Universidad Zaragoza
1542

Trabajo Fin de Grado

INVERSIÓN EN CRIPTOACTIVOS Y DIGITALIZACIÓN EN EL SECTOR BANCARIO

Autor
Jorge Borbón Gonzalo

Director
Beatriz Domínguez Bronchal

Facultad de Economía y Empresa UNIZAR

Curso académico 2021-2022

ÍNDICE

ÍNDICE DE IMAGENES Y TABLAS

ABSTRACTO

El objetivo del trabajo es realizar un análisis en profundidad del sector de las criptomonedas, con especial atención en el Bitcoin, por ser la criptomoneda principalmente dominante del sector. Para ello, se analiza un punto de entrada que permite maximizar la rentabilidad e introducir una tecnología tan disruptiva como las criptomonedas y la *blockchain*. a un sector tan tradicional como la banca. Se estudia la aplicación de la tecnología *blockchain* a la banca y los beneficios que esta puede producir además del impacto económico.

ABSTRACT

We approach this paper focusing on the deep analysis of the cryptocurrency field, on one asset: Bitcoin, the asset with the biggest market share in the sector. By centering on this asset, we will assess an entry point to maximize the return as well as to introduce the banking sector into this disruptive technology. We discuss not only Bitcoin but also the innovative technology behind it, the blockchain, by applying it to the banking sector through the development of applications and assessing and speculating about the economic impact.

1. INTRODUCCIÓN

La intención de este trabajo de fin de grado es la proposición de un precio de entrada y/o idea de inversión tomando como principal participe de este el sector de la banca. Asimismo, se aplica un estudio empírico para posteriormente analizar los resultados y los posibles efectos que podría causar. Más específicamente, el estudio tratará de las criptomonedas, principalmente Bitcoin, introduciendo su historia y finalidad, a la vez que, de la *blockchain*, ya que es una tecnología bastante demandada y utilizada por las principales empresas en el ámbito tecnológico. Mediremos el efecto que esta disruptiva tecnología podría tener en el sector bancario y si en un largo plazo se pudiesen obtener beneficios. Gracias a los datos históricos tanto diarios como semanales obtendremos un precio y fechas esperadas para empezar el proceso de inversión.

Se valorará la implantación de billeteras digitales asociadas a cuentas bancarias, donde un banco podrá dar cobertura a estos servicios utilizándose billeteras "*cold wallet*"[1] y el ahorro que esta tecnología nos puede brindar. Para ello primero habrá que tratar la implantación de una red *blockchain* privada para poder crear billeteras a los clientes. Las aplicaciones de una red *blockchain* nos aportarán otros beneficios y zonas para operar como podría ser la participación bancaria en distintos metaversos. Por otro lado, como complemento a estos servicios, se destinará un porcentaje de la tesorería de la empresa como inversión alternativa en una de estas criptodivisas.

La elección de este tema responde a la gran demanda de esta clase de activos desde que se introdujo la moneda originaria, Bitcoin, en 2009. Sin embargo, hoy en día esta clase de activos y la tecnología que va ligada a ellos ofrece a las empresas nuevas posibilidades de inversión y de mejora de los servicios prestados en el ámbito financiero. Es por eso, que la intención de este trabajo de fin de grado es dar una visión más amplia de la utilización de estos activos en el sector. Un ejemplo de empresas que empiezan a elegir las criptomonedas como referencia, es el discutible caso de empresas como MicroStrategy, una empresa dedicada al *software* OLAP[2] con soluciones para otras empresas y creación de informes, que han ido invirtiendo en Bitcoin periódicamente como inversión alternativa, pero a la vez con la finalidad de usarla como divisa para transacciones. Esta empresa lleva años dedicándose a promover la educación acerca del mundo de las criptomonedas y la *blockchain.*

[1] Término utilizado para definir un dispositivo para almacenar tus criptomonedas sin que estén conectadas a internet.
[2] Es un tipo de software que permite realizar análisis multidimensionales a altas velocidades en grandes volúmenes de datos de un almacén de datos, *data mart* o algún otro almacén de datos unificado y centralizado.

2. EL BITCOIN Y LA *BLOCKCHAIN*

2.1 HISTORIA DE LA *BLOCKCHAIN*

Aunque parece que la historia de la *blockchain* es reciente, tenemos que remontarnos a 1994 cuando Stuart Haber, doctor en ciencia computacional por la Universidad de Columbia, y W. Scott Stornetta, doctor en física por la Universidad de Standford crearon uno de los sistemas de ciberseguridad más eficientes de la historia. Ambos trabajaban en la compañía Bell Communications Research más conocida como "Bellcore". En aquella compañía podían elegir sus propias investigaciones y Scott se planteó la siguiente duda respecto a la autentificación de documentos digitales, ¿cómo puedes estar seguro de que el documento que estás visualizando no es una copia que ha sido modificada? Se llegó a la conclusión de que el problema era irresoluble, debido a que un tercero era necesario para poder verificar el documento, pero entra la siguiente cuestión: ¿Y si ese tercero era parte de una colusión?

Se les ocurrió que, si en vez de un único tercero, se añadiesen más partes al acuerdo para dar fe de la honestidad de cada participante, se podría resolver el problema. Sin embargo, la lista de terceros sería infinita y aun así habría sesgos. Ambos apuntaron que el tiempo es un factor determinante y al crear un sistema de documentos entrelazados haces que todo el mundo sea un testigo de los documentos, por lo que, a lo largo del tiempo, esos documentos son verificados por los testigos como originales.

Estos testigos pueden ser tanto personas físicas, con sus propios ordenadores, como un departamento dentro de una empresa grandes compañías. En la práctica, serían ordenadores programados para verificar la autenticidad de los documentos, que actuarían como testigos, dejando una marca de agua imborrable.

2.2. *BLOCKCHAIN*: ¿EN QUE CONSISTE?

La *blockchain* o cadena de bloques es una base de datos distribuida que se comparte entre los nodos de una red informática. Como base de datos, una cadena de bloques almacena información electrónicamente en formato digital. Las cadenas de bloques son más conocidas por su papel crucial en los sistemas de criptomonedas, como Bitcoin, para mantener un registro seguro y descentralizado de las transacciones. La innovación con un *blockchain* es que garantiza la fidelidad y seguridad de un registro de datos y genera confianza sin necesidad de un tercero de confianza.

Sin embargo, lo que más caracteriza a la *blockchain* es el hash. Las funciones del hash son indispensables para el correcto funcionamiento de la red, siguiendo una serie de propiedades

generaremos una referencia única para cada bloque dentro de la red. El *hash* se formará de la siguiente manera:

-El *hash* utilizará un algoritmo para crear una cadena de bits de manera aleatoria con una determinada largura, creando así un código único. Donde "A" es el *output* del algoritmo, "x" es el input del documento a cifrar e "y" es la fecha de firma del documento, nos dará una cadena de bits "z" que será nuestro certificado, por lo tanto:

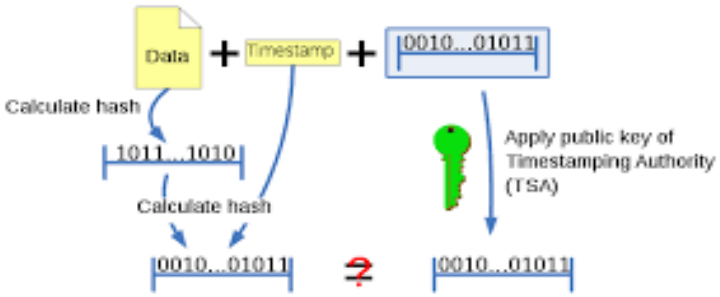
$$z = A(x, y)$$

-*Link* de unión, para que sea imposible falsificar el *hash*, generaremos un link de unión haciendo referencia al *hash* anterior y al futuro *hash* que se vaya a generar, por lo que nuestro nuevo *hash* será el siguiente, tomando como referencia el anterior y añadiendo:
"n" como secuencia inicial de números, y los datos del cliente (en el documento), "ID". Nuestro nuevo *hash*:

$$z_{t+1}(n, ID, x_{t+1}, y_{t+1}, A(x, y))$$

En este nuevo *hash* aparecerá el certificado emitido anteriormente y los datos del siguiente documento generando un nuevo certificado para el nuevo documento en t+1. Con este nuevo *hash* enlazamos el nuevo certificado con el anterior, siendo parte del *hash* totalmente aleatoria, y otra conocida asociada al documento anterior. Para el siguiente *hash* en t+2 la parte aleatoria será considerada como la parte conocida del documento en t+1 y el algoritmo generará un código nuevo aleatorio, así hasta t+ ∞

Imagen 1. Esquema de la creación del hash



Fuente: Wikipedia.

Para que no se pueda falsificar, entra en juego la firma digital, compuesta por el documento y la

fecha de la firma (mencionados anteriormente) y el *software* TSS. Confiando en este *software*, generamos un hash único e inviolable, es decir, el TSS no puede falsificar un documento, ya que los bits que se generaron se modificarán cambiando por completo el hash, "rompiendo" así la cadena. Por lo tanto, cualquier modificación/falsificación de cualquier documento es fácil de detectar.

-Confianza en los usuarios. Todos los usuarios disponen de un generador pseudoaleatorio[3] que permite firmar digitalmente y a la vez asegura las firmas y el valor del *hash* generando secuencias aleatorias que son impredecibles, estos generadores fueron estudiados por Blum y Micali[4] y son los que verifican la veracidad del documento. Con esto lo que se evita es la centralización de la aprobación de los acuerdos en una única entidad o sujeto, siendo aprobados por el público en general (CPUs). En el caso de la cooperación de un número de usuarios deshonestos, los cuales podrían cooperar para verificar un documento falsificado, el sistema llama a los usuarios aleatoriamente gracias al generador pseudoaleatorio, con esto se evitan posibles colusiones, estos usuarios deberán firmar el mismo documento verificando así su autenticidad, con esto evitamos la deliberada selección de usuarios para verificar.

En conclusión, lo que se propuso era un sistema que verificase documentos de texto, audio y vídeo y evitase colusiones (Pacto ilícito en daño de tercero), con el uso del *hash* de única dirección y el generador pseudoaleatorio, esto permitía establecer una estampa temporal para generar una precedencia a la propiedad intelectual del documento sin revelar su contenido.

2.3. HISTORIA DEL BITCOIN

Todavía a fecha de mayo de 2022, sigue sin saberse nada de la historia de la creación del Bitcoin, sus inicios retornan al 31 de octubre de 2008 donde apareció un enlace a un documento en el cual se especificaba un sistema *peer-to-peer*[5] de dinero digital firmado por el autor Satoshi Nakamoto, del cual

[3] Un generador de números pseudoaleatorios, aunque conocido por las siglas PRNG, también conocido como generador de bits aleatorios deterministas (DRBG), es un algoritmo para generar una secuencia de números cuyas propiedades se aproximan a las propiedades de secuencias de números aleatorios. La secuencia generada por el PRNG no es verdaderamente aleatoria, porque está completamente determinada por un valor inicial, llamado semilla del PRNG (que puede incluir valores verdaderamente aleatorios). Aunque las secuencias que están más cerca de ser verdaderamente aleatorias se pueden generar utilizando generadores de números aleatorios de hardware, los generadores de números pseudoaleatorios son importantes en la práctica por su velocidad en la generación de números y su reproducibilidad.

[4] El algoritmo Blum-Micali es un generador de números pseudoaleatorios criptográficamente seguro. El algoritmo obtiene su seguridad de la dificultad de calcular logaritmos discretos.

[5] La computación o *red peer-to-peer* (P2P) es una arquitectura de aplicación distribuida que divide tareas o cargas de

no se sabe ni su identidad ni su procedencia, se desconoce si fue una persona o grupo de personas los que crearon el documento. La primera transacción fue realizada el 6 de febrero de 2009, donde, desde la cuenta de Satoshi fueron enviados 10 BTC (*Ticker*/ Siglas del Bitcoin) a la cuenta de Hal Finney[6], quien descargo el software el mismo día que apareció el *link*.

El Bitcoin ha sufrido muchas prohibiciones y regulaciones desde su lanzamiento como el vaneo del uso de la moneda en China, sin embargo, muchos creen en esta moneda como la divisa del futuro. Países con una inflación desproporcionada utilizan herramientas como esta para que sus activos no pierdan valor y para asegurar transacciones ya que en estos países suele haber mucha corrupción. Es el caso de El Salvador, un país subdesarrollado el cual actualmente tiene como divisa oficial el Bitcoin, ya que desde la publicación de la Ley Bitcoin el 9 de junio de 2021 es de uso legal aprobado por más del 70% de la población, en un breve resumen esta ley propone aportar educación financiera a la población, la regulación del Bitcoin con el par BTC/DLR, exención impuestos y más restricciones. Por otro lado, nos encontramos con el caso de China que ha estado prohibiendo su uso en reiteradas ocasiones a lo largo de la vida de esta criptomoneda.

Actualmente muchas instituciones como MicroStrategy y todos los *exchange* son pioneros en la educación financiera de este activo y sus semejantes, además de en la inversión de gran parte de su tesorería como inversión alternativa, y es que no solo como inversión, sino también ha sido usada como pago, seguidamente pasaremos a la explicación de su funcionamiento y el porqué de tanto apoyo hacia esta.

2.4 BITCOIN, ¿EN QUE CONSISTE?

Es un sistema monetario digital que usa transacciones *peer-to-peer*, evitando intermediarios y regulándose por el *proof-of-work*[7] y el sistema *blockchain*, el cual, a su vez está basado en la

trabajo entre pares. Los pares son igualmente privilegiados, participantes equipotentes en la aplicación. Se dice que forman una red *peer-to-peer* de nodos.

[6] Harold Thomas Finney II (4 de mayo de 1956 – 28 de agosto de 2014) fue un desarrollador estadounidense de PGP Corporation, fue uno de los primeros contribuyentes de Bitcoin y recibió la primera transacción de bitcoin del creador de bitcoin, Satoshi Nakamoto.

[7] *Proof-of-work* trabajo (PoW) describe un sistema que requiere una cantidad de esfuerzo no insignificante pero factible para disuadir los usos frívolos o maliciosos de la potencia informática, como el envío de correos electrónicos no deseados o el lanzamiento de ataques de denegación de servicio. Fue inventado por Cynthia Dwork y Moni Naor en 1993 como una forma de disuadir los ataques de denegación de servicio y otros abusos de servicio, como el spam en una red. Posteriormente fue adaptado para asegurar el dinero digital por Hal Finney en 2004 a través de la idea de "prueba de trabajo reutilizable" utilizando el algoritmo hash SHA-256.

criptografía. Este sistema funciona gracias a un inmenso poder computacional y es que, sin los partícipes en la red (CPUs de minería) y varias características, esta moneda no podría funcionar de forma eficaz. Debido al aumento de transacciones online, el público general tiene que tratar con un tercero para verificar estas transferencias y confiar en ese tercero para que verifique el pago, este intermediario se puede definir como entidad bancaria. Como solución a este gran aumento en el volumen de transacciones este sistema evitaría el doble gasto[8], la corrupción, ya que todas las transacciones son rastreables y las terceras partes pueden corromperse, y generará una privacidad de datos que no existe en el mundo digital actualmente. Además de todo lo mencionado anteriormente, los pagos con *Bitcoin* suponen un avance en cuanto a rapidez en transferencias internacionales y un gran ahorro debido a las mínimas comisiones que se aplican para el continuado y correcto funcionamiento de la propia red.

Actualmente hay 19,032,406 Bitcoins minados, sin embargo, desde su creación hasta hoy, se estima que entre 3 y 4 millones de Bitcoin se han perdido. Por lo que su máximo teórico sería 21 millones, siendo el máximo real 18 millones de monedas en circulación.

La red de Bitcoin tiene una serie de características y mecanismos para que esta funcione correctamente, por lo consiguiente se basará en:

-*El hash,* al igual que lo definido en el uso de la *blockchain*, toma un papel crucial en la red, ya que estos *hashes* están relacionados entre sí, generando una cadena, pero al ser dinero digital uno podría usar la moneda para "pagar" dos veces, en este caso se implementa un algoritmo para que este verifique que esto no ocurre, ambas partes de la transacción deberán firmar el documento anterior, añadiendo estos datos al hash. Todo esto ocurrirá en cada hash futuro que se cree, generando así una cadena irrompible. Por lo tanto, así, evitamos el problema del doble gasto. La transparencia es fundamental, estás transacciones serán públicas para mostrar la dirección que sigue la moneda, y los participantes de la red deberán verificar que esa transacción es correcta y que no hay colusión asegurando que la moneda se ha transferido una única vez, para poder verificar que es correcto se necesitará de la mayoría de la red.

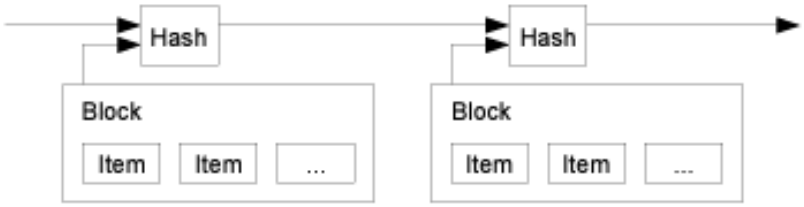
Se tiene que nombrar una característica muy importante del *hash,* la dificultad, y es que esta hace que sea más fácil o difícil minar los bloques. En los primeros años de su

[8] El doble gasto es un defecto potencial del dinero digital por el que una misma moneda digital puede gastarse más de una vez. Esto es posible porque cada moneda consta de un archivo digital que puede duplicarse o falsificarse.

creación la dificultad era mínima, lo que significaba que habías muy pocos usuarios minando bloques en la red, esto generó que se minasen los primeros 210.000 bloques muy rápidamente. Conforme más usuarios entran en la red la dificultad aumenta y por lo tanto cuesta más energías minar, esto implica un mayor gasto, lo que conlleva que solo los equipos que obtienen rentabilidad permanecen en la red, generando así una mayor competitividad y eficiencia ya que cuanto más difícil es el algoritmo, más optimizada estará la red.

-*Servidor de firmas:* Se ha comentado la importancia de la firma digital de documentos para su correcta autentificación, cada hash contendrá la firma digital de los documentos actuales y de los anteriores (cadena), por lo que en caso de alteración de la red el hash probará que los documentos existieron en un tiempo anterior, pudiendo eliminar así cualquier intento de malfuncionamiento de la red. Dentro de cada hash está incluida la información de todos los documentos, en este caso al ser transferencias entre usuarios, se recogerán una cantidad de transferencias en un bloque, este bloque gracias a la información de las transferencias generará un hash único e imposible de predecir. El tamaño de los bloques de Bitcoin ronda en torno a 1 MB.

Imagen 2. Esquema de la cadena de bloques



Fuente: White paper "Bitcoin: A Peer-to-Peer Electronic Cash System" por: Satoshi Nakamoto

Proof-of-work: La prueba de trabajo o *proof-of-work* es el sistema por el cual se rige la red, aunque esta red se basa en el sistema *Hashcash*[9] creado por Adam Back, el *proof-of-work* fue utilizado por primera vez en 1992 para eliminar ataques de spam en los correos electrónico. Con el *proof-of-work* de bitcoin se determina que cada CPU cuenta con un voto para la toma de decisiones de verificación de bloques. Este sistema se encarga de generar los bloques y así los hashes comenzando con 0 bits, utilizará un poder

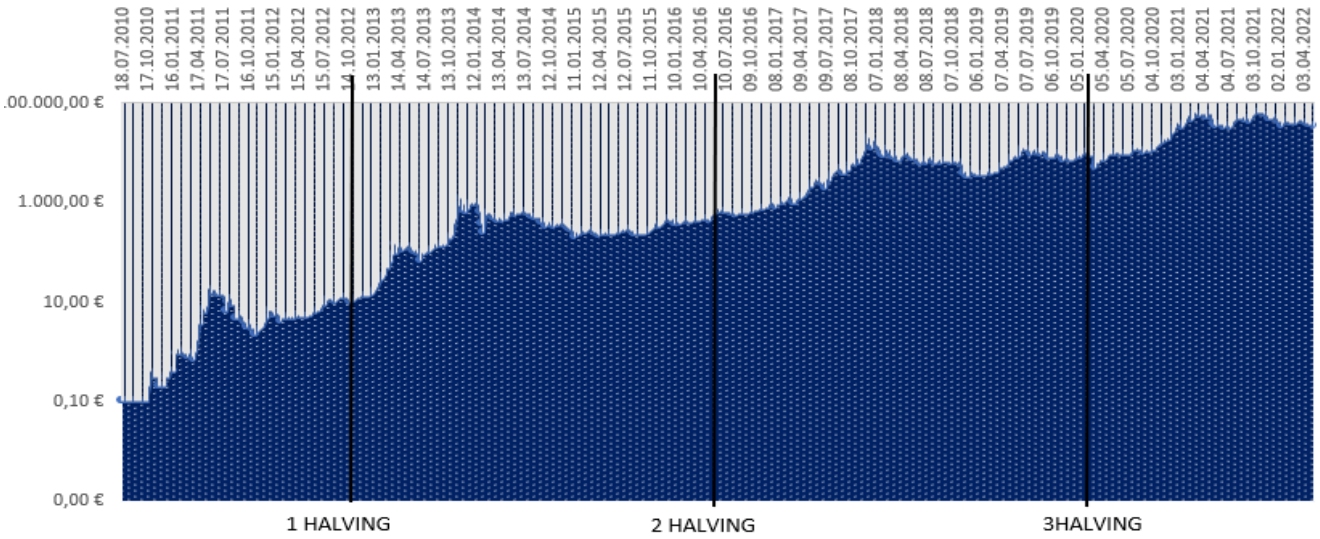
[9] *Hashcash* es un sistema de prueba de trabajo (PoW) creado por Adam Back en 1997, aunque su *Whitepaper* fue publicado en 2002. El objetivo principal de *Hashcash* era minimizar la recepción de grandes cantidades de correos electrónicos no deseados, utilizando la colisión de hashes para ello.

computacional para la creación de los bloques y por lo tanto de los hashes.
Mediante la resolución de algoritmos los bloques son creados y las CPUs que consiguen la resolución de estos obtienen una recompensa por el poder computacional utilizado.

Usuarios: Las CPUs, o nodos, también conocidos popularmente como mineros, son los encargados de hacer que la red funcione, los nodos recopilan todas las transacciones disponibles para almacenarlas dentro de un bloque, antes de eso cada nodo trabaja resolviendo algoritmos para obtener ese bloque, la dificultad de los algoritmos puede variar. Una vez obtenido el bloque se incluirán las transacciones dentro de este y pasará a ser verificado por todos los demás usuarios dentro de esta red, si todo está correcto, este nodo (CPU) recibirá un incentivo, en forma de *bitcoin* para así seguir usando el poder computacional para obtener nuevos bloques y así asegurar la red.
Hay que tener en cuenta que sin los "mineros" la red de *bitcoin* caería y el tiempo medio de minado de bloques es de unos 10 minutos, lo que se tarda en resolver los algoritmos.

Incentivo: Es la recompensa que reciben las CPU por participar y mantener la red. Tenemos que comentar que el incentivo presenta una serie de características que hace que este dinero digital sea único, la emisión de la moneda se hace a través de un algoritmo el cual regula el incentivo por bloque, el nodo que mina el bloque obtiene las comisiones de la red por las transacciones del bloque además de una recompensa originaria de 50BTC que se reduce a la mitad cada 210.000 bloques minados (cada 4 años aproximadamente), esta reducción acabará en el año 2140 llegando a su límite máximo de 21 millones de monedas. Gracias a esta recompensa la red sigue funcionando.
Este evento es el conocido "*Halving*", esto hace del Bitcoin una divisa antinflacionaria, ya que, aunque la recompensa es menor, la gran demanda y la poca oferta generaría una apreciación en el precio de la moneda, por lo que la recompensa sería igual o mayor que la anterior.

Imagen 3. Gráfico logarítmico de los *halving* y el crecimiento de la moneda, pudiendo observar un movimiento cíclico



Fuente: Elaboración propia

2.5. LIMITACIONES Y DESVENTAJAS

Bitcoin es un modelo de monetario seguro, deflacionario y público, a la vez que privado, mostrando solo el ID de tu billetera, sin embargo, debemos tener en cuenta varios aspectos negativos a la hora de considerar esta criptodivisa.

Lo primero de todo es que se ha de tener constancia de donde se guardan las llaves privadas de la billetera en la que se almacenan estas criptomonedas, ya que, sin esas llaves, las monedas son imposibles de recuperar. Pasa lo mismo si perdemos nuestra *cold wallet*.

Otra limitación es la de la enorme volatilidad de este activo, ya que tiene gigantescas fluctuaciones en periodos de tiempo muy cortos, además, los usuarios de la red y propietarios de la moneda no están protegidos debido a que no hay un gobierno que lo respalde. En algunos países se están empezando a regular estos activos, como es el famoso caso de El Salvador, aunque, en otros, la regulación toma otra dirección, es el caso de china que ha prohibido su uso y cualquier negocio relacionado con este.

Una de las peores cosas que le podría ocurrir a la red de Bitcoin, es el caso de la colusión. Hipotéticamente, si más del 50% del poder computacional (las CPU de minería) está controlado por una persona o persona jurídica con fines maliciosos, a la hora de verificar las transacciones, está podría verificarlas al ser la gran mayoría fraudulenta. Por lo que se verificarían cualquier tipo de transacción sea esta autentica o no, llevando la red a la corrupción total y el colapso.

La escalabilidad es otro de los problemas, siendo que empresas como Visa y MasterCard realizan transacciones en milésimas de segundos.

En nuestro caso hay que esperar los 10 minutos de minado y verificación de cada bloque para que la transacción se complete. Obviamente, no se puede comparar Bitcoin con estas empresas, sin embargo, en comparación a una transferencia bancaria internacional o incluso nacional, dependiendo del país, donde estas tardan días en llegar, Bitcoin solo tarda los 10 minutos que se explicaba anteriormente.

3. ANÁLISIS TÉCNICO Y MACROECONÓMICO

Bitcoin es un activo que fluctúa con gran agresividad, teniendo una gran volatilidad. Para poder hacer nuestra inversión, primero se debe hacer un análisis macroeconómico y técnico para centrarnos en el "*momentum*", y así obtener un precio óptimo que hará que nuestra rentabilidad incluso se multiplique.

Lo primero para tener en cuenta es que la cantidad de 21 millones no es cierta, debido a la pérdida de Bitcoins en los primeros años de su creación, se estima que se perdieron entre 3 y 4 millones de bitcoins en los inicios, por lo tanto, su masa monetaria real sería entre 17 y 18 millones. Siendo la cantidad limitada, lo siguiente serán los *halvings*, estos momentos son claves para la inversión en esta moneda, debido a la reducción a la mitad de la recompensa a los mineros, se puede apreciar un comportamiento cíclico del mercado. Para ello analizaremos los *halvings* que han ocurrido hasta el día de hoy.

Hay que tener estas fechas muy presentes, ya que los *halvings* marcan el inicio del ciclo alcista. Bitcoin se lanzó el día 3 de enero de 2009, los *halving* ocurren cada 210.000 bloques minados, aproximadamente cada 4 años, las fechas son las siguientes:

Imagen ***4.*** Tabla con los precios de cierre del día de cada *halving.*

	Fecha	Nº de bloque*	Recompensa	Precio
Lanzamiento	3 de enero de 2009	0	50	0
1 Halving	28 de noviembre de 2012	210	25	2,66
2 Halving	9 de julio de 2016	420	12.5	647,68
3 Halving	11 de mayo de 2020	630	6.25	8.571,98
4 Halving	3 de mayo de 2024	840	3.125	x

Fuente: Elaboración propia

La tabla nos muestra las fechas, los bloques minados que están representados en miles de unidades, los bitcoins obtenidos por la recompensa y el precio en el día del *halving* está expresado en dólares. Se aprecia una x en el precio del 4 *halving* ya que se calcula que ocurrirá con el minado de otros 210.000 bloques el 3 de mayo de 2024, esta fecha podría variar dependiendo la velocidad en la que se minen los bloques.

Se analizarán las rentabilidades que ha tenido el activo desde el día en el que se redujo la recompensa hasta su mínimo y máximo (no histórico) en cada ciclo, analizaremos también la cantidad de días que tarda en alcanzar estas rentabilidades. Se ha comentado anteriormente que cada ciclo dura aproximadamente 4 años, donde se analizan tres escenarios (o fases): escenario de recuperación donde

el precio se recupera y se mantiene, escenario bajista conducido por miedo del inversor y liquidación de beneficios y otro alcista por el "FOMO"[10]"y el aumento de demanda. Para ello utilizaremos la web de Tradingview[11] para poder realizar un análisis a nivel técnico.

Quiero enfatizar en que empezamos el análisis desde el 2012 como primer ciclo, y es que desde que el precio salió a cotización y desde que se empezó a minar los bloques entraba en juego una mínima dificultad del *hash,* por lo que se llegó mucho antes a los 210.000 bloques que los 4 años que suele durar. Esta fase la comentaremos como la fase inicial previa a los ciclos, aunque en esta también se podrán apreciar fase alcista y bajista.

A continuación, pasaremos a analizar los *halvings* que han ocurrido hasta hoy, cada uno contiene tres fases, la fase alcista, fase bajista y fase de recuperación, cada *halving* enlaza la fase de recuperación con la fase alcista para seguir el ciclo económico.

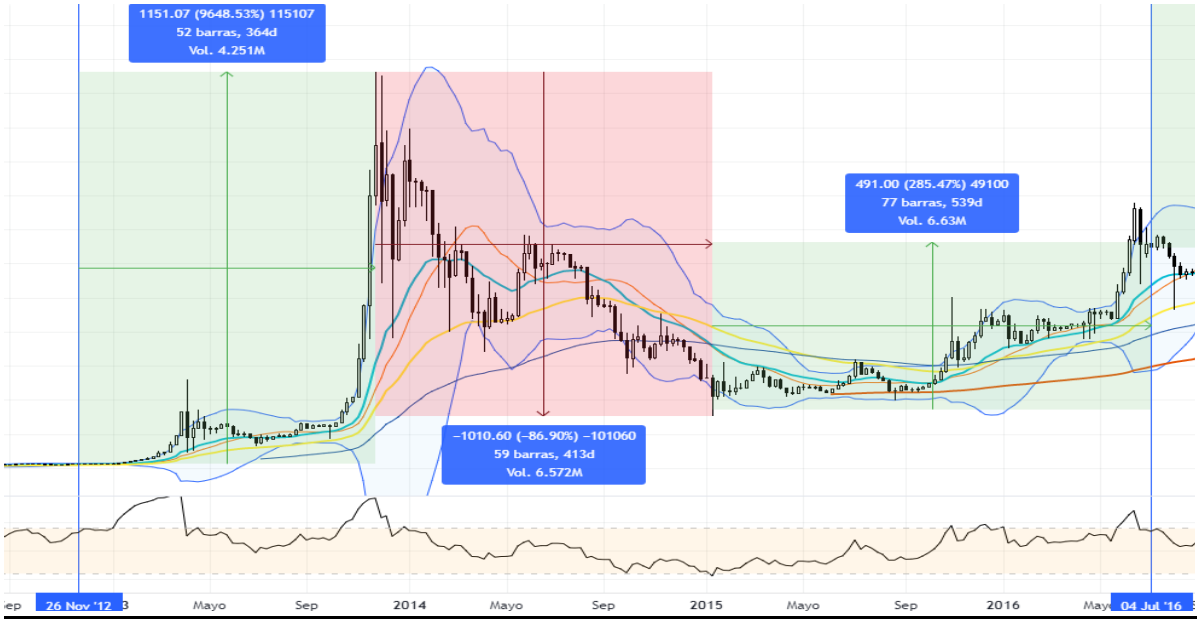
3.1. PRIMER HALVING

Analizando el primer *halving*, podemos observar que, desde los máximos anteriores, el día del primer *halving* el Bitcoin desciende apenas un 26,8% y cierra a $12,22. A partir de ese momento empieza un rally alcista en el que la moneda llega a alcanzar los $1.163 el 30 de noviembre del 2013, esto supone un increíble aumento del 9.648,53%. Este rally ascendiente dura exactamente 367 días. Sin embargo, es necesario notar que dentro de este ciclo alcista se pueden observar grandes caídas. En concreto del 10 al 17 de abril del 2013, el Bitcoin cae un 73,79%, del 25 de abril al 5 de julio del 2013, cae un 57,83%, el 2 de octubre cae un 33,49%, el 25 de octubre cae otro 24,39%, el 10 de noviembre desciende un 22,34%, y el 19 de noviembre, un 43,5%. Estas correcciones no son apreciables en el gráfico de la imagen 3 porque el gráfico es de velas semanales para poder apreciar mejor los movimientos.

He de recalcar que estos descensos agresivos en el precio son debido a las capitulaciones de los mineros. Las capitulaciones se generan cuando los mineros deciden vender gran parte de las reservas de sus Bitcoins para así poder financiarse, pagar facturas (principalmente la de la luz) y/o por consideración de una buena oportunidad de ganancia.

[10] *Fear Of Mising Out* es la sensación de que uno no está al tanto o se está perdiendo información, eventos, experiencias o decisiones de vida que podrían mejorar su vida.
[11] TradingView es un servicio web y red social para *traders*, con una plataforma para el análisis técnico. El sitio fue lanzado en septiembre de 2011.

Imagen 5. Gráfico semanal de BTC/DLR 2012-2026



Fuente: Tradingview (2022)

El rally alcista termina con la caída del 1 de diciembre de 2013donde se produjo un descenso del 28,93%. En este momento empieza la fase bajista, donde en 413 días, el valor del Bitcoin llega a caer un 86,9% llegando hasta los $152.4. Al igual que en la etapa anterior, dentro de esta segundafase, de carácter bajista, también podemos observar varias correcciones alcistas del mercado. Pasado el precio mínimo de caída dentro de esta fase, vemos que empieza una pequeña fase lateral seguida de la recuperación antes del segundo *halving*. Esta tercera fase representa un crecimiento del precio de la moneda desde los mínimos comentados anteriormente del 285,47% y dura un total de 539 días.

3.2. SEGUNDO HALVING

En este segundo ciclo se observa una clara repetición de las tres fases con respecto al ciclo anterior, pero con una subida porcentual menos agresiva. Comenzando el segundo *halving* con un precio de cierre de $647.78, entramos en la primera fase, la fase alcista, que viene seguida de la primera caída de 31,53% (desde los máximos dentro del segundo ciclo). Además de esta caída, la criptomoneda sufre 5 correcciones de más del 30% (33,58%, 33,98%, 32,97%, 38,59% y 39,61%) entre enero de 2017 y diciembre del 2017. La duración de este escenario alcista es de 525 días con un aumento del precio de 2.935,91% que permite alcanzar nuevos máximos con un precio de $19.666.

Imagen 6. Gráfico semanal de BTC/DLR 2016-2020

Fuente: Tradingview (2022)

El 17 de diciembre nada más alcanzar máximos se da comienzo a la segunda fase del ciclo, la fase bajista con un descenso del 43,25% en los siguientes 6 días. Esta fase duraría 364 días con una pérdida máxima dentro del segundo ciclo del 83,84% del valor. Asimismo, a la vez que, en la primera fase, la fase alcista, también apreciamos correcciones, pero en este caso alcistas, aunque nos centramos en estas correcciones alcistas, hay que destacar una subida del 98,96% en febrero del 18 y le seguirán dos correcciones de un aumento del 53% y 46% en los meses siguientes. Esta fase finaliza el 15 de diciembre de 2018 con un precio de $3.122,28.

La última fase de este ciclo es la de recuperación, se puede ver que tuvo una gran caída debido a la alta correlación con el S&P500 y el efecto del Covid-19. La fase de recuperación muestra una clara lateralidad, aunque debemos destacar un aumento en la criptomoneda de 204% dentro de un horizonte temporal de 512 días, el precio de cierre del tercer *halving* y el fin del segundo ciclo se cierra con el precio de $8.825,46 el 11 de mayo de 2020.

3.3 TERCER HALVING

Actualmente nos encontramos en el tercer *halving*, se debe tener en cuenta que en este caso la fase bajista todavía no se ha cerrado según las estimaciones. Comenzando con el precio de cierre del *halving* de $8.825.46 se empieza la fase alcista, se aprecian 5 caídas o correcciones de más del 20% desde nuevos máximos. Desde agosto del 2020 hasta julio del 2021 podemos ver caídas del 20,38%, 31,43%, 26.28, 54,86% y 25,27% antes de los máximos históricos de 69.000 dólares el 10 de noviembre

del 2021. Durante los 548 días que duro la fase alcista se obtuvo una rentabilidad, desde el inicio del tercer *halving*, del 704,95%.

Imagen 7 Gráfico semanal de BTC/DLR 2020-2024

Fuente: Tradingview (2022)

Desde ese mismo momento empieza la segunda y actual fase bajista, donde a 14 de mayo de 2022 llevamos una devaluación en el precio del 63,19% con una duración de 183 días actualmente.

3.4 ANÁLISIS MACROECONÓMICO

Actualmente nos encontramos en un momento de inestabilidad económica y de estanflación. Con el parón mundial del Covid-19 y la gran inyección de liquidez por parte de todos los bancos centrales, principalmente la FED y el BCE. Fue la mayor emisión de deuda mundial desde la segunda guerra mundial. Esto provocó a corto plazo una recuperación económica rápida y eficaz, sin embargo, estas políticas monetarias tienen un efecto negativo a largo plazo como es el de la inflación que estamos viviendo. Con la mayor inflación desde hace décadas en las economías de los países y después de años con los tipos de interés en 0%, los bancos centrales se encuentran en la situación de subir los tipos como ya ha hecho la FED hasta el 1% actualmente. El poco crecimiento actual y esperado de la economía, la alta inflación y la gran subida de tipos esperada van a generar una crisis económica de gran tamaño según apuntaba la secretaria del Tesoro, Janet Yellen, en una entrevista con la CNN "enormes repercusiones económicas para el mundo".

Aumentando el precio de la financiación y sin una aparente subida de salarios, se verá reducido en gran parte el poder adquisitivo y por lo tanto el consumo tanto de familias y empresas, provocando así

un decrecimiento económico, que pasará a recesión y finalmente a crisis. Las bolsas estadounidenses han descendido desde sus máximos históricos casi un 30%, sin embargo, la divisa estadounidense, el dólar, se ha apreciado con respecto a los grandes pares mundiales. Por ejemplo, el par euro/dólar está en 0.96 aproximadamente con altas probabilidades de que lleguen al mismo valor. La mala gestión del BCE relativa a la crisis del Covid-19 y la actual guerra en Ucrania está generando una apreciación del dólar, sin embargo, la inflación es prácticamente la misma tanto en EE. UU. como en Europa.

Imagen 8 Gráfico de la devaluación del dólar como divisa mundial entre 1913 y 2013

Fuente: Resiliencegroup

En la imagen 8 se puede observar el gráfico de la devaluación del dólar, la actual divisa mundial, el cual ha perdido prácticamente la totalidad de su valor. La inflación y las políticas monetarias no han ayudado, con la emisión de deuda nueva el dólar ha ido perdiendo valor continuamente desde que se creó la reserva federal de los Estados Unidos. Se podría hacer predicciones acerca del fin del dólar como divisa mundial si tenemos en cuenta la historia del dinero, siendo que antes del dólar había otras divisas como líderes económicos que han ido desapareciendo, siendo sustituidas por otras más novedosas y poderosas. El conocido inversor Jim Rogers, cofundador del fondo Quantum con el multimillonario George Soros, dijo en una entrevista reciente con Economic Times lo siguiente: "lo que está ocurriendo ahora con el dólar es el fin del dólar estadounidense, porque se supone que una moneda internacional debe ser neutral, pero en Washington están cambiando las reglas. Ahora, si no le gustas a Washington, te ponen sanciones y no puedes usar dólares estadounidenses".

El BCE ha propuesto la emisión de un Euro digital, que básicamente funcionaría como una

stablecoin[12], sin embargo, la inversión en seguridad y creación del euro digital sería bastante grande y estaría regido por un gobierno central, el cual seguirá los pasos que ha ido siguiendo, emitiendo más y más deuda. Algo parecido pasará con el dólar digital, el cual está siendo llevado a cabo por la FED. Las emisiones de estas monedas digitales incrementarían la demanda en el mercado de las criptomonedas ya que asociará el dinero físico y tradicional que se conocen con la tecnología que hay detrás de las criptomonedas

En los mercados de criptomonedas, la *stablecoin* más utilizada es Theter, la cual replica el dólar de manera constante con mínimas fluctuaciones, el algoritmo proporciona seguridad y opera en las *blockchain* de Ethereum, EOS, Tron, Algorand, y OMG[13]. Por lo que esta *stablecoin* podría sustituir las decisiones de un banco central llevándolas a una zona fuera de la política.

Además del momento económico actual hay que tener en cuenta los nuevos proyectos que se están creando como el metaverso[14]. Un lugar digital en el cual pueden hacerse todo tipo de actividades, ya sean de ocio como de negocios, desde una reunión de empresa, inversión inmobiliaria y hasta videojuegos, la lista es infinita. Para todos estos proyectos una moneda digital, token o criptomoneda es necesaria. Según un informe de Bloomberg Intelligence, el metaverso en 2021 estaba valorado en 500.000 millones de dólares americanos y se estima que esta cifra pueda multiplicarse por cinco en el 2030. Una alta demanda por del metaverso es bastante probable, esto resultará en mayor demanda de las criptomonedas.

Como comparación con el entorno bursátil y dato relevante, el valor de mercado de todas las criptomonedas alcanzo el valor máximo de 2,839 trillones de dólares el mismo día que se alcanzaron los máximos de Bitcoin y esperamos que este sea mucho mayor en la siguiente fase alcista, llegando a superar solo el valor de mercado de Bitcoin a las grandes compañías como Apple, Meta, Google y Amazon.

Últimamente se habla acerca de la correlación entre el S&P500 y el Bitcoin*,* esto podría conllevar un riesgo al Bitcoin ya que se supone que es un tipo de activo totalmente diferente al índice americano.

[12] Las stablecoins son criptomonedas cuyo valor está vinculado al de otra moneda, producto básico o instrumento financiero. Las stablecoins tienen como objetivo proporcionar una alternativa a la alta volatilidad de las criptomonedas más populares.
[13] Ethereum, EOS, Tron, Algorand, y OMG son distintas redes autónomas, descentralizadas y basadas en la red *blockchain*. Estos sistemas son seguros, escalables y eficientes; todas estas son cualidades importantes para brindar aplicaciones efectivas en el mundo real.
[14] El metaverso es una realidad digital que combina aspectos de las redes sociales, los juegos en línea, la realidad aumentada (AR), la realidad virtual (VR) y las criptomonedas para permitir a los usuarios interactuar virtualmente. La realidad aumentada superpone elementos visuales, sonido y otras entradas sensoriales en configuraciones del mundo real para mejorar la experiencia del usuario. En contraste, la realidad virtual es completamente virtual y mejora las realidades ficticias.

Analizando los datos históricos semanales desde la primera cotización del Bitcoin hasta el 8 de mayo de 2022 junto con los del S&P500 en el mismo rango de fechas, obtenemos la siguiente tabla:

Imagen 9. Tabla de la Beta del Bitcoin respecto al S&P 500

	PREVIO	1 CICLO		2 CICLO		3 CICLO		FUTURO
	FASE BAJIS	FASE ALCIS	FASE BAJIS	FASE ALCIS	FASE BAJIS	FASE ALCIS	FASE BAJIS	FASE ALCIS
BETA	X	0,30627234	0,071856684	0,46329448	1,417117041	0,2814	1,938525809	X

Fuente: Elaboración propia

La fase alcista se compone de la fase alcista más la fase anterior de lateralidad o recuperación, es decir, en la fase alcista del primer ciclo hemos analizado los datos de la fase alcista más los anteriores a noviembre de 2012 que pertenecen a una fase de recuperación como se puede apreciar en la imagen 9 Por lo tanto, todas las fases alcistas de sus respectivos ciclos contienen además de la fase alcista, la fase de recuperación o lateral de su ciclo anterior. Las Xs muestran inexactitud en datos y falta de estos.

Analizando la tabla podemos llegar a ver un posible patrón en el que las fases alcistas no están apenas correlacionadas con el S&P500 ya que su beta tiene unos valores mínimos de: 0,31, 0,46 y 0,28. Es el caso contrario en las fases bajistas, donde obtenemos un dato que sigue una tendencia al alza hacia la correlación con datos de: 0,07, 1,42 y 1,94. En general, sí que se puede decir que en las fases bajistas el Bitcoin está correlacionado de manera agresiva mientras que en las alcistas no esta tan correlacionado. Se aborda que el Bitcoin se ha ido correlacionado con el índice americano debido a la entrada de inversores institucionales o grandes inversores también llamados “ballenas”, como esta criptomoneda se ha ido haciendo famosa a lo largo del paso del tiempo, la entrada de estos inversores ha generado que sigua el comportamiento del mercado americano.

Con la futura entrada de más inversores institucionales, debido a su gran aumento en el precio y a el aprendizaje del funcionamiento de esta tecnología, generará un incremento las inversiones a largo plazo, mientras que habrá un flujo salidas y entradas cíclico por parte los inversores *retail* por el miedo en las fases bajitas y por el FOMO en las alcistas. Con los datos analizados y las expectativas del mercado podemos decir que se generará a futuro una correlación con el índice cada vez más fuerte. Por lo que cualquier noticia o dato que afecte a cualquiera de estos, afectará al otro de manera indirecta.

3.5. ANÁLISIS DE SENTIMIENTO

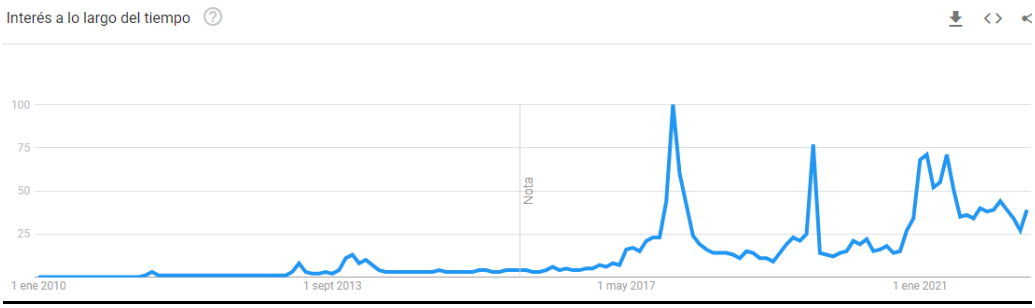
Conforme al análisis de búsquedas de la palabra Bitcoin en google podemos ver que la popularidad del activo va correlacionada prácticamente con una beta de 1 con el precio del activo. Se

puede ver que el momento de más visibilidad del activo fue gracias a la fase alcista del año 2017, este fue un año muy volatil para el activo debido al factor aprendizaje y el descubrimiento del activo.

Hay que tener en cuenta que debido a un aumento en los usuarios en el ámbito de las criptomonedas cada vez veremos un menor repunte en la gráfica, sin embargo, se podrán apreciar aumentos por caidas repentinas del activo.

Por lo tanto un aplanamiento en la gráfica nos indicará que podríamos estar en la fase lateral y un aumento de las busquedas nos indicará el inicio de de la fase alcista.

Imagen 10. Búsquedas de la palabra Bitcoin



Fuente: Google Trends

4.PROPUESTA DE INVERSIÓN

La finalidad es la de intentar obtener un precio de compra óptimo dentro de la fase bajista del ciclo actual mediante los análisis realizados en los puntos anteriores. Para esta propuesta se valoran tanto los días medios de las respectivas fases bajistas y alcistas además de distintos factores.

Se puede concluir con los análisis que, efectivamente el Bitcoin se mueve por ciclos y a su vez, esos ciclos se dividen en 3 fases, es imposible predecir el precio mínimo al que se podrá comprar ya que al ser tan volátil cualquier mala noticia puede hacer que llegue a nuestro precio objetivo. En este preciso caso nos centraremos en el periodo de días que este permanece en cada fase.

Se procede a crear una predicción por rango de días, esta consiste básicamente analizar el número de días que ha durado cada fase y se utilizarán varias fórmulas para intentar conseguir un precio de entrada bajo.

Imagen 11. Tabla de días de las fases

	ALCISTA	BAJISTA	RECUPERACIÓN
1	364	413	539
2	525	364	518
3	548	ACTUAL	X
PROMEDIO	479	388,5	528,5
PROM DIF	91,5	-49	-21
DIAS DIF	639,5	315	497
PREVISTO	657,829531	315	497
MEDIA TOTAL	592,109844	339,5	507,5

Fuente: Elaboración propia

Usamos tres fórmulas, el valor promedio de cada fase, la diferencia promedio entre ciclos de las fases y la fórmula para predecir de Excel. Como se puede ver se han obtenido datos muy diferentes con cada formula, hay que destacar un importante sesgo que afecta al estudio, y es que la muestra es muy pequeña. En el caso de la fase bajista y la recuperación solo tenemos dos muestras y es que no podemos analizar el ciclo previo al 1 ya que fue el de su creación y la dificultad del *hash* era mínima por lo cual el minado de bloque fue mucho mayor y se tardó un periodo menor en conseguir los 210.000 bloques.

Siguiendo el modelo de valoración por múltiplos en campo de las *M&A* y teniendo en cuenta el sesgo, llegamos a la predicción de que la fase alcista durará entorno a los 592 días, la fase bajista alrededor de los 340 días y la fase de recuperación 508 días.

Considerando los porcentajes de fluctuación de las fases vemos que la fase de recuperación y la bajista oscilan en la misma variación, subiendo la bajista -86,90% y -83,84% y la de recuperación de

285,47% y 204,12% en cada ciclo consecutivamente. En cambio, la fase alcista sufre reducciones en la variación de más de la mitad, ya que pasa de los 9648,53% en el primer ciclo a los 2935,91% para posteriormente acabar en un aumento de 704,95% en el tercer ciclo. Por lo que podríamos predecir la variación de precios en la fase bajista y de recuperación ya que oscilarán en torno a los mismos datos. La fase alcista dependerá del entorno macroeconómico y geopolítico en el que nos encontremos en mayo del 2024, considerando sobre todo la beta del Bitcoin ya que se podría encontrar una fuerte correlación a futuro. El precio alcista dependerá en parte del S&P500 y el inversor *retail*.

Con estos datos y teniendo en cuenta el aumento en el volumen de inversores institucionales, podemos especular e intentar predecir que caerá alrededor de un 80% hasta los mínimos máximos de la fase bajista sobre el mes de septiembre y octubre. Un buen rango de precios para entrar sería el de $13.000 y $18.000. Podemos considerar también inversiones periódicas a partir de septiembre hasta meses previos al *halving* de 2024.

Esta se trataría de una inversión en el muy largo plazo, hablamos de más de diez años y su principal función sería de la tesorería, pudiendo utilizarse para la digitalización que se comentará más adelante. En los últimos 12 años el Bitcoin ha obtenido una rentabilidad semanal promedio del 3,31% con una desviación típica del 0,1757, que comparándolo con el S&P500, ha obtenido una rentabilidad semanal media de 0,24% con una desviación típica de 0,02201. Se obtiene una mayor rentabilidad con el Bitcoin debido al *trade-off* entre la rentabilidad y el riesgo.

Imagen *12*. Tabla predictiva del precio y días del Bitcoin

Fuente: Elaboración propia

Las extremas fluctuaciones que ha sufrido el precio del activo no se repetirán en el futuro, lo que veremos será una línea logarítmica en la que el precio se mantendrá estable sin apenas fluctuaciones o muy poco volátiles (ver imagen 3). Por lo tanto, un buen precio de entrada generará una mayor rentabilidad a largo plazo.

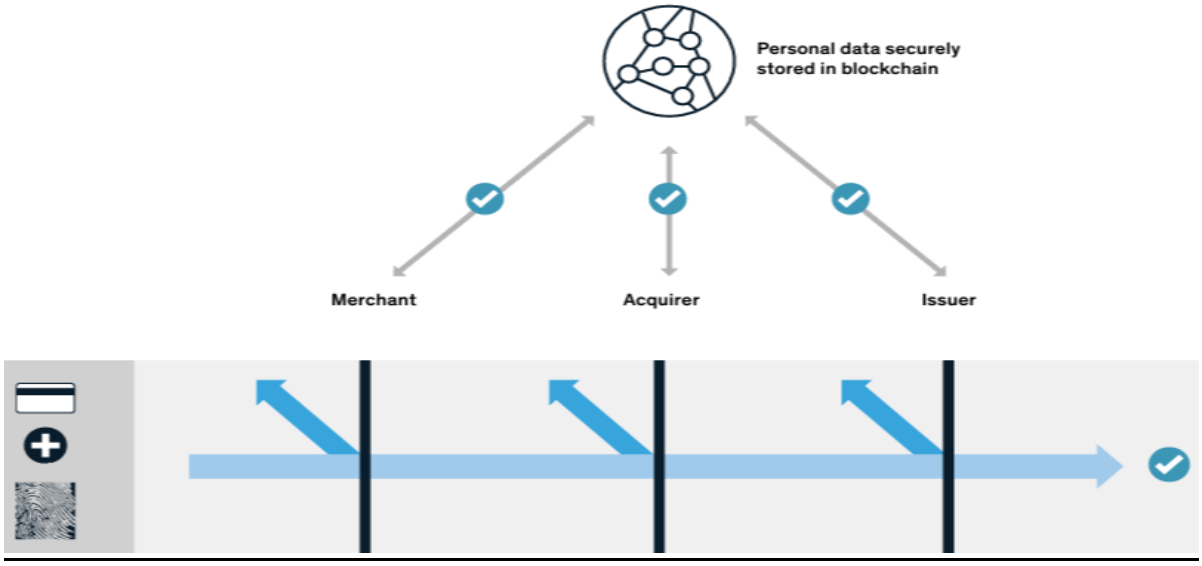
A corto plazo se puede esperar una rentabilidad estimada de entorno al 201%, obtenemos este resultado fijándonos en la media de las rentabilidades en estos periodos, y se ha estimado una rentabilidad con una estimación lineal de en torno a 250% para la fase alcista de 2024. Gracias al análisis se puede obtener un precio esperado entre $51.170 y $69.230 entre los meses de diciembre de 2023 y enero de 2024 y de entre $179.000 y $242.000 entre los meses de septiembre y octubre del 2025. Estimamos que en cada fase alcista la rentabilidad se reducirá la mitad e incluso más, aplanando la curva de rentabilidad hasta llegar a una lateralidad absoluta.

5.APLICACIONES DEL *BLOCKCHAIN*

5.1. ENTORNO MACRO RELACIONADO CON LA TECNOLOGÍA *BLOCKCHAIN*

Recientemente, tanto instituciones internacionales como países han estado mostrando un gran interés hacia esta disruptiva tecnología. Dentro de estas se puede destacar instituciones como el Fondo Monetario Internacional o Naciones Unidas, países desarrollados como Estados Unidos, Reino Unido y Japón están desarrollando aplicaciones con esta tecnología para aplicar a diferentes campos. Por otro lado, en febrero del 2016, el gobernador del *People's Bank of China*, Zhou Xiaochuan comentó la posibilidad de introducir una *blockchain* dentro de los sistemas financieros, más tarde y después de una gran inversión de recursos se publicó el *paper "Chinese Blockchain Technology and Application Development White Paper (2016)",* el cual trata temas de las posibles aplicaciones de la blockchain dentro de los sistemas financieros como el proceso de pago donde ambas partes acuerdan precios, fecha y facilitan su identidad para verificar el pago sin necesidad de terceros.

Imagen 13. Gráfica de la aplicación de la *blockchain* como sistema de *payment clearance.*



Fuente*: McKinsey*

Pero esto no es solo iniciativa de China, los mayores bancos de inversión del mundo ya han empezado a desarrollar aplicaciones con esta tecnología e incluso cuentan con laboratorios propios para desarrollarlas, es el caso de Goldman Sachs, J.P. Morgan y UBS entre otros muchos. E incluso Goldman Sachs publicó una patente para la verificación de las contrapartes de cada transacción basada en la red de *blockchain*. La aplicación de esta tecnología se está desarrollando principalmente por empresas norteamericanas, otros casosde aplicaciones son el de *Nasdaq Stock Market* y el *New York Stock*

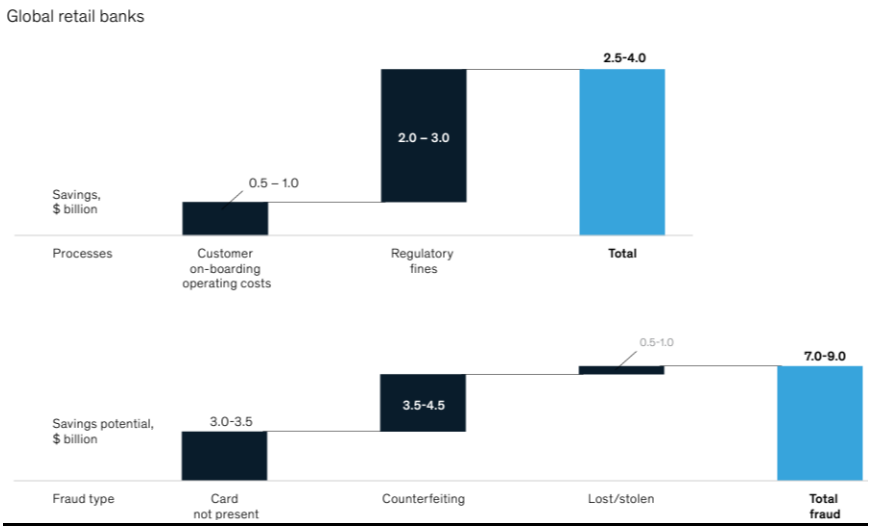
Exchange donde realizaron la primera transacción de *securities* a través de la red de *blockchain*.

Según un estudio publicado por la empresa McKinsey en el entorno global las transacciones internacionales suman la cantidad de 600 mil millones de dólares anuales (usamos dólar como la divisa de cambio más usada) y se estima un crecimiento de entorno al 3% anual. Este tipo de transacciones suelen ser opacas y lentas. Las comisiones además suelen estar en una media entre en 2 y el 3 por ciento.

El gran aumento de *fintechs* en los últimos años ha generado un aumento de la competencia en este sector y han generado una perdida en el volumen de las operaciones, ya que donde una transferencia normal entre entidades (sin tener que pagar comisiones) tardaba mucho tiempo, incluso días, estas transferían el dinero de manera inmediata tardando segundos.

Para que una transferencia pueda tardar segundos o minutos, esta tendría que realizarse a través de una criptomoneda y no a través de dinero fíat, por lo que este ahorro solo podría obtenerse si los bancos operasen con criptomonedas y no con dinero fíat, por lo que no haría falta un organismo central que regulase estas transacciones, ya que estas se regularían mediante la red de *blockchain* y las contrapartes del acuerdo. Aplicando esta tecnología se aumentaría la eficiencia y la transparencia, debido a que los datos en una *blockchain* no se pueden alterar, además de que disminuiría el riego. Según McKinsey la aplicación de la *blockchain* a las transferencias internacionales podría ahorrar en torno a 4 mil millones de dólares anuales.

Imagen 14. Ahorro estimado gracias a el uso de la red *blockchain.*



Fuente McKinsey

El gráfico superior representa el ahorro estimado debido a la reducción de costes para el usuario debido a la red y el aumento de seguridad y verificación de datos que mejoraría la prevención y

blanqueo de capitales, por lo que, al mejorar la seguridad, evitamos las perdidas por multas y sanciones emitidas por el organismo regulador, en este caso los bancos centrales y gobiernos.

5.2. PROPUESTA DE APLICACIONES *BLOCKCHAIN*

La propuesta es la de la creación de una *blockchain* privada con el simple objetivo de maximizar la eficiencia y rapidez no solo en las transacciones tanto nacionales como internacionales si no en disminuir el tiempo de análisis y aumentar la veracidad de los documentos.

Una red privada proporcionará una mayor fluidez de entre deudores y acreedores y una disminución en el proceso gracias al sencillo, rápido y eficiente proceso de verificación de documentos, estos serán los documentos oficiales que las empresas presentan a los organismos oficiales y las propias empresas serán las partícipes de la red *blockchain*. Las empresas tendrán su propio acceso al igual que lo tienen en su banca digital. Sin embargo, el acceso será limitado por la entidad la cual será la que contará con todos los documentos y transacciones de las empresas.

La información de los deudores permanece en la red del emisor de la deuda mediante una versión encriptada, esta será actualizada y renovada a lo largo de la red, gracias a las interacciones que se producen. Solo el emisor de la deuda en este caso la entidad tendrá acceso a todo el contenido de la *blockchain*, mientras que los demás usuarios de la *blockchain* tendrán un acceso restringido.

Una reducción en el tiempo, aumento de la transparencia generará una disminución en los departamentos de prevención de blanqueo de capitales y prevención del terrorismo, este ahorro será dedicado a la inversión en una *blockchain* privada y el mantenimiento de esta.

Dependiendo de la empresa los precios de la creación de una *blockchain* privada varían desde los $120.000 hasta los $500.000 en algunos casos y el mantenimiento de la propia red varia del 10% hasta el 25% del coste de desarrollo de la red. Otra solución sería la creación de un departamento con expertos en el campo del desarrollo de software, el salario anual bruto de estos va desde los 45.000€ hasta los 80.000€ en España. Decantándonos por el proceso de subcontratar a una empresa que preste sus servicios de desarrollo y mantenimiento de la red privada. Subcontratando los servicios tendríamos un gasto esperado de media de $310.000, con un coste anual de mantenimiento de entre el 10% y el 25% por lo tanto gastaríamos anualmente en torno a $31.000 y $77.500 anuales. Sin embargo, los ahorros y el aumento de productividad harán que la entidad genere beneficios.

6. CONCLUSIONES

Se ha visto que los datos macroeconómicos nos indican un claro ajuste del sistema bancario, tecnologías como la *blockchain* han llegado para quedarse y tienen infinidades de aplicaciones. El Bitcoin es un ejemplo del uso de esta tecnología, gracias a sus algoritmos, es la criptomoneda más segura y deflacionaria, lo que la hace perfecta como una inversión inicial para introducirnos dentro de esta tecnología.

Se ha analizado el comportamiento de la moneda desde que apareció en 2009, desde entonces su valor se ha revalorizado desde céntimos de euro hasta un precio a fecha de 5 de junio de 2022 de 29.700 dólares. Siguiendo una tendencia logarítmica el precio de esta criptomoneda se estabilizará cada vez más cuando se vaya acercando a la máxima cantidad de Bitcoin minados.

Por lo que un precio de entrada nos generará una mayor rentabilidad, se ha analizado un precio de entrada entre los $13.000 y $17.000, se obtendrá una rentabilidad esperada en el corto plazo del 201%, llegando a un precio esperado entre $51.170 y $69.230 entre los meses de diciembre de 2023 y enero de 2024. El precio en el largo plazo podría variar debido a la adopción de países subdesarrollados como su divisa, aun así, se ha estimado que superará su antiguo precio máximo llegando a superar por dos e incluso por tres dependiendo de la situación económica global a lo largo del 2024.

Por otro lado, el desarrollo de una red privada de *blockchain* mejoraría la transparencia de la información como la veracidad de esta, reduciendo el coste de análisis y minimizando el tiempo en la obtención de la información aumentaría la eficiencia de la entidad y por lo tanto lo haría la productividad y la rentabilidad. Además, obtendríamos un ahorro en el coste de las transacciones internacionales y obtendríamos el importe de la transacción en minutos, en vez de en horas o en días.

La tecnología involucrada en este tipo proyectos es muy novedosa y no ha sido desarrollada de manera comercial para los bancos, se han realizado pruebas y se han estimado resultados, pero todavía no se ha aplicado de manera global. Con este trabajo se busca introducir a la banca en el complejo mundo de las criptomonedas a través de inversión de parte de su tesorería en el Bitcoin y proponer la aplicación de una red interna privada de *blockchain*, los datos obtenidos en el trabajo son estimaciones y especulaciones ya que esta tecnología no se ha aplicado todavía y no podemos medir con exactitud el ahorro que esta podría conllevar.

7. BIBLIOGRAFÍA

Nakamoto, Satoshi (2009). "*Bitcoin: A Peer-tú-Peer Electronic Cash System Disponible"* Disponible en:
https://bitcoinwhitepaper.co/

Rodriguez, Nelson (03/12/2018) Historia de la *blockchain*, Publicado en 101blockchains.com. Disponible en:
https://101blockchains.com/es/historia-de-la-blockchain/

Biografía de los doctores en *computer science* Haber y Stornetta publicado por Immutable Record. Disponible en:
https://immutablerecord.com/the-co-inventors/

Miller, Charles (28/10/2021) "Stuart Haber and Scott Stornetta: How our timestamping mechanism was used in Bitcoin". Artículo y video entrevista (mp4) Publicado por CoinGeek. Disponible en:
https://coingeek.com/stuart-haber-and-scott-stornetta-how-our-timestamping-mechanism-was-used-in-bitcoin-video/

Página inicial de Microstrategy. Disponible en:
https://www.hope.com/

Stuart Haber y W.Scott Stornetta. (1990) "How to Time-Stamp a Digital Document" *White paper* introductorio de la Blockchain. Disponible en:
https://link.springer.com/content/pdf/10.1007%2F3-540-38424-3_32.pdf

"Bitcoin History" publicado por el blog BitcoinWiki. Disponible en:
https://en.bitcoinwiki.org/wiki/Bitcoin_history

Memoria, Francisco (07/10/2021) "*The First Bitcoin Transactions: From a Test to the Famous Pizza Purchase"*. Publicado por en CryptoCompare. Disponible en:
https://www.cryptocompare.com/coins/guides/the-first-bitcoin-transactions-from-a-test-to-the-famous-pizza-purchase-1/

Gobierno del Salvador (09/06/2021). Ley Bitcoin, con número de decreto 57 en el diario 11, tomo 431. Disponible en:
https://www.asamblea.gob.sv/leyes-y-decretos/resultado-busqueda/bitcoin

"What is Double Spending & How Does Bitcoin Handle It?" (17/04/2022) Publicado por la página web Coinsutra.com. Disponible en:
https://coinsutra.com/bitcoin-double-spending/

*"Bitcoin Average Block Siz*e" (actualidad diaria) Publicado por la empresa YCHARTS, Disponible en:
https://ycharts.com/indicators/bitcoin_average_block_size

Conway, Luke (29/11/2021) *"Bitcoin Halving"*. Disponible en:
https://www.investopedia.com/bitcoin-halving-4843769

Hay, Steven (25/02/2020) "*Bitcoin (BTC) Halving History With Charts & Dates*" Publicado en el blog CoinMama el. Disponible en:
https://www.coinmama.com/blog/the-bitcoin-halving-a-history/

Fechas del Bitcoin e información histórica, publicado en la página web HalvingDates.com. Disponible en:
https://halvingdates.com/crypto.php?sym=btc&name=Bitcoin

Cantidad real y actualizada de Bitcoin minados y circulando, publicado por la página web BuyBitcoinWorldwide.com. Disponible en:
https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there/

Azmaan Onies, Giancarlo Daniele y Tunmise Olayinka (2010-2011) Limitaciones de Publicado en un blog de la Universidad de Standford. Disponible en:
https://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/DigitalCurrencies/disadvantages/index.html

Tuwiner, Jordan (16/01/2022) "US Dollar Devaluation Since 1913" Publicado por la página web

BuyBitcoinWorldwide.com. Disponible en:
https://www.buybitcoinworldwide.com/dollar-devaluation/

Información histórica del Bitcoin diaria y semanal publicado por la página web Investing.com. Disponible en:
https://es.investing.com/crypto/bitcoin/historical-data

Capitulación de mineros, publicado por la página web BuyBitcoinWorldwide.com. Disponible en:
https://stats.buybitcoinworldwide.com/miner-capitulation/

Inflación del dólar (gráfica), publicado por la página web BuyBitcoinWorldwide.com. Disponible en:
https://www.buybitcoinworldwide.com/img/dollar-inflation-chart.png

Imagen de la pérdida de valor del dólar. Disponible en:
https://thumbnails-visually.netdna-ssl.com/purchasing-power-of-the-us-dollar-1913-to-2013_517962b78ea3c_w1500.jpg

Banco Central Europeo (2022) *"A digital euro"*. Disponible en:
https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html

"Report on a digital euro" Emitido por el Banco Central Europeo. Disponible en:
https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

"Blockchain application and outlook in the banking industry" Redactado por Ye Guo y Chen Liang y publicado el 09/12/2016 en Springer Link. Disponible en:
https://link.springer.com/article/10.1186/s40854-016-0034-9

Natalia Dashkevich, Steve Counsell y Giuseppe Destefanis (27/07/2020) *"Blockchain Application for Central Banks: A Systematic Mapping Study"* Publicado en la web IEEE. Disponible en:
https://ieeexplore.ieee.org/abstract/document/9149861

Matt Higginson, Atakan Hilal, y Erman Yugac (07/06/2019) *"Blockchain and retail banking: Making*

the connection" Publicado por la compañía Mckinsey. Disponible en:
https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-and-retail-banking-making-the-connection

Extensión en PDF del artículo anterior.
Chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Blockchain%20and%20retail%20banking%20Making%20the%20connection/Blockchain-and-retail-banking.pdf

Fadilpašić, Sead (07/06/2019) *"McKinsey Finds Three Blockchain Use Cases in Retail Banking"* Publicado por la web Cryptonews. Disponible en:
https://cryptonews.com/news/mckinsey-finds-three-blockchain-use-cases-in-retail-banking-4010.htm

David L. Portilla, David J. Kappos, Minh Van Ngo, Sasha Rosenthal-Larrea, John D. Buretta y Christopher K. Fargo, Cravath, Swaine & Moore LLP (28/01/2022) *"Blockchain in the Banking Sector: A Review of the Landscape and Opportunities"* y publicado por la Universidad de Harvard. Disponible en:
https://corpgov.law.harvard.edu/2022/01/28/blockchain-in-the-banking-sector-a-review-of-the-landscape-and-opportunities/

Daley, Sam (09/06/2022) "*50 Blockchain Companies Paving the Way for the Future*". Publicado el en la web Builtin.com. Disponible en:
https://builtin.com/blockchain/blockchain-companies-roundup

Las 10 mejores empresas de blockchain. Publicado el 19/05/2022 en la web Software Testing Help. Disponible en:
https://www.softwaretestinghelp.com/blockchain-companies/

Salario de un desarrollador de blockchain en España. Publicado el 24/02/2022 por la web Keep Coding. Disponible en:
https://keepcoding.io/blog/cuanto-gana-un-desarrollador-en-espana/