



FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES
DPTO. ANÁLISIS ECONÓMICO Y ECONOMÍA POLÍTICA
GRADO EN ECONOMÍA

TRABAJO FIN DE GRADO
CRIPTOMONEDAS: PASADO, PRESENTE Y ¿FUTURO?

Vº. Bº del Tutor:

Alumno:

D. Francisco Zabala Aguayo

D. Fco. Javier Egaña Huertos

Sevilla, Diciembre de 2018



FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

GRADO EN ECONOMÍA

TRABAJO DE FIN DE GRADO

CURSO ACADÉMICO (2018-2019)

TÍTULO: CRIPTOMONEDAS: PASADO, PRESENTE Y ¿FUTURO?

AUTOR: FCO. JAVIER EGAÑA HUERTOS

TUTOR: D. FRANCISCO ZABALA AGUAYO

DEPARTAMENTO: Análisis Económico y Economía Política

ÁREA DE CONOCIMIENTO: Economía Aplicada

RESUMEN:

Las criptomonedas han llamado la atención de especuladores, bancos, Estados y organizaciones debido a su alta volatilidad y a diversos beneficios para los inversores sobre otros productos financieros, como la falta de regulación o la alta tecnología empleada. El presente trabajo trata de analizar las causas del auge de este producto, partiendo de su historia, su mecanismo y su funcionamiento, así como de los beneficios que reporta y los peligros que conlleva su utilización. Para ello hemos recogido artículos de economistas como Jacobs o Lansky, fieles defensores de las criptomonedas, o Sovbetov, con una opinión más reservada sobre el futuro de éstas.

INDICE

| | |
|-----------------------------------------------------|-----------|
| INTRODUCCIÓN | 5 |
| 1. CRIPTOMONEDAS. ¿QUÉ SON? | 7 |
| 1.1. Definición y mercado | 7 |
| 1.2. Historia y evolución | 9 |
| 1.3. Funcionamiento | 12 |
| 1.4. Valor de la criptomoneda | 16 |
| 2. BENEFICIOS E INCONVENIENTES | 17 |
| 2.1. Pros y beneficios | 17 |
| 2.2. Contras y riesgos | 18 |
| 2.3. Soluciones a los riesgos | 21 |
| 3. CRIPTOMONEDAS EN LA ACTUALIDAD | 23 |
| 3.1. Criptomonedas en distintos países | 23 |
| 3.2. Regulaciones | 25 |
| 3.3. SMLY: La criptomoneda educativa | 28 |
| 4. EL FUTURO DE LAS CRIPTOMONEDAS | 31 |
| 4.1. Previsiones | 31 |
| 4.2. Criptomoneda moneda nacional | 32 |
| 4.3. Criptomoneda moneda mundial | 33 |
| 5. ENCUESTA | 36 |
| 6. BIBLIOGRAFÍA | 48 |

RELACIÓN DE FIGURAS

| | |
|-----------------------------------------------------------------------------|-----------|
| Figura 1. Evolución anual del BTC en USD hasta octubre de 2017 | 11 |
| Figura 2. Evolución del BTC en USD durante la burbuja | 12 |
| Figura 3. Funcionamiento del Bitcoin | 15 |
| Figura 4. Género de los encuestados | 37 |
| Figura 5. Edad de los encuestados | 38 |
| Figura 6. Estado laboral de los encuestados | 38 |
| Figura 7. Conocimiento de los encuestados sobre criptomonedas | 39 |
| Figura 8. Criptomonedas más conocidas por los encuestados | 40 |
| Figura 9. ¿Ha comprado criptomonedas? | 41 |
| Figura 10. Motivo de la compra de criptomonedas | 41 |
| Figura 11. ¿Compraría criptomonedas en el futuro? | 42 |
| Figura 12. Motivo de la compra futura de criptomonedas? | 43 |
| Figura 13. Seguridad de las criptomonedas actualmente? | 44 |
| Figura 14. Seguridad futura de las criptomonedas | 44 |
| Figura 15. Criptomonedas como método de pago | 45 |
| Figura 16. Criptomonedas como bien especulativo | 46 |
| Figura 17. Valoración del futuro de las criptomonedas | 46 |

INTRODUCCIÓN

A partir de finales de 2017, las criptomonedas han estado en boca de todos debido a la última burbuja financiera, la más grande de la historia. Quizás no tan sonada como la del ladrillo, la burbuja de las criptomonedas, o del Bitcoin, ha supuesto aumentos y caídas del valor de estos activos de más del 100 por cien. Esta situación ha llevado a Estados y organizaciones a plantearse si es necesaria una regulación del mercado y a los especuladores y economistas a plantearse el futuro de este activo tan complejo.

La palabra “criptomoneda” se ha hecho un hueco en los telediarios y en el sector financiero, por lo que en este trabajo intentamos ordenar y aclarar los puntos más importantes para la comprensión de por qué y cómo las criptomonedas han llegado a ser activos con valores tan desorbitados. La poca información que nos proporcionan los medios o las entidades bancarias hace que cueste entender el funcionamiento de las criptomonedas y sitúa al inversor en una posición de riesgo al enfrentarse a un producto desconocido.

Por ello, tratamos de recoger los puntos más importantes de la historia y el presente de las criptomonedas para, por último, focalizarlos en el futuro. El objetivo principal no es otro que ofrecer una visión clara de todos los aspectos que envuelven a las criptomonedas.

Para la elaboración de este trabajo, hemos analizado varios artículos científicos. En el último apartado, hemos realizado una encuesta con la que intentamos deducir el futuro que seguirán las criptomonedas bajo la premisa de que, en gran medida, el futuro de las criptomonedas dependerá del conocimiento de estas por parte de los ciudadanos. Para la búsqueda y selección de bibliografía hemos acudido a varias bibliotecas virtuales en las que hemos encontrado artículos científicos, y para la obtención de los datos de la encuesta, utilizamos la herramienta de Google, “Google Encuestas”, siendo todos los datos obtenidos de manera individual.

El trabajo puede estructurarse en cinco apartados.

El primer apartado constituye una explicación básica sobre qué son las criptomonedas y su funcionamiento. Hablamos un poco de su historia para conocer la trayectoria que viene siguiendo este activo y hacemos un repaso global del mercado y su valor.

En el segundo apartado mostramos los beneficios y los riesgos que conllevan las criptomonedas, así como las medidas propuestas para hacer de estas un activo más seguro.

El siguiente apartado muestra la situación actual de las criptomonedas en varios países, las regulaciones a las que están sometidas y vemos el curioso ejemplo de una criptomoneda que abre la ventana a utilizar estos activos para obtener un beneficio no monetario.

El cuarto apartado reúne toda la información recabada en los apartados anteriores y planteamos el futuro que podrían seguir las criptomonedas, desde lo más probable hasta lo más utópico.

Por último, en el quinto apartado vemos los resultados de la encuesta realizada y llegamos a una conclusión sobre lo que pensamos que será el devenir de las criptomonedas

1. CRIPTOMONEDAS, ¿QUÉ SON?

1.1 Definición y mercado

Las criptomonedas son un nuevo activo digital basado en protocolos criptográficos distribuidos en lugar de un material físico con una autoridad centralizada, óptimo para operar como moneda (M. Krafft, Della, Penna, Pentland, 2018). En otras palabras, un activo sin forma física y con las mismas funciones que la moneda tal y como la conocíamos hasta ahora, pero sin encontrarse bajo el control de ninguna autoridad centralizada.

La Autoridad Bancaria Europea (EBA, 2014) define la criptomoneda como un activo digital, que ni es emitido por ningún banco central, ni por ninguna autoridad pública ni está necesariamente ligada a ninguna moneda corriente, sino que es utilizada por personas naturales o legales como medio de cambio electrónico.

Si analizamos la definición, vemos que, en primer lugar, es un activo digital. Esto no implica necesariamente que no pueda tener una representación física, ya sea en billete o en moneda, si no que hace referencia al concepto de “unidad de cuenta”, pero que además, se incluye la consideración de las criptos¹ como dinero privado o mercancía.

En segundo lugar, al no ser emitida por bancos centrales o autoridad pública, ni estar ligada a ninguna moneda fiduciaria, se consigue diferenciar del dinero electrónico, ya que éste si se encuentra fijo respecto a una moneda y por tanto, el cambio siempre estará pactado. El dinero electrónico es un instrumento de pago, por lo cual, el valor monetario se encuentra almacenado en un dispositivo bajo la posesión de un titular. La cantidad que se encuentra almacenada varía dependiendo del titular, ya compre, venda, inyecte o saque dinero (Lansky, 2018). No necesita la intermediación de ninguna cuenta bancaria (Banco Central Europeo, 2000). Sin embargo, con las criptomonedas, el valor monetario varía según el mercado y sin encontrarse bajo ninguna supervisión superior (Lansky, 2018).

¹ Acotación de “criptomoneda”.

Por último, al ser utilizadas por personas naturales o legales, pueden ser utilizadas como medio de cambio para la obtención de bienes y servicios. Además, pueden ser transferidas vía electrónica, almacenadas en un servidor electrónico o transferido físicamente. La segunda característica implica que las criptos sean un “almacén de valor”, pero no por ello quedarán estables con el tiempo, es decir, se verán afectadas igualmente por inflaciones o deflaciones.

El economista checo Lasnky (2018), formula su propia definición de criptomoneda, la más sencilla de las por ahora mencionadas: “Las criptomonedas son monedas digitales descentralizadas mediante un sistema p2p²”. El sistema Peer to Peer (p2p) implica que las criptomonedas sean de posesión anónima y sean independientes de una autoridad central. Además, al utilizar la criptografía para su seguridad, implica una alta dificultad a la hora de ser falsificadas y genera inmunidad frente a interferencias gubernamentales. El sistema criptográfico p2p cumple la función de que las transacciones de criptomonedas sean verificadas por todos los usuarios conectados a la red (Sovbetov, 2018), es decir, el intercambio quedará registrado en todos los ordenadores conectados, mediante la tecnología del Blockchain, que veremos más adelante.

Encontramos en definitiva que para reconocer y definir una criptomoneda, ésta debe de tener las siguientes características:

1. No ser emitida por ninguna autoridad central.
2. No encontrarse bajo la supervisión de ninguna autoridad central.
3. Pueda utilizarse como medio de pago, transacción o especulación.
4. No esté necesariamente fijada a una moneda o tipo de cambio.
5. Sea descentralizada mediante el sistema p2p.

Haciendo referencia al mercado. El mercado de cualquier criptomoneda consiste en un conjunto de órdenes de compra y órdenes de venta. Una orden de compra

²Peer to Peer (p2p) es un sistema criptográfico de intercambio de archivo en el cual se establece una conexión directa entre ordenadores, sin necesidad de un servicio intermedio. Esto implica que la información que se intercambie esté localizada en todos los ordenadores.

es la solicitud de compra de una cantidad de monedas a un precio específico en la orden. Una orden de venta es una solicitud de venta (Krafft, Penna, Pentland, 2018). La transacción tiene lugar cuando un nuevo comprador ofrece un precio igual o superior al precio más bajo de la moneda puesta en venta.

La Autoridad Bancaria Europea (EBA) ofrece una definición de todas las partes que forman el mercado de las criptomonedas.

-Usuario: es aquella persona o entidad legal que obtiene criptomonedas y las utiliza tanto para adquirir bienes como para invertir.

-Comerciantes: todo usuario que acepta criptomonedas a cambio de bienes y servicios.

-Plataformas: es el lugar del mercado. El lugar de encuentro de compradores y vendedores.

-Carteras: no posee el mismo significado que una cartera de valores. Lugar en el que se almacenan las criptomonedas. Cada criptomoneda es enviada a su propia cartera, a la cual se puede acceder mediante una dirección y una contraseña.

1.2 Historia y evolución

Lansky (2018), cuenta que el comienzo del estudio de las criptomonedas lo inició Chaum en 1983 con la redacción de varios artículos, pero no lograba la forma de conseguir la ansiada anonimidad necesaria para crear una criptomoneda. Fue en 1997 cuando Haber y Stornetta diseñaron la estructura predecesora al blockchain, esta última es la utilizada actualmente por las criptos y de la cual hablaremos más adelante.

Con la base del blockchain, apareció la primera (y más conocida) criptomoneda, el Bitcoin (BTC), creada el 3 de enero de 2009 anónimamente bajo el pseudónimo de Satoshi Nakamoto. Hoy día hay más de 600 criptomonedas, como Ethereum (ETH), Ripple (XRP) o Litecoin (LTC) (Lansky, 2018).

Para hacer referencia a la evolución de las criptomonedas y la burbuja que ha tenido lugar, trataremos del Bitcoin, por ser la primera, más conocida y en la que

se ha notado más la fluctuación de los precios. Eso sí, tengamos en cuenta que el resto de criptomonedas han seguido sus pasos, pero con sobresaltos menores.

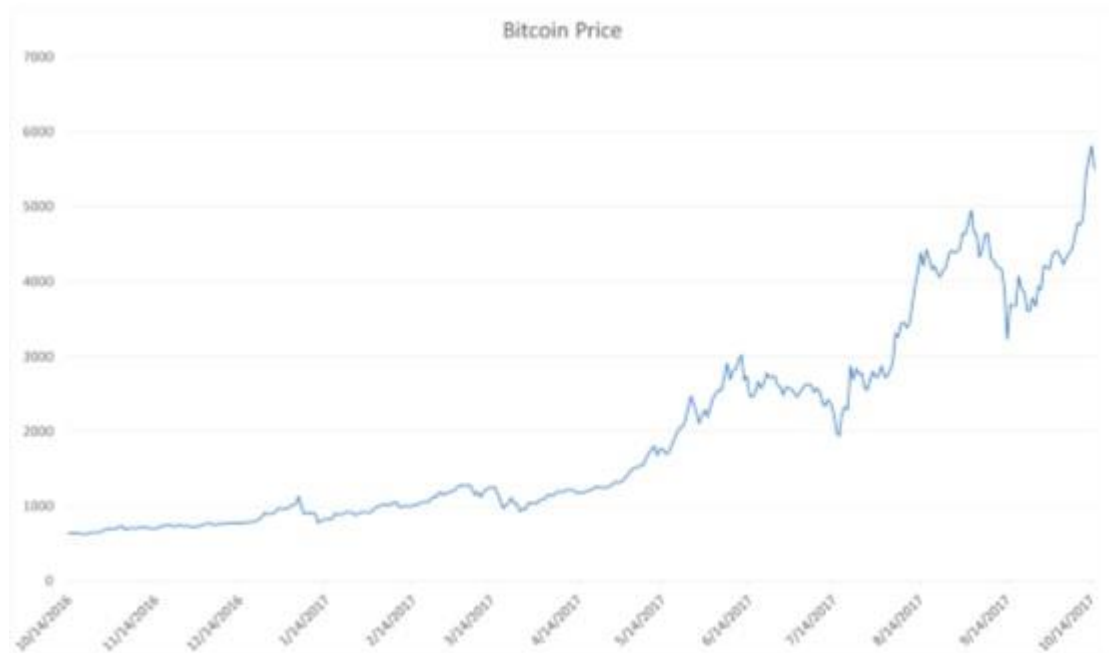
El Bitcoin apareció en el mundo con un precio menor a un dólar, y pronto fue objetivo de una especie humana singular, especuladores (Nahorniak, Leonova, Skorokhod, 2016). Tras los primeros meses desde su aparición, el Bitcoin dejó claro cómo iba a funcionar. Un precio extremadamente volátil con alto riesgo de hackeo (Nahorniak et al, 2016).

Bitcoin fue haciéndose conocida entre especuladores y comenzó a llamar la atención de los gobiernos (Caginalp, 2018), y fue denotando un crecimiento en su precio más o menos controlado, pero siempre en línea ascendente. Se consiguió que las transacciones fueran más seguras y se redujo el número de hackeos, algo que, obviamente, atrajo a más y más público. A su vez, y viendo cómo iba desarrollándose la función especulativa del BTC, nuevas criptomonedas aparecieron para hacerse un hueco en la carrera por el futuro (Lansky, 2018).

La capitalización de mercado de las criptomonedas ha ido creciendo desde 2015. En Mayo de 2017 llegó a ser más de cuatro veces la capitalización en Mayo de 2016 (ElBahrawy, Alessandretti, Kandler, Satorras, Baronchelli, 2017). El valor total de todas las criptomonedas hoy día se estima que ronda los 350 billones de dólares americanos (Jacobs, 2018).

Caginalb (2018) relata la evolución del precio del BTC y cómo éste ha arrastrado a las nuevas criptos. El 'boom' comenzó el 13 de Octubre de 2017, cuando la capitalización de mercado del BTC superó a la de Goldman Sachs y Morgan Stanley.

Fig. 1. Evolución anual del BTC en USD hasta octubre de 2017.



Fuente: Caginalp, 2018

Si puede parecer que la burbuja comenzó a mediados de Mayo y acabó en Octubre, nada más lejos de la realidad. Como observamos en el siguiente gráfico, tras octubre, el precio del BTC subió a ritmos exponenciales y tiró del precio de todas las criptomonedas. En diciembre de 2017 llegó a su máxima y comenzó una corrección agresiva que duraría hasta febrero del año siguiente. Desde el 5 de diciembre hasta el 17, cada día había un aumento más extraordinario del precio de las criptos en general y del Bitcoin en particular, pasando en dos semanas de 12.000 dólares a los 20.000. Cuando no se sabía si explotaría la burbuja o proseguiría su andadura, igual que en una semana el precio subió extraordinariamente, en tan solo cinco días se desplomó el BTC, de los 20.000 a los 11.000. A partir de ahí, el precio volvió a los 6.000 de octubre y ha estado fluctuando sobre ese soporte hasta hoy día.

La especulación a la que las criptomonedas se han visto expuestas, unidas al hecho de que no están resguardadas por ningún metal precioso (como el oro), por ningún

valor real o por ningún gobierno ha dado lugar a la burbuja especulativa de la que acabamos de hablar (Jacobs, 2018).

Fig.2: Evolución del BTC en USD durante la burbuja.



Fuente: Binance y elaboración propia.

Vemos como la evolución de las criptomonedas está marcada por las elevadas fluctuaciones en los precios, los cuales no han parado de crecer, creándose hasta una burbuja.

1.3 Funcionamiento

Nahorniak, Leonova y Skorokhod (2016) explican el funcionamiento de las criptomonedas como un simple contrato de compra-venta. Una parte quiere comprar un bien por 3 BTC (por ejemplo, sería válida cualquier otra cripto) a otra parte. Lo primero es instalar una cartera de BTC (en este caso) en el ordenador o el móvil, que generará automáticamente una dirección de BTC. La parte compradora abre su cartera de BTC, copia la dirección de la cartera de BTC del vendedor y le envía los tres BTC. Por lo tanto, si se quiere enviar cualquier criptomoneda, se necesitan dos cosas: una dirección de la criptomoneda y una clave privada, formando así una cuenta de criptomonedas. La dirección se genera automática y aleatoriamente, y consta de una sucesión de letras y números. La

clave privada es otra sucesión de letras y números pero secreta. Lansky (2018) dice que hay más posibles claves privadas que átomos en el universo. Así, la seguridad de las criptomonedas depende de la calidad de los números aleatorios generados, por ello, la mejor opción es crear una clave de forma criptográfica. Según Lansky (2018), la dirección de la criptomoneda se corresponde con el número de una cuenta bancaria de dinero fiduciario, y la clave privada sería el PIN. A diferencia de la banca tradicional, la seguridad de la cuenta de criptomonedas es menor, ya que la dirección de la cuenta se puede calcular a partir de la clave privada y, por lo tanto, el conocimiento de la clave privada es suficiente para adquirir el control de las unidades de criptomonedas almacenadas. En la banca clásica, el número de la cuenta es necesario también. Además, la tecnología de criptomonedas no permite la devolución o cancelación de una transacción, por lo que en un ataque a una cuenta de criptos, el atacante puede salir inmune (Lansky, 2018).

Los BTC son enviados desde la cartera a la red de BTC, donde la transacción se valida por los nodos de la red. Para que se valide, las transacciones deben de empaquetarse en bloques que cumplan unas reglas, las cuales evitan que bloques anteriores sean modificados. Así, ningún individuo puede controlar lo que aparece en la cadena de bloques. A este proceso se le denomina “blockchain”.

El siguiente y último paso consta de la verificación por parte de los nodos del bloque hasta que llegue al vendedor y reciba sus BTC.

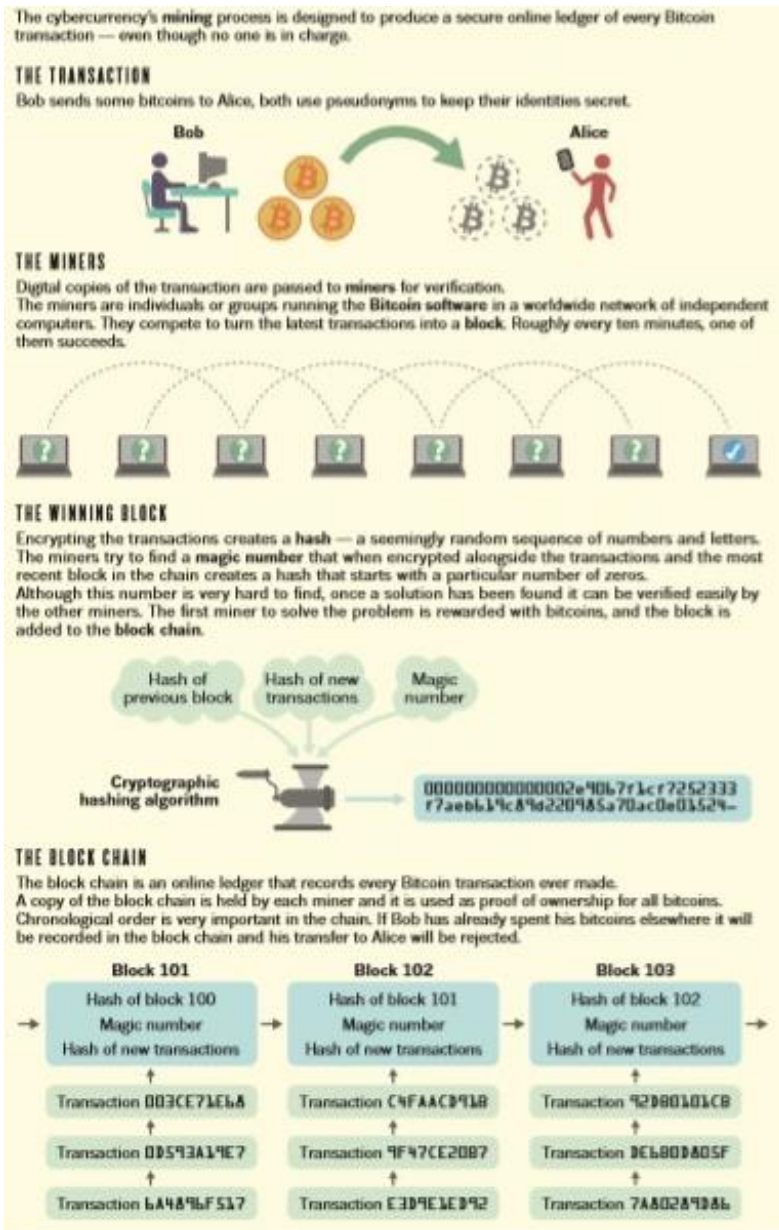
Para entender cómo funciona la tecnología blockchain usaremos un ejemplo propuesto por VisualPolitik, canal de YouTube dedicado al análisis de países y actualidad económica y política.

Imaginamos que queremos comprar una casa en San Francisco por 3 millones de dólares. Para comprarla se ha firmado un contrato con el dueño, pero no podemos asegurarnos de que lo va cumplir pudiendo haber estafa por su parte, y una vez le entreguemos el dinero, que él no nos de las llaves. Por ello, usamos un intermediario, en este caso un notario, que verifique que todo está correcto y nos de las llaves de la casa una vez que entreguemos nuestro dinero. Hay varios

problemas, los intermediarios significan comisiones que pagar y pérdida de tiempo cada vez que se quiera comprobar cualquier parte del contrato, pero sobre todo, el mayor problema es que si alguien pudiera hackear el ordenador del intermediario podría modificar cualquier término del contrato.

Con blockchain, utilizamos un contrato inteligente, no uno normal, es decir, un mini programa automático que se ejecuta de forma automática cuando ocurren ciertas cosas, en este caso, podríamos dejar nuestro millón en una cuenta especial y en el mismo momento que abramos la puerta de la casa, hay un sensor que nos detecta y le manda el dinero al antiguo propietario. Si la llave no encaja en la cerradura, el contrato nunca acabaría con la transacción y el antiguo propietario no recibiría el dinero. ¿Y quién es el encargado de que se cumpla lo que está escrito? Ya no hay un intermediario, en su lugar tenemos una red compuesta por todos los miembros de la blockchain que utilizamos. Hay empresas que se encargan de la realización de estos pagos, por ejemplo, una empresa que se encargue de la compraventa de casas a través de blockchain a través de una plataforma. Todos los vendedores y compradores que usen esta plataforma serían un nodo en esta red. Todos estos usuarios tendrán una copia de nuestro contrato, así cualquiera de ellos lo puede verificar en cualquier momento, pero es que además, el contrato se quedará almacenado para siempre en lo que se conoce como bloque, el cual pasa a formar parte de una cadena de bloques inmutable. Si algún hacker quisiera modificar nuestro contrato, tendría que entrar a la vez en todos los ordenadores de todos los miembros de la blockchain, algo más difícil que entrar en el ordenador de un solo notario. ¿Esto quiere decir que automáticamente tendremos todos los registros de todas las transacciones dentro de esa red en nuestro ordenador? Sí. Pero realmente, para la utilización de criptomonedas, vale con tener un monedero ligero, o virtual, es decir, hay una persona que se ha bajado toda la capacidad de memoria de la red y está dejando que utilizemos la criptomoneda a través de su servidor. Así no tendremos que preocuparnos por el espacio de nuestro ordenador. Son las plataformas de intercambio de criptomonedas, compuestas por “mineros”.

Fig. 3: Funcionamiento del Bitcoin.



Fuente: Revista Feature News (2015)

En esta imagen de la revista Feature News (2015), vemos qué pasa cuando se opera con BTCs.

La transacción debe ser verificada por varios ‘mineros’, es decir, individuos que ejecutan el software del BTC en una red de ordenadores independientes. Estos

compiten por transformar la transacción en un bloque (como explicamos antes). Aproximadamente cada diez minutos, lo consiguen.

Los mineros intentan hallar un número que, una vez se encripte junto con la transacción y el último bloque de la cadena, cree un hash³, el cual comenzará con varios ceros.

Una vez que se ha encontrado el número, éste puede ser verificado fácilmente por otros mineros, pero es el primer minero en encontrarlo el que es “recompensado” con los BTCs. El bloque se añade a la cadena.

El “blockchain” o “cadena de bloques” es un registro online de todas las transacciones de BTCs realizadas.

Todo este proceso es idéntico con cualquier otra criptomoneda.

1.4 Valor de la criptomoneda

Como dice Jacobs (2018) y he mencionado anteriormente, el valor de las criptomonedas es hoy día de 350 billones de dólares americanos. Una moneda nacional está resguardada por una reserva limitada de oro y por el valor del Estado como activo (Jacobs, 2018). Indirectamente, también lo está por la totalidad de la productividad y la capacidad productiva de la nación, pero al final, el valor y la utilidad de la moneda nacional depende del nivel de confianza pública en ella (Jacobs, 2018).

Sin embargo, las criptomonedas no están resguardadas por ninguna reserva de oro, por ningún activo físico o por la productividad potencial de un país, por lo que Jacobs (2018) se plantea de dónde sale ese valor de 350 billones de dólares.

En primer lugar, la criptomoneda es actualmente la única moneda universal que puede ser utilizada a lo largo y ancho de todo el mundo. Y no solo eso, si no que puede ser transferida de forma rápida y a muy bajo coste.

³ Algoritmos que consiguen crear, a partir de una entrada, una salida alfanumérica que representa un resumen de toda la información que se le ha dado.

La segunda fuente de valor de las criptomonedas viene dada por la capacidad de confianza que ha transmitido a las personas. El valor de una moneda aumenta en proporción a la cantidad de población y la productividad de la economía en el área en el que es aceptada. Como moneda utilizada mundialmente, el valor de las criptomonedas está destinado a aumentar exponencialmente teniendo en cuenta que el incremento de aceptación de estas monedas aumenta la demanda de las mismas.

Por último, las criptomonedas tienen la capacidad, junto con internet y otras tecnologías, al encontrarse en una etapa de nacimiento y desarrollo, de crear un potencial de desarrollo tecnológico y de innovación desmesurado. Según Jacobs (2018), tienen el potencial suficiente como para desplazar a los bancos convencionales y a las monedas nacionales en el largo plazo.

2 BENEFICIOS E INCONVENIENTES

2.1 Pros y beneficios

La Autoridad Bancaria Europea (EBA) recoge los beneficios que proporcionan las criptomonedas en su documento “Opinión del EBA sobre las criptomonedas” de 2014. Para ello los clasifica dependiendo del beneficiario, habiendo beneficios económicos y para el individuo.

En cuanto a los beneficios económicos, hace hincapié en la reducción del coste de transacción. Debido a la ausencia de intermediarios, las transacciones se llevan a cabo de manera menos costosa que cualquier otro método de transacción, como pago con tarjeta o transferencia bancaria. Brito (2013) dice que el coste de una transacción de BTC es menos de 0,0005 BTC o bien, menos de un 1% del monto de la transacción. Aun así, hay que tener precaución, ya que los mineros ganan dinero cada vez que se realiza una transacción, si el número de personas que realizan transacciones disminuye, el coste de estas se verían aumentadas.

El EBA hace referencia también a la velocidad de las transacciones de criptos, siendo mayor que las de las monedas fiduciarias. Para el ejemplo del BTC, el

proceso completo de una transacción dura entre 10 y 60 minutos. Como expliqué antes, un nuevo bloque se añade a la cadena con una media de 10 minutos. Comparado con las transacciones a través de tarjetas o transferencias, que necesitan ser comprobadas en algún día laboral y por varios intermediarios, la ventaja de las criptomonedas es abrumadora.

El documento explora la idea de que el crecimiento económico puede venir dado por el uso de las criptomonedas. Se justifica con la lógica de que el uso de las criptos ha generado nuevos tipos de negocios que antes, con los métodos de pagos tradicionales, no existían. Por ejemplo, el minar ha llevado al desarrollo de hardwares especializados en la minería. La necesidad de convertir una criptomoneda en una moneda fiduciaria ha generado nuevas oportunidades de negocio, como plataformas. En general, es el sector de las nuevas tecnologías donde más ha afectado.

En países donde la jurisdicción financiera no permite la convertibilidad de su moneda en otra, donde los servicios financieros son demasiado caros o donde el coste administrativo para la obtención de una cuenta bancaria es inasequible, la estructura de las criptomonedas proporciona una alternativa para conseguir el mismo objetivo: acceder al comercio y efectuar transacciones y pagos.

Haciendo referencia a los beneficios individuales, y tomando como base la idea de que un sistema que se basa en un banco central con autoridad suficiente como para influir en el suministro de dinero, no es lo mejor, la estructura de la criptomoneda permite una mayor seguridad. Pero claro, queda abierta a la ideología personal.

2.2 Contras y riesgos

La EBA recoge unos setenta riesgos diferentes, clasificados según su nivel, siendo bajo, medio o alto. Nosotros no nos pararemos en los setenta, si no que veremos los más importantes o comunes.

En cuanto a los riesgos para los usuarios, observamos que hay un alto riesgo, según la clasificación que proporciona la EBA, de que el usuario sufra pérdidas

durante en el intercambio mediante alguna modificación fraudulenta de la estructura de cualquier criptomoneda. Como explica Lansky (2018), dado al limitado número de usuarios, la capitalización de mercado de las criptomonedas es baja, por lo que cualquier intercambio puede tener un impacto desproporcionado en el precio de mercado, siendo así que el tipo de cambio respecto a una moneda fiduciaria puede cambiar rápidamente.

Como riesgo medio encontramos la opción de que, dado a la cantidad de información, innovaciones y definiciones que no entendemos fácilmente, puede resultar difícil para el usuario la comprensión de todas las características de la estructura de una criptomoneda, por lo que cualquier persona anónima puede crear una criptomoneda con una estructura dada y seguidamente cambiar las funciones de ésta. Además, al ser las transacciones irreversibles, el usuario no puede redimirse.

Que el usuario concorra en pérdidas debido al robo de la cartera virtual en la que guarda sus criptomonedas mediante hackeo se considera de alto riesgo. Las carteras (e-wallet) son un software instalado en el ordenador de un usuario o cualquier aparato útil para ello. Al ser un software puede ser hackeado desde cualquier lugar del mundo, y para más inri, el usuario no tiene derecho a la devolución de lo robado, ya que no existe ningún depósito de protección como para las cuentas bancarias. Lo mismo puede ocurrir cuando el intercambio está teniendo lugar.

La contraseña es la única prueba de propiedad para el usuario, quien tenga la contraseña, tiene el control de la cuenta, y por tanto, de las criptomonedas (Lansky, 2018).

Dada la incertidumbre que rodea las criptomonedas hoy día, y a las amenazas reguladoras por parte de los gobiernos, hay un alto riesgo de que cualquier nueva ley o regulación afecte a los poseedores de criptomonedas de manera negativa. Cuando se realiza un intercambio en una máquina de criptomoneda, los usuarios no pueden garantizarse de que las criptos o la moneda fiduciaria lleguen sin

problema a su destino, ya que estas máquinas no están sujetas a ninguna revisión técnica ni necesitan ningún tipo de licencia.

Los usuarios pueden sufrir pérdidas al realizar un pago para la obtención de un bien. Este pago puede ser incorrectamente debitado y como ya sabemos, ninguna autoridad supervisa el proceso de acuerdo, al contrario, es un intercambio basado en la confianza.

Uno de los mayores riesgos potenciales de las criptomonedas reside en la naturaleza especulativa de éstos activos (Krafft, Penna, Pentland, 2018). La mayoría de los participantes en éste mercado compran y venden esperando que una u otra crypto aumente su valor, lo que puede conllevar a burbujas como la que hemos vivido en diciembre de 2017 (Kraft et al., 2018). Además, el precio puede ser modificado por un pequeño grupo de poseedores de criptos, tal y como dijimos antes. Al ser un mercado poco profundo, el realizador de una orden puede no verla realizada en el momento que él esperaba, es decir, podría encontrarse con dificultades a la hora de querer vender su criptomoneda y que acarree pérdidas o menores beneficios.

BTC, la criptomoneda más estable, podía variar su valor en un 50% en una semana (Lansky, 2018). Aun así, algunas otras como Paycoin, perdieron más del 99,7% de su valor en 2015 (Lansky, 2016).

Como cualquier inversión, conlleva sus riesgos, ya que pueden utilizarse CFDs o ETFs, y siempre que haya apalancamiento de por medio, el riesgo se multiplica, tanto para el inversor, como para las instituciones de crédito (Caginalp, Caginalp, 2018).

Si nos centramos en los utilizadores de criptomonedas para la compra venta, podemos encontrar riesgos a la hora de recibir o utilizar las criptomonedas. Si se acepta una cantidad de criptos a cambio de un bien y esa cantidad no llega nunca a recibirse, no hay ninguna autoridad que pueda velar por el interés del

comerciante. Y aun recibiendo esa cantidad, no se asegura poder utilizarlas para obtención de otros bienes o servicios, o simplemente para pagar facturas.

Un uso que se le da actualmente a las criptomonedas es el movimiento rápido de dinero entre terroristas y organizaciones criminales (Sovbetov, 2018). Lo realizan de forma anónima, ya que el sistema peer-to-peer no necesita una identificación personal y la dirección de la cartera no está ligada a ningún nombre. Además, no hay intermediarios que puedan notificar a las autoridades la existencia de transacciones sospechosas y las pueden realizar a lo largo de todo el mundo (Sovbetov, 2018).

2.3 Soluciones a los riesgos

La EBA (2014) no dedicó su tiempo solo a encontrar las grandes amenazas que rodean a las criptomonedas, sino también a investigar las soluciones que pueden plantearse para erradicar esas amenazas.

Plantea la creación de una entidad llamada “autoridad de gobierno de estructura”. Esta entidad sería una entidad no gubernamental que establecería y gobernara unas normas para el uso de las estructuras de las criptomonedas. Una persona legal, responsable de mantener la integridad de la contabilidad de las transacciones y cualquier otro componente de la estructura de la cripto.

La creación de una autoridad puede parecer incompatible con el concepto de criptomonedas, es decir, como estructura descentralizada que no requiere la aportación de un banco central o gobierno. Aun así, la creación de un cuerpo gubernamental no implica que las criptomonedas estén centralizadas. La función del órgano puede ser descentralizada, ya que si es cierto que la estructura descentralizada de las criptomonedas es segura, los participantes del mercado podrían ser ellos mismos esa autoridad.

Se plantea también la opción de que los participantes en el mercado deban registrarse y ser autorizados antes de comenzar con operaciones de criptomonedas. La autorización solo sería entregada a aquellas personas legales

establecidas en un Estado miembro. La autorización debería ir acompañada de información sobre los riesgos así como de una acreditación de seguridad tecnológica.

Ya se aprobó una licencia para operar en Nueva York, La “BitLicence” creada por el Departamento de Servicios Financieros de la NY en 2015 (Lansky, 2018). Esta licencia fue costosa tanto económica como materialmente, y varias compañías de criptomonedas abandonaron la ciudad, como por ejemplo Poloniex (Lansky, 2018). Aun así, los usuarios suelen preferir un servicio regulado antes que uno sin regular.

Sin embargo, Lansky (2018) opina que hay riesgos que se irán mitigando poco a poco. En cuanto a la volatilidad de los precios debido a la baja capitalización de mercado, opina que, con el tiempo, la creciente expansión de criptomonedas irá gradualmente eliminando el problema, ya que habrá un momento en el que la capitalización sea tal que se hará resistente a las rápidas fluctuaciones. Un solo inversor controlará una porción más pequeña de criptomonedas. Además, Lansky (2018) piensa que la atención y la precaución de los inversores aumentarán con el tiempo, teniendo en cuenta más factores a la hora de comprar una criptomoneda, como la reputación de los creadores o la de los promotores.

Para evitar el problema de las operaciones irreversibles, Lansky (2018) plantea la idea de realizar una “bifurcación dura”, es decir, la creación de una nueva versión de una misma criptomoneda, con la misma información que la anterior pero con actualizaciones. Las dos criptos siguen existiendo, pero se comportan de manera diferente, así apareció, por ejemplo Bitcoin Cash, una bifurcación dura del Bitcoin, con una mayor velocidad de transacción y menor descentralización que el BTC. Una vez creada la nueva criptomoneda, denominada “altcoin”, para poder seguir realizando transacciones con cualquiera de las dos, todos los participantes de la red deben actualizarse. Así pasó con Ethereum (ETH). ETH fue hackeada, por lo que la comunidad ETH realizó una bifurcación dura, creando Ethereum Classic, con la característica de reversibilidad de transacción, pudiendo recuperar las transacciones desviadas por el hacker (Lansky, 2018).

Por último, Lansky (2018) propone una solución para los conflictos de transacciones entre empresas por temas de negocio. Su planteamiento incluye un tercer intermediario que funcione como árbitro en caso de disputa o conflicto, siendo totalmente neutral. El dinero de la transacción sería enviado a una cuenta especial que necesite de varias firmas o claves, suele recibir el nombre de “multisig” del inglés “multisignature”. Existirían tres claves, y cada parte del intercambio poseería una de las claves, siendo la tercera para el árbitro. Para poder realizarse la transacción serán necesarias dos de las tres claves.

3 CRIPTOMONEDAS EN LA ACTUALIDAD

3.1 Criptomonedas en distintos países

Lansky (2018) crea una clasificación compuesta de seis niveles, desde el nivel 0 hasta el 5, para poder clasificar el acercamiento a las criptomonedas de los diversos países: nivel 0 – ignoran, nivel 1- supervisión, nivel 2 – recomendación, nivel 3- dirección, nivel 4- regulación, nivel 5- prohibir o integrar. Dentro de cada nivel ha creado varios grupos. Los distintos estados solo se encuentran dentro de un nivel, el más alto alcanzado, pero pueden estar dentro de diferentes grupos dentro de cada nivel.

Nivel 0 – ignoran: El Estado en concreto no convive con la existencia de criptomonedas, mayormente por la poca importancia que le otorga a éstas. La capitalización de mercado de todas las criptomonedas en estos estados era menor de 6 billones de dólares en 2016 según CoinMarketCap. Originalmente, todos los países se encontraban en este nivel, hoy día, 150 son los que prosiguen ahí.

Nivel 1 – supervisión: Un Estado ha comenzado a percatar la existencia de las criptomonedas y tiene pensado lidiar con ellas en el futuro. A su vez, no han recibido recomendación de comenzar actualmente con ellas. En este nivel encontramos a Croacia e Irlanda.

Nivel 2 – recomendación: Un Estado no solo ha percatado el uso de criptomonedas si no que obtiene información y recomendaciones a cerca de éstas y se las hace saber a sus ciudadanos. La mayoría de las recomendaciones ven la criptomoneda como algo negativo, pero como hemos visto, la Autoridad Bancaria Europea redactó un informe dando puntos positivos de las criptos.

Nivel 3 – dirección: Una autoridad estatal le ha proporcionado al Estado el método de uso de las criptomonedas. Esta guía viene acompañada casi siempre de un aviso de los riesgos que las criptos conllevan. Encontramos países como Argentina, República Checa, Canadá, Singapur y Estados Unidos.

Dentro de este nivel encontramos el grupo de los países que opinan que las criptomonedas no son bienes por lo que no pueden estar sujetos a impuestos o tasas. Son los países de la Unión Europea y Suiza. Además hay países que ven las criptomonedas como activos que proporcionan ganancias por poseerlos o venderlos y no están sujetos a impuestos. Son Australia, Bulgaria, Canadá, Estonia, Alemania, Noruega, Singapur, Suecia y Estados Unidos.

Otro grupo del nivel 3 corresponde con aquellos que opinan que las criptomonedas son bienes y por tanto son merecedoras de estar sujetas a impuestos. Son Hong Kong y Reino Unido.

Por último hay dos grupos más dentro de este nivel, uno que considera que el hecho de minar criptomonedas está sujeto a impuestos, que son Polonia y Eslovenia. Y otro grupo que considera que las criptomonedas deben estar bajo un impuesto de apuestas y azar. A ese grupo solo pertenece España.

Nivel 4 – regulación: La utilización de los servicios ofrecidos por las criptomonedas requiere de una autorización por parte de la autoridad estatal pertinente. Para obtenerla, tienen que reunirse una serie de condiciones. Este nivel incluye al Estado de Nueva York (EEUU), Luxemburgo y Japón.

Nivel 5 – prohibición o integración: El último nivel es obviamente o la total prohibición o la total adopción de la criptomoneda. La prohibición puede llevarse

a cabo mediante varias formas como veremos ahora en los distintos grupos de este nivel.

El primer grupo de este nivel está formado por aquellos países que prohíben las criptomonedas para las instituciones bancarias. Éstas tienen prohibido proporcionar servicios relacionados con las criptos, en particular, el cambio de una cripto por dinero fiduciario. Sin embargo, las transacciones de criptomonedas no están prohibidas entre las personas. Este grupo lo comporta China, Colombia, Islandia y Jordania.

El segundo grupo lo forman aquellos países que realizan una prohibición completa, no solo para los bancos, sino también para las personas. La prohibición puede verse reforzada por la amenaza de prisión, y para llevarla a cabo se utilizan medidas como la censura de páginas webs informativas de criptomonedas y proveedoras de servicios. En este grupo están Bangladesh, Bolivia, Kirguistán, Rusia y Tailandia.

El tercer y último grupo del nivel, y por lo tanto, lo más lejos que se puede llegar es la integración. El Estado se apropiará de una criptomoneda como moneda nacional, una cripto que podrá ser creada por el mismo Estado. También encontramos la opción de que el Estado use la tecnología de las criptomonedas para operar en los servicios administrativos o que pueda invertir el dinero de su banco central en criptomonedas. Hoy día, esta categoría incluye solo dos países: Ecuador e Isla de Man, que están trabajando en la integración de la critpomoenda en sus respectivas administraciones.

3.2 Regulaciones

El rápido desarrollo de las criptomonedas ha conllevado una mayor preocupación a nivel nacional y global, así como la necesidad de rellenar el vacío legal de los diferentes países (Jacobs, 2018).

Por ello, vamos a ver distintos caminos que han seguido algunos países para regular esta moneda tan problemática.

En primer lugar, empezaremos con una regulación muy elevada por parte de Brasil. El 9 de Octubre de 2013, Brasil lanzó la ley número 12.865, la cual normalizaba la creación de dinero electrónico, incluido el bitcoin (Nahorniak, Leonova, Skorokhod, 2016). Además de la creación, mediante esta ley se permite el pago mediante transacciones de dinero electrónico y criptomonedas.

El 3 de diciembre de 2013, el Banco Central de China junto con varias comisiones, consiguieron redactar las “Precauciones contra los Riesgos que entraña el BTC”. El documento explica que las criptomonedas en general no son una moneda por su naturaleza, por lo que no debería circular en el mercado como tal. Desde entonces, los bancos y las instituciones financieras tienen prohibido el uso de criptomonedas, tanto como para comprar y vender, como para prestar un servicio a los clientes (Nahorniak et al. 2016).

Aun en el continente asiático, una ley reguladora fue aprobada por el Gabinete japonés el 4 de marzo de 2016, la cual reconocía la criptomoneda como una forma legal de pago, con exactamente las mismas funciones que una moneda fiduciaria. Por la nueva regulación, las criptomonedas quedan bajo el control de la Agencia de Servicios Financieros de Japón. Toda transacción que tenga las criptomonedas involucradas deberá quedar registrada en dicha Agencia y se deberá aportar anualmente los datos financieros de la persona o empresa (Nahorniak et al. 2016).

Aun con todo esto, la acción gubernamental más efectiva hasta ahora fue tomada en junio de 2015 por el Departamento de Servicios Financieros de Nueva York (Nahorniak et al. 2016). Se consiguió el primer recogimiento de estándares necesarios para la utilización de las criptomonedas del mundo, llamado “BitLicense”. El documento contiene las condiciones que requiere una empresa en su actividad con criptomonedas en el estado de NY. Debido a esta medida, las plataformas Bitfinex y Kraken anunciaron su decisión de abandonar Nueva York debido a la necesidad de obtener esa licencia (Nahorniak et al. 2016). El 22 de septiembre, ya eran 25 empresas las que habían aplicado para conseguir dicha

licencia, siendo solo una, Circle Internet Financial, la que la consiguió sin ningún tipo de obstáculo (Nahorniak et al. 2016).

Dentro de los Estados Unidos, la legislación de California conllevó a que fuera el primer estado americano en autorizar el uso de las criptomonedas, pero con bastantes limitaciones, considerando la criptomoneda como una propiedad personal e intangible y no como una moneda (Nahorniak et al. 2016).

Luxemburgo le otorgó la licencia de institución de pago a la plataforma de cambio de Bitcoin Bitstamp, siendo la primera en el mundo en conseguir una licencia. Mediante el programa denominado “Pasaporte de la Unión Europea”, el cual permite a los proveedores de servicios financieros instalados en un Estado Miembro actuar en el resto de países de la UE, Bitstamp comenzó a operar bajo licencia en los 28 países de la Unión Europea (Nahorniak et al. 2016). Además, el 1 de julio de 2016, Bitstamp inauguró el cambio Euro-BTC y viceversa.

En cuanto a la Unión Europea, Estados Miembros como Bélgica, Chipre, Dinamarca, Holanda, Portugal o España no tienen una regulación clara a cerca de este tema, aun habiéndoseles precavido de los peligros que pueden llegar a conllevar. Aun así, Francia o Alemania si han comenzado los primeros pasos para la regulación de las criptomonedas (Nahorniak et al. 2016).

Pasamos a ver algunas regulaciones en los países miembros que han comenzado a estudiar los peligros y las ventajas de las criptomonedas.

El Banco Nacional Croata observó que la legalización de las criptomonedas no supondría un problema, por lo que por ahora mantiene su legalización para el uso, pero no como moneda (Nahorniak et al. 2016).

Para Francia, las criptomonedas no pueden considerarse una moneda real, por lo que no se puede utilizar como medio de pago bajo la ley francesa. Esta decisión fue tomada tras el reporte de la EBA de 2014.

El Ministerio de Finanzas alemán anunció que no se considerará las criptomonedas como dinero electrónico ni como moneda funcional, si no como dinero privado e instrumento financiero. Para realizar transacciones comerciales se necesitará una licencia por parte del Banco Central (Nahorniak et al. 2016).

El modelo alemán es el que tiene más probabilidades de ser adoptado por el resto de los Estados Miembros: toda entidad que esté involucrada en las transacciones comerciales de criptomonedas, necesitarán una licencia que les permita la utilización de instrumentos financieros.

3.3 SMLY: La criptomoneda educativa

Stefansson y Lentin (2017) redactaron un artículo de investigación acerca del uso educativo que se le podía otorgar a las criptomonedas, encontrando Smiley (SMLY), una criptomoneda utilizada en una universidad de Islandia como método de aprendizaje.

Smiley fue inicialmente creada como método para probar el mecanismo de recompensa en el sistema educativo, y con el tiempo, ha conseguido que éste siga siendo su propósito (Stegansson et al. 2017). Es como cualquier otra “moneda divertida”, es decir, es una moneda casera que no tiene valor intrínseco. Y para que quedara claro que el fin último de la moneda es la diversión y no el beneficio, tanto el nombre (Smiley viene de “smile”, sonrisa en inglés) como el logo, que consta de un icono sonriente con un birrete, fueron creados a conciencia no fuera a caer lugar a dudas.

El mecanismo de recompensa es simple, dar una cierta cantidad de SMLY cuando se ha alcanzado una serie de objetivos. Los anuncios en la plataforma educativa suelen ser “Obtén “x” SMLY al realizar esta actividad. Obtén “y” más al realizar la lección completa.”

Para implementar la recompensa, la plataforma virtual tiene su propia cartera virtual de SMLY, y distribuye automáticamente la cantidad a los estudiantes (Stefansson et al. 2017).

La manera de conseguir los SMLY ha aumentado constantemente, por lo que se puede conseguir la recompensa, no solo realizando las actividades, si no, cuanta más alta nota se saque en dichas actividades, mayor la recompensa. Además, se ha creado un chat entre estudiantes, mediante el cual, la ayuda a otros compañeros viene de la mano de más SMLY (Stefansson et al. 2017).

Cuando se creó la criptomoneda, la Universidad de Islandia llegó a un acuerdo con una cafetería del campus, mediante el cual se podía adquirir café a cambio de SMLY. Y no solo eso, se crearon páginas web, bajo el dominio <http://smlly.is/>, donde los estudiantes podían comprar productos directamente con los SMLY obtenidos en la universidad. Esto conlleva un mayor esfuerzo del alumno para conseguir más SMLY, que a su vez puede utilizarlos para obtener bienes (Stefansson et al. 2017). Se le ofreció a varias empresas participar en la web ofreciendo cupones de descuento en sus productos, pero como era de esperar, ninguna empresa quería recibir SMLY (Stefansson et al. 2017).

Cuando los SMLY fueron introducidos a los estudiantes, éstos no se creían que fueran a poder comprar café, entradas de cine o incluso descuento en vuelos nacionales. El primer experimento concluyó en noviembre de 2014, siendo éste de un mes, y demostrando lo fácil que resultó la inclusión de los SMLY en la plataforma y en el sistema educativo. Para fijar el valor de los SMLY, se comenzó a vender un café por el valor correspondiente a dos horas de trabajo en la plataforma. Esta iniciativa no tuvo mucho éxito, ya que durante varias semanas solo se consiguió vender un par de cafés (Stefansson et al. 2017).

A comienzo de 2015, el mismo curso pero el siguiente semestre, se comenzó a utilizar las SMLY desde el principio. Se llegó a la conclusión de que las recompensas que se ofrecían al principio eran demasiado bajas y se modificó el mecanismo para 2016. Para entonces, SMLY ya tenía algún que otro tipo de cambio con otras criptomonedas, por lo que las recompensas se ajustaron al mercado y fueron más justas (Stefansson et al. 2017). Por marzo de 2017, ya eran 2,8 billones de SMLY las que se habían repartido a los estudiantes, y el valor del

café y de los bienes de la web eran muy similares al valor de mercado. Un total de 3181 estudiantes habían ganado tal cantidad de SMLY, pero de esos 2,8 billones, solo un 24% fueron gastados. Esto puede ser debido a que, aunque 500 estudiantes hayan obtenido un millón de SMLY, el valor real es de diez dólares utilizando el tipo de cambio 100 millones de SMLY = 1 BTC = 1000 dólares (Stefensson et al. 2017). Sin embargo, hubo 34 estudiantes que obtuvieron 25 millones de SMLY o más, y fueron 25 estudiantes los que los gastaron, llegando a la conclusión de que los estudiantes son más propensos a gastar el dinero cuando tienen más (Stefensson et al. 2017).

En la otra cara de la moneda, se observó una serie de abusos por parte de algún estudiante, pero que fue corregido rápidamente. El primero de todos fue un estudiante que, con diferentes cuentas de correo, realizó la misma prueba en la plataforma una y otra vez para obtener la recompensa en cada una de las cuentas. El problema fue detectado fácilmente y se puso fin al abuso inmediatamente con una serie de correos amenazadores (Stefenson et al. 2017).

El segundo abuso detectado fue prácticamente igual, por lo que se tardó menos en detectarse y neutralizarlo. Sin embargo, el tercero fue más elaborado. Alguien utilizó más de 200 cuentas diferentes y trabajó a lo largo de toda la plataforma virtual. Los diferentes correos fueron fácilmente detectados, pero en este caso no sirvieron de nada los correos amenazadores, y al cambiar la recompensa ofrecida por las actividades más comúnmente realizadas por estas cuentas, solo se consiguió que esa persona realizara actividades nuevas y más difíciles. Por suerte, este ataque tuvo lugar en verano y fuera del periodo escolar, por lo que todos los parámetros de la plataforma pudieron ser modificados y se redujo muy considerablemente las recompensas que la plataforma ofrecía, lo que fue suficiente para parar la primera ola de ataques que sufrió SMLY.

Aun así, a mediados de agosto de 2017, una nueva ola de ataques sobrepasó la plataforma virtual. Esta vez fueron 317 personas, no estudiantes, que tardaban una media de 30 segundos en realizar una actividad y consiguieron 210 millones de SMLY. Comparado con los 143 segundos y los 101 millones de SMLY que

tardaban y conseguían 478 estudiantes de la universidad, el abuso era importante. Se consiguió frenar el ataque variando los parámetros para aquellas personas que entraban en la plataforma sin ser estudiantes, diferenciándose así de los de los estudiantes (Stefensson et al. 2017).

4 EL FUTURO DE LAS CRIPTOMONEDAS

4.1 Previsiones

Según ElBahrawy, Alessandretti, Kandler, Pastor-Satorras y Baronchelli (2017), en el corto y medio plazo, los avances en la legislación, el desarrollo técnico y el avance social tendrán una alta repercusión sobre el mercado de criptomonedas. El aumento de la capitalización de mercado atraerá más que probablemente la atención de los especuladores y aumentará el uso de la criptomoneda como método de pago. ElBahrawy et al. (2017) opinan que mientras que el uso de las criptos como activos especulativos conllevará la diversificación y el uso de varias criptomonedas, el uso de éstas como método de pago dará pie a una lucha por la supremacía de una sola criptomoneda, y la ganadora no dependerá solo de sus funciones y estructura, si no, mayoritariamente, del renombre que tenga en la sociedad y lo conocida que sea.

Varios autores como Scott o Sovbetov, han opinado varias veces que el futuro de las criptomonedas vendrá dado por la especulación, por lo que el conocimiento de la población a cerca de estas nuevas monedas será clave en la evolución y el desarrollo de las mismas.

Defienden que la formación de una burbuja supondrá finalmente la estabilidad de un activo que servirá tanto para la especulación, como para método de pago, y que como buen activo especulativo, la popularidad y la importancia que la sociedad le otorgue marcará el devenir de las criptomonedas.

Sin embargo, autores como Jacobs o Lansky van un paso más allá., proponiendo un uso de la criptomoneda muy interesante que veremos con atención más adelante. Proponen el uso de la criptomoneda de una forma global, ya sea como

moneda nacional o moneda mundial, apoyando la globalización y el empeño del ser humano en conseguirla.

En general, el futuro de las criptomonedas parece llegar a buen puerto, ya sea como bien especulativo, como método de pago o dándole un uso más global, todo dependiendo del conocimiento de la población en estas monedas, y el apoyo que reciba por parte de gobiernos y población (Jacobs, 2018).

4.2 Criptomoneda moneda nacional

Lansky (2018) no ve tan lejana la opción de usar una criptomoneda como moneda nacional, ya sea una ya existente, como el Bitcoin, o creando una nueva moneda. La razón de mayor peso para utilizar una criptomoneda como moneda nacional reside en la reducción de los riesgos que la utilización de éstas conlleva, aunque no se lograría la eliminación total.

Si un estado adopta una criptomoneda como moneda legal dentro de su jurisdicción, sería apropiado que fuera el estado el que se viera involucrado en la estructura operativa de dicha criptomoneda así como el inversor único en el equipamiento necesario para la minería (Lansky, 2018). Según Valfells y Egilsson (2016), el coste de minar y los beneficios que otorga serían los mismos. Además, siendo el estado el que apoyara una criptomoneda invirtiendo en ella, la confianza de los ciudadanos aumentaría, así como su capitalización de mercado, haciendo así reducir el riesgo de la rápida fluctuación del valor de dicha criptomoneda (Lansky, 2018).

El problema de la no irreversibilidad de las transacciones haría que las administraciones no pudieran cometer error alguno, un problema que se acentúa con el riesgo de pérdida de fondos si la clave del monedero virtual es divulgada (Lansky, 2018). Aun así, hay una solución siempre y cuando sea el estado el que se encargue de minar las criptomonedas, consiguiendo un poder de minería suficientemente grande como para bloquear la ejecución de una transacción desde una cuenta en concreto (Lansky, 2018). El proceso contiene mucho tecnicismo y es bastante complejo, por lo que obviaremos los detalles del cómo, y nos

centramos en el fin último, que es la reducción de la motivación criminal. Para el problema de la no irreversibilidad de las transacciones, si alguna administración comete un error y otorga más criptomonedas a un ciudadano de las que en un principio eran, la cantidad sobrante debería ser devuelta de inmediato, sin excusas y bajo la amenaza de una sanción (Lansky, 2018).

El último problema que se eliminaría con la adopción de una criptomoneda como moneda nacional es el causado por la distribución global de la red, es decir, que en todo el mundo se puede utilizar, comercializar y especular con esa criptomoneda. Realmente, este problema solo sería eliminado si varios países adoptaran también la criptomoneda como moneda nacional (Lansky, 2018), algo que se acerca a la idea de “criptomoneda como moneda mundial” que veremos en el siguiente apartado.

En general, la idea de una criptomoneda como moneda nacional basa sus ventajas en la reducción de los riesgos que el uso de ésta genera, sacando a la luz los altos beneficios de la misma.

4.3 Criptomoneda moneda mundial

Durante miles de años, la humanidad ha evolucionado, desde su organización en ciudades, tribus, estados y reinos hasta un sistema de estados-naciones (Jacobs, 2018). Puede ser que haya llegado el momento de pasar a una organización más global con una gobernanza más globalizada e instituciones más efectivas (Jacobs, 2018). Tras el fin de la Guerra Fría, el proceso de integración se ha acelerado dramáticamente, con consecuencias tanto positivas como negativas. La caída del muro de Berlín, la desaparición de la Unión Soviética, el rápido ascenso de la democracia, un mayor aumento de la inmigración y el turismo internacional, el crecimiento expansivo de la comunicación global, la globalización de las tecnologías y la creación de la primera institución realmente global, la World Wide Web (WWW) (Jacobs, 2018). A pesar de lo bueno, ha tenido lugar la proliferación de las armas nucleares estatales, crecimiento de la tensión intercultural o el terrorismo.

Económicamente, el fin de la Guerra Fría conllevó la creación de la OMC, que supuso una expansión del comercio global con un alto crecimiento de la Unión Europea y la Eurozona, desregulaciones y una expansión de la banca global, un rápido crecimiento de los mercados financieros internacionales, la globalización de los mercados y de los productos, una competición entre estados para ofrecer mejores condiciones a las inversiones de negocio y una mayor autonomía a las corporaciones multinacionales, que dejan de depender de toda nación (Jacobs, 2018).

Con todas las ventajas que ha supuesto la globalización, todavía queda un paso, y hoy día, con las criptomonedas, estamos más cerca que nunca de alcanzar la globalización total con la utilización de la criptomoneda como moneda mundial (Jacobs, 2018).

Con la idea de usar la criptomoneda como moneda mundial, Jacobs (2018) redacta los beneficios en los que incurriría la sociedad y la economía con una moneda mundial.

El principio básico de la creación del Euro y la Eurozona, fue reducir los riesgos financieros y los costes de transacción (Jacobs, 2018), y como hemos citado anteriormente, el mayor beneficio que puede otorgar una criptomoneda es la reducción en los costes de transacción. La reciente Eurocrisis ha sacado a la luz los problemas que venían teniendo lugar cuando las naciones requerían mayor soberanía nacional en la ausencia de instituciones políticas y económicas centralizadas, incapaces de dirigir la zona monetaria con políticas fiscales y monetarias (Jacobs, 2018).

Los beneficios que conlleva establecer una única moneda global, basada en un Banco Central Mundial se ha considerado durante décadas. En 1994, en la conferencia de Bretton Woods, los Estados Unidos y Gran Bretaña propusieron el establecimiento de una moneda global (Jacobs, 2018). Los británicos apoyaron un plan desarrollado por Keynes, en el cual se creaba una reserva mundial de moneda llamada el “bancor”, y que era administrada por un banco central con la capacidad

de crear dinero (Jacobs, 2018). En cuanto a las criptomonedas, Jacobs (2018) propone crear una institución que se haga cargo de una sola criptomoneda, dejando las demás como activos especulativos, con el poder para crear más y más a través de la minería.

A principio de los 80s, el economista Richard N. Cooper, propuso un esquema radical para el siglo veintiuno, la “creación de una moneda común para todas las democracias con una política monetaria común, así como un Banco Central encargado de tomar las decisiones.” Jacobs (2018), apoyando la idea de Cooper, piensa que una vez que la comunicación, el transporte, la tecnología, el comercio de bienes y servicios, la banca y las inversiones se han globalizado, un sistema monetario nacional deja de tener sentido, ya que no puede ser completamente efectivo en el mercado global.

Hay varios premios Nobel que apoyaron la creación de una moneda global, como Joseph Stiglitz en 2016 o Robert Mundell en 1999. Este último propuso que el Banco Central Global podría tener la moneda única respaldada por una reserva de dólares, yenes, euros y oro, y es con esta idea con la que Jacobs (2018) erradica el problema de la falta de valor de las criptomonedas (pág. 8). Una criptomoneda sería respaldada por una reserva mundial de varias monedas, por lo que tendría un valor intrínseco y no un valor irreal o vacío.

Sin embargo, los políticos más conservadores prosiguen su lucha por poner la soberanía nacional por encima de la administración de la economía doméstica, y no abren sus ojos para observar un mundo en el que la fuerza de un mercado internacional reta la noción de un mercado nacional (Jacobs, 2018). Aun así, Jacobs (2018) opina que no se tardará mucho en tornar la opinión de dirección, como ya dijo Mundell “Es sorprendente con qué rapidez los pensamientos cambian, y los políticos pueden huir de sus viejas y antiguas ideas”. Y para dar más esperanza, recuperamos una frase de Eatwell y Taylor, que dice que “Lo que es utópico un día, al día siguiente es sabiduría convencional.”

Así que debido a la controversia y a las actuales dificultades que suponen establecer una moneda mundial con una autoridad centralizada, Jacobs (2018) apunta que la cuestión que hoy día hay que plantearse es hasta donde llega el potencial de las criptomonedas en el sistema financiero global y qué agencia regulatoria ha de tomar el control para imponer un uso efectivo al mal uso que tiene lugar por culpa de la especulación, la evasión fiscal y otro tipo de actividades criminales.

5 ENCUESTA

Partimos de la base de que la evolución de las criptomonedas dependerá en gran medida del conocimiento que la gente tenga de ellas. Es decir, si la población comienza a informarse y a “darle bombo” como quien dice, las criptomonedas tomarán un papel importante en la economía y en la sociedad mundial, ya sea como bien especulativo o como medio de transacción, ya que la idea de adoptar o crear un criptomoneda como moneda nacional o mundial parece todavía algo utópico.

Por esta misma razón, la encuesta se basa en el conocimiento de las personas en las criptomonedas actualmente y en el futuro que le ven. Para la realización de esta encuesta he tomado una muestra de 350 personas, y las preguntas que he realizado son las siguientes:

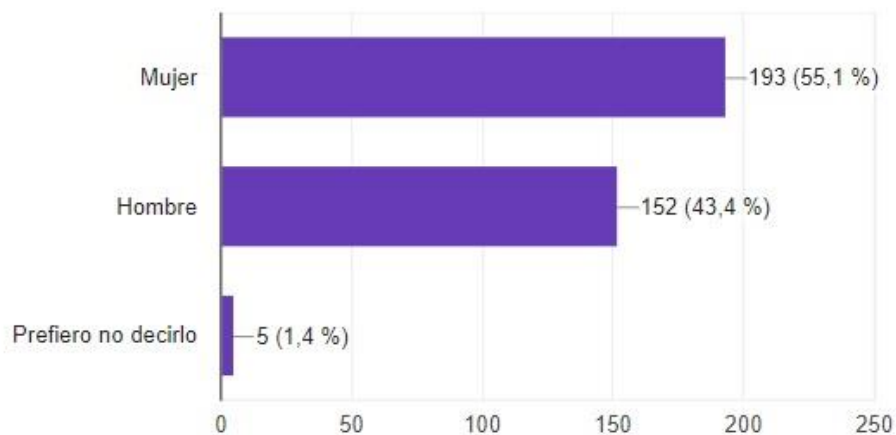
1. Hombre/Mujer
2. 18-24; 25-34; 35-55; >55 EDAD
3. ¿Estudias/trabajas?
4. En caso afirmativo, ¿en relación con el mundo de la economía/mercados/finanzas?
5. ¿Has oído hablar alguna vez de las cryptomonedas?
6. En caso afirmativo, ¿cuál(es)?
7. ¿Has comprado alguna vez cryptomonedas?
8. En caso afirmativo, ¿cuáles?
9. ¿Con qué motivo? (especulativo/transacción)

10. Si no has comprado, ¿te gustaría comprar alguna vez?
11. ¿Con qué motivo? (especulativo/transacción)
12. ¿Ves las criptomonedas seguras?
13. ¿Crees que tomarán un papel importante como método de pago?
14. ¿Crees que se quedará en un “bien” especulativo?
15. En general, ¿cuánto futuro le ves a las criptomonedas? 0-10.

Como lo que nos interesa es saber el conocimiento o el no conocimiento de las criptomonedas, la pregunta CINCO resulta el fin de la encuesta para aquellas personas que NO han oído hablar nunca de las criptomonedas.

El resultado de la encuesta ha sido el siguiente:

Fig. 4: Género de los encuestados

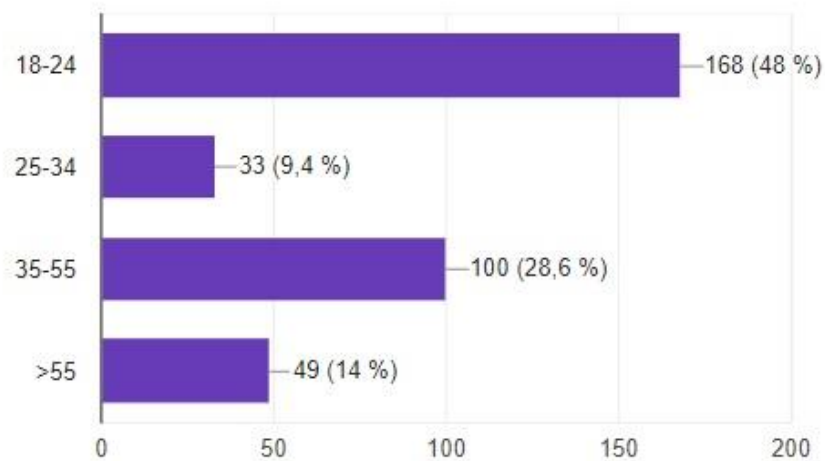


Fuente: Elaboración propia

De las 350 personas que han contestado a la encuesta, el 55,1% (193) son mujeres y el 43,3% (152) hombres.

El 1,4% (5) restante prefería no decirlo.

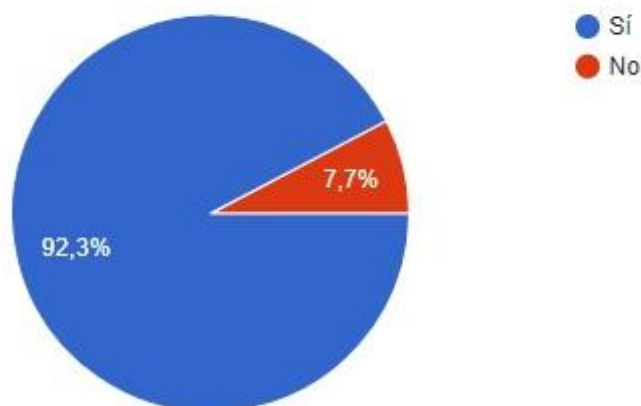
Fig 5. Edad de los encuestados.



Fuente: Elaboración propia

El 48% (168) de los encuestados se encuentra entre los 18 y los 24 años. El 28,6% (100) entre los 35 y los 55. El 9,4% (33) entre 25 y 34 y el 14% (49) son mayores de 55. Con estos datos observamos que la encuesta se ha realizado mayormente a jóvenes y a adultos con, presumiblemente, una vida ya formada. De esta manera podremos observar dos perspectivas totalmente diferentes, aquella de un joven, con mayor aversión al riesgo y una mayor proyección del futuro, y aquella de un adulto con mayor temor a los cambios y menor aversión al riesgo.

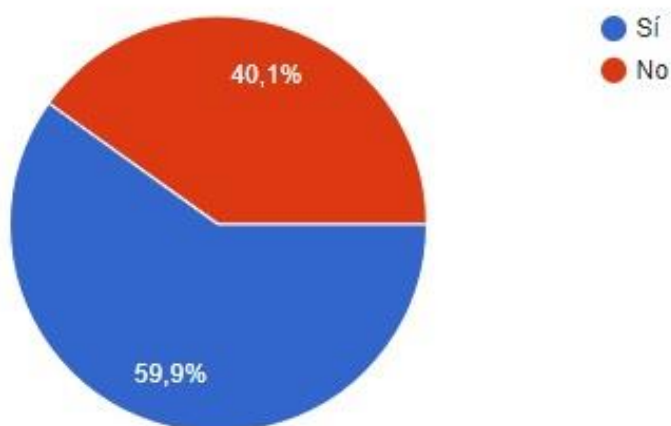
Fig 6. Estado laboral de los encuestados



Fuente: Elaboración propia

El 92,3% (323) de los encuestados trabaja o estudia, y de ellos, solo un 28,2% (91) lo hace en relación con el mundo de la economía, de los mercados o de la finanza. Esta pregunta intenta averiguar el nivel de formación de los conocedores o no de las criptomonedas, aun no siendo un indicador totalmente fiable.

Fig 7. Conocimiento de los encuestados sobre criptomonedas.



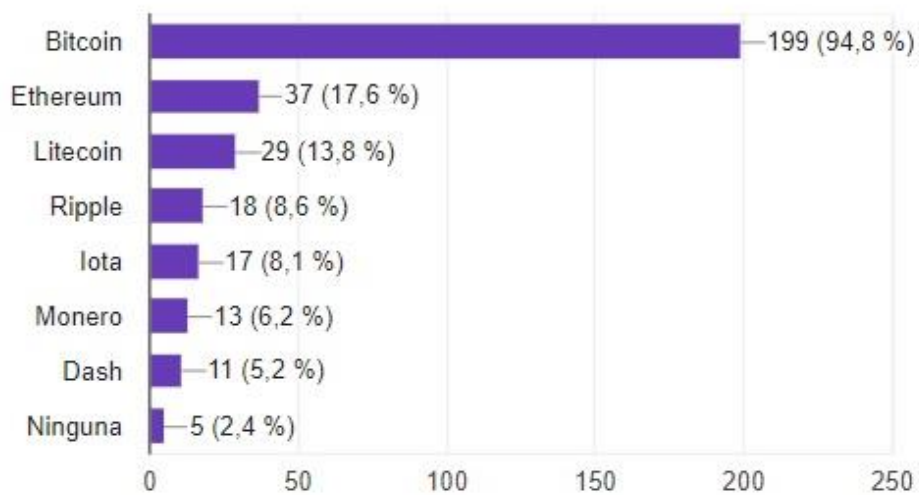
Fuente: Elaboración propia

De todos los encuestados, el 59,9% (206) ha oído hablar alguna vez de las criptomonedas, dejando el 40,1% (138) restante como desconocedores de éstas. En ese 59,9% encontramos a la totalidad de los estudiantes o trabajadores con relación al mundo de la economía, mercados o finanza, lo que indica que las criptomonedas se han hecho un hueco importante en su sector y es difícil no reconocer su existencia e importancia. También encontramos un alto número de estudiantes o trabajadores, así como más adultos que jóvenes.

A partir de ahora, realizamos los porcentajes sobre el 59,9% de los encuestados iniciales, es decir, sobre 206 personas.

Para conocer las criptomonedas más conocidas entre los encuestados, presentamos una lista con las 7 criptomonedas de mayor capitalización y las más sonadas. Esta lista la comportan: Bitcoin, Ethereum, Litecoin, Ripple, Iota, Monero y Dash. Los resultados fueron los siguientes.

Fig. 8: Criptomonedas más conocidas por los encuestados.

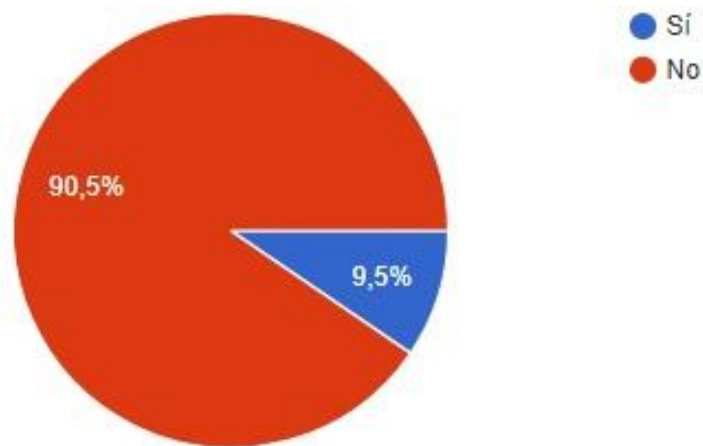


Fuente: Elaboración propia

La más conocida, sin duda alguna, es el Bitcoin, con un 94,8%, le siguen Ethereum y Litecoin. Es una respuesta que era de esperar, debido a la burbuja que han sufrido las criptomonedas encabezada por el BTC, además de ser la primera criptomoneda que se creó.

Una vez observadas las criptomonedas más conocidas, damos un paso más y preguntamos si han comprado alguna vez alguna criptomoneda. Esta pregunta reduce el marco de la encuesta a unos pocos, los cuales entendemos que conocen más de este instrumento que el resto de los encuestados, ya que suponemos que para comprar, han debido de informarse. Igualmente, no resulta un indicador totalmente fiable.

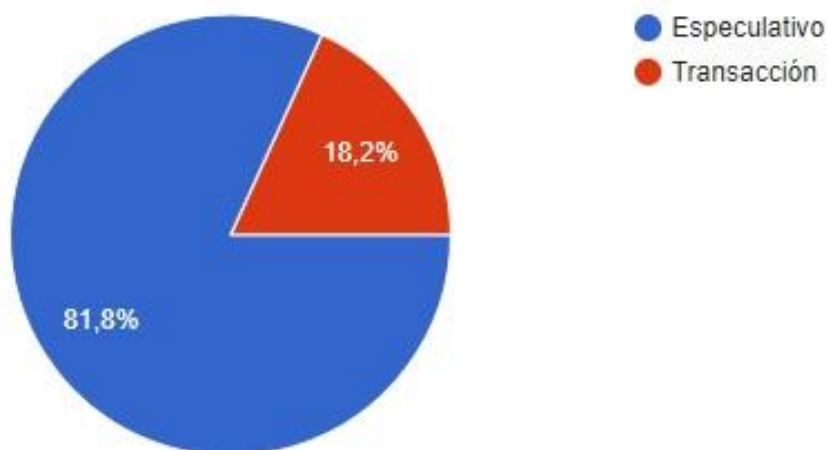
Fig. 9: ¿Ha comprado criptomonedas?



Fuente: Elaboración propia

El 90,5% (190) no han comprado nunca una criptomoneda, siendo el 9,5% (20) los únicos que han dado el paso de comprar y aventurarse. Dentro de estas 20 personas encontramos un 80% de adultos y el 20 restante de jóvenes. Con esto observamos que al ser un producto muy volátil, y tener un alto riesgo, solo han invertido aquellos que poseen una cierta cantidad de dinero con la que pueden “jugar” y probar un poco.

Fig. 10: Motivo de la compra de criptomonedas



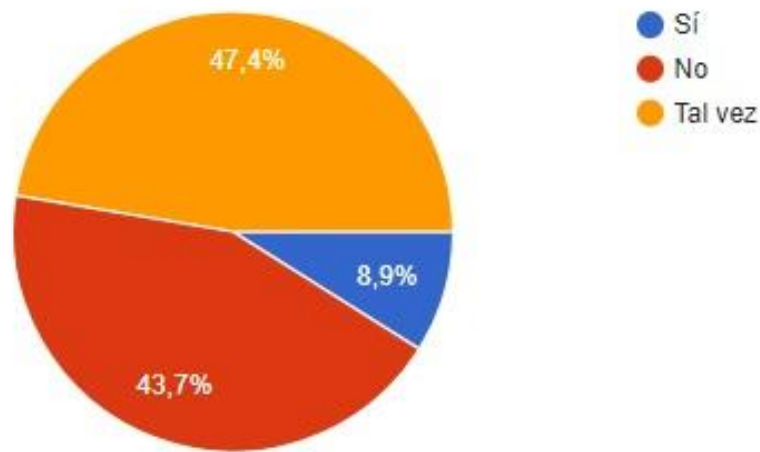
Fuente: Elaboración propia

De estas 20 personas, el 81,8% (18) compró criptomonedas por motivo especulativo, y el 18,2% (4) restante por motivo transacción. Hubo dos personas que compraron por ambos motivos, siendo mayor de 35 todo aquel que compró por motivo transacción.

En cuanto a las criptomonedas que compraron, hay una similitud con las criptomonedas más parecidas. Tenemos en cuenta que una misma persona ha podido comprar más de una criptomoneda. 11 personas compraron Bitcoin, hubo 7 que compraron Ethereum y 4 que compraron Litecoin. Observamos que como era de esperar, aun habiendo encuestados con portfolios de más de una criptomoneda, la más demandada es el Bitcoin.

Volvemos ahora a todos los encuestados conocedores de las criptomonedas para saber si comprarían alguna vez alguna criptomoneda. Con este resultado esperamos conocer el futuro que auguran a las criptos. Si comprarían, quiere decir que ven que puede ir a buen puerto.

Fig. 11: ¿Comprarías criptomonedas en el futuro?

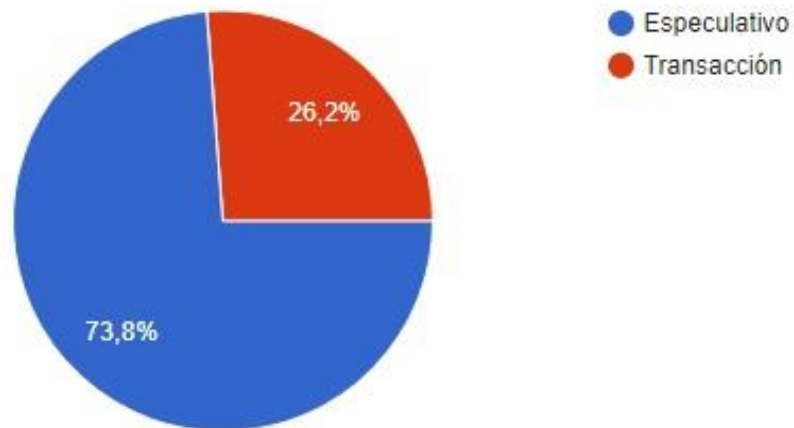


Fuente: Elaboración propia

El 43,7% (83) de los encuestados están seguros de que no les gustaría comprar criptomonedas. Tan solo a un 8,9% les gustaría comprar criptomonedas seguro en un futuro. El resto, el 47,3% (90) quizás compren o quizás no. Podemos empezar a observar

por donde irán los tiros. La mayoría no sabría qué hacer, por lo que existe incertidumbre en el futuro de las criptos.

Fig. 12: Motivo de la compra futura de criptomonedas.

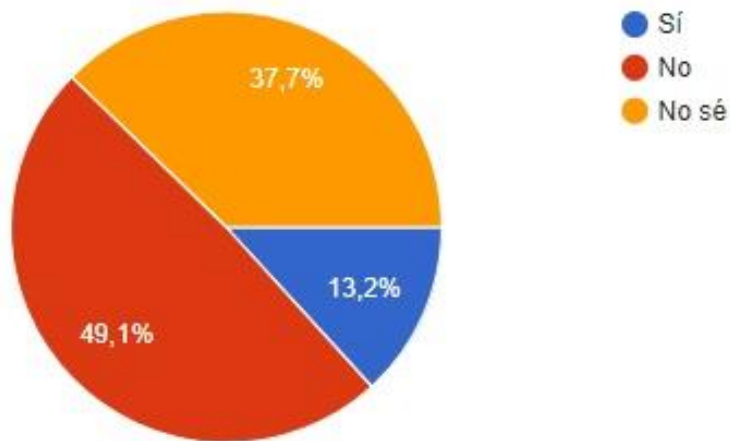


Fuente: Elaboración propia

A las personas que comprarían o que quizás lo hagan, les preguntamos con qué fin lo harían. El 73,8% dice que lo harían por motivo especulativo, y tan solo el 26,2% lo harían por motivos de transacción. Vemos con esto que el futuro de las criptomonedas puede estar ligado a la especulación más que a otra función.

Para conocer un poco más sobre el pensamiento que tienen las personas a cerca de las criptomonedas, preguntamos si creen que son seguras actualmente.

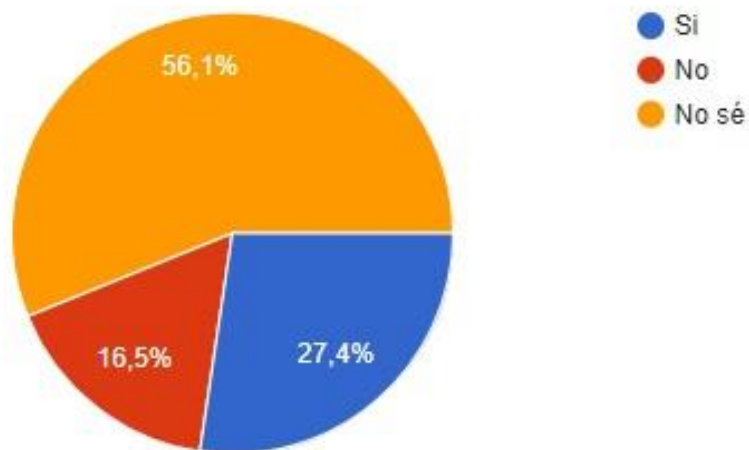
Fig. 13: Seguridad de las criptomonedas actualmente



Fuente: Elaboración propia

La gran mayoría, el 49,1% opina que no, no lo son. Tan solo un 13,2% opina que sí, aunque casualmente, la mayoría son compradores de criptomonedas. El 37,3% restante no sabrían decir si las consideran seguras o no.

Fig. 14: Seguridad futura de las criptomonedas.



Fuente: Elaboración propia

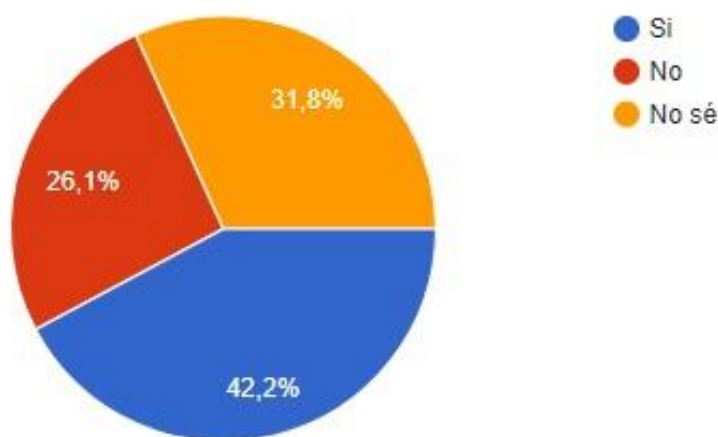
Respecto al futuro, la cosa cambia en cuanto a seguridad. Tan solo el 16,5% de los encuestados opinan que las criptomonedas no serán seguras en el futuro. Un 27,4% opina

que sí, y el 56,1% restante no sabría qué decir. Con estos resultados observamos que hay un aumento en la confianza de las criptomonedas cuando hablamos de futuro. Aunque es cierto que no especificamos de cuánto se trata ese “futuro”, pasamos de 104 personas que no ven las criptomonedas seguras actualmente a tan solo 35 que las siguen viendo inseguras en el futuro. Al igual que hay un aumento de la confianza y una disminución de la desconfianza, se observa un incremento en la incertidumbre.

Plantándonos más en el futuro, preguntamos si las criptomonedas tomarán un papel importante como método de pago o si quedará como un bien especulativo. O quizás las dos.

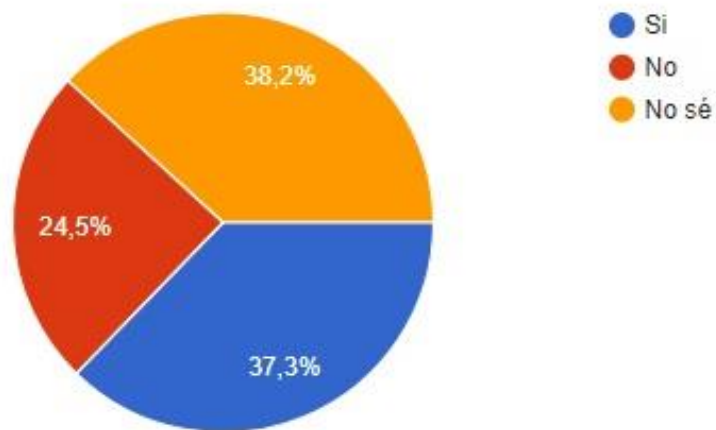
En cuanto al método de pago, un 42,2% opina que sí, que serán utilizadas como método de pago. Un 26,1% opina que no y un 31,8% no sabe. En cuanto a quedar como bien especulativo, el 37,3% cree que servirá como activo con el que especular, un 24,5% piensa que no, y el 38,2% restante no sabe. Con esta información, vemos que la mayoría de las personas dudan sobre qué pasará con las criptomonedas, aunque hay un elevado número de encuestados que opina tendrán un papel en el futuro, ya sea como activo especulativo o como método de pago.

Fig.15: Criptomonedas como método de pago.



Fuente: Elaboración propia

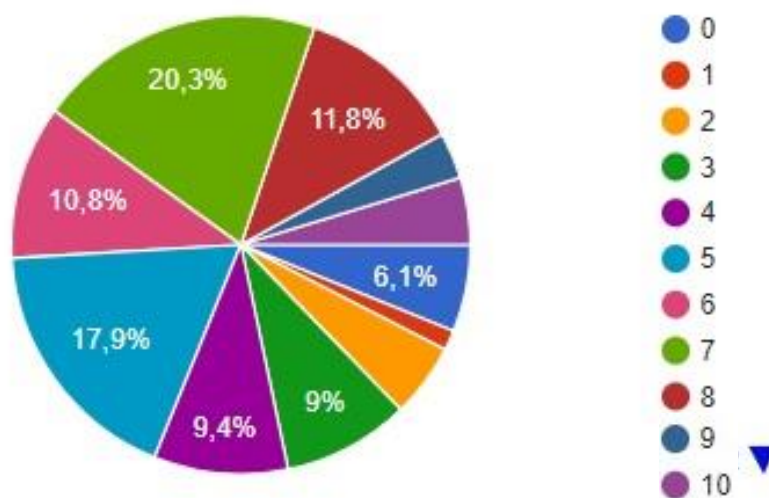
Fig. 16: Criptomonedas como bien especulativo.



Fuente: Elaboración propia

Por último, la pregunta más general de todas, la que engloba todo lo relacionado con las criptomonedas, consta de evaluar del cero al diez el futuro de las criptomonedas, siendo cero “las criptomonedas no tienen ningún tipo de futuro” y diez “las criptomonedas serán el futuro en todos los sentidos”.

Fig. 17: Valoración del futuro de las criptomonedas.



Fuente: Elaboración propia

Hay un 6,1% de los encuestados que le otorgan un 0 al futuro de las criptomonedas y un 4,7% que le otorga un 10. Son porcentajes bajos ya que es muy complicado que se quede en uno de esos dos extremos, sin embargo, el mayor porcentaje es para el 7 con un 20,3% seguido del 5 con un 17,9%. El tercer y el cuarto lugar, muy ajustado, corresponden al 8 con un 11,8% y al 6 con un 10,8% respectivamente. Se observa fácilmente que el grosso de los encuestados bascula entre el 5 y el 8 (60,8%), por lo que como conclusión podemos sacar que nuestros encuestados opinan que las criptomonedas tomarán un papel importante en algunos aspectos, pero no en todos.

Si tomamos esta muestra de 350 personas como muestra representativa, y bajo la premisa de que el futuro de las criptomonedas depende del conocer y de la opinión de la gente, podemos llegar a la conclusión de que el futuro que le espera a las criptos es incierto. La mayoría no saben por dónde saldrán los tiros y no confían plenamente en ellas, factor importante en la evolución de éstas.

BIBLIOGRAFÍA

Autoridad Bancaria Europea (2014). EBA Opinion on virtual currencies.

Caginalp, C., Caginalp, G. (2018). Valuation, liquidity Price, and stability of cryptocurrencies. *Proceedings of the National Academy of Sciences. Vol. 115, no. 6. 1131-1134*

ElBahrawy, A., Alessandretti, L., Kandler, A., Pastor-Satorras, R., Baronchelli, A. (2017). Evolutionary dynamics of the cryptocurrency market. *Royal Society Open Science*. Recuperado de <http://rsos.royalsocietypublishing.org/content/4/11/170623>

Extance, A. (2015). Bitcoin and Beyond. *Feature News. Vol. 526, no. 22.*

Fonseca, J. (2018). ¿Por qué a los bancos les gusta Blockchain? *VisualPolitik*. Youtube. Recuperado de <https://www.youtube.com/watch?v=DAjtCmA-vxE>

Jacobs, G. (2018). Cryptocurrencies and the Challenge of Global Governance. *Cadmus. Vol. 3, no 4.*

Krafft, P., Della Penna, N., Pentland, A. (2018). An Experimental Study of Cryptocurrey Market Dynamics. *Cornell University Library*. Doi: <https://doi.org/10.1145/3173574.3174179>

Lansky, J. (2018). Possible Satate Approaches to Cryptocurrencies. *Journal of Systems Integration, University of Finance and Administration in Prague*. Doi: [10.20470/jsi.v9i1.335](https://doi.org/10.20470/jsi.v9i1.335)

Nahorniak, I., Leonova, K., Skorokhod, V. (2016). Cryptocurrencies in the development of digital single market in European Union. *Intereulaweast. Vol. 3.*

Scott, B. (2016). How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance? *United Nations Research Institute For Social Development. No. 2016-1. Recuperado de <http://hdl.handle.net/10419/148750>*

Sovbetov, Y. (2018). Factors Influencing Cryptocurrency Prices. *Journal of Economics and Financial Analysis. Vol. 2, no 2. 1-27 Doi:10.1991/jefa.v2i2.a16*

Stefansson, G., Lentin, J. From Smileys to Smileycoins: Using a Cryptocurrency in Education. *Ledger. Vol. 2. 38-54 Doi: 10.5915/LEDGER.2017.103*