Universidad Pontificia Comillas

Facultad de Ciencias Humanas y Sociales

Grado en Relaciones Internacionales

Trabajo Fin de Grado

Criptomonedas y el Sistema Monetario

Perspectivas y oportunidades

Estudiante: José María Andreu Sáez-Benito

Director: Karin Martín Bujack

Madrid, junio 2018

Índice

Índice de figuras

Resumen

Pocos activos han tenido una entrada en los mercados financieros internacionales como la han tenido las criptomonedas. Comparada muchas veces con la Burbuja de los Tulipanes de Holanda en el siglo XVII, el crecimiento que ha experimentado la cotización de las criptomonedas parece vislumbrar un futuro incierto en el que se conjuga innovación tecnológica con incertidumbre.

No obstante, estas criptomonedas no han aparecido por casualidad ni son producto de la suerte. Son el resultado de un trabajo de investigación y desarrollo por parte de ingenieros informáticos para crear un instrumento que se adapte al medio financiero. A pesar de su no oficialidad, esto no implica que no tengan un trasfondo teórico fuerte que sustente sus innovaciones. Por ello, revisar la teoría económica acerca de los conceptos monetarios es fundamental para analizar el trabajo de los ingenieros informáticos ya que permitirá ver su nivel de comprensión al mundo que quieren complementar. Para esta revisión los conceptos monetarios de la Escuela austríaca son una gran guía para conocer los objetivos de los creadores de las criptomonedas debido a que es una de las teorías económicas que más influencia ha tenido en este ámbito.

Por tanto, para tener un análisis insesgado de la realidad de las criptomonedas es fundamental que se tengan en cuenta aspectos económicos teóricos y mecanismos del sistema monetario para comprender las funciones que han de tomar las criptomonedas.

Palabras clave: Blockchain, Criptomoneda, Divisa, Hash, PIB, Proof of work, Problema de los bizantinos, Redes distribuidas, Token, Escalabilidad, Encriptación, P2P.

Abstract

Few assets have had an entry into the international financial markets as the cryptocurrencies have had. Compared many times with the Bubble of the Tulips of Holland in the XVII century, the growth that has experienced the price of the cryptocurrencies seems to glimpse an uncertain future in which technological innovation is combined with uncertainty.

However, these cryptocurrencies have not appeared by chance nor are they the product of luck. They are the result of a research and development work by computer engineers to create an instrument that adapts to the financial environment. Despite their lack of official status, this does not imply that they do not have a strong theoretical background to support their innovations. Therefore, review the economic theory about monetary concepts is essential to analyze the work of computer engineers as it will allow to see their level of understanding to the world they want to complement. For this review the monetary concepts of the Austrian School are a great guide to know the objectives of the creators of cryptocurrencies because it is one of the economic theories that has had the most influence in this field.

Therefore, to have an unbiased analysis of the reality of cryptocurrencies, it is essential that theoretical economic aspects and mechanisms of the monetary system are considered in order to understand the functions that cryptocurrencies must perform.

Keywords: Blockchain, Cryptocurrency, Currency, Hash, GDP, Proof of work, Problem of the Byzantines, Distributed networks, Token, Scalability, Encryption, P2P.

I. Introducción

1. Propósito y contextualización del tema

El propósito de este trabajo es realizar una revisión de la principal literatura especializada en la teoría cuantitativa del dinero, la composición del sistema monetario internacional y las criptomonedas y sus principales características. A través de esta revisión se ambiciona recoger las principales conclusiones sobre estas materias por parte de autores especializados, para así alcanzar una visión sintetizada de cada uno de los elementos estudiados en un contexto común.

La teoría cuantitativa del dinero ha sido elegida porque es aquella que tiene mayor aceptación en el campo teórico y ha sido demostrada como cierta en varios de sus preceptos principales, a la vez que todavía no ha sido refutada. Además, uno de los fundamentos teóricos sobre los que se construyó el concepto de las criptomonedas es esta teoría económica. Por tanto, se presenta como idónea para encarar el análisis económico de nuevos medios de pago descentralizados que han aparecido.

El análisis de la composición del sistema monetario internacional también se presenta como crucial para el análisis que plantea este trabajo. Los mecanismos del sistema monetario entrañan ciertas actividades y conocimientos que completan el concepto de dinero haciendo que sea una realidad social en transformación con unas dimensiones mayores a las sospechadas.

Finalmente, queda revisar y responder a las preguntas de la cuestión de las criptomonedas. Las criptomonedas, aunque aparecidas a principio de década, han tenido una entrada espectacular en la sociedad durante el año 2017. La extrema volatilidad de sus mercados ha conseguido ser un foco de atención para curiosos y escépticos, pero realmente parece que esta tecnología solo está levantando sus alas. En este trabajo se realizará una revisión de cuáles son las cualidades que reúne el dinero y se intentarán comprobar si se presentan en las criptomonedas. Igualmente, se le echará una mirada al nuevo mundo de posibilidades que abre esta tecnología innovadora a la sociedad y a la economía. Como cualquier invento revolucionario parece que las criptomonedas, y especialmente su tecnología base la Blockchain, van a sobrepasar los objetivos para los que fueron creados. La amplia aplicación de esta nueva tecnología en la creación de redes descentralizadas y públicas puede tener unos efectos futuros que en la actualidad son muy difíciles todavía de adivinar.

2. Objetivo

El objetivo de este trabajo será estudiar la posibilidad e idoneidad de la incorporación de las criptomonedas al sistema monetario actual. Para ello se tendrán en cuenta las conclusiones obtenidas por la teoría cuantitativa del dinero y la Escuela austríaca, así como las características del sistema monetario actual. Por ende, los principales objetivos serán:

- Revisar la principal bibliografía correspondiente a la teoría cuantitativa del dinero. Asimismo, se revisará literatura concerniente a la interpretación provista por la Escuela austríaca.
- Acotar y estudiar las principales características del sistema monetario.
- Estudiar el fenómeno actual de las criptomonedas y la tecnología que permite su funcionamiento. Además, también será necesario tener en cuenta las consecuencias de su uso.
- Analizar las posibles aplicaciones que tiene la tecnología Blockchain.
- Estudiar la idoneidad de la incorporación de las criptomonedas al sistema monetario internacional.
- Discutir las distintas alternativas que se presentan para esta incorporación.

3. Estructura de trabajo

El trabajo va a estar estructurado en dos bloques temáticos, cada uno con una naturaleza diferenciada. Estos dos bloques serán el Marco Teórico y el Estado de la Cuestión

El primer bloque será el Marco Teórico. En el marco teórico que estudiaran los principales conceptos teóricos sobre el dinero que nos proporciona la teoría cuantitativa del dinero y las perspectivas que incluyen la Escuela austríaca. Asimismo, se estudiará la evolución y características actuales del sistema monetario durante el último siglo. Finalmente, este bloque concluirá con un desarrollo exhaustivo de las criptomonedas y de la tecnología que permite su funcionamiento. Este bloque será crucial para el análisis de la cuestión porque proveerá de fundamentos teóricos sobre los que sustentar la revisión de la literatura especializada en los efectos prácticos.

El segundo bloque será el Estado de la Cuestión. En este bloque se entrará a analizar los efectos prácticos del uso de las criptomonedas en la sociedad y la economía, y los posibles usos que se le podría dar. Este bloque, a pesar de tener una gran base en la literatura revisada, será el que destaque por la mayor subjetividad en el trabajo. Esta subjetividad viene dada por la incertidumbre que genera actualmente el sistema criptomonetario debido a su falta de regulación y la velocidad con la que ha entrado en escena. Aunque en la actualidad se haya convertido en un fenómeno que atrae la atención, los derroteros que va a tomar esta tecnología son prácticamente inescrutables. En este bloque se tendrá en cuenta esa incertidumbre, pero se intentará sintetizar los efectos más evidentes que tiene el uso de estas nuevas redes de pagos.

II. Estado del Arte

1. Teoría Monetaria y Sistema Monetario

1.1 Teoría Monetaria y concepto de dinero

1.1.1. Teoría cuantitativa

Para explicar el funcionamiento del dinero es necesario acudir a una teoría monetaria mediante la que intentar comprender los mecanismos y componentes del sistema monetario. En este sentido, la teoría Cuantitativa es la teoría monetaria con mayor aceptación en la economía teórica, y práctica, para explicar el funcionamiento del dinero (Humphrey, 1974). Este hecho hace que se vaya a utilizar como guía para analizar la función del dinero. Asimismo, esta teoría es una de las pocas teorías neoclásicas supervivientes y su resistencia se basa en que sus preceptos básicos son muy aceptados, a pesar de que las consideraciones más complejas son un punto de discusión muy candente entre distintas escuelas.

Esta teoría tiene su origen en los estudios de Francisco de Vitoria y la Escuela Escolástica de Salamanca acerca de la influencia que tiene la oferta monetaria sobre el valor de los recursos tras el descubrimiento de minas de plata en las colonias españolas en el siglo XVI (Grice-Hutchinson, 1989), y ha sido incluida y mejorada por distintas escuelas económicas entre sus temas de estudio. Es importante mencionar que la oferta monetaria es la cantidad de unidades monetarias y otros instrumentos líquidos que circulan en la economía de un país en un momento determinado (Times, 2018).

Entre las escuelas que la mencionan y discuten se incluyen aquellas que predican las dos corrientes de economía más seguidas en la actualidad; la escuela Keynesiana y post-Keynesiana que apoyan la intervención estatal en la economía y, a pesar de ser sus mayores críticos, utilizan la teoría Cuantitativa como base para construir su teoría monetaria, y las Escuela Austríaca y de Chicago que la apoyan fielmente y abogan por una liberalización del sistema económico y monetario (Humphrey, 1974).

Es curioso que esta teoría económica encuentra un alto nivel de consenso entre los autores acerca de los efectos de los cambios de las variables en el sistema monetario en el largo plazo. La mayoría afirman que en el largo plazo existe correlación positiva y causalidad

entre la variación de la cantidad monetaria disponible y el poder adquisitivo de la unidad monetaria de intercambio (Patuti & Tatulescu, 2013). Pero en cuanto a cómo influye y en qué intensidad en el corto plazo existen serias discrepancias. Además, aunque el hecho de que la oferta monetaria tenga un efecto sobre la economía sea aceptado por todos, tampoco se llega a ningún acuerdo en cuanto a si este efecto es positivo o negativo y si su utilización es conveniente o no. Este pequeño consenso ha permitido al menos que se haya podido formular una ecuación monetaria que incluye los preceptos básicos mínimos. Es la siguiente:

$$MxV=PxT \quad (1)$$

Donde M es el agregado económico que representa la cantidad de unidades monetarias y otros activos líquidos disponibles, V es la velocidad con la que el dinero cambia de manos en un periodo económico definido, P es el nivel de precios (que muestra el poder adquisitivo de la unidad monetaria) y T representa el número de transacciones realizadas en ese periodo concreto.

Con respecto a esta ecuación, la escuela Keynesiana y Post-Keynesiana afirman que en el corto plazo el poder adquisitivo de la unidad monetaria por el número de transacciones resulta en el valor nominal Producto Interior Bruto (a partir de ahora mencionado como PIB) (Keynes, 1936). Por tanto, para tener efectos positivos sobre el PIB es necesario aumentar la cantidad de dinero o la velocidad con la que cambia de manos. Además, incluyen un concepto teórico muy importante que es el rol que pueden tener las unidades monetarias como medio de pago diferido al Estado. Es decir, que a través de una mayor emisión de unidades monetarias el Estado puede cobrar por anticipado bienes y servicios que prestaría a la sociedad y podría así también aumentar el PIB de esa sociedad. Es importante mencionar que, aunque conectan sus razonamientos con esta ecuación, esta corriente prefiere utilizar su propia fórmula para el PIB.

$$Y = C + I + G + (X-M) \quad (2)$$

La escuela de Chicago, encabezada por Milton Friedman, ha sido la que ha estudiado con mayor profundidad la ecuación cuantitativa (1) en términos empíricos. Friedman (1959) se encargó de estudiar los efectos que había tenido en los precios de la economía estadounidense los cambios en la cantidad de unidades monetarias disponibles entre los años 1870 y 1954. En su estudio nos muestra, a diferencia de las creencias Keynesianas, que un cambio en la cantidad de unidades monetarias disponibles tiene un efecto directo

sobre su poder adquisitivo. Es decir, si aumenta el número de unidades monetarias el precio de los productos y servicios sube y por tanto su poder adquisitivo decrece. Entonces, la ecuación (1) siempre se mantiene en equilibrio, y sus componentes crecen o decrecen en función de lo que haga la cantidad total disponible.

En contraposición con la Escuela de Chicago, que pretende explicar el funcionamiento del dinero a través de pruebas empíricas, está la Escuela austríaca se centra en la obtención de verdades o razones (preceptos) universales en la economía a través del análisis de los motivos y factores implicados. Por lo tanto, difieren en los métodos para analizar la economía, pero concluyen en los principios generales que la rigen. La escuela austríaca acepta la teoría Cuantitativa y, además, desarrolla un análisis conceptual para guiar en la interpretación de los datos económicos apoyándose en conceptos propios como el análisis del ciclo económico y de la demanda monetaria (Hayek, 1931). Además, esta escuela tiene un enfoque muy curioso acerca del dinero. Mises considera el dinero como el conjunto de todos los saldos de caja de los individuos en la sociedad. Con esto se refiere a que el dinero básicamente es el conjunto de las diferencias entre lo que aportan las personas a la economía y lo que consumen, por ende, el dinero es el excedente de producción de una sociedad.

1.1.2. Formación del concepto de dinero

Debido a lo anteriormente mencionado utilizaremos los conceptos de la escuela austríaca para analizar el dinero al tener una mayor riqueza conceptual en esta área. Son muy útiles el análisis de Carl Menger en su obra *"On the Origin of Money"* (1892) y el de Ludwig von Mises *"The Theory of Money and Credit*" (1912) para este análisis. En sus obras, el dinero se considera como una construcción social que permite realizar intercambios indirectos entre individuos. Esto significa que el dinero no es un activo sino un sistema. Cabe destacar desde un principio que la escuela austríaca defiende que no existe ningún valor absoluto en la economía, sino que todos son subjetivos dependiendo de la circunstancia y del agente (Mises, 1912).

Un intercambio indirecto se da cuando una persona adquiere un activo o servicio a través de otro activo o medio que no es el que el aporta a la sociedad por su profesión. Es decir, si una persona trabaja en una fábrica de tornillos su aportación al sistema productivo son

tornillos, no obstante, no intercambia esos tornillos que produce por otros bienes y servicios que quiera adquirir. Este sería el caso de un intercambio directo. Sin embargo, el trabajador de la fábrica intercambiará su producción por un activo que permita adquirir cualquier activo o servicio ofrecido en la economía (Menger, 1892).

Por tanto, el dinero es una función social que permite el intercambio indirecto. Para que funcione ha de reunir tres cualidades (Menger, 1892). Primero, supone una unidad de contabilidad y de valoración subjetiva de los distintos bienes y servicios susceptibles de intercambio (Mises, 1912). Es decir, a través de los mecanismos de la oferta y la demanda se acuerdan los valores que cada agente da a los activos que se quieren intercambiar en función de una unidad base cuantitativa y consensuada, la unidad monetaria. Además, esta unidad de contabilidad permite la creación de un sistema de registro de derechos de cobro, los cuales se representan en las unidades monetarias. Finalmente, esas unidades monetarias son un instrumento de transmisión de estos derechos de cobro (Lunn, 2014). Esta triple naturaleza permite la creación de un sistema que coordine y estandarice el intercambio indirecto entre agentes, construido sobre la unidad monetaria.

No obstante, para que este sistema funcione la unidad monetaria ha de estar materializada en un activo que sirva como medio de registro físico de ese intercambio. Además, este objeto tiene que ser capaz de asegurar una contraprestación en caso de que no se quiera retener durante más. Entonces, esta contraprestación habrá de tener el mismo valor subjetivo que el activo o servicio renunciado en la operación de intercambio indirecto para que el sistema mantenga sus cualidades. Por todo esto, este activo ha de tener las cualidades de divisibilidad y durabilidad. También, su contraprestación debe ser conocida ya sea porque el valor del objeto utilizado es aceptado o porque está respaldada por una institución que la asegura.

En el sistema financiero internacional actual ese activo físico actualmente está representado por las divisas. Una divisa es una unidad monetaria respaldada por una institución estatal o supraestatal y cuya aceptabilidad solo está asegurada en el territorio donde esa institución tiene autoridad. Existen casos como en el Euro en el que la institución que lo respalda es un organismo de una organización internacional. Por tanto, continuando con el análisis de Menger (1892), se explicará el proceso social que ha llevado a la imposición de las divisas como unidad monetaria.

Primera fase: El valor de la contraprestación depende del objeto que se utilice

Siguiendo con el análisis de Menger (1892) y Mises (1912), vemos que el método de asegurar esa contraprestación con el uso activos físicos con un valor reconocido y extendido fue el primero en ser aplicado. En este primer sistema de intercambio indirecto se adoptaron ciertos bienes, cuyo valor era universalmente aceptado por sus cualidades intrínsecas, como unidades monetarias. Por tanto, priman una serie de características para los bienes; Primero, han de ser comúnmente aceptados ya sea por su utilidad o por su valor. Esto incluye objetos con una estética llamativa, metales y piedras preciosas, o con una utilidad ampliamente reconocida, como en el caso de las semillas de cacao en Latinoamérica precolombina. Además, han de ser fácilmente divisibles y almacenables (Lunn, 2014). En este último caso, los metales preciosos tenían ventaja por su maleabilidad (Menger, 1892). Finalmente, estos objetos habían de ser resistentes al paso del tiempo ya que respaldan valores demasiado importantes para ser destruidos por la erosión.

Este sistema se basa en el cálculo del valor económico de los bienes mediante la comparación con el valor de un bien que sirve de referencia de intercambio. Por tanto, el cálculo del valor de los otros bienes es una ecuación con dos incógnitas en la que el precio del bien a calcular es inferido a través del valor base de la unidad monetaria de comercio. En este sistema, el consenso es vital para el mantenimiento de la actividad comercial, y en ello encuentra un gran problema. El consenso depende mucho de la coordinación del valor que se le da a la unidad base en los distintos puntos de comercio, ya que el valor dado puede variar de un lugar a otro por distintos factores. Por tanto, se puede destruir el consenso sobre el valor del bien, aunque siga siendo aceptado como unidad monetaria. Esta pérdida de consenso sobre el valor se da por las limitaciones de la comunicación entre puntos comerciales y la falta de confianza hacia los canales de comunicación.

Además de las limitaciones dadas por la coordinación, este sistema enfrenta diversos problemas relacionados con las limitaciones dadas a la naturaleza física de la unidad monetaria. La divisibilidad encuentra un límite físico al igual que la transmisibilidad un límite espaciotemporal.

Segunda fase: La contraprestación se asegura mediante la soberanía

Para cubrir con las deficiencias del sistema de consenso de valor económico de las unidades comerciales, se empezaron a desarrollar métodos de fijación del valor de las unidades económicas a través de "Terceros fidedignos". Estos terceros fidedignos determinan el valor de las unidades monetarias ya sea fijo, acotado en un intervalo o libre, dependiendo de la preferencia que se tenga. No obstante, la confianza en esta valoración tiene que estar respaldada completamente por un componente de soberanía y poder jurídico sobre un territorio y gentes.

Estos terceros fidedignos, comenzaron siendo Estados que acuñaban unidades monetarias mediante activos físicos con un determinado coste de producción y adquisición (Mises, 1912). Los Estados, aseguraban la autenticidad y aplicabilidad de estas unidades monetarias para transacciones en el territorio y las personas que estaban bajo su soberanía. Por lo tanto, al ser universalmente aceptado en un territorio y personas concretas, el valor económico de esa unidad monetaria depende de su coste de producción y de la variedad y calidad de bienes y servicios que se podían obtener como contraprestación en el territorio soberano del Estado emisor (Menger, 1892). Y la diferencia entre el valor y su coste de producción se conoce como el ingreso por señoraje de la acuñación.

Es necesario mencionar que en este punto es cuando el concepto de dinero como pago diferido al Estado (Keynes, 1936) de la corriente keynesiana gana peso. Es a partir de este punto que el sistema monetario y de intercambios indirectos es susceptible a cambios aplicados por el Estado para incentivar distintas situaciones.

Este nuevo sistema, permite una mayor coordinación de los distintos puntos comerciales, y se puede alcanzar un mayor y más rápido consenso comercial. Esta coordinación, se obtiene a través de la concentración local de la capacidad de elección de la unidad monetaria de los agentes económicos que actúan en los distintos puntos comerciales. Esta concentración del poder de decisión significa arrebatarle la capacidad de elección a los agentes. Sin embargo, permite obtener un consenso y coordinación máximo a nivel local. Esta concentración local se asegura mediante la soberanía sobre ese territorio, normalmente representada mediante prácticas coercitivas. Esto es necesario en una situación de limitación física de la divisibilidad y espacio-temporal de las comunicaciones, que además son crecientes a medida que uno se aleja del nivel local (Menger, 1892). Este sistema ha sido ampliamente aceptado como el más idóneo en

situaciones de interconexión comercial y división del trabajo en las que no exista una única institución soberana, ya que permite la obtención simplificada de bienes y servicios sin exponerse a los cambios que se pueden producir en gustos y preferencias en la valoración de las unidades monetarias en distintos territorios.

Es imprescindible mencionar que en este sistema el acuñamiento de la unidad monetaria no ha de tener que ser obligatoriamente provisto por el Estado cuya soberanía asegura la aceptabilidad (Menger, 1892). Este rol lo puede llevar a cabo una institución que se apoye en la soberanía transmitida de los Estados para la valoración y creación de las unidades monetarias, mientras que se el estado el que asegure su uso. Este es el caso de la actualidad, en la que estas funciones son llevadas a cabo por los Bancos Centrales, cuya autoridad deriva de la soberanía transmitida de uno o más estados, sin tener que ser la propiedad de estas instituciones de carácter público. Es decir, organizaciones privadas pueden ser encargadas de la emisión y acuñación de la unidad monetaria, apoyándose en la soberanía brindada por uno o más Estados. Este es el caso en la Reserva Federal en Estados Unidos, o en el Bank of England, que son bancos privados, en incluso del Banco Central Europeo (BCE a continuación) aunque con mayor participación pública (BCE, 1992).

Como problemas de este mecanismo, existen varios y de naturaleza compleja. El primero de ellos es que este sistema a nivel internacional lleva a que el valor de las divisas sea variable dependiendo del Estado soberano, siendo aquellas divisas de Estados con grandes e importantes mercados internos las más fortalecidas, y sus ciudadanos los más empoderados para la adquisición de bienes extranjeros (Eichengreen, Chitu, & Mehl, 2015). Esto lleva a que personas de países con menor fortaleza económica tengan menor competitividad relativa a nivel internacional. Asimismo, el papel de las instituciones encargadas de la impresión de divisa puede tener un efecto desestabilizador. El hecho de que todas las divisas actuales tenga un valor real superior a su coste supone que se produzcan beneficios en la emisión de divisa conocidos como el señoreaje (Imrohoroglu, 1996), que puede llevar la aplicación de políticas monetarias poco favorables para incrementar los ingresos privados.

1.2. Características del Sistema y prácticas monetarias

Los sistemas monetarios nacionales durante la gran mayoría del tiempo mantuvieron la cobertura de la contraprestación a través de la soberanía para el comercio local, mientras que para el comercio internacional se utilizaba la cobertura a través de activos con valor aceptado. Esto se debe fundamentalmente a la falta de conocimiento, o interés, con respecto al mercado interno de la otra parte. Este caso se puede ver con China, que nunca mostró interés en comerciar con las naciones europeas durante el siglo XVIII (García Guerra, 2006), y solo aceptaba los pagos en Reales de a Ocho españoles debido a su alto contenido en plata, material valorado en China. No obstante, es paradójico que el valor del Real español tuviera un gran crecimiento en Europa occidental para esa época debido no solo por su gran valor en plata, sino porque indirectamente la soberanía china permitía comerciar con esa divisa en China (García Guerra, 2006). Este último es un ejemplo claro de como históricamente ambos métodos han estado en funcionamiento en distintas combinaciones, habiendo habido un gran número de divisas que han ganado preponderancia a nivel internacional por sus características de aceptabilidad y valor (Eichengreen, Chitu, & Mehl, 2015).

En el último siglo, gracias a industrialización global y a la expansión del comercio y la innovación financiera, las divisas han dejado de ser fabricadas a partir de materiales con alto valor, para así facilitar su creación y la extensión de la posibilidad de pago. Esto ha sido empujado por el hecho de que el avance el transporte ha permitido la obtención de importaciones con una velocidad nunca vista, lo que lleva a una mayor internacionalización de los productos, y por tanto a una mayor cotización de aquellas divisas que permiten adquirir mejores bienes y servicios (Yamashita, Kurumatani, Sasaki, Kawamura, & Ohuchi, 2005). Por tanto, actualmente el criterio para juzgar una divisa ha variado desde su valor material y comercial, a simplemente su valor comercial (Eichengreen, Chitu, & Mehl, 2015).

Desde comienzos del proceso de interconexión global, y especialmente tras la creación de un sistema político internacional alrededor de las Naciones Unidas, se ha ido creando sistema monetario internacional en el que todas las economías están en un estado de interconexión a través de las divisas. En este sistema, la última divisa con preponderancia internacional ha sido el dólar, y además su imposición también supuso la creación de un sistema coordinado de consenso para los tipos cambiarios. Éste se ha construido sobre la

creación del Fondo Monetario Internacional y el papel del dólar como principal divisa de reserva (Eichengreen, Chitu, & Mehl, 2015).

Una divisa de reserva es una cantidad de divisa mantenida por los bancos centrales y otras instituciones financieras importantes para prepararse para las inversiones, transacciones y obligaciones de deuda internacional, o para influir en su tipo de cambio doméstico. Un gran porcentaje de los productos básicos, como el oro y el petróleo, tienen un precio en la moneda de reserva, lo que hace que otros países tengan esta moneda para pagar por estos bienes (Investopedia, 2018).

1.2.1 Sistema Monetario internacional

El sistema monetario actual está caracterizado por la existencia de instituciones internacionales de asesoría y asistencia financiera como el Fondo Monetario Internacional, que proveen la flexibilidad necesaria a los Estados miembros para afrontar déficits de divisas debido a desequilibrios comerciales y financieros, y por el rol del dólar como divisa por excelencia tanto para el comercio como para las finanzas (Eichengreen, Chitu, & Mehl, 2015).

El papel principal del dólar como divisa de reserva fue adquirido tras la Convención de Bretton Woods de 1944, y la posterior la creación del Fondo Monetario Internacional (Bordo, 2017). A partir de entonces, a través del acuerdo fundacional del FMI, todos los Estados miembros se comprometían al establecimiento de tipos de cambio fijos basados en el dólar estadounidense, que era la única divisa con convertibilidad al oro. Este sistema de cambios fijos se mantuvo hasta 1971, cuando colapsó en lo que fue conocido el cierre de la ventilla del oro. Debido a que durante las décadas de 1950 y 1960 Estados Unidos había sido el principal benefactor y proveedor para la reconstrucción de los principales países europeos y asiáticos devastados tras la Segunda Guerra Mundial, las reservas internacionales en dólares se habían expandido, imponiéndose el dólar como principal divisa de reserva de valor tras la caída de la libra (Eichengreen, Chitu, & Mehl, 2015). No obstante, debido a los gastos que tenía que afrontar por la Guerra Fría Estados Unidos se había encontrado con dos grandes obstáculos para mantener el equilibrio de pasivos de dólar con el oro en la reserva; la financiación a bandos contra comunistas había llevado a una excesiva impresión de dólares, especialmente tras la guerra de Vietnam, además, de

mantener un conflicto con dos de los principales productores de oro que eran la URSS, y Sudáfrica, el cual estaba sancionado comercialmente debido a las políticas de apartheid. Esto provocó que para 1964 los pasivos asociados al dólar fueran mayores que la reserva de oro (Bordo, 2017).

Este desequilibrio se fue conjuntando con distintos factores que llevaron a la quiebra del sistema. Hubo varios trabajos teóricos que confirmaban este colapso como el de Robert Triffin (1978), y su famoso dilema del dilema de Triffin, o el principio de la Trinidad Imposible (Aizenman, 2010). Además, entre los países europeos ya recuperados empezaba a haber un deseo del abandono del sistema que juzgaban como únicamente beneficioso para Estados Unidos. Todo esto hizo que finalmente el sistema de patrón oro se abandonara, así como los tipos de cambio fijo eliminándolos de los estatutos del FMI.

El dilema de Triffin merece una atención especial ya que plantea un hecho que no se pudo superar en ese momento de crisis del sistema monetario ya que todavía sigue mostrando sus efectos. Este dilema afirma que es imposible que un solo Estado pueda mantener la carga de aportar liquidez al sistema financiero internacional con una divisa de reserva sin que se creen crisis cíclicas (Triffin, 1978). Al convertirse el dólar en divisa de reserva todos los Estados adquieren principalmente dólares para componer su reserva de divisas, normalmente a través de captación de inversión o exportando a Estados Unidos. A la misma vez, Estados Unidos ofrece una alternativa de inversión segura con los bonos del Tesoro estadounidense por su posición de divisa de reserva, lo que hace para los excedentes de económicos de las naciones extranjeras se inviertan en compras al tesoro. En un escenario de crecimiento económico global tanto el déficit comercial como la deuda de Estados Unidos incrementan hasta llegar al punto en el que la economía deja de crecer por el tamaño de la deuda, lo cual comienza una recesión económica que se traslada a todos los miembros del sistema. Las consecuencias de este dilema se han podido ver tanto en ese año 1971 como en las posteriores crisis. La Trinidad Imposible es un argumento interesante que se utilizó en la época para la apertura del mercado de divisas. Este argumento apoyado en el modelo de Mundell y Fleming de 1961 implica que es imposible combinar a la vez política monetaria independiente, tipos de cambios fijos y apertura de capitales (Aizenman, 2010).

Por tanto, tras la experiencia del sistema de Bretton Woods y la asunción de la Trinidad Imposible, en 1971 se reforma el Fondo Monetario Internacional, y a partir de entonces ninguna moneda queda valorada únicamente a través del oro. El valor de los tipos de

cambio se convierte variable, aunque en algunas ocasiones limitado por bandas de fluctuación, y queda respaldado por las reservas de oro y otros activos sin riesgo. Una de las novedades introducidas es que en el balance de los bancos centrales se aceptan como activos la deuda soberana y bonos de grandes compañías, así como la eliminación de los tipos fijos respecto al oro, aunque se crean los tipos fijos respectos a otras monedas flotantes (Bordo, 2017).

A pesar de que en este nuevo sistema la fijación del precio viene dada por los mercados de intercambio de divisas, las instituciones financieras siguen pudiendo influir en el tipo de cambio de la divisa a través de la depreciación y la apreciación. La gran diferencia con devaluación y revaluación es que estas últimas son la modificación en el tipo de cambio por la nueva fijación de uno nuevo por la institución financiera que lo domina, mientras que las primeras son la variación del tipo de cambio respondiendo a la oferta y a la demanda. Debido a que el mercado está liberalizado desde 1971, las instituciones monetarias han desarrollado mecanismos para incentivar y desincentivar el uso de su divisa y así apreciarla o depreciarla.

Un mecanismo muy común es el del coeficiente de reserva. El coeficiente de caja es un porcentaje de los depósitos que una entidad financiera que tiene que mantener en reservas líquidas. Un aumento en el coeficiente de caja significa una restricción en la cantidad total que un banco puede invertir, y por tanto suponen la reducción de la creación de dinero bancario y de cantidad total de divisa circulando y viceversa. Eichengreen, Chitu y Mehl (2015) descubren que el hecho de que una divisa sea reserva tiene influencia sobre su tipo de cambio. Sin embargo, descubren que incentivar el uso de la divisa nacional como reserva es más inefectivo y costoso que desincentivarlo.

Además, existe otros medios más heterodoxos para influenciar los tipos de cambio. El último y más conocido en Europa son las expansiones cuantitativas. Estas expansiones son una compra de deuda nacional por parte del Banco Central con el objetivo de reducir los intereses y mantener la inflación creciente. Este mecanismo se ha aplicado en la Unión Europea desde el año 2015 y también por el Banco Central de Japón.

2. Divisas criptográficas

2.1 Criptomonedas ¿Qué son y cómo funcionan?

2.1.1 Contexto tecnológico

Las tecnologías de la información han alcanzado un papel fundamental en la vida del ser humano durante las últimas décadas. Estas nuevas herramientas han supuesto un salto cualitativo en materias como la computación y tratamiento de la información, modelización y conservación de datos, así como en la transmisión de estos. Esta ventaja para el manejo de la información y los datos es lo que ha llevado a que hayan gozado de gran implantación tanto en los mercados como en las instituciones (Böhme, Christin, Edelman, & Moore, 2015).

Sin embargo, cuando nos planteamos el rol que las tecnologías informáticas en el mundo monetario podemos concluir que su adaptación no ha sido completa. Gracias a la revisión de los conceptos monetarios realizada anteriormente conocemos las características principales del dinero (Menger, 1892). Estas características del dinero son totalmente adaptables al medio digital, no obstante, la limitación con la que se encuentra es que la unidad monetaria de esta función de cambio está ligada a un activo físico, conocido como divisa en el sistema actual. Esta conexión con un activo físico provoca que su transmisión sea más costosa en tiempo y espacio que la de un activo digitales gracias a los avanzados sistemas de telecomunicaciones actuales. Por ello, para que se produzca la completa digitalización del dinero, las divisas han de ser activos digitales para que las transacciones no se vean lastradas por el carácter local de las divisas físicas.

Esta asimetría en la velocidad de transmisión puede ser difícil de figurar ya que actualmente vivimos en una economía en la que la gran mayoría de las transacciones están digitalizadas, no obstante, esta digitalización es únicamente es superficial. Generalmente, estas transacciones digitalizadas son llevadas a cabo a través de sistemas construidos por empresas, como PayPal, Visa o SWIFT, que permiten una mayor coordinación y eliminación de los pasos necesarios para el pago telemático, pero no implican que la transmisión de divisa física sea instantánea (Harwick, 2016). Estas empresas desempeñan una posición central en el proceso de pago digital, ya que unen al comprador y al vendedor a través de instituciones bancarias. Por la cual, funcionan como un gran registro de

operaciones de individuos, cuyos saldos canjean con los bancos ya sea cobrando o pagando divisas.

Sin embargo, en estos sistemas la dependencia en las entidades bancarias es muy grande debido a su rol de verificar el balance de la cuenta del individuo, previo a aceptar la transacción, y después actualizarlo cuando se ha recibido la información de la transacción. La entidad encargada del procesamiento del pago únicamente almacena operaciones pendientes de pago y cobro de instituciones financieras asociadas, que agrupan y saldan en mayores volúmenes. Por lo tanto, aunque parezca al individuo que la operación de intercambio ha sido realizada de manera digital, la única transmisión que ha habido es la de la información de su pago o cobro hacia la red del proceso de operaciones que se dedica de realizar las transacciones con las unidades monetarias físicas con la entidad bancaria, obteniendo ambas partes por ello una comisión (Anderson, 2012).

Este sistema de pagos telemáticos ha facilitado la velocidad y eficiencia de las transacciones, aunque se ha encontrado con una serie de problemas que han sido la motivación para el desarrollo criptomonetario. El primero es la imposibilidad de realización de pagos telemáticos en caso de que no se pertenezca a una entidad bancaria miembro de la red de pagos o se tenga conexión directa con el operador, y el segundo es que este sistema abre la puerta a la aplicación de cuotas excesivas debido al enorme papel de los intermediarios y al carácter privado monopolístico de la red. Finalmente, cabe destacar que este proceso implica la existencia y dependencia en varios intermediarios, lo que supone mayores cuotas y lentitud en el proceso por su carácter lineal y la imposibilidad del operador de controlar los sistemas de los agentes que operan con él (Anderson, 2012).

2.1.2 Aparición de las criptomonedas

Fueron estas características la que motivaron a desarrollarse sistemas de contabilización de operaciones de transacciones descentralizados durante el final del siglo XX. Para ello, se desarrollaron diversos algoritmos para la creación de sistemas de pago telemático basados en divisas virtual, destacando entre ellos Hashcash (Buterin, 2013), que permitía el cifrado de transacciones con la tecnología criptográfica Hash.

Esta tecnología criptográfica conocida como Hash, es un sistema de encriptación de datos pseudo-aleatorio creado por la Agencia Nacional de Seguridad de Estados Unidos que se utiliza como método para la encriptación de información, aunque existen diferentes variedades. Además, Hashcash también fue innovador al incorporar protocolos para evitar el uso maligno de la red, conocidos como *proof of work* (Buterin, 2013). Estos protocolos, establecen una dificultad variable para la incorporación de información encriptada a través de la tecnología hash en la red (Bitcoinwiki, 2018). Esta dificultad es creciente a mayor potencia computacional, lo que permite mantener la integridad del sistema y asegura una participación colectiva y de buena fe, a la vez que manteniendo un nivel estable de seguridad. Es decir, en caso de que un individuo pretenda incorporar información maliciosa en el sistema, le será más difícil a cuanta mayor potencia tenga su equipo informático. Esta tecnología está muy extendida entre los operadores de correos electrónicos para evitar los correos Spam (Swan, 2015).

Estos sistemas, no obstante, no consiguieron para sustituir el rol del dinero físico debido a la ausencia de una institución que respaldara y alabara esos activos virtuales utilizados como unidades monetarias, y así centralizara el sistema para establecer una base de datos protegida y segura (Buterin, 2013). Además, ante la ausencia de una institución centralizadora tampoco existía ningún algoritmo que permitiera la creación de un libro de registro público, de libre acceso y basado en sistemas compartidos, que aseguraran un no monopolio sobre el hardware, y por ende de la información contenida (Buterin, 2013).

La solución a este problema se encuentra en el año 2009 con la publicación del Bitcoin P2P e-cash paper (Nakamoto, 2009). Este documento divulgado por el autor todavía no identificado conocido como Satoshi Nakamoto supuso el origen de las criptomonedas, y la creación protocolo necesario para el manteniendo de un sistema de registro de operaciones descentralizado, conocido como Blockchain (Nakamoto, 2009). El Bitcoin tendrá que esperar para nacer efectivamente al año 2011, tras la creación del primer bloque de operaciones, conocido como bloque matriz, que sustenta su sistema de registro, y con el establecimiento de sus primeros nodos, que eran los hardware que permitía funcionar el sistema compartido. A partir de entonces entrará en funcionamiento, y supondrá como inspiración para el resto de criptodesarrolladores.

Este libre de registro que significa una criptomoneda tiene una característica muy interesante que se relaciona con la teoría económica que se ha revisado. Este concepto se parece mucho a la imagen que tenía Mises del dinero. Los saldos positivos de estos libros

de registros constituyen la cantidad de criptomonedas que se pueden enviar y utilizar, por tanto, acaban siendo dinero bajo la mirada teórica de Mises (1912) .

Esta nueva forma de transmitir la información y de asegurar su contenido, es el espacio en el que la tecnología Blockchain puede tener una mayor incidencia en el sistema monetario. Adaptándose a las múltiples dimensiones del dinero, el protocolo Blockchain ha permitido la creación de las criptomonedas, activos digitales que conforman redes de almacenamiento de transacciones de información. Esta información transferida no son únicamente transacciones de unidades monetarias respaldas por balances positivos en la red, sino que también pueden abarcar contratos, documentos y una gran variedad de archivos digitales (Swan, 2015).

2.1.3 Las redes distribuidas y el problema de los bizantinos

Para el comienzo de la era de internet el único método para desarrollar registros de transacciones accesibles para varios miembros era que uno de los miembros participantes en la red de transacciones se encargara del mantenimiento de la base de datos que contenía de la información del registro. Además, este miembro tenía que proveer conexión a la base de datos al resto de miembros. Es por esto por lo que se tenían que constituir bases de datos privadas para el almacenamiento de esta información (Nakamoto, 2009). Este hecho llevaba a que la información fuera susceptible de robo y modificación en caso de ataque a la red que contuviera la base de datos privada, además de no proporcionar ninguna garantía de veracidad y consenso de los datos.

El primer paso para solucionar el riesgo de las bases privadas y la asimetría de información y consenso entre los miembros de las redes compartidas se tomó con la creación de la compañía Napster, pionera en el desarrollo de las redes distribuidas que funcionaban con tecnología *Peer to peer (compañero a compañero* a partir de ahora referido como P2P). Este tipo de redes están conformadas por varios miembros en constante comunicación que soportan y almacenan los datos de la red de manera distribuida (Buterin, 2013). Este nuevo modelo permite que el peso del almacenamiento no recaiga únicamente en un miembro, y además evita que la capacidad de adición y edición no sea un privilegio exclusivo del miembro encargado del almacenamiento de la base de datos.

No obstante, estas redes distribuidas tienen que afrontar un obstáculo considerable como es el representado por el juego mental del problema de los generales bizantinos (Pérez-Solà & Herrera-Joancomartí, 2014). El problema de los generales bizantinos es una alegoría utilizada en informática para explicar una situación análoga a la que se puede afrontar en estas redes. Este problema expone una situación hipotética en la que el ejército Bizantino, comandado por un grupo de generales repartidos por el campo, está asediando una ciudad. El problema de esta situación planteada es que los generales quieren acordar la estrategia más eficiente para alcanzar los objetivos y que todos se ven obligados a seguir, sin embargo, cabe la posibilidad de que haya generales corruptos cuyos intereses sean opuestos al de los otros generales, y que modifican la información para que no se alcance el consenso necesario con el que acordar la estrategia que consiga los objetivos (Schwartz, Youngs, & Britto, 2014). Este problema es muy común en las redes distribuidas donde los miembros, nodos, son los generalas y para que estas redes sean públicas es necesario desarrollar un sistema que permita alcanzar el consenso entre miembros rápidamente y que asegure su veracidad. Esto se consiguió con la creación del protocolo Blockchain que se explica a continuación (Pérez-Solà & Herrera-Joancomartí, 2014).

2.2. La Blockchain como piedra angular del sistema

La Blockchain, cadena de bloques en español, es la tecnología que ha permitido el desarrollo de las criptomonedas y la creación de libros de registro públicos mediante redes distribuidas públicas (Nakamoto, 2009). Esto se debe a que ha provisto la solución al problema de los Generales Bizantinos. Esta solución se encontró en el mismo documento que dio nacimiento al bitcoin, que fue el primer documento en llamarla Blockchain.

La importancia de la Blockchain es que supone el primer protocolo de seguridad para las redes distribuidas. El problema de los bizantinos había sido la mayor inseguridad en estas redes ya que la información que recibías podía tener peligro de ser maliciosa, no obstante, la Blockchain propone una serie de normas que permiten el funcionamiento de la red a la vez que proveen seguridad a las transacciones en ella (Schwartz, Youngs, & Britto, 2014). Se podría decir que la Blockchain es el código de Hammurabi de las redes distribuidas ya que establece unas maneras de actuar para asegurar la seguridad y el funcionamiento de

las redes distribuidas, de la misma manera que lo haría un sistema legislativo en una sociedad colectiva.

En las redes distribuidas que utilizan la tecnología Blockchain, cada dueño de un dispositivo de la red, conocido como nodo, se encarga de almacenar todo el registro y de verificar e introducir las transacciones ocurridas en la red. Los nodos verifican que las transacciones realizadas se hacen acorde a los requerimientos de seguridad de la red según, lo previsto por su Blockchain, y que se disponen de fondos suficientes para hacer la operación, y así evitar el problema de doble gasto (Buterin, 2013). Una vez verificadas las operaciones, estas son agrupadas en bloques de transacciones que son introducidas en el registro público por estos nodos. Este proceso se conoce como minado, y a parte de un mecanismo de seguridad, constituye el medio de acuñación de la mayoría de las criptomonedas (Nakamoto, 2009). La emisión de nuevas monedas se produce para recompensar a los nodos por su trabajo de verificación ya que cada transacción incluye una tasa por parte de los participantes además de una recompensa del sistema por cada bloque minado (Nakamoto, 2009). Debido a este proceso de verificación y agrupación en bloques es por lo que esta tecnología en castellano se conocería como la cadena de bloques. Esta cadena se caracteriza por su resistencia gracias a tres mecanismos de seguridad informática desarrollados en el documento de Nakamoto.

El primer mecanismo que permite la invulnerabilidad del sistema son las referencias necesarias del encabezado. Cada bloque ha de incluir entre su información, a parte de las transacciones, un encabezado para así asegurar que el bloque es genuino. Este encabezado tiene que contener una referencia a los bloques que le preceden, que además también tiene que estar encriptada (Buterin, 2013). Este mecanismo permite que, en caso de introducir un bloque maligno no genuino del sistema, sea necesario desencriptar y conocer todos los bloques que conforman el registro de transacciones. Esta encriptación de las referencias a los bloques anteriores se realiza a través del segundo mecanismo de defensa, que es el cifrado mediante tecnología Hash. Como ya se revisó previamente, Hash es un método de encriptación pseudo-aleatorio que permite que archivos de tamaño variable sean encriptados en archivos de un tamaño constante. Finalmente, el tercer mecanismo de seguridad es el *proof of work* que ha sido mencionado previamente en la sección 2.1. 2.. Este último mecanismo asegura que en caso de que un miembro tenga un poder excesivo en la red le será más difícil introducir un bloque en la red.

Por lo tanto, una vez revisados el contexto tecnológico y la tecnología que permite el funcionamiento de las criptomonedas, se va a realizar una revisión de cómo es el sistema criptomonetario actual.

2.3. Ecosistema criptomonetario

Cabe destacar que en la terminología actual criptomoneda es todo aquel activo digital transmisible en una red distribuida y desarrollada mediante Blockchain (White, 2015). Sin embargo, dentro de esta clasificación encontramos una subdivisión de criptomonedas dependiendo de su función. Encontramos las Altcoins (monedas alternativas), que son aquellos activos digitales que cumplen con la triple función del dinero, y han sido creadas tras el Bitcoin, y los Token, que son criptomonedas que representan a un activo físico en forma de bien o servicio (Narayanan & Miller, 2017).

El Bitcoin supuso la aparición de la primera criptomoneda, y su sistema de registro de operaciones, la Blockchain, ha supuesto una tecnología revolucionaria para la transmisión y almacenamiento de información en forma de activos digitales y el mantenimiento de redes distribuidas descentralizadas. La reinterpretación de esta tecnología a través potenciar distintas características de los activos digitales que se pueden transmitir a través de la red es lo que ha dado origen a la expansión de los distintos tipos de criptomonedas, conocidas como Altcoins (Buterin, 2013). Estas variaciones en el código utilizado para programar la Blockchain permite que haya una riqueza de redes criptográficas de naturaleza tanto pública como privada, y con divisas de características diferentes. Generalmente, las variaciones del uso de la Blockchain se han centrado en potenciar distintas funcionalidades, pero son las transacciones de activos digitales y el soporte de plataformas autónomas descentralizadas las principales funciones que se han explotado. Además, la titularidad de los nodos, o servidores que verifican las transacciones de información, puede tener distintas personalidades.

2.3.1 Tipos de redes

Redes de transacciones

La creación y soporte de una red transacciones de activos digitales que cumplen con las funciones del dinero es la ocupación original la tecnología Blockchain, y, por tanto, Bitcoin es el principal ejemplo (Extance, 2015). En este tipo de redes distribuidas, la programación de la Blockchain sigue un propósito único, que es constituir un libro de registro público para las operaciones en la red (Larsen & Thomas, 2018). Originalmente, este tipo de redes distribuidas son públicas y, por tanto, el acceso a la información es libre desde los servidores o nodos, donde dicha información está almacenada. No obstante, en la actualidad se han desarrollado nuevos tipos de redes que, aunque distribuidas, la propiedad de los servidores no es pública y la información contenida no es libremente accesible.

Por tanto, estas criptomonedas son las que más puramente suponen divisas virtuales, ya que la utilidad de los activos digitales que circulan en la red es la de proveer una unidad monetaria que permita una función de cambio a los miembros con un valor numérico determinado. En este tipo, la acuñación suele tener un volumen controlado. Dentro de esta clasificación encontramos a varias de las criptomonedas que actualmente gozan de mayor capitalización de mercado, entre las que destacan Bitcoin(BTC), Bitcoin Cash (BCH), Litecoin (LTC), Monero (XMR) y Dash (DASH). Las principales diferencias que existen dentro de este grupo se encuentran con respecto al tipo y cantidad de información que es accesible acerca de las operaciones y los titulares de estas. En este tipo de redes la aceptabilidad del activo digital, criptomoneda, como medio de pago es fundamental, ya que es una condición necesaria para que se considere como un buen medio de cambio indirecto (Mises, 1912).

La primera modificación que vio el código de Blockchain ha sido aquella que ha permitido la creación de redes de transacciones de información, en la que los activos digitales no cumplían únicamente el rol de función de cambio que tiene el dinero, sino que transmitían otro tipo de información. En este tipo de redes distribuidas la estructura puede ser tanto pública como privada, y el tipo de activo digital es heterogéneo. Uno de los primeros ejemplos de este tipo fueron Namecoin y Colour Coin, que permitían un registro de los diversos nombres y colores en forma de activo digital (Buterin, 2013), para así conseguir un consenso universal e inmutable sobre el derecho a un nombre o las

características de un color. No obstante, la principal modificación que ha habido en estos activos digitales ha sido en el área de las transacciones. Se han desarrollado nuevas redes que permiten una mayor apertura a sistemas externos a la red, siendo el ejemplo más usado el de a sistemas de transacciones con divisas fiduciarias. Este ejemplo es el de Ripple (XRP) y Stellar (lumens), que han creado redes en las que los activos digitales que se intercambian representan operaciones financieras bancarias, las cuales pueden agrupar en mayores volúmenes y así reducir las cuotas de intermediación (Swan, 2015). En este caso al ser provisto un servicio de transacción de activos digitales no monetarios, existen dos tipos de activos digitales, aunque solo una criptomoneda. Un activo digital se encarga de ser el vector de transmisión de información dentro de la red, mientras que el segundo activo, el cual cae en la consideración de criptomoneda, se utiliza para retribuir los servicios recibido (Schwartz, Youngs, & Britto, 2014). En este sistema, el activo digital utilizado para el pago de servicios es el que tiene un valor tangible ya que está altamente correlacionado con el valor del servicio prestado.

Redes de plataforma y tokens

Dentro de esta categoría incluimos a las criptomonedas que forman parte de redes distribuidas para el soporte de Organizaciones Autónomas Descentralizadas (Wood, 2017). En este tipo de sistema el código de la Blockchain está programado para permitir el diseño y soportar plataformas autónomas creadas por terceros en base a la tecnología de la red, y proporcionar un funcionamiento autónomo, personalizable y seguro. Por ello, este tipo de redes desarrollan un código base con varias características que se pueden potenciar de diversas formas, dependiendo de las preferencias individuales. Este nuevo tipo de redes además de permitir la función de cambio del dinero, han instaurado un nuevo concepto criptográfico que son los contratos inteligentes (Hirai, 2017). Los denominados contratos inteligentes son activos digitales para la transferencia de datos entre miembros de la red, pero que no cubren únicamente la función de cambio de divisas virtuales, sino que permiten crear contenidos interactivos en los que se puedan transmitir distinta información como pudieran ser contratos legales o financieros, derechos sobre servicios, como es el mantenimiento de una red construida sobre una plataforma (Narayanan & Miller, 2017).

En este tipo de red, la criptomoneda juega un papel dual. Además de ser una función de cambio para realizar transacciones con divisas virtuales, también suponen el medio de pago de los servicios que proporciona la red a través de contratos inteligentes. Por tanto,

el valor de estas criptomonedas no se basa únicamente en el valor consensuado que tiene como función de cambio y su aceptabilidad, sino que se tiene en cuenta el valor de los servicios de mantenimiento de redes que se puede obtener a través de ellas (Arsov, 2017). Dentro de esta categoría, la red que tiene mayor preeminencia es Ethereum y su ciptomoneda Ether (ETH), pero también son destacables la red EOS y su criptomoneda EOS, NEO y su criptomoneda NEO o Cardano y su criptomoneda ADA.

El hecho de que este tipo de redes con función de plataforma permitan la creación de nuevas redes para organizaciones autónomas descentralizadas, hace que aparezca un nuevo concepto criptográfico, el token. En estas nuevas redes no son necesarios activos digitales para su funcionamiento porque esta red está soportada por la red de la plataforma que realiza las operaciones mediante la altcoin original, que podría ser Ether, EOS o NEO por ejemplo (Atzei, Bartoletti, & Cimoli, 2017). No obstante, estas nuevas redes dentro de los servicios provistos por la plataforma gozan de la capacidad de creación de criptomonedas conocidas como Tokens. Estos Token tienen una relación directa con la actividad de la empresa emisora, y suelen ser derechos sobre bienes o servicios, con la característica necesaria de ser consumibles e intercambiables. El valor de estas criptomonedas está muy relacionado al valor subjetivo del servicio o activo con el que está relacionado.

2.3.2 Propiedad de las redes

Finalmente, es necesario comentar que la titularidad de los nodos, o servidores, que mantienen la red también representa una característica para diferenciar criptomonedas. La propiedad de estos nodos puede darse principalmente en tres formas; pública, privada y federada (BlochainHub, 2018).

Los nodos de propiedad pública implican que cualquier persona puede entrar a formar parte de la red en la forma de nodo, y por tanto realizar funciones de verificación de operaciones y de almacenamiento del registro público, así como incluir nuevos elementos y acceder a anteriores (Nakamoto, 2009). Este es el tipo de red que más se ha establecido en la actualidad, y se caracteriza normalmente por ser de código abierto, es decir, que es de conocimiento público el código que permite la programación y funcionamiento de esta red. Este tipo de red es la que más tiene que afrontar el problema de los generales

Bizantinos, por lo que la aplicación de los protocolos proof-of-work está muy extendida lo que provoca que el tiempo de procesamiento y verificación de transacciones sea mayor y no escalable (Schwartz, Youngs, & Britto, 2014).

Las redes federadas son aquellas en las que una organización se la encargada de llevar a cabo el liderazgo de la red, y por tanto goza de la capacidad de elección de los miembros que forman parte de la red y son encargados de la verificación de transacciones. Esta característica implica que la entrada de miembros está limitada, pero sigue siendo abierta a otras organizaciones que pasen los filtros necesarios para asegurar la integridad de la red (BlochainHub, 2018). Este tipo de redes son mejores para afrontar el problema de los Generales Bizantinos ya que al estar controlado el acceso a la condición de nodo verificador, un menor nivel de consenso es necesario y goza de mayor escalabilidad y privacidad que en las redes públicas. Este es el caso de las redes Stellar, Corda o R3.

Finalmente, existe el caso de las redes privadas. En este caso el propietario del hardware que compone los nodos encargados de la verificación es único, y por tanto posee derecho de adición sobre la Blockchain (BlochainHub, 2018). La identidad Blockchain de estas redes están abiertamente cuestionada, sin embargo, el desarrollo de un registro distribuido es la base de su funcionamiento a pesar de que sea privado. Aunque la adición sea de carácter privado, el acceso a los componentes del registro distribuido suele ser libre a través de los medios dispuestos por el poseedor de la red. Esta red, aunque sea distribuida se enfrenta a los mismos riesgos que una base de datos privada, y es que si se consigue vulnerar su seguridad todos los datos del registro son susceptibles de modificaciones y sustracciones. No obstante, esta red tiene una mayor escalabilidad que cualquier otra y permite un mayor cumplimiento de las legislaciones en materia de protección de datos.

III. Estado de la cuestión. Criptomonedas como complemento y/o alternativa de divisas fiduciarias

Una vez revisados los principales conceptos acerca del sistema monetario y de las criptomonedas, es hora de comenzar a revisar la idoneidad de las criptomonedas para formar parte del sistema monetario.

Durante el año 2017 y comienzos del 2018 se ha producido la expansión de la capitalización y cotización de mercado de las criptomonedas que ha conseguido atraer el foco mediático sobre ellas, a la vez que ha empezado un debate acerca su papel futuro en la sociedad. Este nuevo debate ha producido una gran cantidad de literatura acerca del futuro rol de las criptomonedas, y esta sección se encargará de la revisión de esta literatura gracias a los conceptos económicos y criptomonetarios previamente considerados. Esta revisión la llevaré a cabo teniendo en cuenta los dos escenarios más probables y populares que han trazado los principales autores.

El primer escenario que se considerará será la situación en la que el estatus legal de las criptomonedas se consolide como una mercancía digital, no como divisa, con valor dado por los mercados, pero sin ninguna función monetaria respaldada por una personalidad jurídica soberana. Mientras, el segundo escenario sería aquel en el que la tecnología criptomonetaria se adapta a las estructuras monetarias actuales, permitiendo así la digitalización de la divisa. Este último escenario ya ha sido desarrollado por algunos autores.

1. Situación actual de las criptomonedas en el sistema económico y financiero:

El primer escenario constituye el más probable viendo la tendencia actual de los sucesos y regulaciones que conciernen a las criptomonedas. Este escenario es la continuación de la situación actual en la que las criptomonedas mantienen el estatus legal de mercancía. Esta mercancía puede constituir un medio de pago en especia, cuya aceptación depende de los agentes del mercado, pero sin ningún respaldo institucional para garantizar y estabilizar el poder adquisitivo de estas criptomonedas. Este medio de pago se considera pago en especia de acuerdo los cánones sociales ya que todo pago en mercancías no monetarias fiduciarias es considerado como tal (Menger, 1892). Sin embargo, siguiendo la concepción austríaca del dinero como una construcción social y no estatal, este

producto o activo se considera dinero en cuanto se use como medio de intercambio indirecto (Mises, 1912).

Este escenario se caracteriza por ser un paralelismo de la situación teórica pre-monetaria planteada por Mises en su obra dado que existen una gran variedad de activos, criptomonedas, con distintos poderes adquisitivos (Mises, 1912). Siguiendo la teoría de Mises, la tendencia en este sistema criptomonetario es la eliminación de esta variedad de activos que cubren la función del dinero. Aunque Mises menciona este proceso como necesario para la elección de un medio de pago universal, también comenta que realmente este proceso históricamente se ha dado para dos activos, la plata y el oro, de características similares pero que ninguna ha llegado a imponerse totalmente sobre la otra. No obstante, como hemos visto en la sección de los tipos de criptomonedas, algunos de esos activos a parte de tener un valor como medio de intercambio también tienen un valor que corresponde a los servicios por los cuales se puede canjear.

Este proceso de eliminación y elección de los distintos medios de pago se está dando en la actualidad entorno al Bitcoin y Ether. Ambas monedas son los principales medios de pago para la obtención del resto de criptomonedas en los diferentes sitios de intercambio, y además gozan de poder adquisitivo sobre algunos bienes y servicios. Al mismo tiempo, también representan a la perfección los tipos de altcoins que están surgiendo en el ecosistema criptomonetario. El Bitcoin representa una criptomoneda de un sistema de transacciones mientras que Ether es un tipo de altcoin de un sistema de soporte de plataforma. Sin embargo, ambas criptomonedas no se pueden considerar consolidadas ya que existen una gran variedad de criptomonedas de sistemas de transacciones y de soporte de plataformas con distintas características y cuyo uso era desconocido, pero va en incremento.

En este proceso de elección de medios de pago no entraría las altcoins consideradas como tokens ya que su naturaleza se ajusta más a un medio de pago diferido por el cual se obtiene un derecho sobre un servicio futuro a través de la adquisición de estas criptomonedas. Aunque es cierto que pueden cumplir la función de dinero, al igual que todo activo portable, divisible y perenne, sus características no están orientadas hacia esa función.

La situación actual permitiría la existencia y expansión de medios de pagos descentralizados e independientes de instituciones y regulaciones financieras, con las que

coexistirían. Es por ello, que en este contexto podríamos encontrar tanto oportunidades y ventajas como limitaciones y barreras.

1.1 Oportunidades y ventajas

1.1.1. Cualidades similares al dinero

La primera y principal ventaja de este escenario que podemos encontrar es la adaptación de estos nuevos activos digitales al concepto de dinero. Esta adaptación la podemos concluir gracias al análisis de los conceptos monetarios y criptomonetarios realizados en el apartado del Estado del Arte. Esta adaptabilidad permite que se pueda alcanzar el objetivo original de las criptomonedas desde su concepción, que es el establecimiento de un sistema de pagos descentralizado y autónomo. Este sistema descentralizado permitiría que las variaciones en el valor y poder adquisitivo de los medios de pago respondiera únicamente a los mecanismos de la oferta y la demanda, además de una oferta monetaria conocida, endógena y previsible. Asimismo, apoyándome en las conclusiones del trabajo "Emergence and Estability of Key Currencies in Artificial International Trade" (Yamashita, Kurumatani, Sasaki, Kawamura, & Ohuchi, 2005), se puede concluir que un sistema económico abierto y con agentes financieros independientes permite la emergencia de divisas internacionales y a la estabilización de los valores de las mismas, permitiendo así la obtención del medio de pago único concebido por Mises.

Además, aunque por su naturaleza las criptomonedas puedan ser estancas ya que sus sistemas no compatibles entre sí directamente se han desarrollado softwares para la creación de sitios de intercambios. El mayor ejemplo es Opentransactions el cual provee un software para la creación de un lugar de almacenamiento de criptomonedas que a la misma vez agiliza la convertibilidad entre ellas (Opentransactions), a parte también existen varios mercados privados para intercambio. Por tanto, este nuevo sistema de pagos descentralizado y compuesto por distintas unidades monetarias podría ser la respuesta para el dilema de Triffin porque abre la posibilidad de que las criptomonedas ocupen el papel de reserva mundial.

1.1.2. Reserva de valor

La siguiente ventaja que mencionar es que podrían llegar a alcanzar el estatus de activos refugio y de reservas de valor. El primer ejemplo de una moneda cubriendo esta función se vivió en el año 2013 con el comienzo de la crisis bancaria de Chipre. Tras el inicio la crisis, que provocó la congelación de los depósitos y la prohibición de retiradas de efectivos, hubo una inversión considerable en bitcoin desde la isla mediterránea y otras zonas con riesgo potencial de bancarrota de sus sistemas financieros, como España y Grecia (Cohan, 2013). Esta inversión aumentó un 20 por ciento el valor del Bitcoin en solo la semana pasada y un 41 por ciento en un mes (Cox, 2013). Este hecho, aunque sea un argumento a favor, se puede considerar un caso aislado ya que el valor del bitcoin ha sido muy fluctuante y su capacidad para mantener valores estables ha sido limitada (Gangwal & Longin, 2018), es por ello que de momento no cumple las condiciones aunque tenga potencial como activo refugio y reserva de valor (Bouri, Molnár, Azzi, Roubaud, & Hagfors, 2016).

1.1.3. Sustitutivo monetario

Un apartado de la política monetaria en el que las criptomonedas pueden suponer un salto cualitativo es en la sustitución monetaria. La sustitución monetaria es el fenómeno que se produce en un estado cuando la demanda de divisas extranjeras por parte de los residentes locales ya no está ligada a los requisitos de comercio exterior y transacciones, sino que se usa como una reserva de valor e incluso como el medio de intercambio local (Calvo & Végh, 1992). Por ello, la sustitución monetaria generalmente afecta a la composición de los depósitos y en ocasiones al dinero circulante, por lo que suele suponer una reducción del agregado monetario M1 (Hsing, 2007). El agregado monetario M1 representa todas las unidades monetarias físicas y los depósitos en una economía (Banco de España). La sustitución monetaria ha sido muy común en países de Latinoamérica, África, Asia y Europa de este, especialmente en los países con altos niveles de inflación y pocas garantías políticas. Un ejemplo es el caso de la hiperinflación de Zimbabue (Noko, 2011), siendo esta sustitución monetaria efectuada a través del dólar, conocida como dolarización. Normalmente es una consecuencia de una mala política monetaria, especialmente cuando un gobierno trata de financiar sus déficits comerciales a través de

la inflación (Elkhafif, 2003), y lleva a los ahorradores a una situación de depreciación sistemática de sus depósitos en divisa nacional, que se reducen, y aumentan aquellos en una divisa extranjera. Esta situación conlleva una serie de efectos negativos como son aumento en el déficit de la balanza de pagos, la pérdida de capacidad para reaccionar a shocks exógenos y el debilitamiento del sistema financiero excesivamente expuesto a pánicos bancarios y producir una profunda crisis bancaria (Calvo & Végh, 1992).

No obstante, aunque la sustitución monetaria tiene efectos negativos, estos no son más que la continuación de los efectos negativos de las malas prácticas que han llevado a una economía a ese punto. Por tanto, la sustitución monetaria se puede concebir como un fenómeno con efectos positivos. El hecho de que haya sustitución monetaria permitida ayuda a los ciudadanos a sortear los problemas de la inflación rampante de su economía nacional (Calvo & Végh, 1992), y acentúa las malas prácticas del gobierno. Revisando la literatura acerca de este hecho se concluye que la única solución para revertirla a largo plazo es la mejora la productividad y de la competitividad de la economía, que en última instancia reducirá la presión sobre la moneda doméstica de la depreciación y traerá la estabilidad requerida a la economía (Elkhafif, 2003). En consecuencia, la existencia de una divisa virtual descentralizada y fácil de transmitir, como algunas criptomonedas, puede ser en los países con inestabilidad una alternativa fiable para el ahorro y el intercambio de la manera que M-PESA lo está siendo en África subsahariana (Jack, Suri, & Townsend, 2010), la cual es tan utilizada como la divisa fiduciaria.

1.1.4. Orientación pro-negocio

Finalmente, es importante mencionar la orientación hacia el negocio. Ya ha sido mencionado previamente que muchas criptomonedas pertenecientes a redes federadas y redes privadas se caracterizan por no ser descentralizadas y adoptar la tecnología Blockchain para desarrollar herramientas pro-negocio, especialmente para el sector FinTech (Larsen & Thomas, 2018). No obstante, las criptomonedas pertenecientes a redes descentralizadas suponen una herramienta muy útil. Todas las criptomonedas pertenecientes a redes de mantenimiento de plataformas tienen como objetivo el pago diferido de servicios (Buterin, 2013), e incluso algunas redes de transacciones son útiles para el desarrollo de negocio. En el artículo “Reputation and Reward: Two Sides of the

Same Bitcoin" (2016)se expone como el bitcoin por su descentralización puede permitir una mayor velocidad para el pago de incentivos a usuarios que proveen información a determinados negocios. Asimismo, la tecnología Blockchain tiene una gran utilidad para el establecimiento de bases de datos distribuidas de mayor seguridad y menores cuotas por uso que permiten que mecanismos como la custodia de activos en una operación de transacción necesite menos intermediarios y tiempo de ejecución (Micheler, 2015).

También, las tokens se han convertido en una gran herramienta para financiar actividades y evitar canales financieros típicos (Hacker & Thomale, 2017). La emisión de tokens con los que se puede adquirir servicios prestados por la empresa emisora o bienes permite que se produzca la posibilidad de adquirir derechos sobre estos servicios por adelantado. Funcionan como una especie de contrato de futuros sobre servicios o bienes que permite cobrar por ellos sin haberlos prestado y haber incurrido en el coste. Esta característica permite tener mayor flexibilidad en algunos negocios ya que pueden adelantar cobros de servicios potenciales que se pueden llegar a prestar o no. Muchos de los compradores pueden ser inversores que esperan que el servicio o bien que se ofrece a cambio se revalorice, y por tanto se obtenga un beneficio inmediato sobre una obligación opcional. En esta función tienen un papel importante las Emisiones Iniciales de Moneda (Initial Coin Offering en inglés, a partir de ahora mencionado como ICO) en las que se venden grandes cantidades de tokens para afrontar los primeros pasos de la actividad de las empresas emisoras. En el año 2017 las ICO emitidas alcanzaron un valor de 3.000 millones de dólares (Hacker & Thomale, 2017).

1.1.5. Efectos positivos sobre la teoría cuantitativa

Como hemos comentado al principio del marco teórico, el funcionamiento de la teoría cuantitativa al corto plazo es un foco de discusión entre los economistas teóricos. El principal punto de discusión es la velocidad del dinero. La escuela de Chicago afirma que la velocidad es constante y que nunca varía, pero los economistas Keynesianos proveen una ecuación propia para el cálculo de la velocidad, la cual consideran que es variable.

Fuera de debates teóricos acerca de su naturaleza, la velocidad del dinero se considera como la velocidad a la que se intercambia el dinero de una transacción a otra. También se refiere a cuánto se usa una unidad de moneda en un período de tiempo determinado.

Básicamente, es la velocidad a la que las personas gastan dinero. Actualmente la velocidad del dinero se calcula en base al Producto Nacional Bruto, que es un agregado económico que incluye todas las transacciones realizadas en un Estado.

La creación de un registro público de transacciones puede ser una herramienta de utilidad vital para calcular la velocidad del dinero ya que va a permitir tener acceso a todas las transacciones individualizadas. Este hecho permitirá que no sea necesario utilizar agregados económicos que al acumular un gran volumen de información de distinta naturaleza puede incurrir en sesgos.

1.2. Limitaciones

Los beneficios, aunque obvios, se encuentran con una serie de limitaciones que actualmente están desequilibrando la balanza en contra de las criptomonedas. Estas limitaciones no se reducen únicamente al área técnica, sino que abarcan distintas dimensiones por la complejidad socioeconómica del dinero, cuya función quieren abarcar.

1.2.1. Limitaciones económicas

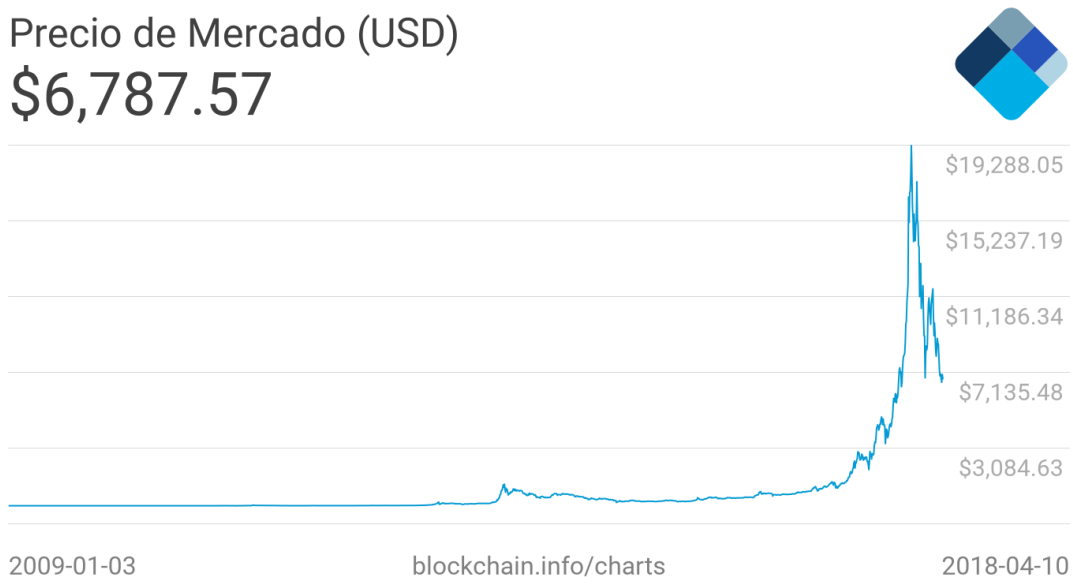
Dado a que el dinero tiene una posición central en la sociedad actual, más aún tras la definitiva imposición de la economía de mercado en la mayoría de los estados en la década de 1990, los obstáculos económicos que ha de superar se presentan como fundamentales para su éxito.

El primer obstáculo que habrá de considerarse es la excesiva fluctuación y consiguiente volatilidad del valor de las criptomonedas. Para analizar la volatilidad, la literatura disponible está limitada hasta el año 2017, el cual ha sido el más volátil de su historia, y refleja que la volatilidad de las cotizaciones y los volúmenes de negocio son excesivos hasta este año. (Bouri, Molnár, Azzi, Roubaud, & Hagfors, 2016) , (Gangwal & Longin, 2018) y (Gandal & Halaburda, 2016) analizan las variaciones que ha habido en los precios de las principales criptomonedas en el periodo de tiempo comprendido entre 2010 y 2016, en el caso de (Gandal & Halaburda, 2016) hasta 2014. Durante este periodo se ha producido un alta volatilidad (Gangwal & Longin, 2018) y efectos de red, lo que implica

que la volatilidad afecta a todas las criptomonedas por su correlación positiva (Gandal & Halaburda, 2016), siendo la media de la volatilidad del periodo un 6% (Hafner, 2018).

Es importante tener en cuenta que el año 2017 ha sido el año en el que la capitalización de mercado y el volumen de operaciones de las criptomonedas más ha subido en su corta existencia. Aunque no se vaya a hacer un tratamiento estadístico de los datos, como en los trabajos mencionados, se ve necesario hacer referencia a los datos actuales de cotización y volumen de transacciones. Es por ello por lo que se presentarán dos gráficas correspondientes con la evolución del valor y del volumen de transacciones del Bitcoin con respecto al dólar, ya que es la criptomoneda más representativa del mercado al suponer el 43,3% de la capitalización total y el 35,1% del total del volumen de transacciones para abril de 2018.

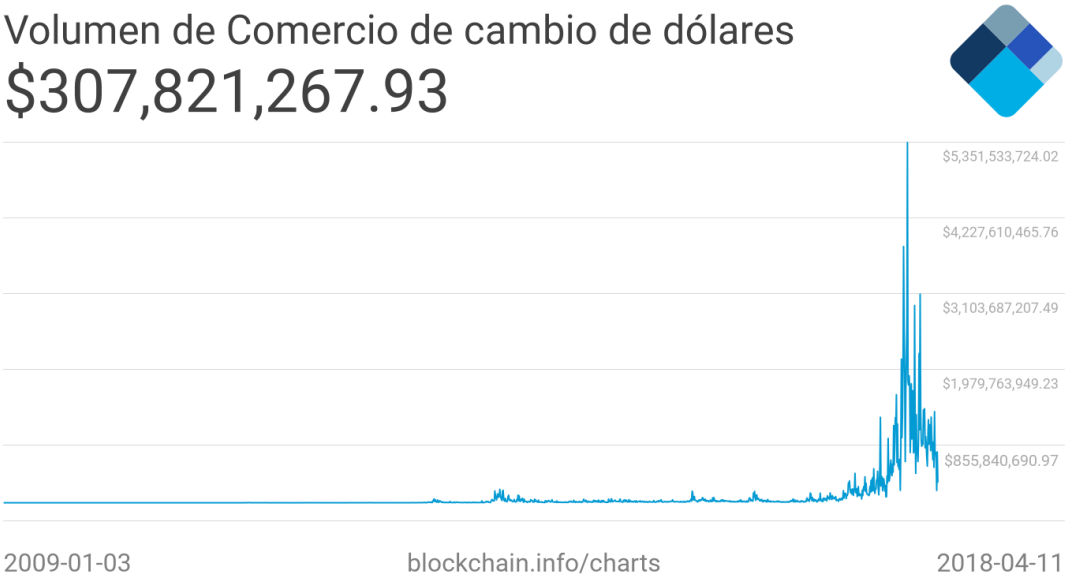
Gráfico I: Cotización de mercado del Bitcoin con respecto al USD



Fuente: www.Blockchain.info/charts

En este gráfico podemos comprobar que el valor actual del Bitcoin con respecto al dólar es de 6.787,57 $, mientras que el día 16 de diciembre era de 19.499 $, una caída del 65% del valor de diciembre en solo cuatro meses. Los datos sobre el volumen de negocio también son muy representativos para ver la inestabilidad del Bitcoin. Su volumen de transacciones ha pasado de 5.351.533.724,02 $ en su pico de diciembre a 307.821.267,93 $ para el 11 de abril. Este dato es muy ilustrativo para comprobar el carácter especulativo del Bitcoin durante su periodo de máxima cotización.

Gráfico II: Volumen de comercio de Bitcoin



Fuente: www.Blockchain.info/charts

Previamente se ha mencionado que esta volatilidad excesiva es el mayor impedimento que encuentran las criptomonedas para su consideración como activo refugio (Bouri, Molnár, Azzi, Roubaud, & Hagfors, 2016) y como reserva de valor (Gangwal & Longin, 2018), lo cual resulta una gran limitación para que las criptomonedas puedan jugar un papel importante como medio de pago y como medio de sustitución monetaria.

Además, estas excesivas fluctuaciones no permiten que de momento sean un medio de pago fiable ya que implica una actualización constante de los precios de aquellos bienes y servicios intercambiables por ellas. Este es un impedimento considerable si tenemos en cuenta la importancia que tienen las proyecciones presupuestarias en el mundo empresarial, especialmente en las empresas que cotizan en el mercado de valores. Un ejemplo de cómo esta excesiva volatilidad del valor de las criptomonedas puede llevar a su no aceptación por negocios es el caso de Steam, uno de los pioneros en aceptación de Bitcoin como medio de pago. Esta empresa de videojuegos retiró Bitcoin como medio de pago en diciembre de 2017 tras la alta volatilidad en el valor de Bitcoin, siguiendo el ejemplo de Stripe y Microsoft que la habían abandonado durante el año 2017 (Rapoza, 2018).

La última limitación económica por mencionar es la posible reducción de los ingresos por señoreaje de las organizaciones emisoras de las monedas fiduciarias por la reducción de

su uso. El señoreaje es la diferencia entre el valor nominal de la divisa emitida y su coste de producción. Estos ingresos por señoraje suponen una parte considerable de los ingresos de las instituciones financieras encargadas de la emisión de divisas y en casos de sustitución monetaria, como a la que aspiran las criptomonedas, supondría una reducción de los ingresos derivados de la política monetaria, necesarios para el mantenimiento del sistema fiduciario.

1.2.2. Limitaciones Sociopolíticas

Una vez revisadas las limitaciones que se puede encontrar la implantación de las criptomonedas en el plano económico es necesario revisar las que se puede encontrar en el plano sociopolítico. Esta dimensión sociopolítica vale la pena ser revisas debido a que como menciona Mises el dinero es una construcción social, y la política se puede considerar todo aquello que envuelve los mecanismos de organización social.

En el plano social uno de los primeros hechos que nos podemos encontrar es la dificultad para la adaptación de las nuevas tecnologías en la sociedad. Dado que tanto las criptomonedas como la tecnología que permite su uso son innovaciones con una vida relativamente corta, su uso y entendimiento todavía se encuentra limitado. Esta falta de asimilación puede correr en su contra ya que como hemos resaltado, el dinero es una construcción social y por ende depende de la sociedad para su funcionamiento. Sin embargo, como se ha comprobado con anteriores innovaciones revolucionarias, la adaptación a las nuevas tecnologías no sueles suponer una barrera infranqueable. Previamente se había mencionada a M-Pesa como un ejemplo de éxito de un medio digital de pago (Jack, Suri, & Townsend, 2010). M-Pesa es una empresa africana de telefonía que permite a sus usuarios almacenar cantidades monetarias en un balance propio y disponer de sus saldos para hacer frente a los pagos. El triunfo de esta iniciativa se puede considerar como un argumento a favor del posible triunfo de las criptomonedas para su uso. Saliendo de los medios de pago otros ejemplos pueden ser traídos para comprobar como la adaptación de nuevas tecnologías no es tan traumática para la sociedad, como podría ser el caso de Estonia (Björklund, 2016). Estonia, una antigua república soviética independizada tras la caída de la URSS, ha conseguido alcanzar una completa digitalización de la estructura estatal y de los procesos.

Otro hecho social que puede tener incidencia en el uso de las criptomonedas es su actual estigmatización como medio de pago clandestino y para actividades ilícitas. Esta

concepción sobre las criptomonedas está muy extendida actualmente y una prueba de ello es la declaración del CEO de J.P. Morgan Chase, Jamie Dimon, afirmando que considera las criptomonedas más como un medio de pago para actividades ilícitas que como una alternativa fiable (Hackett, 2018). Esta creencia viene del hecho de que en las transacciones de criptomonedas el origen y el destino de las transacciones son anónimos ya que están encriptados (Buterin, 2013). Este hecho no permite que se conozca a ninguna de las dos partes de la transacción sino el montante de la operación, pero si consideramos tal caso en las divisas fiduciarias el anonimato se repite. Es decir, en una transacción de divisas fiduciarias no se puede conocer ni el origen ni el final ni el monto a no ser que esta transacción se haya realizado a través de una institución financiera o de procesador de pago, como VISA o PayPal. En consecuencia, una transacción mediante divisas fiduciarias es tanto o más clandestina que con criptomonedas, solo que los canales de pago y las instituciones de depósito tienen una mayor regulación estatal. No obstante, como se ha mencionado en el apartado referido a las carteras de criptomonedas, existen organizaciones para el depósito y transmisión de criptomonedas, como coindesk, sobre las que en caso de que se regularan se podría tener un control de las partes participantes en las transacciones.

En el apartado político vamos a tener en cuenta cual podría ser el mayor impedimento que se encontrarían las criptomonedas con respecto a las autoridades sociales. Como ya se ha mencionado cuando se consideraba la sustitución monetaria, uno de los principales efectos de esta es la pérdida del señoreaje. Este señoreaje constituye una fuente de ingreso necesaria para las autoridades monetarias para costear el sistema monetario fiduciario, por lo cual en caso de sustitución monetaria este ingreso se vería reducido. Además, el uso del dinero a través de una divisa fiduciaria tiene una gran dependencia sobre la soberanía del estado sobre un territorio. La principal característica de esta soberanía es que permite la aceptación de esa divisa sobre el territorio a través de su poder coercitivo. En el caso de que existiera una sustitución monetaria en un territorio no permitida por la autoridad de este, la soberanía de esta autoridad se vería erosionada por el uso de otra divisa no controlada y la posibilidad de que haya transacciones en el territorio que escapen de su regulación.

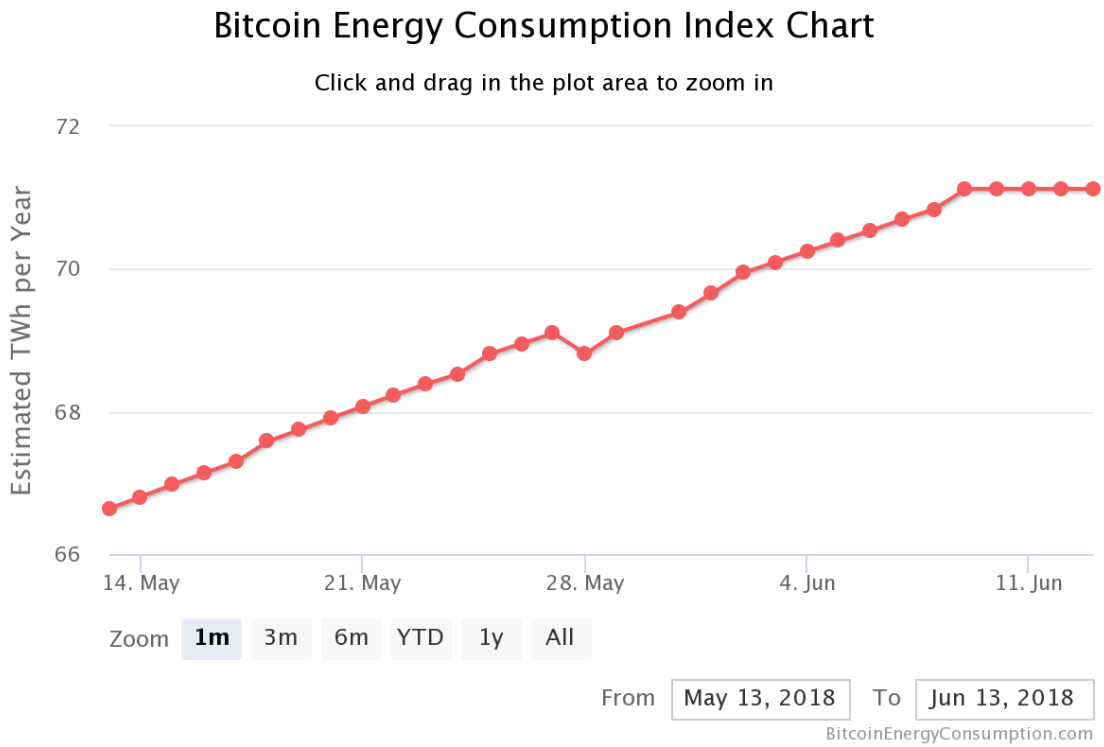
Además, aunque actualmente existe un clima de avance en la regulación legal de las criptomonedas, este puede cambiar en cualquier momento. El trabajo de Hacker y Thomale (2017) realiza un análisis de cómo está derivando la legislación en Estados

Unidos y la Unión Europea. Evitando tecnicismos legales, la conclusión que se obtiene de su trabajo es que el trabajo legislativo actual está avanzando hacia la consideración de las criptomonedas como activos y no como medios de pago. Bierer (2016) revisa si las criptomonedas podrían entrar en la categoría de garantía real, lo cual termina recomendando. Una garantía real es una propiedad u otro activo que un prestatario ofrece como una forma para que un prestamista pueda asegurar el préstamo. Es especialmente interesante el artículo de Chohan (2018) en el cual describe las BitLicense que son licencias emitidas en el estado de Nueva York para regular a los operadores de criptomonedas. También cabe destacar la regulación que se está dando en Asia porque está siendo la más activa. Lai (Lai, 2018) comenta que China, Hong Kong, Singapur, Japón y Corea del Sur son actualmente los Estados más activos, e incluso China y Corea han prohibido las ICO. Aunque la legislación pueda suponer un impedimento, su avance supone un argumento a favor del uso de las criptomonedas.

1.2.3. Limitaciones medioambientales

Estas limitaciones, aunque sean de una naturaleza inesperada tienen que ser mencionadas porque tienen una importancia creciente. El consumo energético que conlleva el uso de las redes criptográficas está aumentando a un ritmo vertiginoso y solo Bitcoin tiene un consumo energético anual similar al de Chile y representa el 0.32% del consumo energético global (Digiconomist, 2018). Esta tendencia parece que no tiene una reversión inmediata, sino una intensificación como se puede ver en el gráfico III, y puede suponer un riesgo futuro para la continuidad de su uso (Holthaus, 2017).

Gráfico III: Consumo energético del Bitcoin



Fuente: https://digiconomist.net/bitcoin-energy-consumption

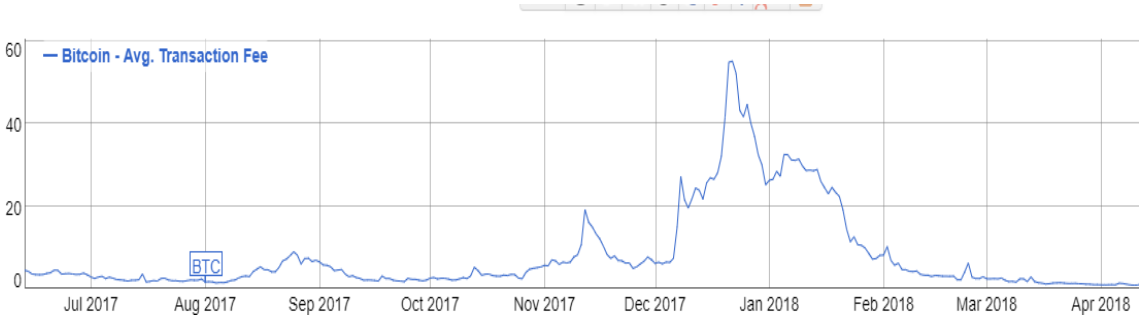
Probablemente este alto consumo se debe a que al estar la tecnología en fase inicial todavía no se ha alcanzado el consumo óptimo de energía por la falta de desarrollo. Además, las normas que establece la Blockchain requieren de un alto consumo de potencia computacional para mantener la integridad de la red.

1.2.4. Limitaciones tecnológicas

Entre las limitaciones tecnológicas que se han encontrado mediante la revisión de la literatura, se va a destacar una en especial. Ésta es el problema de la escalabilidad. Como ya se ha mencionado en el apartado anterior, la tecnología todavía se encuentra en su etapa inicial por lo tanto la innovación será una fuerza para tener en cuenta para esta limitación.

El problema de la escalabilidad se refiera a la capacidad que tienen las redes de mantener la calidad de su funcionamiento cuando el volumen de operaciones aumenta (Zohar, 2017). Actualmente este se ha convertido en un gran problema para las redes de criptomonedas porque está suponiendo que para desincentivar el uso de la red se aplique unas cuotas mayores por la verificación de los bloques como podemos apreciar en el gráfico IV. No obstante, este problema ya se ha comenzado a afrontar con la innovación tecnológica. Se están desarrollando un tipo de redes compatibles con las criptomonedas que permite la verificación de operaciones a mayor velocidad y manteniendo la integridad del sistema (Poon & Dryja, 2015). Estas nuevas redes se conocen como las redes *lightning.*

Gráfico IV: Comisiones medias diarias de Bitcoin por bloque



Fuente: https://bitinfocharts.com/comparison/bitcoin-transactionfees.html#1y

2. Potencial adaptación de las criptomonedas al sistema financiero

2.1. Conclusiones de la revisión

Una vez contemplados todos los efectos tanto positivos como negativos que tiene la implantación de las criptomonedas en el sistema financiero actual, podría ser conveniente explorar los efectos posibles de una adaptación de las criptomonedas al sistema financiero actual que permita aprovechar las características más positivas de las criptomonedas.

Del apartado anterior podemos extrapolar una serie de beneficios relacionados con las criptomonedas. El primero de ellos es su adaptabilidad a las características del dinero descritas por la Escuela austríaca. Hay que añadir también que la existencia de divisas descentralizadas y no sujetas a un Estado también abre una puerta para solucionar el dilema de Triffin si son utilizadas como divisa de reserva. Además, si se consigue estabilizar el mercado criptográfico estas nuevas divisas también representan una alternativa potencial como reserva de valor. Asimismo, suponen una buena herramienta para evitar los efectos negativos de las malas prácticas económicas y una fuente alternativa de financiación independiente para pequeñas empresas. Finalmente, también son una herramienta informática que puede permitir dar un salto cualitativo a la investigación y comprensión de los fenómenos monetarios.

Igualmente se pueden concluir una serie de limitaciones que pueden desvirtuar las cualidades anteriormente mencionadas. Desde alta volatilidad del precio hasta efectos medioambientales. No obstante, estas limitaciones se caracterizan por derivar de la situación marginal actual de las criptomonedas con respecto a la vida política. La falta de consideración legal actual de las criptomonedas no favorece que su desarrollo se consolide a una velocidad mayor ya que genera una mayor incertidumbre sobre los potenciales inversores y usuarios. Además, los mercados que no se encuentran bajo regulación legal justa, que no implica intervención, suelen presentar situaciones de alta volatilidad.

Por todo esto la alternativa de la adaptación de las criptomonedas al sistema actual no es tan descabellada ya que si se llegan a acuerdos entre varias partes se puede alcanzar la consolidación de esta tecnología en el sistema monetario.

2.2. Discusión de la revisión

La adaptación de las criptomonedas al sistema monetario se podría plantear desde dos alternativas; la adaptación mediante la creación de una divisa internacional independiente y la adaptación mediante la implementación del formato de las criptomonedas en las divisas fiduciarias actuales.

La primera alternativa que se presenta en esta discusión es la de mantener el sistema actual, pero incluir los beneficios que se atribuyen a las criptomonedas. Una manera de afrontar esta alternativa sería la creación de una divisa internacional por parte de todos los Estados para que desempeñe el papel de divisa de reserva internacional. La función de esta divisa se asemejaría mucho a la de los derechos especiales de giro (DEG) que se utilizan en el Fondo Monetario Internacional (FMI). No obstante, permitiría gozar de todos los beneficios tecnológicos y económicos de las criptomonedas que no presentan los DEG. La emisión de esta criptomoneda podría recaer sobre una Organización Internacional creada para tal función o sobre una ya existente. Aunque los DEG son emitidos ya por una Organización Internacional, el FMI, esta Organización no se caracteriza por la igualdad entre sus miembros. El poder de decisión en el FMI depende de la aportación a las reservas del fondo, lo que deja en situación de ventaja a las economías financieras y avanzadas sobre el resto. No obstante, la Organización Mundial de Comercio (OMC) por su parte es muy igualitaria en tanto al poder de decisión de sus miembros que gozan de un voto cada uno con el mismo peso. Por tanto, la emisión de esta divisa criptográfica internacional bajo el paraguas de la OMC podría ser una alternativa viable.

La segunda alternativa sería la adaptación al formato criptomonetario de las divisas fiduciarias tradicionales. Esta alternativa ya está siendo planteada actualmente. Kartik y Yatish (2016), dos investigadores indios ya han planteado y desarrollado un ejemplo de esta alternativa. En su trabajo plantean la creación de un sistema internacional monetario basado en las criptomonedas que permita su utilización a nivel nacional e internacional. De su sistema es interesante ver que han desarrollado un punto de comercio en el que las distintas criptomonedas nacionales podrían ser intercambiadas instantáneamente. Fuera del campo teórico también se han presentado alternativas. Un estudio realizado por la compañía Deloitte (Pawczuk, 2018) analiza la posibilidad de la creación de criptomonedas respaldadas por Estados. Este estudio también considera que una

adaptación del formato de las criptomonedas a las divisas fiduciarias clásicas tendría amplios beneficios sobre la economía y sobre las políticas monetarias. En esta alternativa también cabe la posibilidad planteada en la primera alternativa de crear una criptomoneda internacional que cumpliría el papel de reserva de divisa y así se podría superar el dilema de Triffin.

También, ambas alternativas supondrían una solución para las limitaciones tecnológicas y medioambientales que hemos mencionado en la revisión de la literatura. La existencia de cualquiera de las dos alternativas implicaría que la principal criptomoneda internacional pudiera construirse sobre una red federada o privada. Como hemos visto en el marco teórico, estas redes permiten una mayor eficiencia en la superación del problema de los bizantinos que las redes públicas y por tanto presentarían una mayor escalabilidad y un menor consumo energético. Además, al ser los dueños de los nodos de estas criptodivisas poderes públicos la confianza sobre estos nodos podría ser máxima. El acceso a la información monetaria contenida en los nodos en este caso no sería libre, no obstante, se podrían desarrollar legislaciones para fomentar la transparencia en este aspecto.

IV. Conclusión

Una vez realizada la exhaustiva revisión acerca de las criptomonedas y su posible relación con la economía y el sistema monetario es hora de cerrar una serie de conclusiones:

-Su adaptabilidad a las características del dinero descritas por la Escuela austríaca.

-Son una solución al dilema de Triffin si son utilizadas como divisa de reserva.

-Alternativa potencial como reserva de valor.

-Herramienta para evitar los efectos negativos de las malas prácticas económicas y una fuente alternativa de financiación independiente para pequeñas empresas.

-También son una herramienta informática que puede permitir dar un salto cualitativo a la investigación y comprensión de los fenómenos monetarios.

-Han supuesto la creación de una tecnología fundamental para el funcionamiento de las redes distribuidas.

-Son adaptables al sistema monetario actual

Estas conclusiones también están acompañadas por una serie de limitaciones. No obstante, estas limitaciones pueden ser superadas si se decide tal cosa. Hecho que hemos revisado en la última sección.

Finalmente cabe mencionar una serie de recomendaciones futuras en caso de que se quiera afrontar un análisis sobre esta cuestión teniendo en cuenta diversos aspectos no previstos en este trabajo. La primera de todas es encarar este trabajo desde otra perspectiva económica. Aunque la Escuela austríaca sea una inspiración para el mundo criptográfico, no es la que tiene mayor aplicación en el mundo actual.

La siguiente recomendación es la ampliación del estudio de aplicación de las criptomonedas para otros usos que no sean únicamente monetarios. Como hemos visto en el marco teórico, las transacciones son solo una de las capacidades de las que disfrutan las transacciones, no obstante, pueden realizar una mayor aportación al sistema económico. Son una alternativa fiable para el desarrollo de sistemas de el pago por uso, donde se produzca la eliminación de publicidad como único medio de ingreso. Además, también se pueden extrapolar a la organización estatal no monetaria como sería en

documentos y procesos administrativos, prestaciones sociales, prescripción y control de consumo de sustancias controladas o contratos inteligentes.

Finalmente, la última recomendación para estudios posteriores es tener en cuenta efecto que tendrán las innovaciones tecnológicas que están por venir. La instalación de redes 5G en la próxima década ya es un hecho, y por ello son necesarias en un análisis para estimar el uso de pagos criptomonetarios. Finalmente, el ordenador cuántico es otro actor para tener en cuenta en este nuevo sistema criptográfico que se está gestando. Este ordenador ya ha sido diseñado y verificado, por lo que su desarrollo en las próximas décadas también se puede dar por sentado. LA manera en la que este ingenio revolucionará la capacidad de cálculo también se presenta como fundamental para la estimación de la evolución de las criptomonedas.

Bibliografía

Aizenman, J. (2010). The Impossible Trinity (aka The Policy Trilemma). *NBER*, 1-21.

Anderson, R. (2012). Risk and Privacy Implications of Consumer Payment Innovation in the Connected Age . *CONSUMER PAYMENT INNOVATION* , 99-117.

Arsov, A. (2017). Periodic Table of Cryptocurrencies: Blockchain Categorization . *Independent researcher* , 1-16.

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts. *Universitá degli Studi di Cagliari*, 1-22.

Banco de España. (n.d.). *Glosario Política Monetaria*. Retrieved from Banco de España: https://www.bde.es/bde/es/utiles/glosario/glosarioPolt/

BCE. (1992). *Protocolo sobre los estatutos del Sistema Europeo de Bancos Centrales y del Banco Central Europeo.* Francfurt: Tratado constitutivo de la Comunidad Europea.

Bierer, T. (2016). Hashing it out : Problems and Solutions Concerning Cryptocurrencies used as Article 9 Collateral . *Journal of Law, Technology & the Internet, Vol. 7*, 79-94.

Bitcoinwiki. (2018). *Proof of work*. Retrieved from https://en.bitcoin.it/wiki/Proof_of_work

Björklund, F. (2016). E-government and moral citizenship: The case of Estonia. *Citizenship studies, 20(6-7),* , 914-931.

BlochainHub. (2018). *Blockchains & Distributed Ledger Technologies*. Retrieved from https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology and Governance. *Journal of Economic Perspectives—Volume 29, Number 2*, 213–238.

Bordo, M. D. (2017). The Operation and Demise of the Bretton Woods System; 1958 to 1971. *Hoover Institution, Economics Working Paper 16116*, 1-36.

Bouri, E., Molnár, P., Azzi, G., Roubaud, D., & Hagfors, L. I. (2016). On the hedge and safe haven properties of Bitcoin: Is it really more than a diversifier? *Finance Research Letters 20*, 192–198.

Buterin, V. (2013). *Ethereum white paper. .* Retrieved from GitHub repository.: https://github.com/ethereum/wiki/wiki/White-Paper#merkle-trees

Calvo, G. A., & Végh, C. A. (1992). Currency Substitution in Developing Countries: An Introduction. *Revista de Análisis Económico Vol. 7 Nº 1*, 3-27.

Chohan, U. W. (2018). Oversight and Regulation of Cryptocurrencies: BitLicense . *Notes on the XXI century* , 1-7.

Cohan, P. (2013, 04 02). *Forbes.* Retrieved from Are Bitcoins Safer Than Cyprus?: https://www.forbes.com/sites/petercohan/2013/04/02/are-bitcoins-safer-than-cyprus/#7cf3133952f2

Cox, J. (2013, 04 02). *NBC.* Retrieved from Bitcoin Bonanza: Cyprus Crisis Boosts Digital Dollars: https://www.cnbc.com/id/100597242

Delgado-Segura, S., Tanas, C., & Herrera-Joancomartí, J. (2016). Reputation and Reward: Two Sides of the same Bitcoin. *Sensor*, 1-23.

Digiconomist. (2018, 06 14). *Digiconomist.* Retrieved from https://digiconomist.net/bitcoin-energy-consumption

Eichengreen, B., Chitu, L., & Mehl, A. (2015). Stability or Upheaval? The Currency Composition of International Reserves in the Long Run. *IMF economic review*, 354–380.

Elkhafif, M. A. (2003). Exchange Rate Policy and Currency Substitution the of Africa's Emerging Economies. *R&D Management 15, 1*, 1 - 11.

Extance, A. (2015). BITCOIN AND BEYOND. *Nature*, Vol. 526, 21-23.

Friedman, M. (1959). The Demand for Money: Some Theoretical and Empirical Results. *Journal of Political Economy, Vol. 67, No. 4* , 327-351.

Gandal, N., & Halaburda, H. (2016). Can We Predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market. *Games , vol. 7, 16*, 1 - 21.

Gangwal, S., & Longin, F. (2018). *Extreme movements in Bitcoin prices: A study based on extreme value theory.*

García Guerra, E. M. (2006). ITINERARIOS MUNDIALES DE UNA MONEDA SUPRANACIONAL: NACIONAL: EL REAL DEA OCHO O PESO DURANTE LA EDAD MODERNA. *Instituto de Historia. Consejo Superior de Investigaciones Científicas.* , 241-257 .

Grice-Hutchinson, M. (1989). El concepto de la Escuela de Salamanca: Sus origenes y su desarrollo. *Revista De Historia Económica / Journal of Iberian and Latin American Economic History7(S1),* , 21-26.

Hacker, P., & Thomale, C. (2017). Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law. 1-44.

Hackett, R. (2018, 01 09). *Fortune.* Retrieved from http://fortune.com/2018/01/09/bitcoin-price-chase-jamie-dimon/

Hafner, C. (2018). Testing for bubbles in cryptocurrencies with time-varying volatility. *ResearchGate*.

Harwick, C. (2016). Cryptocurrency and the Problem of Intermediation. *The Independent Review, v. 20, n. 4*, 569-588.

Hayek, F. A. (1931). Prices and production. *London School of Economics*, 1-160.

Hirai, Y. (2017). Defining the Ethereum Virtual Machine for Interactive Theorem Provers. *Ethereum Foundation*, 1-15.

Holthaus, E. (2017, 12 05). *grist.* Retrieved from https://grist.org/article/bitcoin-could-cost-us-our-clean-energy-future/

Hsing, Y. (2007). Tests of the functional form, the substitution effect, and the wealth effect of Mexico's money demand function. *Revista de Economia del Rosario Bogotá 10* , 43–53.

Humphrey, T. M. (1974). The Quantity Theory of Money: Its Historical Evolution and Role in Policy Debates. *FRB Richmond Economic Review, Vol. 60*, 2-19.

Imrohoroglu, S. (1996). International Currency Substitution and Seigniorage in a Simple Model of Money. *Economic Inquiry, vol. 34*, 568 - 578.

Investopedia. (2018). *Reserve currency.* https://www.investopedia.com/terms/r/reservecurrency.asp.

Jack, W., Suri, T., & Townsend, R. (2010). Monetary Theory and Electronic Money: Reflection on the kenian Experience. *Economic Quarterly—Volume 96, Number 1*, 83–122.

Kartik, H., & Yatish, S. (2016). The K-Y Protocol: The First Protocol for the Regulation of Crypto Currencies. 1-11.

Keynes, J. M. (1936). The General Theory of Employment, Interest and Money . 1-263.

Lai, K. (2018). ICO regulation in Asia. *International Financial Law Review*.

Larsen, C., & Thomas, S. (2018, 02 23). *YouTube*. Retrieved from "Ripple - The Enterprise Blockchain" | Talks at Google: https://www.youtube.com/watch?v=B7Tiz3JQeYc&t=2558s

Lunn, J. (2014). Money: The Unauthorized Biography. *Christian Scholar's Review*, 405-410.

Menger, K. (1892). On the Origin of Money. *The Economic Journal, Vol. 2, No. 6* , 239-255.

Micheler, E. (2015). Custody Chains and Asset Values: Why Crypto-Securities are worth contemplating. *Cambridge Law Journal, 74(3)*, 505–533.

Mises, L. v. (1912). *The Theory of Money and Credit.* Munich: Duncker and Humblo.

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from bitcoin.org: https://bitcoin.org/bitcoin.pdf

Narayanan, A., & Miller, A. (2017). Research for Practice: Cryptocurrencies, Blockchain and Smart Contracts; Hardware for Deep Learning. *COMMUNICATIONS OF THE ACM* , VOL. 60, NO. 5; 48-51.

Noko, J. (2011). Dollarization: The case of zimbabwe. *Cato Journal 31(2)*, 339-366.

Opentransactions. (n.d.). Retrieved from http://opentransactions.org/wiki/index.php?title=Main_Page

Patuti, A., & Tatulescu, A. (2013). EMPIRICAL EVIDENCE FOR THE QUANTITY THEORY OF MONEY: ROMANIA – A CASE STUDY. *Romanian Statistical Review*, 12-19.

Pawczuk, L. (2018). State-Sponsored Cryptocurrency: Adapting the best of Bitcoin's Innovation to the Payments Ecosystem. *Deloitte*, 1-8.

Pérez-Solà, C., & Herrera-Joancomartí, J. (2014). Bitcoins y el problema de los generales bizantinos. *RECSI*, 241-244.

Poon, J., & Dryja, T. (2015). The bitcoin lightning network: Scalable off-chain instant payments. 1-59.

Rapoza, K. (2018, 02 02). *Forbes*. Retrieved from Here's One Reason Why Bitcoin Is In Freefall: https://www.forbes.com/sites/kenrapoza/2018/02/02/heres-one-reason-why-bitcoin-is-in-freefall/#575eb94167c8

Schwartz, D., Youngs, N., & Britto, A. (2014). *Ripple Lanbs Inc.* Retrieved from https://ripple.com/files/ripple_consensus_whitepaper.pdf

Swan, M. (2015). *Blockchain: The Blueprint of the New Economy.* Retrieved from O'reilly media: http://www.sapcoin.net/blockchain/blockchain-by-melanie-swan.pdf

Times, F. (2018, 06 13). *ft.com/lexicon.* Retrieved from http://lexicon.ft.com/Term?term=money-supply

Triffin, R. (1978). Gold and the Dollar Crisis: Today and Tomorrow. *ESSAYS IN INTERNATIONAL FINANCE Nº132*, 1-22.

White, L. H. (2015). The Market for Cryptocurrencies. *Cato Journal*, Vol. 35, No. 2, 383 - 402.

Wood, G. (2017). ETthereum: A secure decentralised generalised transaction ledger. *EIP-150 REVISION* , 1-32.

Yamashita, T., Kurumatani, K., Sasaki, Y., Kawamura, H., & Ohuchi, A. (2005). Emergence and Stability of Key Currency in Artificial International Trade. *New Generation Computing*, vol 23, 13-22.

Zohar, A. (2017). Securing and Scaling Cryptocurrencies. *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17)*, 5161-5164.