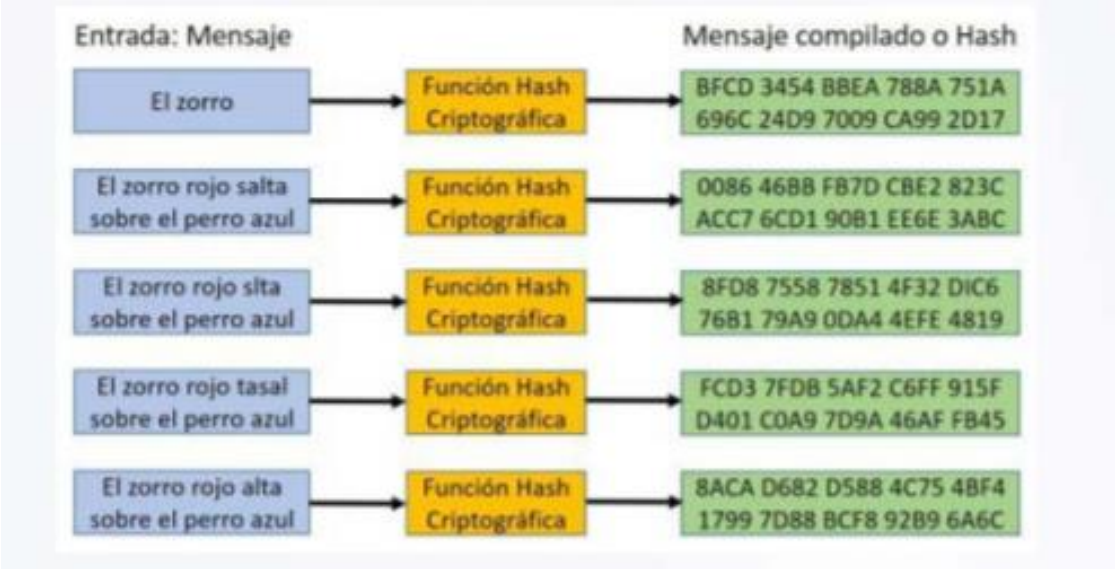
5.3. FUNCIONES HASH Y MINERIA

Es importante abordar de manera conjunta estos dos puntos, ya que la minería consiste en la búsqueda o cálculo del hash de cada uno de los bloques.

El hash es una operación criptográfica, la cual nos permite resumir cualquier tipo de entrada, ya sea un texto, un archivo… en una cadena alfanumérica de longitud fija.

Como vemos en el siguiente ejemplo, no importa el tamaño de la entrada, la función hash nos dará una cadena de la misma longitud sea cual sea el tamaño de la entrada.

[22] Primera red P2P y ventajas: https://tecnologia-facil.com/que-es/que-es-p2p/

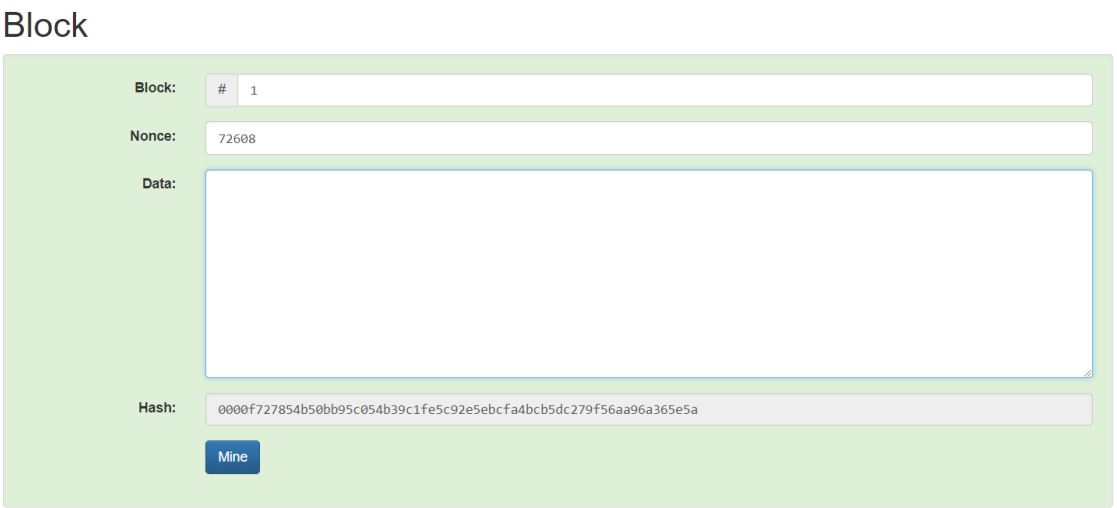


Fuente: *http://campus.ief.es/*

En la red Bitcoin la entrada a resumir por la función Hash[23] es el conjunto del bloque. Cada bloque se compone de 5 grandes áreas: altura o número de bloque, el Hash del bloque anterior de la cadena, un numero aleatorio o nonce, las transacciones del propio bloque y el hash del propio bloque.

Continuaremos apoyándonos en un ejemplo desarrollado por un profesor[24] universitario en la página web https://anders.com/blockchain/block.html

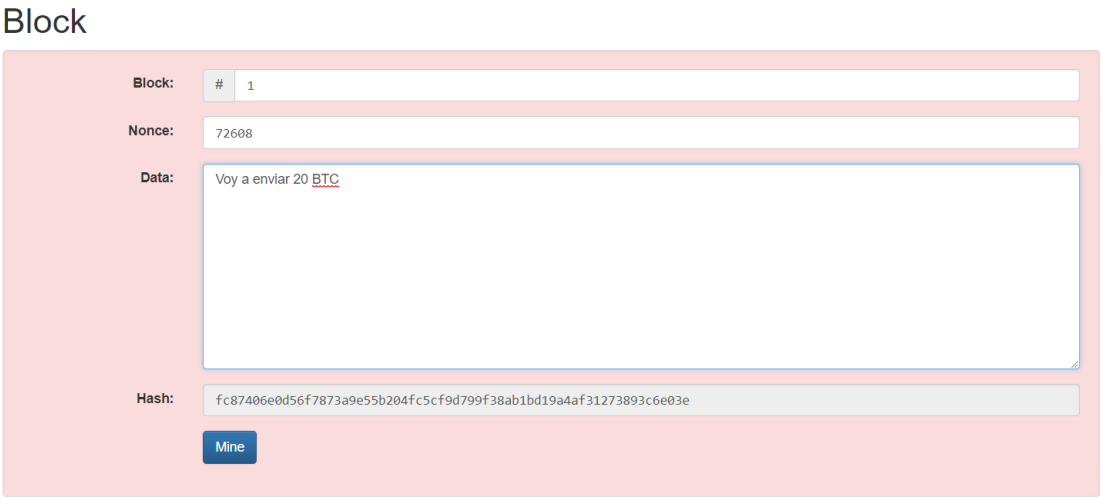
En primer lugar, tenemos lo que sería un bloque sencillo sin estar dentro de la cadena, pues éste tiene todas las áreas previamente mencionadas salvo el hash del bloque anterior, ya que como digo, no está enlazado dentro de una cadena.



Fuente: *https://anders.com/blockchain/block.html*

[23] Hash aspectos técnicos: curso de criptomonedas http://campus.ief.es/
[24] Ejemplo práctico cadena de bloques: https://anders.com/blockchain/block.html

Como podemos ver, tenemos el número de bloque, el número aleatorio o nonce, un área de datos (data), y el hash resultante del contenido del bloque. Al añadir un texto en el área de datos, veremos cómo nuestro hash cambia radicalmente, ya que al cambiar un solo Bit de datos el hash resultante es muy distinto.



Fuente: *https://anders.com/blockchain/block.html*

Como vemos al añadir el texto ``Voy a enviar 20 BTC´´ el hash cambia.

Ahora bien, la función hash y la cadena de bloques es algo muy común en cualquiera de las diversas criptomonedas que existen, pero una de las peculiaridades de cada una de ellas, es la dificultad que se añade al hash. Pero ¿Cuál es esta dificultad?; Como hemos visto anteriormente, la red Bitcoin está configurada con la intención de que se genere un bloque cada 10 minutos, y es precisamente la dificultad del hash, la que hará que se generen en este intervalo de tiempo, dificultando al total de mineros de la red su obtención. Esta dificultad no es más que, para hacer que el hash de un bloque sea válido, éste debe comenzar con una cantidad fija de ceros. Es decir, un hash de dificultad 7, irá precedido de siete ceros, uno de dificultad 12, de doce ceros, etc.

Ej: 0000000000000016b155434b26c45406284d447d8b51b52142c61aa559242b87

Se trataría de un hash de dificultad 14.

Como hemos visto, un bloque se compone de varias áreas, pero ante la resolución de un hash con una dificultad determinada, la labor de un minero consiste en probar de manera aleatoria distintos números en el área de numero aleatorio o nonce. Es decir, si el hash de un bloque es el ``resumen´´ del propio bloque y 3 de las 4 áreas que componen éste, son fijas (altura del bloque, las transacciones que lo componen y el hash del bloque anterior), el minero debe probar uno a uno números aleatorios (nonce) hasta que la función hash comience con el numero estipulado de ceros.

En la imagen anterior vemos que ese bloque no sería válido, ahora lo minaremos obteniendo un hash que en nuestro ejemplo será de dificultad 4:

Fuente: https://anders.com/blockchain/block.html

Como vemos tras minar el bloque, nuestro nonce ha cambiado para que nuestro hash comience por 4 ceros. Como digo, la resolución del hash es como tener una ecuación con tres factores fijos, una incógnita, y un resultado que ``conocemos´´. Pero la peculiaridad de esta ecuación es que no tiene solución mediante fórmulas, únicamente se puede resolver probando números uno a uno hasta que el resultado del hash comience por el numero estipulado de ceros.

Podríamos resumir el proceso de la minería como una gran carrera entre todos los mineros que componen la red, siendo el minero vencedor aquel que obtenga en primer lugar el numero o nonce con el que se obtiene un hash con la dificultad acordada.

Cabe señalar que la dificultad del hash puede ser revisada en un periodo de cada 2016 bloques minados, de manera que se estudia el poder computacional de la red entre todos los nodos que la conforman en ese momento, para así fijar una dificultad del hash que siga haciendo que la generación de un bloque sea de 10 minutos aproximadamente. Se puede añadir o disminuir complejidad, pero hasta la fecha, en la mayoría de los cambios lo que se ha hecho es aumentar complejidad, haciendo que cada vez sea necesario un equipo más potente para poder minar con alguna opción éxito.

Un minero no es más que una persona con un equipo capaz de sostener el software determinado para operar en la red Bitcoin.

El proceso de minado ha sido algo muy rentable, por lo que hay numerosas empresas que se han formado con el objetivo de obtener la recompensa de Bitcoins al minar bloques. Resolver los problemas matemáticos que se plantean requiere entonces cada vez más poder de procesamiento: mientras que en los comienzos de la red hasta 2011 aproximadamente, con un PC era suficiente para minar, ahora se requiere un hardware especializado que consume mucha energía para superar la llamada Prueba de Trabajo (PoW) donde se realizan miles de millones de cálculos por segundo para intentar encontrar la respuesta que creará el nuevo bloque. Y así es como nacen, se distribuyen y se mantienen los bitcoins.

Fuente: http://campus.ief.es/FALTemarioNav.aspx?IDItem=58137&modo=1

Por último, como hemos señalado en el apartado de generación de la moneda, el proceso de minar lleva consigo una recompensa. Esta recompensa se divide cada 4 años y llegara un momento en que finalice la emisión de Bitcoins, por lo que dejaría de ser algo rentable, para ello existe también un sistema de comisiones al minero, ideado por el creador de Bitcoin, Satoshi Nakomoto. Cada transacción lleva consigo asociada una comisión (actualmente puede llevarla o no), esta comisión da preferencia a la transacción para entrar antes en el próximo bloque a generar y será este sistema de comisiones, la que, tras el fin de emisión de Bitcoins permita que la red siga funcionando, ya que el total de nodos en la red es de vital importancia para asegurar su invulnerabilidad al fraude. Se estima que estas comisiones actualmente son de 1 BTC por bloque (es decir, la suma de todas las comisiones de todas las transacciones de un bloque).

La cualidad principal que aporta el hash a la cadena de bloques es que la hace inmutable, es decir, como hemos visto, una vez que se crea un nuevo bloque, se obtiene el hash de dicho bloque. Este hash pasa a ser un componente del próximo bloque, del que se obtendrá un nuevo hash, el resultado de esta configuración, en la que cada hash forma parte del siguiente bloque, es que si alguien intentara manipular la información de una transacción o cualquier tipo de información contenida en el bloque variaría su hash radicalmente, y al ser este un componente del bloque siguiente, veríamos como la cadena deja de ser válida. Es imposible alterar la información de un bloque que forma parte de la cadena.

5.4. MONEDEROS Y CRIPTOGRAFIA

Para poder adentrarnos en la red bitcoin, en primer lugar, necesitaremos lo que se denomina un monedero. En Bitcoin, el monedero[25] es una aplicación la cual puede ser instalada en nuestro ordenador o smartphone y además proporciona un par de llaves, una clave o llave pública y una clave o llave privada, este es el primer paso para poder operar en la red. Estas llaves son formuladas a partir de un proceso criptográfico asimétrico, pero empecemos desde más atrás; un proceso criptográfico más sencillo es el simétrico, que es aquel mediante el cual, yo consigo encriptar o desencriptar un mensaje mediante una única clave, un ejemplo muy popular y fácil de comprender es el ``cifrado cesar[26]´´ que consiste en reemplazar cada letra del texto original por una letra que se encuentre ``n´´ veces más adelante en el alfabeto.

Fuente: https://www.youtube.com/watch?v=3qk1fy6rOJM

En este ejemplo querríamos cifrar la frase ``Hola mundo´´ con un n=3 obteniendo como resultado el texto que aparece en la imagen, con este tipo de criptografía únicamente necesitaríamos conocer una única llave, lo cual no lo hace extremadamente seguro. La llave debería estar muy bien respaldada tanto por el emisor, como el receptor, ya que cualquier persona que se topara con esa llave o clave podría desencriptar el mensaje. Pero pasemos ahora al método criptográfico asimétrico[27], en este método se generan dos pares de llaves o claves, una pública, que se puede entregar a cualquier persona y otra privada, que se debe guardar de modo que nadie tenga acceso a ella. Ambas pertenecen a la misma persona, y la clave publica está ligada matemáticamente a la clave privada, una genera a la otra.

El modelo criptográfico con dos pares de llaves funciona de manera que, los mensajes se encriptan con la clave pública del receptor del mensaje, que debe ser conocida por el emisor, es como una dirección pero que a la vez se usa para encriptar el mensaje. Pero para desencriptarlo, solo podrá, el que tenga acceso a la clave privada vinculada a esa clave pública o dirección, con la que previamente se encriptó el mensaje. Veremos un ejemplo sencillo de una transacción en el apartado siguiente.

[25] Monedero aspectos técnicos: http://campus.ief.es/FALTemarioNav.aspx?IDItem=58138&modo=1

[26] Ejemplo cifrado cesar criptografía simétrica: https://www.youtube.com/watch?v=3qk1fy6rOJM

[27] Criptografía asimétrica: https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

Con esto se soluciona el problema de la criptografía simétrica en donde el problema principal surge de tras encriptar el mensaje, como hacer llegar la clave para desencriptarlo.

Además, los métodos criptográficos garantizan que ese par de claves sólo se puede generar una vez, de modo que se puede asumir que es imposible que dos personas hayan obtenido casualmente el mismo par claves. Se pueden poseer tantos monederos como se quieran y de manera gratuita.

Para introducir este modelo en el sistema bancario tradicional, éste funciona de manera que la llave pública hace las veces de nuestra dirección bancaria y nuestra clave privada se asemeja a nuestro PIN, por lo que, para darse una transacción entre dos usuarios, el usuario emisor ha de conocer la clave pública del usuario receptor para que así pueda darse la transacción, en resumen:

La dirección pública: es aquella con la que el usuario se identifica de cara al mundo. Cualquiera que sepa la dirección pública podrá enviar bitcoins a esa persona en cualquier momento.

La clave privada: es aquella que permite autentificar, acceder a los fondos que tenga en esa dirección o realizar envíos a un usuario. Por este motivo es muy importante que nunca se divulgue la clave privada pues daría a cualquiera que la supiera acceso a los fondos. La mayoría de las aplicaciones Bitcoin se aseguran de mantener la clave privada protegida bajo contraseña (cifrada).

Fuente: http://campus.ief.es/FALTemarioNav.aspx?IDItem=58138&modo=1

Es importante entender que los bitcoins que se atribuyan a un monedero no serán un archivo guardado en su ordenador o smartphone, no se encuentran dentro de la aplicación, sino que se trata de un valor que la cuenta puede tener. De la misma manera, la cuenta del banco no representa dinero que está literalmente ahí, sino que es un valor que el banco le

da a la cuenta. Los bitcoins se encuentran alojados en la cadena de bloques, que está en internet y distribuida entre miles de nodos y todos ellos tienen una copia de todo el libro de cuentas que es donde se encuentra el valor actual de mi dirección pública. Cabe señalar que lo único imprescindible para operar en la red bitcoin es conocer nuestra clave privada, cuya complejidad, como vemos en la imagen anterior, la hace muy difícil, por no decir imposible de recordar. El poseedor de la clave privada de la misma manera que el PIN, da acceso al uso de ese monedero.

Por tanto, la salvaguarda de la clave privada es uno de los conceptos más importantes de la red bitcoin.

La clave de la seguridad de bitcoin reside en la clave privada, si alguien consigue entrar en un ordenador y robar la clave, podrá vaciar ese monedero. Para evitar este riesgo, la aplicación permite cifrar el monedero con una clave de acceso, lo que hace imposible su robo, pero por defecto no se hace porque no existe opción de recuperación de contraseña, esto es, si se olvida la clave se pierde el acceso al monedero.

Existen otro tipo de monederos, que se encuentran alojados en casas de cambio, monederos online que nos permiten acceder a los mismos remotamente, y se encargan de alojar las claves privadas. Esto fue lo que realizo en primera instancia MT Gox y por tanto la clave privada no reside en un dispositivo del usuario, sino se encuentra en los servidores de esta pasarela de pago, lo cual hace que, en conceptos de seguridad, el usuario sufra una pérdida de la misma.

Veremos cómo funciona el par de llaves en una transacción de Bitcoin en el siguiente apartado.

5.5. TRANSACCIONES

Como ya sabemos, en cada bloque se pueden alojar más de 2000 transacciones[28], generalmente entre 2000 y 2500, el bloque con mayor número de transacciones fue de unas 2700 transacciones. En cada una de las transacciones que componen un bloque, podremos encontrar: una dirección pública por parte del emisor, una cantidad de Bitcoins que se transfieren de una cuenta a otra, otra dirección publica por parte del receptor de la transferencia y una firma digital de la transacción por parte de la clave privada de la dirección pública del emisor.

Para entender cómo funciona realmente una transacción de Bitcoins lo facilitaremos mediante una analogía, ya que es algo más complejo que simplemente enviar una transacción.

En este ejemplo nuestra clave privada sería una llave física y nuestra clave o dirección pública un candado, con la peculiaridad de que solo tenemos una llave (clave privada) e infinitos candados (clave o dirección pública), y que cada uno de nuestros candados (clave o dirección publica) pueden ser abiertos mediante nuestra única llave (clave privada).

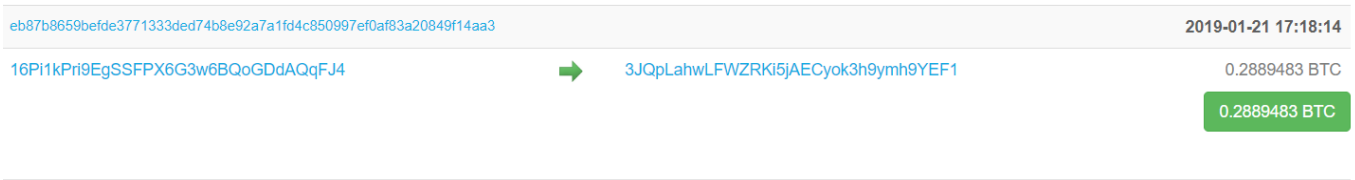
[28] Transacciones de Bitcoin aspectos técnicos: http://campus.ief.es/

Ahora supongamos una transacción entre un usuario A y un usuario B. El usuario A quiere transferir al usuario B una cantidad determinada de Bitcoins.

Como hemos mencionado anteriormente los Bitcoins se encuentran alojados en la red Bitcoin o Blockchain y nuestra cuenta, que está alojada en la red, tiene un valor determinado. Para realizar una transferencia, la criptografía asimétrica dota a los usuarios del sistema de seguridad y anonimato, mediante los dos pares de llaves. Usando esta analogía en la que nuestra llave o clave pública funciona como un candado y la llave o clave privada, hace las veces de llave de dichos candados, con la peculiaridad mencionada previamente, intentaré explicar cómo se desarrolla una transacción:

Si quisiéramos enviar algo a otra persona, pero no confiamos por dónde va a viajar nuestro envío (internet), la criptografía utiliza un sistema muy eficiente. Imaginemos nuestra cuenta de Bitcoin custodiada por uno de nuestros candados, ahora queremos enviar cierta cantidad de Bitcoins a un usuario B. Para realizar la transacción en la red Bitcoin, pediríamos al usuario B su clave publica, es decir, funciona como una dirección bancaria. En nuestro ejemplo, le pediríamos a B que nos enviara uno de sus candados. Acto siguiente, abriríamos nuestra caja con nuestra llave (clave privada), en donde residen nuestros Bitcoins custodiados con uno de nuestros candados, para posteriormente realizar el envío a B, pero protegido por el candado que nos envió B y del que únicamente B podrá abrir con su llave privada.

De este modo, los Bitcoins que queremos enviar a B recorrerán la red, pero protegidos con un candado que sólo B puede abrir mediante su llave o clave privada. Con este ejemplo quiero intentar explicar que una transacción en la red Bitcoin tiene mucho más detrás, ya que mediante este sistema, dota de la capacidad a emisor y receptor de encriptar y desencriptar las transacciones, ambos se aseguran anonimato y seguridad en la transacción frente a terceros, ya que como he mencionado anteriormente si entráramos en la red Blockchain.com en donde podemos ver las transacciones que se añaden a cada bloque, veremos la dirección publica de emisor y receptor, la cantidad de Bitcoins que se emiten y una firma digital vinculada a la clave privada del emisor, es decir, cualquier persona, ya sea que trabaje como minero, o que simplemente quiera hacer una consulta, no podrá ver nombres, ni ninguna información que facilite (al menos de manera sencilla) la identificación de las personas físicas vinculadas en una transferencia determinada. Además, como sabemos, la red Bitcoin está al margen de cualquier institución reguladora por lo que no rinde cuentas a ningún país o gobierno, lo que como intento explicar, hace muy complicado identificar a las personas que hay detrás de una transacción de Bitcoin.



En la imagen anterior, vemos una trasferencia a fecha 21 de enero de 2019 alojada en el bloque número 559496 de la cadena[29], en donde como vemos, aparecen la dirección publica de emisor y receptor, la cantidad de Bitcoin que se emiten y en la esquina superior izquierda la firma digital vinculada a la clave privada del emisor de la transacción.

De esta manera quiero explicar que un Bitcoin no es un archivo que posees en tu ordenador o smartphone, como un archivo de música o imagen que puedas duplicar. El bitcoin siempre estará en la red, simplemente, el que lo posea tiene acceso a la entrada de esa parte de la red y una vez que se transfiere, lo que realmente se transfiere es esa llave criptográfica que nos da legitimidad a transferirlo, en ningún caso saldrá de la red por eso es una referencia en cuanto a transparencia y anticorrupción.

CAPITULO VI: CONCLUSIÓN

Mis conclusiones difieren en gran medida dependiendo si hablamos de Bitcoin o bien de Blockchain. Bitcoin para la Blockchain o cadena de bloques, no es más que el contenido del bloque, en este caso se compone de transacciones, por lo que el éxito de Blockchain es independiente a Bitcoin u otra criptomoneda. Después de realizar este estudio, no tengo ninguna duda de las grandes aplicaciones de esta herramienta al mundo.

Llama especialmente la atención su uso en los Smart contracts o contratos inteligentes, puesto que ofrece una salvaguarda total de la propiedad privada. Creo que no es difícil imaginar a corto plazo que los contratos referidos a transmisión de bienes se realicen mediante un soporte o plataforma similar, ya que una de las grandes cualidades de la cadena de bloques o Blockchain es que es inmutable una vez que un dato es registrado y almacenado. Esta tecnología logra entonces que cada propiedad esté registrada a un titular, y dicho registro podría ser almacenado en la Blockchain. Esto sin duda reduciría el riesgo de fraudes, por la facilidad de consulta y la seguridad de la que se provee al sistema, además de reducir comisiones de mediación y disminuir la necesidad de intermediarios.

Por contra, si hablamos de Bitcoin, actualmente dista mucho de poder ser considerada como una moneda fiable, ya que pese a las grandes ventajas que ésta tiene en términos de intercambio de valor, la gran volatilidad que sufre la misma le condiciona directamente para poder ser considerada como tal, únicamente puede ser considerada como elemento de especulación. Bitcoin es sin duda un gran proyecto, posee características positivas e interesantes que la hacen más eficiente si evaluamos el dinero como método de

[29] Bloque número 559496 de la Blockchain de Bitcoin: https://www.blockchain.com/es/btc/block/000000000000000000006f88315d32002d917fe34239c77c342a631a811353464

intercambio de valor y su necesidad de almacenarlo. El paradigma actual requiere de intermediarios financieros que realicen el servicio de custodiar nuestro patrimonio, es decir, el dinero es una cosa y almacenarlo otra distinta, las criptomonedas podrían hacer un mejor papel y abaratando de manera total los costes. Sencillamente, las criptomonedas en sí mismas, poseen la capacidad de ser custodiadas virtualmente en la cadena de bloques sin que tenga un coste añadido. Pero pese a la mejora de eficiencia de una criptomoneda frente a las monedas actuales, el hecho de que no esté respaldada por ningún país o gobierno hace que sea muy complicado que pueda integrarse por sí misma al panorama económico, además, el hecho de que surjan diversas de las mismas, dificulta aún más el proceso, pues provoca incertidumbre. Bitcoin u otra criptomoneda solo podrá introducirse con peso en un país o región si la comunidad deposita su confianza como método de intercambio, pero es mucho más probable que si finalmente se adopta el uso de las criptomonedas, éstas tengan algún tipo de regulación o bien haya grandes empresas que apoyen una moneda determinada.

Es indudable que Blockchain es útil, y el que se integre a procesos más sencillos demostrando su eficiencia es una gran pasarela para que la sociedad lo vaya conociendo y quizás en el futuro, finalmente, se aborde el tema de si el sistema económico deba ser reformulado

BIBLIOGRAFÍA

- Oliver Blanchard, Macroeconomía (2017), 7ªedición, Pearson.
- Banco Central, definición propuesta por https://www.eleconomista.es/diccionario-de-economia/banco-central
- Objetivo Banco Central: https://economipedia.com/definiciones/funciones-y-objetivos-bancos-centrales.html
- Objetivo Banco central: https://economipedia.com/definiciones/funciones-y-objetivos-bancos-centrales.html
- Dinero legal: https://www.vivus.es/blog/prestamopedia/tipos-dinero/
- Dinero bancario: https://sites.google.com/site/economia20parabachillerato/temario/tema-7-el-mercado-de-dinero/2-el-mercado-monetario
- Corrientes de pensamiento del que emanan las criptomonedas: https://www.genbeta.com/a-fondo/que-son-los-cypherpunks-y-por-que-son-tan-importanes-en-la-lucha-por-la-privacidad
- Wei Dai como precursor: *http://www.weidai.com/bmoney.txt*
- "Bitcoin: A Peer-to-Peer Electronic Cash System": https://bitcoin.org/bitcoin.pdf
- Información provista de Satoshi Nakamoto en el Instituto de Estudios Fiscales en relación a Blockchain y Bitcoin, http://campus.ief.es/
- Redes P2P: https://tecnologia-facil.com/que-es/que-es-p2p/
- Clasificación según el acceso a los datos: https://es.bitcoinwiki.org/wiki/Clasificaci%C3%B3n_de_blockchains
- Clasificación según los permisos: https://www.miethereum.com/blockchain/#toc15
- Descripción red P2P: https://www.miethereum.com/blockchain/#toc4
- Primera red P2P y ventajas: https://tecnologia-facil.com/que-es/que-es-p2p/
- Ejemplo práctico cadena de bloques: https://anders.com/blockchain/block.html
- Ejemplo cifrado cesar criptografía simétrica: https://www.youtube.com/watch?v=3qk1fy6rOJM

- Criptografía asimétrica: https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

- https://www.blockchain.com/es/btc/block/000000000000000000006f88315d32002d917fe34239c77c342a631a811353464

APENDICES

APENDICE 1

HISTORIA DEL DINERO[30]

``El Bitcoin tiene notables diferencias con las monedas fíat o fiduciarias, pero sin duda, una gran cualidad del Bitcoin es que nos hace preguntarnos que es el dinero´´

En este apéndice, mi objetivo es presentar brevemente y justificar el porqué del nacimiento del dinero y de los agentes y factores que rigen nuestra economía. Pues no son leyes físicas que estaban ahí antes que nosotros y con las que hemos tenido que lidiar, son en todo caso, mecanismos que hemos creado.

El primero en presentar, será entonces el propio dinero y su evolución hasta nuestro tiempo.

Pero ¿Qué es el dinero?

El dinero es un lenguaje. Un lenguaje que nos permite expresar valores transaccionales entre la gente, una herramienta que utilizamos para medir de manera cuantitativa una transacción.

Es importante conceptualizar debidamente a raíz de porqué nace el dinero, o de dónde nace el dinero. De la misma manera en que la rueda fue un invento emanado de la necesidad de transportar objetos, el dinero surge con la necesidad de comerciar, es decir surge con la evolución de los mercados.

Inicialmente, para que se diera el intercambio de mercancías entre dos usuarios el método empleado era el trueque. Éste tenía diversas dificultades, la principal era encontrar una contraparte que poseyera el bien que se precisaba y que, a su vez, demandara el producto con el que se contaba. En segundo lugar, había que establecer qué cantidad del bien A y del bien B eran equivalentes, de tal manera que ambas partes quedasen satisfechas con el trato.

Para superar estas dificultades surgió el dinero mercancía. Hubo de diversos tipos, pero todos ellos debían poseer las mismas 5 características: era relativamente escaso, fácilmente reconocible, puede dividirse en piezas más pequeñas, se puede sustituir una pieza por otra de igual valor, y es fácil de transportar, en la antigua roma era la sal.

El dinero mercancía consiste entonces en bienes u objetos que tienen valor por sí mismos, además del valor de cambio al ser utilizado como moneda. Una de sus principales características es que su valor es observado directamente por quienes utilizan dicho dinero. Ejemplo: tener una moneda que contenga oro equivale a poseer físicamente dicha cantidad de oro.

El mensaje subyacente es que el dinero no surge a raíz de los gobiernos, surge por la necesidad de comerciar.

[30] Apoyado en el documental “Bitcoin, la nueva moneda digital”

El problema del dinero mercancía, es que no era muy estable y duradero, se necesitaba un sistema más estable. Hace más de 2500 años se acuñaron las primeras monedas en lo que es ahora Turquía y China. Estas compartían las mismas 5 cualidades del dinero mercancía y además eran muy duraderas, en algunos casos las monedas es lo único que queda de civilizaciones enteras.

Fueron entonces los metales preciosos los que acabaron imponiéndose de manera global como forma de dinero debido a su amplia aceptación.

Las monedas funcionaban, pero sólo si la gente confiaba en el rey o emperador que las ponía en circulación, es decir, sino les engañaba con el contenido de oro o metal que estas poseían.

La utilización de las monedas significaba también que una autorización controlaba el suministro de moneda, el dinero y el poder político estaban inextricablemente unidos, centralizados. Acuñar moneda de forma regular y predecible, favoreció el crecimiento económico y la estabilidad.

Las monedas, se convirtieron entonces en una unidad contable y objetiva que permitía a la gente comprar cosas en territorios muy extensos.

En la historia de la economía, la invención del papel moneda y de los bancos comerciales tal y como los conocemos, surge a raíz de dos figuras de la edad media, orfebres y mercaderes.

Los mercaderes internacionales hicieron una gran revolución con la invención del papel moneda, los billetes que utilizamos hoy. Estos mercaderes reconocieron que la deuda de una persona tiene valor y que puede comerciarse con ella, o transferirse. Cuando estos pagares provenían de fuentes fiables, podían utilizarse como una forma de dinero, papel moneda. Este dinero no estaba basado en mercancías o en metales, sino en la palabra de alguien que prometía pagar lo acordado. Familias importantes de mercaderes del siglo XV actuaban como cámaras de compensación para esos pagares, y era sostenible por la confianza en esa promesa de pago. Funcionaba así; un comerciante A pedía un cargamento por valor de 100 monedas de oro a un comerciante B, su promesa de pagar a este comerciante se escribía en un papel. Por su parte, el comerciante B debía 100 monedas de oro a otro socio comercial C. Las partes no incurrían en los gastos de transportar e intercambiar las monedas de oro, lo que se transfería era el papel. Todos estaban de acuerdo en que ese papel tenía valor, 100 monedas de oro, pero solo porque todos confiaban en la solvencia del comerciante.

A esto, debemos de sumar el nacimiento de los precursores de los banqueros, los orfebres de la edad media.

Los orfebres, se dieron cuenta de que algunas de las monedas que almacenaban para la gente estaban acumulando polvo en sus cámaras, la gente realmente no las necesitaba. Entonces, el orfebre se plantea prestárselas a la comunidad y cobrar un interés por el préstamo, y al prestarlas, se da cuenta que la gente ni siquiera las quiere, solo quieren un papel que diga que las monedas de oro están en el banco, en poder del orfebre. Por lo que el orfebre ya puede hacer prestamos con papel, y así los orfebres, los precursores de los banqueros de hoy, adquirieron el poder de imprimir dinero.

Este papel dinero de mercaderes y bancos circulaba cada vez más y empezó a rivalizar con las monedas acuñadas por la corona, las autoridades estaban perdiendo el poder que les daba controlar o emitir moneda, ya no podían grabar con impuestos esa nueva clase de dinero. Además, su ambición era cada vez más grande, debido a las nuevas oportunidades comerciales y de colonización. Durante siglos los países lucharon por conseguir grandes flotas y declararse las guerras unos a otros. Los impuestos anuales no eran suficientes para respaldar el coste de las guerras, reyes y reinas tienen que pedir dinero prestado a cuenta de futuros impuesto, necesitan una innovación financiera, los bonos de gobierno. Los prestamos los hacen familias ricas de mercaderes y orfebres que se han convertido en poderosos financieros y banqueros, han nacido la deuda soberana y el déficit público.

Llegamos a 1694 con la creación de uno de los primeros bancos centrales del mundo, el banco central de Inglaterra. Ésta era una institución privada con el monopolio de emitir billetes de banco, papel que podía intercambiarse por una cantidad igual de oro de las reservas del gobierno. El banco central no tardo en controlar toda la deuda de la corona.

Cuando estados unidos se independizó de gran Bretaña, el primer artículo de la nueva constitución concedía al congreso el derecho exclusivo a acuñar dinero y el valor de esa moneda estaba ligado al oro de las reservas del gobierno.

En 1913 banqueros y políticos de Estados Unidos decidieron en interés del país que debían crear un banco central permanente, la reserva federal. Entre sus funciones estaba el aumentar o contraer el suministro de una única moneda nacional, el billete de la reserva federal. El dólar estaba ligado al oro, y el control estratégico de la moneda impediría la formación de burbujas financieras susceptibles de estallar, entonces llego 1929. La gran depresión tendría un efecto profundo en la política monetaria, en todo el mundo.

Pronto, la reserva federal, había imprimido casi todo el dinero que podía imprimir legalmente para inyectar vida a la economía y como necesitaba oro para respaldar el dinero de nueva emisión, en 1933 el presidente Roosevelt promulgó una orden ejecutiva que obligaba a todos sus ciudadanos, a vender su oro a la reserva federal a un precio fijado o ir a la cárcel. La reserva federal ofrecía mucho más dinero a los países extranjeros por su oro, muchos aceptaron la oferta, el flujo de oro creció y el dólar se extendió por todo el mundo.

La segunda guerra mundial devastó casi todas las economías del mundo, pero no la de estados unidos. El dólar se había convertido en la divisa más estable y fiable del mundo, otros países vincularon su divisa al dólar que todavía podía cambiarse por oro. De hecho, Estados Unidos poseía más de la mitad de toda la reserva de oro del mundo. En las siguientes décadas más dólares fluyeron a diversos países extranjeros, los gobiernos comenzaron a devaluar sus monedas con metales más baratos y a imprimir más dinero de las reservas de oro que tenían. El vínculo entre los metales preciosos y el papel moneda se estaba resquebrajando.

Como ejemplo podemos nombrar la moneda de 50 centavos de 1966 de circulación regular de Australia. Esta moneda contiene un 80% de plata y en 1966 valía 50 centavos, hoy vale alrededor de 8 dólares solo por su contenido en plata.

En 1966 diversos países exigieron a Estados Unidos oro a cambio de sus dólares de papel, habían acumulado más dólares que Estados Unidos oro en sus reservas. Aquello devino en un debate entre el valor del dólar y de las divisas extranjeras

En 1971 el presidente Nixon zanjo el debate, la divisa de EE. UU. ya no dependía del patrón oro, ya nadie podría exigir legalmente oro a EE. UU. a cambio de sus dólares de papel.

Entonces el dólar pasó sostenerse únicamente en la fe y el crédito del gobierno de EE. UU., el país más rico que había conocido el mundo ligaba su futuro a una sola palabra, confianza.

Hasta aquí hemos nombrado como nacen diversos agentes y términos que rigen nuestro sistema financiero actual. El propósito del primer capítulo será mediante un modelo simplificado entender como interactúan estos agentes en la actualidad y como el banco central intenta lograr sus objetivos, para en los siguientes capítulos centrarnos en la criptomoneda Bitcoin en un contexto técnico de la misma.

APENDICE 2

CRISIS 2007, BITCOIN 2008[31]

Creo oportuno hablar de la crisis financiera de 2007, que evidencio la falta de transparencia del sistema financiero actual, la cual fue sin duda un motor para el éxito acelerado de bitcoin y de otras criptomonedas.

A principios del año 2000 y hasta 2007 las economías mundiales, tanto avanzadas, como menos desarrolladas, experimentaron una expansión sostenida.

La tasa de crecimiento media anual de la producción mundial fue del 4,5%, con las economías avanzadas (el grupo de los aproximadamente 30 países más ricos del mundo) creciendo al 2,7% anual y las restantes economías (los otros 150 países del mundo) creciendo a un ritmo aún más rápido del 6,6% anual.

Sim embargo, en 2007 comenzaron a aparecer indicios de que la expansión podría estar tocando a su fin. Los precios de la vivienda de Estados Unidos, que se habían duplicado desde el año 2000, iniciaron su caída. Los economistas comenzaron a preocuparse. Los optimistas creían que, aunque los menores precios de la vivienda podrían inducir una caída de la construcción residencial y un menor gasto de los consumidores, la Fed podría reducir los tipos de interés para estimular la demanda y una recesión. Los pesimistas creían que el descenso de los tipos de interés podría no ser suficiente para sostener la demanda y que Estados Unidos podría atravesar una breve recesión.

Resulto que los pesimistas no habían sido suficientemente pesimistas.

Conforme continuaban cayendo los precios de la vivienda, quedo claro que los problemas eran más profundos. Muchas de las hipotecas que habían sido concedidas durante la anterior expansión eran de mala calidad. Numerosos prestatarios se habían endeudado en exceso y cada vez tenían menos capacidad para pagar las cuotas mensuales de sus hipotecas. Además, con los precios de la vivienda a la baja, el importe de su deuda hipotecaria a menudo superaba el precio de la vivienda, ofreciéndoles un incentivo para dejar de pagar. Y esto no fue lo peor: los bancos que habían concedido las hipotecas, a menudo las habían empaquetado y agrupado en forma de nuevos títulos y luego habían vendido estos títulos a otros bancos e inversores. A su vez, estos títulos se reempaquetaron a menudo en nuevos títulos y así sucesivamente. El resultado fue que numerosos bancos, en lugar de mantener las propias hipotecas, poseían esos títulos, que eran tan complejos que la tarea de calcular su valor resultaba casi imposible.

Esta complejidad y opacidad transformo una caída de los precios de la vivienda en una gran crisis financiera, una evolución que pocos economistas habían anticipado. Sin conocer la calidad de los activos que otros bancos mantenían en sus balances, los bancos se mostraron reacios a prestarse mutuamente por temor a que el banco al que le prestaba fuera incapaz de devolver el crédito.

Incapaces de tomar prestado, y con activos de valor incierto, muchos bancos se vieron en problemas. El 15 de septiembre de 2008, un importante banco, Lehman Brothers, quebró, con efectos dramáticos. Como los vínculos entre Lehman y otros bancos eran tan opacos, muchos otros bancos corrían aparentemente el riesgo de quebrar también. Durante

[31] Macroeconomía Oliver Blanchard 7ª edición, capítulos 4,5 y 6

algunas semanas, dio la impresión de que el conjunto del sistema financiero podía colapsar.

La crisis financiera se transformó rápidamente en una importante crisis económica. Los precios de las acciones de desplomaron. A finales de 2008, las acciones habían perdido la mitad o más de su valor desde su anterior cuota máxima. Además, pese al hecho de que la crisis se originó en Estados Unidos, las cotizaciones bursátiles en Europa y en los mercados emergentes cayeron tanto como las estadounidenses.

Afectado por la caída de los precios de la vivienda y el desplome de las cotizaciones bursátiles, y preocupado porque esto pudiera ser el inicio de otra Gran Depresión, el público redujo drásticamente su consumo. Preocupadas por las ventas y con incertidumbres sobre el futuro, las empresas recortaron drásticamente sus inversiones. Con los precios de la vivienda a la baja y muchas casas vacías en el mercado, la construcción de nuevas viviendas se redujo considerablemente. Pese a las medidas tomadas por la Fed, que redujo los tipos de interés hasta cero, y por el gobierno estadounidense, que recortó los impuestos y aumentó el gasto, la demanda cayó, al igual que la producción. En el tercer trimestre de 2008, el crecimiento de la producción estadounidense paso a ser negativo, permaneciendo en esta situación durante 2009.

Cabría haber esperado que la crisis se limitara a Estados Unidos, pero como sabemos, no fue así. La crisis estadounidense se transformó rápidamente en una crisis mundial. Otros países se vieron afectados a través de dos canales, siendo el comercio el primero de ellos. Conforme los consumidores y empresas estadounidenses reducían el gasto, parte de ello cayó sobre las importaciones de los bienes extranjeros. Desde la perspectiva de los países que exportaban a Estados Unidos sus exportaciones cayeron, al igual que a su vez, lo hacia la producción. El segundo canal fue financiero. Los bancos estadounidenses, con urgente necesidad de fondos en Estados Unidos, repatriaron fondos desde otros países, ocasionando también problemas a los bancos de esos países. Conforme estos bancos entraban en dificultades, el crédito se paralizó, induciendo caídas del gasto y de la producción. Asimismo, los gobiernos de varios países europeos habían acumulado importantes volúmenes de deuda y ahora estaba incurriendo en fuertes déficits. Los inversores comenzaron a plantearse si la deuda podría ser devuelta y demandaron tipos de interés mucho más altos. Enfrentados a esos elevados tipos de interés, los gobiernos redujeron drásticamente sus déficits, mediante una combinación de menor gasto y mayores impuestos. Esto indujo, a su vez, caídas adicionales de la demanda y la producción. En Europa, el descenso de la producción fue tan grave que este singular acontecimiento recibió su propio nombre, *la crisis del euro.* En resumen, la recesión en Estados Unidos se transformó en una recesión mundial. En 2009, el crecimiento medio en las economías avanzadas fue del -3,4%, con diferencia la menor tasa de crecimiento anual desde la Gran Depresión. El crecimiento se mantuvo positivo en las economías emergentes y en desarrollo, pero siendo 3,5 puntos porcentuales menor a la media del periodo 2000-2007.

APENDICE 3

PANICO BANCARIO Y BANCO CENTRAL COMO PRESTAMISTA DE ULTIMA INSTANCIA[32]

Pensemos en un próspero banco, un banco que tenga una buena cartera de préstamos. Supongamos ahora que comienza a rumorearse que no va bien y que no podría recuperar algunos préstamos. Creyendo que el banco puede quebrar, las personas que tienen depósitos en él querrían cerrar sus cuentas y retirar el dinero en efectivo. Si son bastantes las personas que toman esa decisión, el banco se quedará sin fondos. Dado que los prestamos no pueden recobrarse fácilmente, no podrá satisfacer la demanda de efectivo y tendrá que cerrar.

El temor a que un banco cierre puede hacer que cierre realmente, aunque todos sus préstamos fueran buenos inicialmente. La historia financiera de Estados Unidos está llena de pánicos bancarios hasta la década de 1930

El problema reside entonces en la naturaleza de los activos y pasivos de los bancos. Pues como hemos mencionando en el capítulo de los intermediarios financieros, la mayor parte de los activos de los bancos suelen ser préstamos a personas u empresas, y los pasivos suelen ser depósitos a la vista. En un caso en que gran parte de los depositantes de un banco quisieran retirar sus depósitos a la vista, esto traería serios problemas al banco. Los bancos necesitarían reembolsar ese dinero, normalmente los prestatarios no tienen los fondos disponibles al haberlos utilizado para pagar facturas, comprar un coche, una hipoteca… La venta esos préstamos a otro banco probablemente también sea complicada, ante la dificultad de estimar el valor de los préstamos para este segundo banco al carecer del conocimiento específico de los prestatarios que si tiene el banco original. En general cuanto más difícil sea estimar el valor de los activos del banco, más probable es que el banco simplemente sea incapaz de venderlos o tenga que hacerlo a precios de liquidación forzosa, que son precios muy por debajo del auténtico valor de los préstamos. Sin embargo, esas ventas solo empeoran las cosas para el banco. A medida que cae el valor de los activos el banco podría terminar siendo insolvente y quebrar. A su vez, conforme los inversores se dan cuenta de que esto podría suceder, encuentran más motivos incluso para querer retirar sus fondos, obligando al banco a realizar más ventas forzosas y agudizando el problema. Obsérvese que esto puede ocurrir aun cuando las dudas iniciales de los inversores carecieran de todo fundamento y el banco fuera totalmente solvente. La decisión de los inversores de retirar sus fondos y las ventas forzosas que ello induce podrían convertir a un banco solvente insolvente.

También hay que tener en cuenta, que el problema es más susceptible de finalizar en pánico bancario cuanto más líquidos sean sus pasivos. Esto es evidentemente lo que ocurre con los depósitos a la vista que pueden ser retirados inmediatamente.

El hecho de que la mayoría de los activos del banco sean préstamos, faltos de liquidez, y que sus pasivos sean en su mayor parte, depósitos a la vista que tienen gran liquidez, les hace especialmente vulnerables a los pánicos bancarios. La gente puede retirar rápidamente su dinero, pero los bancos encuentran series dificultades para recuperar

[32] Macroeconomía Oliver Blanchard 7ª edición, capítulos 4,5 y 6

convertir sus activos, como digo, el problema está en la naturaleza de sus activos y pasivos.

¿Qué puede hacerse para evitar estos pánicos bancarios?

Otra posible situación es la denominada banca restrictiva, que obligaría a los bancos a mantener únicamente bonos del Estado líquidos y seguros, como las letras del Tesoro. Serían otros intermediarios financieros diferentes los que concederían los préstamos. Esto probablemente eliminaría los pánicos bancarios. Algunos cambios en la regulación estadounidense han ido esta dirección, limitando algunas operaciones financieras a los bancos que captan depósitos, pero distan mucho de crear una banca restrictiva. Una deficiencia de la banca restrictiva es que, aunque realmente pudiera eliminar los pánicos bancarios, el problema podría desplazarse al sistema bancario en la sombra, generando pánicos en este.

El problema, se ha abordado en la práctica de dos maneras. En primer lugar, intentando limitar la aparición de pánicos bancarios. En segundo lugar, si aun así estos ocurriesen, el banco central inyectaría fondos en los bancos para que no tuvieran que realizar ventas forzosas.

Para limitar los pánicos bancarios, los gobiernos de los países más avanzados han creado un sistema de seguro de depósitos. Estados Unidos, por ejemplo, creó el seguro federal de depósito en 1934. El Gobierno estadounidense ahora asegura cada deposito a la vista hasta un máximo que, desde 2008, asciende a 250.000 dólares para evitar que los depositantes se asusten y acudan a retirar su dinero.

Sin embargo, el seguro de depósitos tiene sus propios problemas. A los depositantes, al no tener que preocuparse por sus depósitos, ya no les preocupan las actividades de los bancos donde los tienen, por lo que estos bancos pueden actuar indebidamente concediendo prestamos que no concederían si no existiera el seguro. Así, podrían asumir demasiados riesgos y demasiado apalancamiento.

Y como desgraciadamente revelo la crisis, el seguro de los depósitos no es suficiente. En primer lugar, los bancos utilizan otras fuentes de fondos distintas de los depósitos, a menudo endeudándose a un día con otras instituciones financieras e inversores. Estos otros fondos no están asegurados y, durante la crisis, muchos bancos se vieron realmente afectados por los pánicos y, esta vez, no de los depositantes tradicionales sino de los proveedores mayoristas de fondos. En segundo lugar, las instituciones financieras distintas de los bancos pueden sufrir el mismo problema, con inversores deseando recuperar rápidamente sus fondos y con activos difíciles de liquidar o vender con rapidez.

Así, en la medida en que los pánicos bancarios no pueden evitarse totalmente, los bancos centrales han creado programas para inyectar fondos en los bancos en caso de pánicos. En tales circunstancias, el banco central aceptara prestar a un banco con el respaldo del valor de sus activos, pudiendo evitar éste las ventas forzosas. Tradicionalmente estas inyecciones se han reservado a los bancos, sin embargo, la reciente crisis nuevamente ha desvelado que otras instituciones financieras pueden sufrir pánicos y necesitar también estas inyecciones.

Exactamente igual que el seguro de depósitos, esa provisión de liquidez (como se la denomina) por parte del banco central no es una solución perfecta. En la práctica, los bancos centrales podrían tener que afrontar una difícil elección. Evaluar que instituciones financieras aparte de los bancos pueden tener acceso a esa provisión de liquidez es una cuestión delicada. Estimar el valor de los activos y, por tanto, decidir cuánto puede prestarse a una institución financiera, también puede ser difícil. El banco central no querría inyectar fondos a una institución financiera que es realmente insolvente; pero, en medio de una crisis financiera, resultaría muy difícil determinar la diferencia entre insolvencia e iliquidez.

APENDICE 4

CRONOLOGIA BITCOIN[33]

En esta Cronología pretendo señalar las fechas más relevantes relacionadas con el Bitcoin, necesarias para poder apreciar el desarrollo exponencial que ha tenido la moneda, desde su creación oficial en 2009 hasta la actualidad.

- Agosto 2008: El creador Satoshi Nakamoto, registró la página web Bitcoin.org, la cual sería la base de la moneda.
- Octubre 2008: Se publica el diseño del logo de la propia moneda.
- Enero 2009: Se lanza la primera red bitcoin y, además, se produce la primera emisión de la moneda. Tiene lugar en esta misma fecha la primera transferencia de Bitcoins de Satoshi Nakamoto a un colega, Hal Finney.
- Octubre de 2009: Se publica el primer tipo de cambio con respecto al dólar, con un dólar se podían comprar 1.309´03 Bitcoins.
- Mayo 2010: Se produce la primera transacción con bitcoins, un programador de florida compró 2 pizzas por 10.000 bitcoins. Con el tipo de cambio actual serían aproximadamente 45 millones de euros (tipo de cambio a día 12/11/2018).
- Junio de 2010: Nakamoto se retira del proyecto y lo hace con una gran cantidad de bitcoins, lo que le convierte actualmente en una de las personas más ricas del mundo según la revista Forbes.
- Julio 2010: Se lanza la primera pasarela de pago, MT Gox. Es una página web en la que se permite cambiar moneda fiduciaria o fiat (euro, dólares, libras…) por bitcoins.
- Febrero 2011: Se alcanza la paridad de la moneda bitcoin con el dólar.
- Junio 2011: El precio del bitcoin se desploma hasta un céntimo de dólar, al conocerse un problema de robo de cuentas en MT Gox, alrededor de 600 cuentas son robadas, esto provocó que los inversores estimen que la moneda no es lo suficientemente segura. El creador de MT Gox denuncia un robo por parte de unos hackers de estas cuentas.
- Marzo 2013 Bitcoin: Se dispara la cotización de bitcoin, básicamente por la crisis chipriota (Crisis Financiera en Chipre 2012-2013) Básicamente debido a que al ser una moneda que no está bajo el control de ningún organismo, país… en

[33] Cronología propuesta por el curso de criptomonedas: http://campus.ief.es/

situaciones de crisis financiera, se considera que puede no sufrir en casos que se den situaciones similares a las de un corralito tanto como las que sufre una moneda fiduciaria o fiat.

- Julio 2013: Los gemelos Winklevoss, populares por reivindicar la auditoria de Facebook, solicitan la apertura de un fondo de inversión en Bitcoin, más tarde en plena ola del Bitcoin en diciembre de 2017 venderían este fondo haciéndoles de esta manera entrar en la lista Forbes.
- Octubre 2013: Se abre primer cajero automático de Bitcoin (BTM) en una cafetería de Vancouver (Canadá).
- Noviembre 2013: La Reserva Federal (Fed), comunica al Senado Estadounidense que no tiene autoridad para supervisar la divisa Bitcoin, manifiesta la incapacidad de supervisar y organizar la moneda. El precio del Bitcoin supera por primera vez los 1.000 dólares, siendo hace tan sólo dos años había alcanzado la paridad con el dólar. Y alcanza, además, la paridad con la onza de oro.
- Enero de 2014: El número de Bitcoin en circulación supera los 12 millones.
- Febrero 2014: Mt Gox se declara en quiebra en Tokio puesto que no han podido superar el episodio de robo de cuentas de dos años atrás, y denuncia la desaparición de 850.000 bitcoins (unos 387 millones de dólares) que habrían sido robados por piratas informáticos.
- Octubre 2014: Se instala el primer cajero de Bitcoin en España, en el centro de Madrid.
- Febrero 2016: La autoridad financiera de Japón promueve una modificación de la normativa para considerar a Bitcoin como una moneda corriente.
- Diciembre 2016: El valor total de los bitcoins en circulación supera los 14.000 millones de dólares según Reuters.
- Marzo 2017: Se crea la primera tienda física en la que se puede comprar Bitcoins, llamada ``House of Nakamoto´´ de Viena, en honor a su creador.
- Abril 2017: Japón se convierte en el primer país en legalizar el Bitcoin como forma de pago, esta opción es la que han elegido la mayoría de los países y la que tenemos actualmente aquí también en España.
- Julio 2017: Un tribunal en Tokio comienza el juicio al creador de Mt Gox acusado de fraude en 2014, en el que fue condenado y actualmente se encuentra en la cárcel. Cómo podemos ver el tema de la seguridad es básico dentro de la moneda

digital y no supone un problema técnico de seguridad sino más bien humano relacionado con las personas al cargo de esta moneda.

- Agosto 2017: Aparece una bifurcación de la moneda a raíz de un desacuerdo dentro de la comunidad y hace que nazca Bitcoin
- Diciembre 2017: Bitcoin alcanza su máximo histórico superando los 20.000 dólares por bitcoin
- Enero 2018: El valor de Bitcoin se desploma un 70% debido al inicio de las inspecciones de fraude, una vez más a problemas de negocio como son los herederos de MT Gox, Coinchek y Bitifinex.
- Abril 2018: La agencia tributaria reclama información a 16 bancos sobre cuentas que operan con criptomonedas.
- Mayo 2018: En Islandia, uno de los países con más empresas dedicadas a la minería por habitante, se contabiliza que el consumo eléctrico de estas empresas de minería de Bitcoin supera al de las familias.
- Junio 2018: Un robo masivo de criptomonedas en Corea del Sur en la casa de cambio Bithumb provoca una nueva caída del valor del Bitcoin. Como seguimos viendo estos problemas de seguridad no tanto de los protocolos que rige la moneda o de la propia moneda sino de los interfaces humanos necesarios para intercambiarlos son los que han llevado a las diferentes cotizaciones de la moneda.