

Ignacio López Domínguez

Profesor de la Universidad Complutense de Madrid, España.
Departamento de Administración Financiera y Contabilidad

@ ilopez@ccee.ucm.es

id 0000-0001-5929-9308

■ Recibido / Received
8 de noviembre de 2019

■ Aceptado / Accepted
31 de enero de 2020

■ Páginas / Pages
De la 19 a la 43

■ ISSN: 2531-0054

José Antonio Medina Melón

Profesor de la Universidad Complutense de Madrid, España.
Departamento de Administración Financiera y Contabilidad

@ joamedin@ccee.ucm.es

Análisis financiero de las nuevas monedas digitales (criptomonedas)

Financial Analysis of the new digital coins (cryptocurrencies)

El mercado de criptomonedas ha evolucionado enormemente a un ritmo sin precedentes a lo largo de su corta vida. Desde la emisión en enero de 2009 de la moneda virtual pionera, el *bitcoin*, más de 1500 criptomonedas han sido desarrolladas y lanzadas al mercado, aunque la mayoría con relativamente poco éxito. Las investigaciones sobre esta industria son aún de escasa relevancia, y la mayoría están dedicadas más al estudio del *bitcoin* que a la gran diversidad de criptomonedas existentes. El presente trabajo de análisis trata de obtener evidencias empíricas acerca de la nueva realidad financiera que acontece con la generalización de las criptomonedas en el mundo inversor, así como su relación con otros tipos de activos comparables. Estudiaremos la evolución de sus cotizaciones, analizando estadísticamente estos valores y obteniendo conclusiones acerca de su posible establecimiento como medio de pago impulsado por el incesante auge del comercio electrónico, o como forma de financiación de los nuevos proyectos de empresas y su consideración como activo de inversión.

PALABRAS CLAVE: monedas digitales, mercado financiero, financiación, correlación, tendencias.

The cryptocurrency market has evolved tremendously at an unprecedented rate throughout its short life. Since the issuance of the pioneer virtual currency, Bitcoin, in January 2009, more than 1500 cryptocurrencies have been developed and launched to the market, although most with relatively little success. Research on this industry is still of little relevance, the majority being more dedicated to the study of Bitcoin than to the great diversity of existing cryptocurrencies. This research tries to obtain empirical evidence about the new financial reality that occurs with the generalization of cryptocurrencies in the investment world, as well as its relationship with other types of comparable assets. We will study the evolution of their prices, statistically analyzing these values and obtaining conclusions about their possible establishment as a means of payment driven by the incessant boom of electronic commerce, or as a form of financing for new business projects and their consideration as an investment asset.

KEYWORDS: digital coins, financial market, financing, correlation, trends.

1. Introducción

En enero de 2009 se emitió lo que en ese momento era la primera criptomoneda, el *bitcoin*. Desde esa fecha, se ha desarrollado un enorme número de este tipo de monedas, si bien muchas de ellas con poco éxito. Seguramente, por esta escasa vida, son aún pocas las investigaciones sobre estas monedas, y la mayoría de ellas están enfocadas a la que, hasta ahora, más éxito ha tenido, el *bitcoin*.

En las siguientes líneas se aborda el análisis de la realidad financiera en el ámbito inversor de este nuevo activo, así como su relación con otras inversiones de mayor tradición.

Debido a que la industria de las criptomonedas es aún muy joven y hay factores que cada día impactan en ella, no se pueden encontrar muchos recursos académicos con información completamente actualizada. Por ello, casi toda la información recogida en este trabajo proviene directamente de síntesis de fuentes online, de páginas especializadas en la materia o de conocimiento adquirido por medio de la lectura de noticias del sector.

El apartado 2 se dedicará a esclarecer qué son las criptomonedas, explicando de una manera comprensible las reglas que permiten su funcionamiento y también describiendo sus características monetarias. El apartado 3 abarcará la información acerca de las principales criptomonedas por capitalización en la actualidad, señalando sus implicaciones en las finanzas y lo que las diferencia de las monedas de curso legal conocidas hasta ahora. A continuación, en el apartado 4 se explica cómo funciona el nuevo método de financiación de proyectos y/o empresas, las *Initial Coin Offerings* (ICO).

En el apartado 5 se realiza una comparativa entre las características de las criptomonedas y otros activos que guardan valor monetario, como la divisa fiat o los metales preciosos, para acercarnos un poco más a nuestro objetivo. Los apartados 6 y 7 se dedican a informar acerca de las ventajas y desventajas y sobre las mínimas regulaciones en la actualidad de las divisas virtuales.

Finalmente, en el apartado 8 se realiza un análisis financiero de todos estos activos mencionados para obtener un estudio de la evolución de su cotización, volatilidades y grado de correlación entre ellas. El apartado 9 abarca las principales conclusiones de la presente investigación.

2. Acercamiento a las criptomonedas

2.1. Definición de criptomoneda

Una criptomoneda puede definirse como una divisa digital o virtual que usa criptografía para su seguridad y no está emitida por ninguna autoridad central, lo cual la deja prácticamente inmune a interferencias o manipulaciones de los gobiernos. La criptografía es el proceso de convertir información legible en un código prácticamente indescifrable para dar seguimiento a compras y transferencias. Otra definición válida es la de una moneda electrónica que se basa en una cadena de firmas digitales (Nakamoto, 2008).

2.2. Un breve repaso por los orígenes

El primer dato jamás conocido sobre las criptomonedas se remonta a los años 80 con el movimiento llamado «*cypherpunk*», que abogaba por el uso de la criptografía como herramienta de cambio social y político. Sin embargo, no es hasta 2009 cuando impulsados por la crisis de liquidez en los mercados financieros, una persona o grupo de personas aún sin identificar, bajo el pseudónimo de Satoshi Nakamoto, publican un artículo en un foro de internet titulado «Bitcoin: un sistema de dinero electrónico de igual a igual», un sistema de dinero electrónico *peer-to-peer* (P2P) para evitar un doble gasto, es decir, que una persona pague dos veces una misma compra. Este artículo sería la piedra angular de la creación del *bitcoin*, la primera moneda virtual basada en un sistema digital (*blockchain* o cadena de bloques).

Normalmente, este registro se realiza mediante un servidor central (un banco central) que mantiene registros sobre los balances. Este sistema P2P es usado por plataformas conocidas de descarga de contenido como Utorrent o Ares, en donde los miembros de la comunidad comparten su archivo cada vez que alguien quiere descargarse determinada película, por ejemplo. En una red descentralizada, no necesitas este servidor. Cada *peer* de esta red realiza ese mismo trabajo y necesita tener una lista con todas las transacciones para comprobar si las futuras transacciones son válidas o son un intento de doble gasto: debe ser validada por todos los miembros de la red.

La primera transacción jamás registrada con *bitcoin* se produjo el 18 de mayo de 2010, hace ya diez años, cuando una persona en California publicó en un foro que enviaría *bitcoin* si alguien le llevaba personalmente dos pizzas a su casa. Un londinense se las envió a domicilio a través de una cadena de pizzerías y recibió a cambio 10 000 *bitcoin*, hoy equivalentes a más de 60 millones de euros.

En cuanto al resto de criptomonedas, *litecoin* fue lanzada en el año 2011, convirtiéndose en la segunda moneda más importante por capitalización por detrás de *bitcoin*. Esta moneda modificaba el protocolo original de *bitcoin*, aumentando la velocidad de transacción con la idea de ser más apropiada para transacciones del día a día (Farrell, 2015). Más tarde, en el año 2013, otra de las monedas de nuestro estudio fue creada y lanzada al mercado: *ripple*. Dos años después, en 2015, se produjo la llegada al mercado de una de las monedas virtuales más revolucionarias de la actualidad, *ether*. En líneas posteriores veremos la evolución del mercado de criptomonedas y su peso relativo respecto al rey, el *bitcoin*.

2.3. Las carteras virtuales o *wallets* y la confirmación de transacciones

Monedas como el propio *bitcoin* u otras como *ether* o *litecoin*, que más adelante abarcaremos, consisten en una red de *peers*, que, como se mencionó antes, individualmente tienen un registro de la historia completa de todas las transacciones y, por consiguiente, del balance de cada cuenta.

Cada persona posee una clave pública y otra privada de su cartera, donde se guarda el montante total de sus monedas virtuales (una cartera o *wallet* puede estar localizada en un *pendrive*/USB o vía online en plataformas como Coinbase o Kraken). La clave pública viene

a ser como el número de cuenta bancaria, que compartes públicamente cuando necesitas recibir una transacción, por ejemplo. La clave privada es como el PIN o la firma digital de tu cuenta, que utilizas para firmar y dar autorización a una transacción desde tu cuenta. Esta nunca queda expuesta públicamente y además es imposible de averiguar.

Al igual que el dinero en efectivo o las materias primas, las criptomonedas pueden perderse, ser robadas o destruidas. Podemos mencionar el caso famoso de un británico que tiró a la basura un *pendrive* que contenía una cartera de 7.000 BTC, unos 49 millones de euros.

La confirmación es el concepto crítico de las criptomonedas. Cada usuario que participa en la red de confirmaciones de la moneda trata de verificar que los datos de la transacción son correctos para que dicha transacción se produzca y se añada al bloque del libro mayor o *publicledger*. Una vez que la transacción es confirmada, es imposible de modificar y pasa a ser parte de un registro inmutable de transacciones históricas: el *blockchain* (Ameer, 2017).

Sólo los mineros pueden confirmar dichas transacciones. Los mineros son «aquellos que aseguran la red y son compensados por su trabajo en forma de comisiones de transacción o nuevas monedas emitidas» (Farell, 2015). Algunas recompensas se reciben en forma de *token* o ficha de la criptomoneda (por ejemplo, en *bitcoins* la recompensa actual es de 12 BTC por bloque, creándose un bloque cada 10 minutos en el que se incluyen unas 2000 transacciones). Según el número de transacciones confirmadas por cada minero, obtienen una proporción del total de recompensa por bloque.

Cada bloque está conectado con el bloque anterior y el bloque siguiente. Cuando se crea el bloque #2197, este contiene también toda la información de las transacciones del bloque #2196 a través de lo que se conoce como *hash*. El *hash* es la combinación de números y letras que identifica todas las transacciones contenidas en cada bloque. Su apariencia es tal que «1DZEazabbJqtr2uciLFNxvgm1GBuS5kaej». De la misma manera, cuando se cree el bloque #2918, este contendrá a su vez los *hash* de los 2917 bloques anteriores. Por ello se conoce como cadena de bloques; todos están conectados.

Mediante la existencia de lo que se denomina como *Proof of Work* (PoW) o Prueba de Trabajo, en la mayoría de criptomonedas se evita que alguien pueda controlar la comunidad de mineros y puedan crear bloques fraudulentos para obtener recompensas: transacción de A a B de 1 BTC y de nuevo de B a A de 1 BTC.

Los *hashes* creados para cada bloque tendrán que empezar por cierto número de ceros, cuya cantidad es modificada cada cierto número de bloques. Esto hace que la tarea sea dificultosa y se necesiten miles y miles de pruebas y errores para obtener el código *hash* que cumpla los requisitos. De este modo, se hace inviable la existencia de transacciones falsas ya que se necesita un gasto de energía muy alto para obtener el *hash* y controlar más del 50 % de la capacidad de procesamiento de la comunidad de mineros a escala global para su aprobación, algo imposible.

No solo se utiliza como mecanismo de verificación el comentado *Proof of Work* (PoW), sino también varios más. A continuación, detallamos el funcionamiento básico de cada mecanismo (Farell, 2015):

- **Proof of Work (PoW):** las transacciones no son verificadas hasta que se consume cierta cantidad de energía. Para llegar a un acuerdo para añadir un bloque, cada nodo debe intentar resolver un algoritmo matemático que cumpla ciertos requisitos (con dificultad creciente). Una vez resuelto, el nuevo bloque es añadido y publicado a todos los nodos.

- **Proof of Stake (PoS):** para poder verificar la transacción en cierta moneda y recibir una recompensa, el minero debe poseer él mismo dicha moneda. Las probabilidades de que encuentre la solución y cree el nuevo bloque dependerán de la cantidad de monedas que ostente, y no de su poder computacional. Esto hace que se produzca menor gasto de energía. En general, las monedas que usan el mecanismo PoS no tienen una oferta de moneda limitada y son, por tanto, inflacionarias. A veces ocurre que los creadores de la moneda se quedan con la mayoría de verificaciones, esto es, de recompensas.
- **PoW/PoS, híbrido:** se utiliza el mecanismo PoW para la emisión de moneda y distribución entre los mineros. Sin embargo, con el tiempo, el mecanismo PoS sustituye al mecanismo PoW, creando una criptomoneda con consumo eficiente de energía a largo plazo.
- **Byzantine Consensus:** red distribuida, donde cada servidor de la red se enfrenta al problema de decidir si los otros servidores de la red están mandando mensajes correctos (información verdadera sobre transacciones) dentro una lista cerrada de nodos (*UniqueNodeList*). Cada servidor transmite transacciones y el resto de servidores vota sobre ellas cada pocos segundos, hasta que el algoritmo aprueba o rechaza llegar a consenso. En *ripple*, es necesario el 80 % de aprobación del grupo de nodos para llegar a consenso, haciéndolo más infranqueable a ataques sobre la red.

Como conclusión, en PoW los mineros invierten dinero *fiat* en capacidad de procesamiento para obtener criptomonedas y venderlas para pagar la electricidad, es decir, habrá mucho volumen de venta para poder pagar y comprar más potencia de procesamiento (mercado a la baja o controlado).

Sin embargo, en las monedas que usan PoS, los mineros invierten dinero *fiat* para comprar criptomonedas y ganar más cantidad de estas. Cuanto más ganen, más comprarán. El precio siempre irá al alza a largo plazo (mercado inflacionario).

2.4. El mundo de la minería: creando criptomonedas a modo de recompensa

La creación o emisión de nuevas criptomonedas se produce como consecuencia de la verificación de cada bloque. Cada vez que un bloque se verifica y se añade a la cadena, se genera nueva cantidad de dicha criptomoneda para pagar a la comunidad que verificó dichas transacciones. Como se ha comentado, dependiendo del sistema de verificación que posea el protocolo de cada criptomoneda, las recompensas se distribuirán con más probabilidad a cierto tipo de nodos de la red.

Para encontrar el *hash* (producto de una función criptográfica) que conecte el nuevo bloque con el predecesor, los ordenadores realizan «prueba y error». La dificultad de este puzle se va incrementando a medida que se crean más monedas y solo cada cierto tiempo se crean cantidades específicas de *tokens*.

Para el caso de criptomonedas con cantidad máxima de emisión, como el *bitcoin* o el *ripple*, cuando en el largo plazo se alcance dicha cantidad preestablecida por sus protocolos,

las comisiones por transacción tendrán que aumentar para compensar a los mineros ya que no se emitirán más monedas como recompensa (Farell, 2015).

Un caso particular de las actividades mineras es la existencia de *pools* de minería, que son grupos de mineros que acuerdan compartir ganancias de bloques en proporción al poder de *hash* de minería contribuido. Los mineros pueden elegir redirigir su poder de *hash* a un *pool* de minería distinto en cualquier momento.

Como comenta en su artículo Tuwiner (2017), mientras que los *pools* de minería son ventajosos para un minero que trabaja de forma particular, ya que liman las diferencias de las ganancias y las hacen más predecibles, por otro lado provoca la concentración de poder en el propietario del *pool* de minería. Esto hace que se produzca una relativa centralización de la red, justo lo que se quería evitar con las divisas virtuales. Los principales países con granjas de minería son China y Estados Unidos.

2.5. Características transaccionales de las criptomonedas

Las principales características que sustentan la diferenciación de las criptomonedas respecto a divisas tradicionales de curso legal son las siguientes:

- **Irreversibles.** Una transacción no puede ser modificada tras ser confirmada y añadida al libro de registros, se garantiza la integridad de la información.
- **Anónimas.** Ni las cuentas ni las transacciones están conectadas a identidades reales. Cada cuenta tiene un número de dirección aleatorio de 30 caracteres que no está ligado a ninguna identidad.
- **Rápidas y globales.** Se propagan casi al momento por la red y son confirmadas en varios minutos. Ya que son confirmadas por una red global, no importa, en cuanto a tiempo, la lejanía entre las cuentas de origen y destino de la transacción.
- **Seguras.** Los fondos que se poseen en criptomonedas están encriptados con clave privada, con la que solo el dueño puede enviar fondos.
- **Sin necesidad de permisos.** Alta facilidad para descargar o usar online gratis un programa donde poder recibir y enviar criptomonedas.

En su estudio acerca de la posibilidad del blanqueo de dinero con criptomonedas, Brenig, Accorsi & Muller (2015), establecen características comparativas, tanto en el marco contextual como en el transaccional, y sus efectos positivos o negativos en cuanto a suponer incentivos para la realización de lavado de dinero. Implica añadir características adicionales a las mencionadas como principales y un análisis comparativo clarividente.

De tabla 1 podemos extraer que la amplia mayoría de factores inherentes a las criptomonedas proveen incentivos positivos para que los criminales las empleen en sus actividades de blanqueo de dinero. Únicamente se señala la limitada aceptación y la alta volatilidad de su precio como incentivos negativos. Por su parte, las cinco características transaccionales mencionadas aumentan los incentivos respecto al uso de instrumentos financieros tradicionales. De esta manera, las criptomonedas parecen ser un estimulante para el blanqueo de capitales por parte de criminales.

Tabla 1. Comparación de criptomonedas y otros instrumentos financieros

Instrumento Factores		Instrumentos financieros	Criptomonedas	Incentivos para blanqueo	
				Directos	Indirectos
Contextuales	Aceptabilidad	Global	Limitada	-	
	Administración	Diseñada y emitida por autoridad central	Minería y almacenamiento descentralizado		+
	Nivel de autenticación	Identificación personal	Identificación anónima		+
	Volatilidad de precios	Relativamente estable	Alta	-	
Transaccionales	Flexibilidad	Depende del proveedor del servicio	Sin posibilidad de fallo	+	+
	Irrevocabilidad	Revocables	Irrevocables	+	+
	Procesamiento de pago	Basado en intermediarios	Sin intermediarios		+
	Portabilidad	Internacional	Internacional	+	+
	Rapidez	Hasta varios días	Instantáneo	+	+
	Comisiones	Comisiones variadas	Bajas o inexistentes	+	
Ejemplos		Tarjeta de crédito, transferencia online, Paypal, etc.		<i>Bitcoin, ether, litecoin, etc.</i>	

Fuente: Brenig *et al.* (2015).



2.6. Principales características monetarias

En cuanto a la parte monetaria, podemos destacar los siguientes rasgos:

- **Oferta controlada o limitada.** La mayoría de las criptomonedas en curso limitan la oferta de *tokens* a un número específico y marcan un calendario de emisión continuo con una fecha límite para que se complete la oferta total de su moneda. Por ejemplo, en el caso del *bitcoin*, la oferta va decreciendo con el tiempo (cada año se emite un menor número de la misma) y alcanzará los 21 millones de monedas en torno al año 2030. Este calendario de emisión está escrito en el código de las mismas, por lo que no hay dudas acerca del número total que habrá en un futuro.
- **Cantidad divisible.** Cada unidad de criptomoneda puede ser dividida en varios decimales, dividiéndose en hasta ocho decimales en BTC o 18 decimales para ETH.
- **Fungibilidad.** Cada unidad de criptomoneda tiene el mismo valor que cualquier otra existente, al igual que ocurre con las monedas *fiat* (que se explicarán más adelante). Esto es una característica monetaria esencial.

- **Transferabilidad.** Las criptomonedas son fácilmente transferibles entre dos cuentas y el proceso es semejante al de una transacción bancaria en cuanto a facilidad para el usuario.

Las criptomonedas son un ataque al ámbito de alcance de la política monetaria, ya que son dinero limitado y no modificable por ningún gobierno o institución central. No ejercen control sobre la inflación o deflación manipulando la oferta monetaria, como sí hacen los bancos centrales. De esta forma, al no emitirse más unidades de la moneda, el valor se preserva ya que, si aumentase la circulación de forma masiva, este decrecería.

3. Principales criptomonedas por capitalización

A continuación se muestra una tabla con las seis primeras monedas virtuales por *ranking* de capitalización a 11 de mayo de 2018, fecha de la última recogida de datos diarios, así como las fechas en que empezaron a ser operativas. Como *bitcoin cash* es una ramificación de *bitcoin*, excluirémos a tal moneda de nuestro estudio, para únicamente analizar monedas de diferentes características. De la misma forma, no incluiremos a EOS por la escasa información disponible de cotizaciones al llevar en el mercado menos de un año.

Tabla 2. Principales criptomonedas por capitalización (11/05/2018)

Criptomoneda	Fecha de inicio	Capitalización USD
1. Bitcoin	03/01/2009	\$ 152 754 125 485
2. Ethereum	30/07/2015	\$ 68 746 577 440
3. Ripple	02/02/2013	\$ 27 239 507 638
4. Bitcoin Cash	01/08/2017	\$ 24 089 829 421
5. EOS	26/06/2017	\$ 12 504 031 516
6. Litecoin	13/10/2011	\$ 7 923 310 528

Fuente: Elaboración propia a base de datos de Coinmarketcap.com (2018).

3.1. Bitcoin

El BTC es la criptomoneda más importante que jamás haya existido y la primera en lanzarse (2009) por el usuario anónimo Satoshi Nakamoto. Usa tecnología P2P para operar sin autoridades centrales ni bancos, gestionando la red las transacciones y la emisión de moneda colectivamente. Es la moneda que cotiza en un mayor número de mercados y con el valor más elevado (alcanzando una capitalización máxima de 326 000 millones de dólares, que la situaría en el top 10 del índice NASDAQ 100, por ejemplo).

Algunas de sus características principales son:

- **Facilidad para pago móvil.** Permite realizar pagos con tecnología NFC mediante un código QR de tu *wallet*, parecido a los pagos con tarjetas bancarias *contactless*.

- **Seguridad y control.** Posee seguridad criptográfica de nivel militar, lo que permite tener alta protección contra el fraude si se protegen bien las claves.
- **Pagos internacionales rápidos.** No hay bancos intermediarios que hagan esperar tres días hábiles, ni comisiones extra o limitaciones en la cantidad mínima o máxima que puedes enviar.

Su funcionamiento consiste en lo siguiente:

- Cuando una persona transfiere una determinada cantidad de BTC a su destinatario, la red global de usuarios mineros verifica que los datos sean correctos y, una vez verificados, la transacción se realiza y se añade al historial público de transacciones dentro del bloque correspondiente. Dicho historial queda replicado en todos los usuarios. La verificación tiene que ser confirmada por una mayoría de la red de mineros para evitar que se produzcan actos fraudulentos o dar prioridad a unas transacciones frente a otras.
- Solo se crea un bloque cada 10 minutos, con un tamaño de 1 MB cada uno y que contiene en formato TXT toda la información, dentro del cual caben unas 2000 transacciones. Los mineros reciben recompensas por validar las transacciones, que se van reduciendo a la mitad cada 2016 bloques creados.

3.2. Ethereum (ether)

El caso de Ethereum es particular. En sí, es una plataforma que permite desarrollar aplicaciones descentralizadas usando la tecnología *blockchain*. Es una herramienta para crear contratos inteligentes. *Ether* es la criptomoneda de la plataforma Ethereum.

Estos contratos inteligentes sirven generalmente para:

1. **Mantener un almacén de datos que representa información útil para otros contratos:** por ejemplo, un contrato que graba el alta de un miembro de una organización particular.
2. **Ejecutar un contrato entre múltiples usuarios en caso de que ciertas condiciones se cumplan,** como puede ser un contrato que automáticamente paga una cantidad de dinero a quien sea que dé una respuesta válida a un problema matemático.
3. **Otros usos:** sistemas de votación (en empresas o en elecciones, por ejemplo), intercambios financieros, plataformas de micromecenazgo, propiedad intelectual y organizaciones descentralizadas autónomas.

La plataforma Ethereum está diseñada para que los usuarios creen sus códigos software, que se ejecutan por sí mismos bajo ciertas circunstancias acordadas de antemano por las partes, y para que se utilice su moneda *ether* como pago. Las principales diferencias con *bitcoin* son las siguientes:

- No hay un límite máximo de *ethers* en circulación. Mientras la tecnología Bitcoin tiene una limitación en la emisión de 21 millones de BTC.
- El tiempo de confirmación de las operaciones es de 16 segundos en Ethereum y de 10 minutos en Bitcoin.

- Los nodos de confirmación de Ethereum están muy concentrados en los creadores. Esto hace que el sistema no sea tan descentralizado como el de Bitcoin.

3.3. Ripple

Ripple fue creada como una red de pagos digitales para transacciones financieras al instante. Desde su nacimiento, se ha ido especializando en pagos transfronterizos (pagos entre distintos países).

El sistema de Ripple está diseñado para entidades financieras y proveedores de pagos de todo el mundo. Esta tecnología evita que las transacciones transfronterizas pasen por intermediarios.

Por tanto, Ripple aporta los siguientes beneficios:

- Operaciones al instante.
- Ahorro de costes.
- No existen problemas de escalabilidad y trazabilidad en tiempo real.

3.4. Litecoin

Está considerado como el hermano pequeño del *bitcoin*, ya que funciona del mismo modo, aunque posee un límite de monedas mucho más elevado, situado en los 84 millones de *litecoins*, por lo que tiene mayor liquidez en el mercado de divisas.

Es la moneda más utilizada por las personas que tienen menos experiencia en el mundo de las criptomonedas, porque su funcionamiento es más sencillo y menos exigente, ya que el tiempo de generación de bloques es de 2,5 minutos en lugar de los 10 minutos del *bitcoin*, por lo que se puede gestionar con ordenadores más sencillos y existe mayor agilidad para realizar un gran número de transacciones.

A continuación, se muestra una tabla ilustrativa con la oferta máxima de monedas preestablecida en su código que serán emitidas y el número de transacciones que cada una puede realizar por segundo comparándolas con otras formas de pago aceptadas:

Tabla 3. Emisión máxima y número medio de transacciones por segundo de las principales criptomonedas

Moneda	Oferta máxima	Transacciones, de media, por segundo
VISA	–	24 000
Ripple	38 305 873 865	1500
Paypal	–	193
Bitcoin Cash	21 000 000	60
Litecoin	84 000 000	28
Dash	22 000 000	48
Ether	Sin máximo	20
Bitcoin	21 000 000	7

Fuente: Elaboración propia en base al artículo de Howmuch.net (Raul, 2018).

3.5. Otras criptomonedas de distinta índole

3.5.1. Lisk (LSK)

La plataforma descentralizada Lisk permite la implementación, distribución y monetización de aplicaciones y *blockchains* personalizadas. Se asoció con Microsoft para integrar Lisk en su *blockchain* llamada Azure, donde los desarrolladores pueden desarrollar, probar e implementar globalmente aplicaciones de la *blockchain* Lisk usando la plataforma en la nube de Microsoft y su infraestructura. Además, es un software de código abierto que permite tener una visión clara de lo que están haciendo otros desarrolladores y, de esta forma, mejorar las nuevas aplicaciones y funcionalidades construidas en la red Lisk.

3.5.2. Tronix (TRX)

Tron es un protocolo *blockchain* para un sistema de contenido gratuito de entretenimiento, que permite a cada usuario publicar libremente, almacenar y poseer información, y, de forma descentralizada, decidir la distribución y suscripción de contenidos. Esto permite a los creadores de contenido publicar, poner en circulación y gestionar sus activos digitales, formando un ecosistema de contenido descentralizado. Tronix está basado en Ethereum, y usa su moneda *ether* como unidad básica en la plataforma.

3.5.3. SolarCoin (SLR)

Su objetivo es generar un registro descentralizado, incorruptible y auditable de la energía solar producida por cualquier individuo o empresa. Registrando su instalación energética en la *blockchain* de SolarCoin, los propietarios reciben un crédito digital (1 SolarCoin) por cada megavatio/hora producido. Trata de recompensar a los propietarios de estas instalaciones por su contribución y limitar la dependencia y riesgo de los subsidios estatales.

3.5.4. LBRY Credit (LBR)

Planea ofrecer una biblioteca mundial de contenido multimedia, desde libros y películas hasta canciones y videojuegos, al mismo tiempo que ofrece la opción de la venta digital de esas mismas obras. Todo controlado únicamente por los usuarios: son ellos los que decidirán si su contenido tendrá un valor y qué valor tendrá, y solo ellos cobrarán las ganancias, sin intermediarios. LBRY está diseñado, sobre todo, para eliminar la brecha existente entre los creadores y los usuarios finales. También existe una política contra contenido inadecuado y el intercambio de contenido ilegal, según la cual los infractores reciben su respectiva sanción.

3.5.5. Telegram Open Network (GRAM)

Telegram, el servicio de mensajería instantáneo y basado en la nube, ha lanzado TON, que, combinando tiempos de transacción mínimos con seguridad y escalabilidad, tiene como

objetivo ser una alternativa a VISA/Mastercard para la economía descentralizada, sobre todo teniendo en cuenta la gran base de usuarios que puede tener para empezar el proyecto (200 millones de usuarios en el mundo).

3.5.6. MobileGO (MGO)

MobileGo es una aplicación móvil que engloba todas las funciones que solemos tener repartidas en distintas aplicaciones, ya que realiza las siguientes funciones: optimiza las aplicaciones y las protege, transfiere archivos desde el ordenador, hace copia de seguridad de toda la información del móvil, optimiza la velocidad del móvil, etc.

3.6. Evolución del mercado de criptomonedas

Tras haber comentado algunas de las principales criptomonedas del mercado, a continuación vamos a observar cuál ha sido el peso relativo de estas en cuanto a la posición de dominancia histórica del *bitcoin* en el mercado de criptomonedas, según su capitalización en el conjunto de mercados donde operan.

Podemos observar cómo, a lo largo del periodo estudiado, el peso en el mercado de Bitcoin va decreciendo continuamente. En agosto de 2015, suponía más del 80 % de capitalización del mercado de criptomonedas, reduciéndose a pesos relativos irrelevantes el resto de activos de divisa virtual. Hasta abril de 2017, se mantiene en niveles cercanos al 80 %, fecha a partir de la cual comienza a perder importancia. En julio de 2017 se produjo el mayor acercamiento al reinado absoluto de Bitcoin: BTC supone un 40 % y ETH un 33 %.

En la actualidad, con datos actualizados a 11 de mayo de 2018, se observa cómo el reparto de importancia es más equitativo, con BTC en niveles del 37 %, las criptomonedas minoritarias se apuntan un 25 %, seguido del *ether* con un 17 % y el *ripple* un 7 %.

Por tanto, podría decirse que la tendencia está cambiando y las *altcoins* de menor tamaño van acaparando cada vez más la inversión del mercado.

4. Las ofertas públicas de moneda (ICO)

Las ICO o *Initial Coin Offerings* son peticiones de capital que realizan las empresas de nueva creación (*startups*) y también las empresas más consolidadas que quieren financiar el desarrollo de su actividad principalmente en negocios relacionados con *blockchain* y que son usadas para superar los procesos regulados y rigurosos de captación de capital requeridos por instituciones bancarias o inversores privados de *venture capital*. En una ICO, un porcentaje de la empresa es vendida a los inversores iniciales del proyecto a cambio de una cantidad de la criptomoneda emitida a modo de acción de la propia empresa, normalmente valorada en *bitcoin*.

Cuando la *startup* quiere captar fondos mediante una ICO, crea un plan de negocio donde establece de qué va el proyecto, qué necesita para completarse totalmente, cuánto dinero necesita para llevarlo a cabo (referidos en cantidad de USD), cuántos *tokens* de la nueva criptomoneda de la empresa se quedan los empresarios del proyecto y cuántos se emiten, cuál es el precio de cada *token* y la duración de la campaña de captación de capital.

Si el dinero captado con la ICO no cumple con los requerimientos mínimos de fondos de la empresa, este es devuelto a los inversores y la ICO se declara nula. Estos inversores iniciales están normalmente motivados a comprar *tokens* de la empresa con la esperanza de que el proyecto tenga éxito y se traduzca en un aumento del valor de la criptomoneda. La misma motivación sigue a los inversores de Ofertas Iniciales de Capital (ICO) en empresas tradicionales. Sin embargo, las ICO tienen un peligro muy elevado debido a que, al no estar reguladas por autoridades financieras como la SEC (Securities Exchange Commission; autoridad del mercado de valores estadounidense) o la CNMV (Comisión Nacional del Mercado de Valores; autoridad del mercado de valores en España), los fondos que desaparecen como consecuencia de iniciativas fraudulentas, nunca pueden ser recuperados. Por tanto, existe un riesgo mucho más alto en invertir en dicho tipo de proyectos que en proyectos de empresas que emiten acciones de forma regulada.

4.1. Tipos de ICO

Cabe señalar que existen dos tipos de emisión de criptomonedas para financiar proyectos. En la mayoría su precio se referencia a BTC o ETH. A continuación se explica en qué consiste cada tipo de emisión de *tokens* en una ICO (Wilmoth, 2017):

- **Utilitytokens.** Representan acceso futuro a los productos y servicios de la empresa. No están diseñadas como inversiones especulativas. Al vender *utilitytokens*, la empresa promueve su negocio haciendo que los propios inversores del proyecto paguen sus productos y servicios con dicha moneda. Por ejemplo, Filecoin levantó 257 millones de dólares vendiendo sus *tokens*, que permitirán a sus dueños tener acceso a su nube de almacenamiento descentralizado.
- **Security Tokens.** Funcionan como las participaciones, en cuanto a que su valor se deriva del desarrollo de la empresa y tienen derecho a rendimientos económicos (dividendos). Este tipo de *token* es minoritario en la actualidad.

Recientemente, en septiembre de 2017, el Banco Popular de China prohibió oficialmente las ICO, obligando a las empresas que habían recaudado fondos por medio de tal sistema a devolver íntegramente el dinero a sus inversores. El Banco Central declaró la imposibilidad de usar *tokens* como moneda en el mercado. Fue una muestra más de los problemas que las criptomonedas están encontrando en las regulaciones nacionales. Empresas como Kodak o Telegram ya han publicado su intención de emitir sus propias monedas virtuales, y gobiernos como el de Venezuela también están trabajando para financiarse emitiendo su propio *token* (el Petro, cuyo valor está basado en los recursos naturales de Venezuela, como petróleo, oro, diamantes y gas).

4.2. Evolución de captación de financiación por ICO

Tras extraer información de la base de datos más relevante en la actualidad (Icodata.io, 2018) de los años 2014, 2015, 2016, 2017 y hasta abril de 2018, podemos observar la evolución de este tipo de financiación en los últimos años:

Tabla 4. Evolución de número y financiación de ICO

Año	Capital en millones USD	Número de ICO
2014	16,03	2
2015	6,08	3
2016	94,01	30
2017	6094,63	872
2018	3901,05	607
2018 prev	11 703,15	1821

Fuente: elaboración propia a partir de datos de Icodata.io (2018).

El número total de ICO con éxito ha ido evolucionando exponencialmente, desde cantidades apenas relevantes de 2014 a 2016, a su eclosión en los años 2017 y 2018 con 872 y 607, respectivamente, con una previsión en el año 2018 de casi el doble del total de 2017. En cuanto al montante total de estas captaciones de capital, también se observa el punto de inflexión del año 2017, pasando de menos de 100 millones en el año anterior a 6094 millones de dólares. Esto refleja el monumental tamaño que está adquiriendo esta forma de financiación en las empresas de la nueva era.

5. Comparación con otras formas de dinero

En este apartado vamos a realizar un análisis comparativo de distintas características financieras que poseen las criptomonedas, las divisas de curso legal o monedas *fiat* y los metales preciosos, para ver en qué puntos coinciden y en cuáles discrepan, con el fin de encontrar similitudes que puedan acercar la divisa virtual a un activo usado como forma de pago común (como la divisa *fiat*) y/o como reserva de valor (como los metales preciosos).

Tabla 5. Las criptomonedas y sus comparables

	Criptomonedas	Monedas <i>fiat</i>	Metales preciosos y petróleo
Oferta limitada	La cantidad que se va a crear suele ser fija, aunque hay monedas que no tienen un máximo de emisión	Los bancos centrales pueden emitir más moneda para implantar políticas económicas	Tienen un suministro limitado, son recursos escasos
Fungible	Da igual tener una moneda que otra dentro del mismo tipo	La mayoría de moneda fiduciaria es idéntica y fungible	Una onza de oro o un litro de crudo tienen el mismo valor en otra parte del mundo
Divisible	Un BTC es divisible hasta ocho decimales y un ETH hasta 18	Normalmente divisible hasta dos decimales.	Divisible, pero con coste y dificultad.

(Continúa)

Tabla 5. Las criptomonedas y sus comparables (Cont.)

	Criptomonedas	Monedas fiat	Metales preciosos y petróleo
Falsificación	No puede ser falsificado, ya que el rastro de cada unidad puede ser perseguido y verificado	La moneda fiat tiene una larga historia de falsificaciones	Se puede intentar falsificar, pero el tipo de material es fácilmente identificable
Pérdida de valor	En monedas de oferta limitada, no existe pérdida de valor, aunque sí en monedas con oferta ilimitada	Si hay X USD y se crean más, estos cada vez valen menos, por lo que pierden valor a lo largo del tiempo	El oro o la plata no pierden valor a lo largo del tiempo, al igual que otros metales preciosos
Fácilmente transferibles (forma de intercambio)	Pueden enviarse al instante a todo el mundo, y las transacciones son confirmadas en minutos	Transferido de una manera fácil, aunque los tiempos de espera suelen ser de 24 horas para la transferencia nacional y de 72 horas para la internacional	Requiere estar presente para poder intercambiarse. Puede ser enviado a largas distancias, pero con un alto coste
Centralización	Son monedas descentralizadas, basadas en la confianza de la red y en la criptografía	Controlada por los gobiernos y los bancos centrales	No están controladas por una autoridad
Anonimato	Se pueden rastrear, pero no se puede conocer la identidad de los usuarios que han realizado las operaciones	Todas las transacciones digitales están vinculadas a una identidad	No se puede vincular a una persona

Fuente: elaboración propia en base a Nava Jurado (2017).

6. Ventajas y desventajas

Las principales ventajas de las criptomonedas son las siguientes:

- Están descentralizadas, es decir, no las controla ninguna institución ni gobierno.
- Se pueden utilizar a nivel global, siempre que el país no las prohíba.
- Son muy seguras y, si las adquieres, serán de tu propiedad en exclusiva.
- Ofrecen privacidad en las transacciones, puesto que son anónimas.
- No hay intermediación y todas las transacciones se realizan de persona a persona.
- Las transacciones con criptodivisas son bastante más rápidas que con dinero fiat.
- Las criptodivisas sirven para realizar transacciones tanto online como en establecimientos físicos, aunque la oferta es más limitada.

En cuanto a las desventajas de las criptomonedas, podemos mencionar las siguientes:

- **Regulación.** Creciente interés a nivel mundial por parte de organismos y gobiernos para regular el mercado de criptodivisas y frenar la captación de dinero por medio de ICO.

- **Lavado de dinero negro.** Las propiedades inherentes a las criptomonedas, como su anonimato e irrevocabilidad de las transacciones sin dejar rastro evidente para las autoridades, hacen que el proceso de lavado de dinero (*moneylaundering*) pueda realizarse sin mayor complicación. Tal y como explica Brenig *et al.* (2015), las personas que cometen actividades criminales encuentran facilidad en lavar su dinero mediante la compra de criptomonedas. Hoy en día estamos viendo cómo salen a la venta activos de gran valor, como casas y coches, que se ofertan exclusivamente en *bitcoin*.
- **Actividades fraudulentas, hackeo y financiación del terrorismo.** Las criptomonedas son usadas para la compra de bienes y servicios en el mercado negro (la llamada *deep web*), donde se emplean para el pago de drogas, pornografía, documentos confidenciales, así como para armas y munición. En este sentido, se conoce que organizaciones terroristas obtienen financiación en criptomonedas y con ellas adquieren todo tipo de material militar que necesitan.

Otros países como Corea del Norte, al que se aplican medidas restrictivas comerciales para evitar su continua militarización, también han sido acusados de hackear plataformas de intercambio para robar criptomonedas y obtener financiación. Muy sonado fue el caso de hackeo de Mt. Gox, una plataforma de intercambio de *bitcoin* que sufrió el robo de casi 350 millones de dólares en 2014, forzándola a declararse en bancarrota y desaparecer. Recientemente, en 2018, la compañía de *trading* de criptomonedas Coincheck fue el objetivo del mayor hackeo hasta el momento, con una pérdida de aproximadamente 530 millones de dólares valorados en monedas NEM.

- **Economía deflacionaria.** A diferencia de las divisas *fiat*, que pueden ser impresas infinitas veces por un banco central, ciertas criptomonedas como el *bitcoin* no pueden nunca generar inflación mediante la impresión de ellas. La característica de una cantidad de dinero fija hace que la divisa tienda a ser deflacionaria (más poder de compra con el tiempo). Muchos economistas opinan que esto sería un desastre, ya que la gente tendería a ahorrar dinero en vez de gastarlo, esperando a que los precios caigan más. Esto haría que disminuyera el consumo y la inversión y llevaría a una situación de ralentización económica.

Sin embargo, otros expertos creen que esta acumulación de dinero puede vencerse por la bajada de precios de los vendedores, hasta un punto donde el instinto de ahorro del consumidor desaparezca. Como el vendedor también está motivado a acumular dinero, el descuento en sus precios se convierte en el precio de equilibrio en el que los instintos de ahorro de compradores y vendedores concurren. Queda por ver si el aspecto deflacionario de la moneda es realmente un problema cuando no está causado por una retracción rápida de la economía.

7. Regulación de organismos y gobiernos en torno a las criptomonedas

Mientras que el mercado de las criptomonedas está en expansión y posee suficiente potencial para revolucionar la forma de enviar dinero, el hecho de que no sea globalmente reconocido como moneda de pago oficial para bienes y servicios hace que no se facilite su estandarización por los organismos y gobiernos. Una vez que se produzca gradualmente su aceptación como moneda alternativa de pago y forma de financiación (ICO), su volatilidad se reducirá

exponencialmente y dejaremos de hablar de las criptomonedas como un activo de alto riesgo y a punto de estallar. A continuación abordaremos cómo se encuentra la regulación en torno a ellas en distintas partes del mundo.

Tabla 6. Regulación actual por países sobre las criptomonedas

Geografía	Regulación
Corea del Sur	Quiere obligar a todos los <i>exchanges</i> a identificar a sus usuarios previamente, acabando así con las transacciones anónimas y el paraíso fiscal virtual que suponían hasta ahora. Aquellas cuentas cuyos nombres de usuario no coincidan con los de su cuenta bancaria quedarán deshabilitadas
Japón	Exigir a los usuarios que se registren con documentos oficiales para su identificación. Requerimientos estrictos de seguridad y transparencia para permitir operar a casas de cambio
China	El mayor consumidor y productor a nivel mundial de <i>bitcoins</i> ordenó cerrar las casas de cambio de criptomonedas que operaban en el país (septiembre de 2017). Prohibición a bancos y compañías de medios de pago la realización de transacciones de alto montante con criptomonedas. Prohibición de ICO. Pensando en prohibir la minería de <i>bitcoin</i> para acabar con el consumo intensivo de energía
Rusia	El presidente Putin ha anunciado que publicarán una ley el 1 de julio de 2018 que regule las criptomonedas, con especial hincapié en lo que se refiere a las ICO y recaudación de dinero
Estados Unidos	La SEC aumenta el control sobre las ICO, prohibiendo varias de ellas recientemente por sospechas de estafa y fraude. Existencia de pago de impuestos por plusvalías en criptomonedas
Europa	Existe consideración de regular las criptomonedas del BCE; actualmente la UE quiere identificar a los usuarios de plataformas de intercambio de criptomonedas para que tributen. En países como Alemania o Finlandia, existe ya la obligación de tributar por ganancias de capital
España	Hacienda requiere información a entidades que intervienen en la compraventa de criptomonedas (<i>brokers</i>) y también a empresas que aceptan a las mismas como forma de pago para la compra de sus productos. Del mismo modo, advirtió de que hay que declarar y pagar impuestos por las plusvalías obtenidas en la compraventa de criptomonedas en el IRPF y en el impuesto de sociedades para el caso de empresas
Australia	Sistema de gravación de impuestos sobre ganancias de capital en criptomonedas

Fuente: elaboración propia.

8. Análisis de datos: rentabilidad, volatilidad y correlación

8.1. Comparativa con metales preciosos, petróleo, divisas *fiat* y acciones

Para tomar datos con el mismo horizonte de tiempo y que puedan ser congruentes, en este estudio se analizarán *bitcoin*, *ethereum*, *ripple* y *litecoin*, excluyendo a *bitcoin cash* y NEO ya

que solo tenemos datos desde 2017 y sería un análisis demasiado cortoplacista. Por tanto, la fecha de inicio del estudio será el 8 de agosto de 2015, cuando estas principales criptomonedas empezaron a cotizar simultáneamente.

Para realizar el estudio propuesto, hemos obtenido los valores de cotización diarios de las cuatro criptomonedas en análisis, de metales preciosos (oro y plata), petróleo Brent, divisas *fiat* (euro y libra esterlina) y, por último, de las dos mayores empresas del mercado estadounidense (Apple y Microsoft) y del mercado europeo (Anheuser-Busch InBev y Louis Vuitton).

A partir de las cotizaciones diarias, realizando cálculos estadísticos hemos obtenido la siguiente tabla representativa con sus rentabilidades y volatilidades:

Tabla 7. Rentabilidad y volatilidad por tipo de activo de la muestra

	Rentabilidad			Volatilidad			
	Diaria	Anualizada	Periodo	Intradiaria	Diaria	Anualizada	Periodo
Ether	0,94 %	2963,88 %	90 112,06 %	4,63 %	7,45 %	142,33 %	3750,95 %
Ripple	0,79 %	1662,26 %	7981,03 %	3,61 %	9,68 %	184,87 %	4872,05 %
Litecoin	0,54 %	612,94 %	3461,56 %	3,15 %	6,33 %	120,94 %	3187,41 %
Bitcoin	0,43 %	380,83 %	3134,29 %	2,42 %	4,14 %	79,06 %	2083,70 %
Microsoft	0,11 %	33,25 %	106,42 %	0,82 %	1,43 %	22,58 %	495,28 %
Brent	0,11 %	32,08 %	51,53 %	1,49 %	3,20 %	51,34 %	1136,97 %
Louis Vuitton	0,09 %	24,42 %	68,45 %	0,90 %	1,53 %	24,50 %	540,76 %
Apple	0,08 %	21,05 %	57,53 %	0,83 %	1,47 %	23,23 %	509,45 %
Oro	0,03 %	7,50 %	19,35 %	0,61 %	0,81 %	13,02 %	289,93 %
Plata	0,02 %	5,55 %	9,30 %	1,09 %	1,30 %	20,94 %	466,53 %
EUR/USD	0,01 %	3,24 %	8,39 %	0,39 %	0,52 %	8,34 %	190,59 %
GBP/USD	-0,02 %	-4,40 %	-13,11 %	0,47 %	0,67 %	10,77 %	240,16 %
AB InBeb	-0,04 %	-9,21 %	-28,17 %	0,90 %	1,35 %	21,50 %	474,53 %

Fuente: elaboración propia.

Una vez ordenada la tabla, de mayor a menor rentabilidad promedio (tanto diaria como anual), extraemos que las cuatro criptomonedas han experimentado subidas diarias, en promedio, con valores dentro de un rango de 0,43-0,94 %, muy por encima del rango obtenido por los activos comparables del estudio (de - 0,04 % a 0,11 %). En términos anualizados, ponderado por el número de sesiones cotizados por cada activo anualmente, la brecha es aún

mayor situándose el valor más cercano (Microsoft) 12 veces por debajo de la criptomoneda de menos rentabilidad (*litecoin*). También hay que destacar la rentabilidad total del periodo, que en las criptomonedas del estudio se sitúa en el rango 3134-90 112 % de rentabilidad, que son valores que se encuentran a años luz de las rentabilidades obtenidas por el petróleo Brent, el oro y la plata, las divisas *fiat* o las acciones de empresas.

Si hablamos de volatilidades, se aprecia de una forma clara que las criptomonedas han estado también a la cabeza de esta estadística, con valores intradiarios rondando el 3,5 %, muy lejano de las volatilidades promedio diarias de 0,47-1,49 % de los activos comparables. En valores diarios la diferencia es aún mayor.

Por su parte, la volatilidad anualizada, ha sido calculada como la multiplicación de la volatilidad promedio diaria y la raíz cuadrada del número total de sesiones cotizadas en un año completo por activo. Este valor refleja también una larga brecha entre criptomonedas y resto de activos comparables, aunque hay que destacar que el crudo Brent (51,34 %) alcanza valores muy cercanos al *bitcoin* (79 %).

Concentración por categorías

Para una visión más específica, se ha realizado un estudio más conciso realizando ponderaciones de cada activo para incluirlos dentro de una categoría de estudio. Los metales preciosos (oro y plata) se ponderan al 50 % cada uno, al igual que las divisas *fiat* (euro y libra esterlina). Por su parte, las criptomonedas y las acciones de empresas se ponderan de acuerdo con su peso por capitalización, siendo los siguientes, y pasando a USD la capitalización de empresas europeas a tipos actuales (1,1944 EUR/USD):

Tabla 8. Capitalización y peso relativo a su categoría

	Capitalización	% peso/total
Bitcoin	154 142 000 000	58,29 %
Ether	72 233 800 000	27,31 %
Ripple	29 641 400 000	11,21 %
Litecoin	8 439 920 000	3,19 %
Apple	926 847	45,94 %
Microsoft	752 347	37,29 %
AB InBev	161 752	8,02 %
Louis Vuitton	176 566	8,75 %

Fuente: elaboración propia.

Teniendo en cuenta estos cuadros de ponderación, y obteniendo la categoría «metales preciosos» y «divisa *fiat*» como el promedio de sus dos valores, se ha obtenido la siguiente tabla resumen del estudio de rentabilidades y volatilidades:

Tabla 9. Rentabilidades y volatilidades por categoría de activo

	Rentabilidad			Volatilidad			
	Diaria	Anual	Periodo	Intradiaria	Diaria	Anual	Periodo
Criptomonedas	0,61 %	1237,40 %	27 445,08 %	3,18 %	5,73 %	109,54 %	2886,84 %
Petróleo	0,11 %	32,08 %	51,53 %	1,49 %	3,20 %	51,34 %	1136,97 %
Empresas	0,08 %	23,47 %	69,84 %	0,84 %	1,45 %	22,96 %	504,11 %
Metales preciosos	0,02 %	6,53 %	14,32 %	0,85 %	1,06 %	16,98 %	378,23 %
Divisas <i>fiat</i>	0,00 %	-0,58 %	-2,36 %	0,43 %	0,59 %	9,56 %	215,37 %

Fuente: elaboración propia.

En términos de rentabilidad, el promedio diario de las criptomonedas es seis veces mayor que la del crudo Brent y 20 veces que la de los metales preciosos. De forma anual, también se aprecia una diferencia elevada. Por tanto, en términos de rentabilidad, el comportamiento de las principales divisas virtuales ha sido totalmente desorbitante, lejos de aquella obtenida por activos tradicionales. Esto no nos asombra, ya que son activos de corta edad.

En cuanto al riesgo, medido por la volatilidad de los rendimientos, las conclusiones obtenidas son las siguientes. Primero, de forma intradiaria el petróleo se sitúa en la mitad de los niveles de agitación de las criptodivisas, mientras que los activos más comparables por características (divisas *fiat*) experimentan niveles siete veces inferior. En segundo lugar, la volatilidad diaria también refleja dos mundos paralelos: niveles cercanos al 6 % en las criptodivisas y niveles entre 0,59 y 3,20 % para aquellos activos más tradicionales. El comentario es el mismo para niveles anualizados y del periodo total de estudio.

Tabla 10. Volatilidad diaria de criptomonedas por año

Volatilidad diaria	BTC	ETH	XRP	LTC
2015	3,49 %	9,64 %	4,93 %	4,07 %
2016	2,51 %	6,92 %	3,74 %	3,01 %
2017	4,99 %	7,30 %	14,38 %	8,69 %
2018	5,52 %	6,40 %	8,29 %	7,16 %

Fuente: elaboración propia.

Si hacemos hincapié en la evolución de la volatilidad diaria, apreciamos cómo la volatilidad de los rendimientos diarios aumenta sustancialmente en todas, excepto en *ether*, que en 2018 obtuvo su volatilidad mínima desde su lanzamiento. En contraparte, *ripple* y *litecoin* han visto en 2018 también reducida su volatilidad pero sigue siendo alrededor de un 40 % superior a la de 2015. Por último, *bitcoin* se ha estancado en valores cercanos al 5 %.

Análisis de correlación

Debido a que el oro, la plata, el petróleo, el euro y la libra esterlina tienen muchos menos días de cotización que las criptomonedas porque no cotizan los siete días de la semana, para hacer un análisis de correlación adecuado hemos tomado como valores *dummies* el promedio del día anterior y posterior para aquellas sesiones sin dato en los días del año en que no cotizaban estos activos. De esta forma, obtenemos el total de 1.008 datos de sesiones para analizar cuál es la correlación entre cada una de las criptomonedas y los activos comparables.

A continuación se representa el número de sesiones de la muestra durante el periodo estudiado. La primera fila representa el total de sesiones del periodo y la segunda fila la diferencia negativa en sesiones respecto a las de las criptomonedas:

Tabla 11. Número de sesiones cotizadas por activo

	Criptos	Oro	Plata	Brent	EUR	GBP	Apple	Microsoft	AB InBev.	LV
Sesiones	1008	718	718	711	738	720	668	668	679	679
Diferencia		290	290	297	270	288	340	340	329	329

Fuente: elaboración propia.

Una vez realizada la interpolación de datos para conseguir el mismo número de valores para cada activo, se ha realizado un análisis de correlación.

Tabla 12. Coeficientes de correlación con las criptomonedas

	BTC	ETH	XRP	LTC	Promedio
BTC	1,00				
ETH	0,92	1,00			
XRP	0,83	0,90	1,00		
LTC	0,96	0,94	0,88	1,00	
Oro	0,47	0,50	0,41	0,45	0,46
Plata	0,03	0,04	0,03	0,00	0,03
Brent	0,77	0,75	0,64	0,73	0,72
EUR	0,76	0,81	0,66	0,77	0,75
GBP	-0,07	-0,03	0,01	0,00	-0,02
Apple	0,82	0,81	0,65	0,77	0,76
Microsoft	0,86	0,87	0,71	0,83	0,82
AB InBev	-0,64	-0,67	-0,56	-0,65	-0,63
LV	0,79	0,78	0,63	0,74	0,73

Fuente: elaboración propia.

De la tabla anterior podemos extraer las siguientes conclusiones:

- En cuanto a la correlación existente entre criptomonedas, observamos un altísimo grado entre ellas, con valores superiores a 0,83. Esto es, por cada 1 % de aumento en la cotización de BTC, por ejemplo, el XRP aumenta un 0,83 %.
- Por su parte, hallamos un coeficiente promedio de correlación elevado con la evolución de la cotización de las cuatro principales criptomonedas del crudo Brent (0,72), EUR/USD (0,75), Apple (0,76), Microsoft (0,82) y Louis Vuitton (0,73). La plata y GBP/USD apenas coinciden con ellas, con coeficientes cercanos a cero. Destacar la correlación inversa promedio de 0,61 con las acciones de Anheuser-Busch InBev.
- El estudio de la correlación entre criptomonedas y el resto de activos puede no tener implicaciones claras ya que para poder realizar los cálculos ha sido necesaria la interpolación de las cotizaciones para aquellas fechas sin valor; esto hace que la muestra para el análisis no sea totalmente real.

8.2. Comparativa con las mayores empresas del mundo por capitalización

Para tener un poco más de perspectiva del tamaño que están alcanzado las criptomonedas en los mercados internacionales, se ha recogido en la siguiente gráfica la capitalización de las cinco principales criptomonedas a fecha 11 de mayo de 2018 y de multinacionales de distintos sectores y países que ostentan una posición de liderazgo en el mercado.

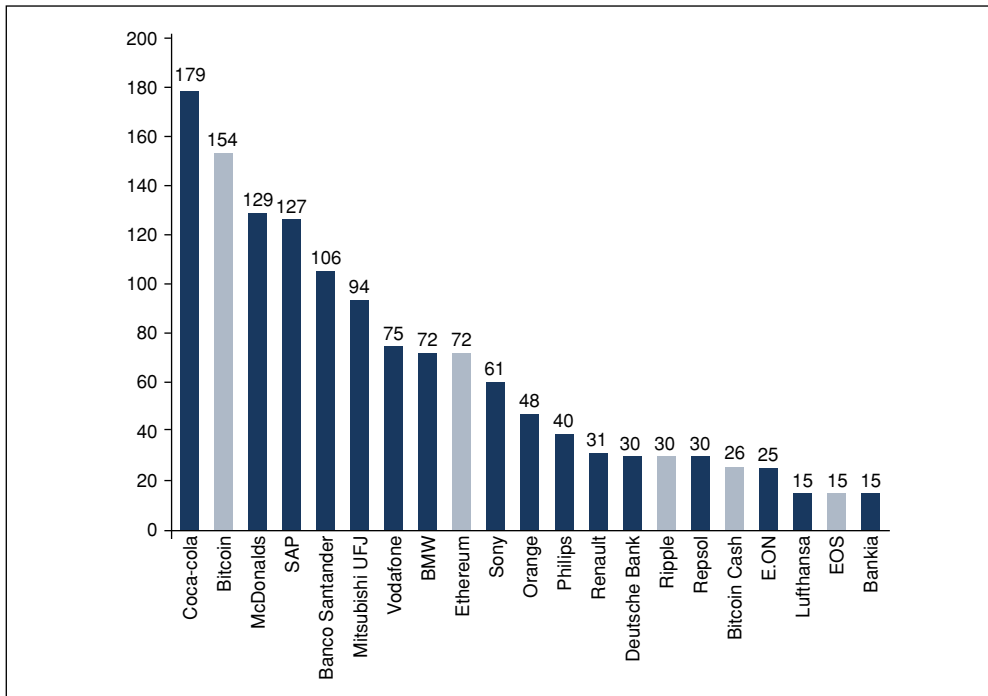


Figura 1. Capitalización en miles de millones de USD. Fuente: elaboración propia.

Tal y como se aprecia en la gráfica, vemos que si Bitcoin fuese una empresa, su tamaño por valor en el mercado financiero sería superior a empresas de gran envergadura como McDonalds, SAP o Banco Santander. Por su parte, Ether tendría un tamaño similar a Vodafone y BMW, mientras que Ripple y Bitcoin Cash se asemejarían a empresas como Renault, Deutsche Bank, Repsol o la alemana E.ON. La quinta criptomoneda por capitalización, EOS, estaría valorada por el mercado al mismo nivel que gigantes alemanes como Lufthansa o el banco español Bankia.

9. Conclusiones

El auge del comercio electrónico y la entrada en una de las mayores crisis financieras de la historia llevó a hacer realidad unas ideas que databan de los años 80, logrando en la actualidad un elevado interés internacional por parte de inversores, empresas, reguladores y gobiernos. Como vimos, la descentralización, la rapidez, la irrevocabilidad y el anonimato son los principales motores de estas nuevas formas de pago, cuyo sistema de incentivos para confirmar transacciones hace viable su existencia futura. Por otra parte, ha habido recientemente hackeos a bolsas de intercambio de criptomonedas, con los que muchos inversores perdieron sus carteras, sembrando dudas acerca de su seguridad o también el establecimiento de *pools* de minería que provocan una cierta centralización de las confirmaciones de transacciones (justo lo que se quería evitar).

El estudio de Brenig *et al.* (2015) nos acercó a una de las mayores críticas que las criptomonedas reciben en la actualidad, que es el incentivo que suponen para actividades de blanqueo de capitales. Las causas principales que apoyan esta teoría son su anonimato, instantaneidad de pagos y la inexistencia de intermediarios financieros.

Algunos rasgos monetarios de las criptodivisas (cantidad divisible, fungibilidad y transferibilidad) se asemejan funcionalmente a aquellos de las monedas de curso legal. Destacar la pérdida de peso relativa del *bitcoin* en el mercado, que llegó a suponer alrededor del 80 % de la capitalización total, pero desde principios del 2017 otras criptomonedas minoritarias de reciente creación han visto enfocado el interés de la comunidad inversora, suponiendo aquellas un 25 % mientras que Bitcoin acumula «únicamente» el 36,80 % del valor de inversión en criptodivisa.

La nueva forma de captación de fondos por empresas relacionadas con *blockchain*, las conocidas como ICO (*Initial Coin Offerings*) son una revolución, ya que no tienen que verse sometidas a rigurosos controles para poder captar financiación para sus proyectos, como sí tienen que enfrentarse las empresas que quieren empezar a cotizar en bolsa, y evitan las trabas para obtener préstamos bancarios en sus etapas iniciales. Para el año 2018, se prevé una captación a nivel mundial de 11.703 millones de dólares, duplicando la financiación en ICO del año anterior.

Otro de los aspectos clave en el entorno es la evolución de la regulación a nivel mundial. Uno de los países más estrictos en restricciones es China, que tiene prohibido el funcionamiento de casas de cambio con criptomonedas, la captación de fondos a través de ICOs y está cerrando el cerco a los *pools* de minería. Otros países, como Japón y Corea del Sur, dirigen más su atención a la identificación de los usuarios para poder grabar sus beneficios de

capital y controlar posibles movimientos para lavado de dinero negro. Estados Unidos aboga por un control más exhaustivo de las ICOs, rechazando aquellas que remitan sospechas de fraude, mientras que España solicita información a entidades que intermedian en la compra-venta y las que aceptan estas divisas como forma de pago para adquirir sus productos y/o servicios. De momento, como vemos, los movimientos de las distintas autoridades mundiales son diversos pero no se ponen de acuerdo en cuanto a qué debería regularse.

Tras el análisis de las cotizaciones diarias de las cuatro principales criptomonedas al inicio del estudio, del petróleo Brent, metales preciosos como oro y plata, divisas de curso legal y las mayores empresas americanas y europeas, obtuvimos evidencias empíricas que eran objeto del presente trabajo. Como era de esperar, en términos de rentabilidad, las criptomonedas reflejaron los valores más altos. Comparativamente, el Brent y las empresas seleccionadas fueron las que más se acercaron en rentabilidad diaria (6 veces menos), estando a años luz en valores anualizados y del período. De ahí extraemos que las criptomonedas aún no están en el momento de ser utilizadas de forma generalizada por su elevado riesgo de cambio de valor.

En volatilidades, también ocurrió la misma diversidad de resultados, aunque situándose el crudo Brent a aproximadamente la mitad del valor de las criptomonedas en todos los horizontes temporales estudiados. Por su parte, las divisas de curso legal apenas experimentaron volatilidad.

Finalmente, con el estudio de los coeficientes de correlación, utilizando cotizaciones interpoladas para aquellas fechas sin cotización, vimos correlaciones positivas bastante altas en el Brent, EUR/USD, Microsoft y Louis Vuitton, y correlación negativa destacable de AB Inbev. Sin embargo, estos resultados no son muy representativos ya que la interpolación suaviza las diferencias y estos datos «dummies» han supuesto entre el 40 y el 50% del total de datos de cotización de la mayoría de activos comparables para dicho análisis

Adicionalmente nos gustaría señalar que el uso exclusivo de una o dos monedas descentralizadas en el plano mundial, en vez de las alrededor de 180 monedas oficiales en circulación, haría que existiese una mayor integración y conexión entre todos los países del mundo y facilitaría el comercio entre ellos, eliminando el riesgo de divisa. De la misma manera, el control de la inflación es una medida necesaria para poder ajustar ciclos económicos y quizá un mercado libre totalmente no pueda conseguir por sí mismo niveles de inflación o deflación que reconduzcan la situación económica, siendo un aspecto negativo la generalización de las criptomonedas en este sentido.

Sin embargo, los países con instituciones débiles y monedas nacionales inestables, refiriéndome principalmente a países con dictaduras en donde el gobierno mueve a su propio interés la política monetaria y restringe su uso, pueden ver crecer su uso. Por ejemplo, en Venezuela su moneda local es muy inestable y la impresión masiva de dinero está provocando niveles de hiperinflación. Aquellas personas que guarden su capital en una criptomoneda (cuando se produzca la estabilización de su valor) pueden escapar de las restricciones de uso de la moneda local y de la pérdida continua de poder adquisitivo, ya que las criptomonedas cotizan en USD, BTC o ETH principalmente. También sería válido este argumento para la mayoría de países africanos. Adicionalmente, esta generalización de las criptomonedas, en su etapa estable, provocaría una apertura aún mayor del comercio mundial, ya que no habría que cambiar a dólares la moneda local como ocurre ahora para realizar compras internacionales.

Bibliografía

- Ameer, R. (2017). What is Cryptocurrency: Everything You Need To Know. Recuperado de <https://blockgeeks.com/guides/what-is-cryptocurrency/>, 10 de enero de 2018.
- Antonopoulos, A. M. (2014). *Mastering Bitcoin*. Recuperado de <https://www.safaribooksonline.com/library/view/mastering-bitcoin/9781491902639/ch08.html>.
- Brenig, C., Accorsi, R. y Muller, G. (2015). Economic Analysis of Cryptocurrency Backed Money Laundering. *Twenty-Third European Conference on Information Systems* (2015), 1-18. <https://doi.org/10.18151/7217279>.
- Coinmarketcap.com. (2018). Top 100 Cryptocurrencies by Market Capitalization. Recuperado de <https://coinmarketcap.com/>, 20 de abril de 2018.
- Cryptocompare.com. (2018). Ongoing ICOs. Recuperado de <https://www.cryptocompare.com/>, 7 de mayo de 2018.
- Farell, R. (2015). An Analysis of the Cryptocurrency Industry. *Wharton Research Scholars Journal. Paper*, 130. Recuperado de http://repository.upenn.edu/wharton_research_scholars%0Ahttp://repository.upenn.edu/wharton_research_scholars/130.
- Gil-Alana, L. A., Abakah, E. J. A y Rojo, M. F. R (2020). Cryptocurrencies and stock market indices. Are they related? *Research in International Business and Finance*, 5
- Icodata.io. (2018). Funds raised in ICOs. Recuperado de <https://www.icodata.io/stats/2018>, 20 de abril de 2018.
- Makarov, I. y Schoar, A. (2019). Trading and arbitrage in cryptocurrency markets. *Journal of Financial Economics*.
- . Price discovery in cryptocurrency markets. *AEA Papers and Proceedings*, 109, 97-99.
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Www.Bitcoin.Org*, 9. <https://doi.org/10.1007/s10838-008-9062-0>.
- Nava Jurado, A. (2017). Valor fundamental del bitcoin. *Instituto de Estudios Bursátiles*.
- OECD. (2018). Broad Money (M3). Recuperado de <https://data.oecd.org/money/broad-money-m3.htm>, 25 de abril de 2018.
- Raul. (2018). Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal? Recuperado de <https://howmuch.net/articles/crypto-transaction-speeds-compared>, 18 de febrero de 2018.
- Tuwiner, J. (2017). Pools de minería Bitcoin. Recuperado de <https://www.buybitcoinworldwide.com/es/mineria/pools/>, 24 de abril de 2018.
- Wilmoth, J. (2017). ICO 101: Utility Tokens vs. Security Tokens. Recuperado de <https://strategiccoin.com/ico-101-utility-tokens-vs-security-tokens/>, 24 de abril de 2018.