Facultad de Ciencias Económicas

Búsqueda de una alternativa al modelo *Stock-to-Flow* para predecir el valor de Bitcoin.

Autor: José Sintes Tejedor

Director: María Eugenia Fabra Florit

MADRID | Junio 2023

ÍNDICE DE CONTENIDOS

ÍNDICE DE IMÁGENES

Resumen

Durante la década pasada, Bitcoin surgió y ha terminado por alcanzar niveles de valorar que obligan a reflexionar sobre si este activo puede llegar a marcar una disrupción en distintos aspectos de nuestra vida. El valor de Bitcoin puede estar basado en dos características peculiares: digital y escaso. Esta segunda característica es la que marca la génesis de este Trabajo de Fin de Grado.

La escasez de Bitcoin viene regulada en su código original que limita la emisión de este en un máximo de 21 millones. Además, el ritmo de producción de este queda limitada también en el propio código que establece unas medidas para facilitar o dificultar la producción según la demanda de trabajo de los mineros, manteniéndola así en unos niveles constantes.

El modelo *Stock-to-Flow* parte de esta premisa para su desarrollo, entiendo que el precio de bitcoin viene determinado por esta relación. Hasta noviembre de 2021, el acierto de este modelo en la predicción del valor de Bitcoin obtuvo unos altos niveles de precisión, consolidándose como una referencia dentro del mercado. Sin embargo, en esa fecha y con la llegada de Bitcoin a su mayor valor histórico, el modelo predijo una continuación en el ascenso del precio, pero la realidad es que lo que se ha producido es un desplome en su valor.

En este trabajo, se busca valorar si el fallo de este modelo se debe a un error en sus premisas fundamentales y buscar un nuevo modelo que pueda predecir de manera acertada el valor de Bitcoin.

Palabras calve

Bitcoin, modelo, *Stock-to-Flow*, regresión lineal, flujo, existencias, masa monetaria.

Abstract

During the past decade, Bitcoin was created and has reached levels of value that prompt reflection on whether this asset can disrupt various aspects of our lives or not. It´s value may be store in two peculiar characteristics: digital and scarce. It is the latter characteristic that forms the genesis of this thesis.

The scarcity of Bitcoin is regulated in its original code, which limits its issuance to a maximum of 21 million units. Furthermore, the rate of production is also constrained within the code, which establishes measures to ease or hinder production based on the miners' work demand, thereby maintaining it at constant levels.

The Stock-to-Flow model is based on this premise for its development, understanding that the price of Bitcoin is determined by its relationship with its scarcity. Until November 2021, this model achieved high levels of accuracy in predicting the value of Bitcoin, establishing itself as a reference in the market. However, at that time, with Bitcoin reaching its all-time high, the model predicted a continuation of the price increase, but what actually happened was a collapse in its value.

This study aims to assess whether the failure of this model is due to an error in its fundamental premises and to seek a new model that can accurately predict the value of Bitcoin.

Key Words

Bitcoin, Stock-to-Flow, model, linear regression, flow, stock, monetary supply.

1. CAPÍTULO I. INTRODUCCIÓN

1.1 ESTADO DE LA CUESTIÓN OBJETO DE INTERÉS.

En la última década, Bitcoin ha pasado de ser un programa informático de nueva creación prácticamente desconocido para el conjunto de la población a ser uno de los activos que más debate ha levantado dentro de la sociedad, así como uno de los que mejor rendimiento ha ofrecido en ese intervalo de tiempo.

Durante este tiempo, muchos medios de comunicación y algunos analistas como Peter Schiff (2022) han mostrado su rechazo este activo por diversos motivos: alta volatilidad y su carácter no regulable y antigubernamental entre otros. Es cierto, que la complejidad de su sistema, el desconocimiento de la población respecto de los sistemas informáticos y su intención de alterar el sistema de pagos internacional (Nakamoto, 2008) no han ayudado a que el recibimiento de Bitcoin haya sido más sencillo.

Sin embargo, ha habido otros expertos como Antanopoulos (2017), Saylor (2023) o Ammous (2016) que sí han observado que las propiedades de Bitcoin podrían aportar un valor diferencial al panorama económico internacional. Estas propiedades le permitiría alcanzar una cuota importante de la población, sobreponiéndose a las dificultades señaladas en el párrafo anterior. Este planteamiento ha provocado que el valor de Bitcoin creciese de manera exponencial durante la última década.

En esta tabla podemos observar el retorno anual ofrecido por alguno de los principales activos que cotizan en el mercado americano (las empresas de pequeña capitalización y alta capitalización, índices bursátiles, bonos, el oro o las materias primas) en el periodo comprendido entre 2011 y 2020. El rendimiento anual medio de Bitcoin durante este tiempo ha sido 9 veces superior al índice de NASDAQ 100, que es el que más se le acerca.

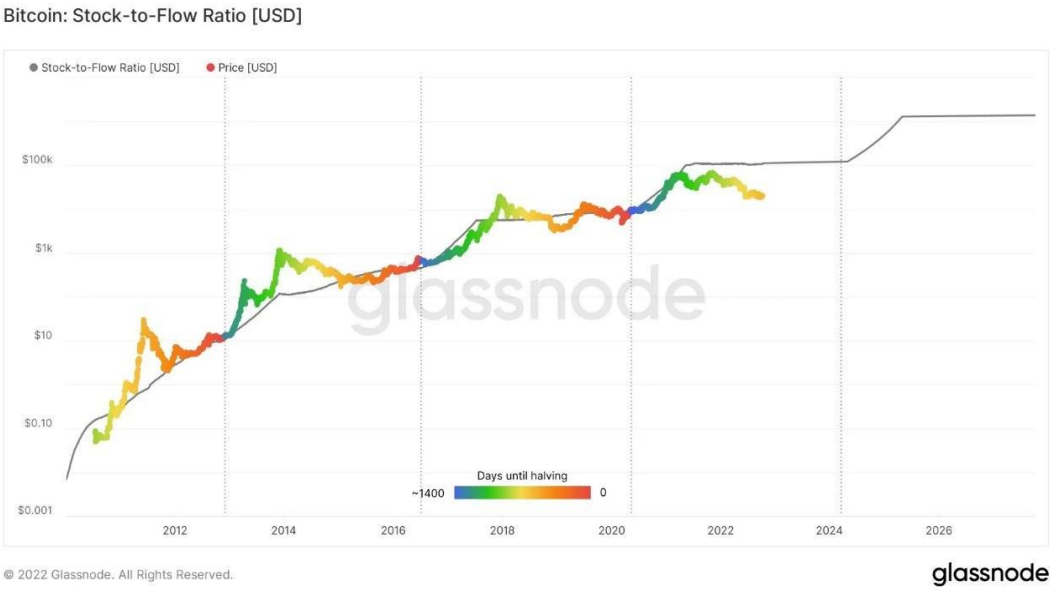
Imagen 1 Retorno de Bitcoin entre 2010 y 2020

		Asset Class Total Returns over Last 10 Years (as of 12/31/20)										Data Source: YCharts	
ETF	Asset Class	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2011-20 Cumulative	2011-20 Annualized
N/A	Bitcoin ($BTC)	1473%	186%	5507%	-58%	35%	125%	1331%	-73%	95%	301%	9591687%	214.9%
QQQ	US Nasdaq 100	3.4%	18.1%	36.6%	19.2%	9.5%	7.1%	32.7%	-0.1%	39.0%	48.6%	537.8%	20.4%
GLD	Gold	9.6%	6.6%	-28.3%	-2.2%	-10.7%	8.0%	12.8%	-1.9%	17.9%	24.8%	28.6%	2.5%
IWM	US Small Caps	-4.4%	16.7%	38.7%	5.0%	-4.5%	21.6%	14.6%	-11.1%	25.4%	20.0%	189.3%	11.2%
SPY	US Large Caps	1.9%	16.0%	32.2%	13.5%	1.2%	12.0%	21.7%	-4.5%	31.2%	18.4%	262.8%	13.8%
TLT	Long Duration Treasuries	34.0%	2.6%	-13.4%	27.3%	-1.8%	1.2%	9.2%	-1.6%	14.1%	18.2%	118.2%	8.1%
EEM	EM Stocks	-18.8%	19.1%	-3.7%	-3.9%	-16.2%	10.9%	37.3%	-15.3%	18.2%	17.0%	33.8%	3.0%
LQD	Investment Grade Bonds	9.7%	10.6%	-2.0%	8.2%	-1.3%	6.2%	7.1%	-3.8%	17.4%	11.0%	81.0%	6.1%
TIP	TIPS	13.3%	6.4%	-8.5%	3.6%	-1.8%	4.7%	2.9%	-1.4%	8.3%	10.8%	43.2%	3.7%
PFF	Preferred Stocks	-2.0%	17.8%	-1.0%	14.1%	4.3%	1.3%	8.1%	-4.7%	15.9%	7.9%	77.5%	5.9%
BND	US Total Bond Market	7.7%	3.9%	-2.1%	5.8%	0.6%	2.5%	3.6%	-0.1%	8.8%	7.7%	44.9%	3.8%
EFA	EAFE Stocks	-12.2%	18.8%	21.4%	-6.2%	-1.0%	1.4%	25.1%	-13.8%	22.0%	7.6%	68.6%	5.4%
EMB	EM Bonds (USD)	7.7%	16.9%	-7.8%	6.1%	1.0%	9.3%	10.3%	-5.5%	15.5%	5.4%	72.4%	5.6%
HYG	High Yield Bonds	6.8%	11.7%	5.8%	1.9%	-5.0%	13.4%	6.1%	-2.0%	14.1%	4.5%	71.4%	5.5%
BIL	US Cash	0.0%	0.0%	-0.1%	-0.1%	-0.1%	0.1%	0.7%	1.7%	2.2%	0.4%	4.8%	0.5%
VNQ	US REITs	8.6%	17.6%	2.3%	30.4%	2.4%	8.6%	4.9%	-6.0%	28.9%	-4.7%	129.6%	8.7%
DBC	Commodities	-2.6%	3.5%	-7.6%	-28.1%	-27.6%	18.6%	4.9%	-11.6%	11.8%	-7.8%	-45.1%	-5.8%
Highest Return		BTC	BTC	BTC	VNQ	BTC	BTC	BTC	BIL	BTC	BTC	BTC	BTC
Lowest Return		EEM	BIL	GLD	BTC	DBC	BIL	BIL	BTC	BIL	DBC	DBC	DBC
% of Asset Classes Positive		65%	94%	41%	65%	41%	100%	100%	6%	100%	88%	94%	94%

Fuente: Charlie Bilello (2021)

Con el auge de Bitcoin en los mercados, se fueron desarrollando distintos modelos que trataban de predecir el precio de este activo. Entre ellos, el más destacado ha sido el modelo *Stock-to-flow* que relacionaba directamente el precio con la escasez de Bitcoin. La teoría en la que se basa este modelo defiende que el precio de Bitcoin se podía explicar únicamente atendiendo a la relación existente entre las monedas que se encuentran en circulación en un momento dado y las que se van a producir durante el próximo año. Hasta noviembre de 2021 el modelo se consideró como el modelo de referencia del mercado basándose en esta teoría. Sin embargo, desde ese momento, el precio predicho por el modelo se ha desligado del precio real de Bitcoin, como se puede observar en la gráfica.

Imagen 2 Modelo *Stock-to-Flow*



Fuente: Glassnode.

El desligue del precio predicho y el precio real de Bitcoin abre la opción para debatir acerca de que variables pueden haberse omitido en el modelo o si se debe apostar por un modelo con un enfoque completamente nuevo que pueda adaptarse mejor a la realidad actual de Bitcoin.

1.2 OBJETIVO DEL TRABAJO

El objetivo de este trabajo es desarrollar un nuevo modelo que permita predecir el precio de Bitcoin, basándose en las principales suposiciones del modelo stock-to-flow. Para ello, se va a analizar las características del modelo Stock to Flow que ha sido la referencia del mercado para predecir la tendencia del precio del bitcoin. A partir de este análisis y apoyándose en otros estudios, en este trabajo se pretende encontrar un nuevo modelo que perfeccione la capacidad predictora de este. No obstante, parece importante remarcar que el objetivo inicial es que este nuevo modelo se base más en un análisis de cuestiones fundamentales de Bitcoin, más que en un mero modelo de análisis técnico.

Para lograr este objetivo, en primer lugar, se va a realizar un extenso estudio teórico. En el mismo se va a tratar tanto el funcionamiento del modelo *Stock-to-Flow*, como el de una blockchain y de Bitcoin.

Una vez realizado, este estudio se procederá a analizar las cuestiones que provocaron el desligue entre el valor predicho por el modelo y su valor real desde noviembre de 2021,

desde un punto de vista técnico.

Finalmente, se tratará de desarrollar un nuevo modelo que perfeccione el modelo *stock-to-flow*, añadiendo nuevas variables que le permitan entender mejor los distintos aspectos que afectan al ecosistema de Bitcoin.

1.3 METODOLOGÍA.

Para la realización de este trabajo, se ha utilizado documentos académicos - para el desarrollo del marco teórico- y herramientas de programación - para el análisis técnico de la cuestión.

Respecto de la primera parte, se ha revisado diversos *papers*, artículos académicos y noticias obtenidos. Es fundamental que el lector pueda comprender las diversas cuestiones técnicas y teóricas que la red de Bitcoin ofrece.

Respecto de la segunda, la primera herramienta utilizada ha sido Microsoft Excel[1] en la que se realizó ciertas manipulaciones a los datos descargados, de cara a prepararlos para su correcta utilización en el modelo. Posteriormente, el desarrollo del nuevo modelo se ha realizado en el entorno de *Jupyter Notebook* utilizando el lenguaje de programación de *Python*[2].

[1] Enlace al Excel:
https://docs.google.com/spreadsheets/d/16JE6PVUlzt7iMVsCNqigDtxpEsFy9pEB/edit?usp=sharing&ouid=104023027200646174396&rtpof=true&sd=true

[2] Enlace al código:
https://drive.google.com/file/d/1M77gwWJg_g66anJNKaFu91k31xueWFEc/view?usp=sharing

2. CAPÍTULO II. MARCO TEÓRICO

2.1 BLOCKCHAIN

Antes de empezar a analizar el concepto de Bitcoin, es necesario comprender y conocer el funcionamiento y la estructura básica de una *blockchain*. IBM lo define como:

"Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved. Business runs on information. The faster it's received and the more accurate it is, the better. Blockchain is ideal for delivering that information because it provides immediate, shared and completely transparent information stored on an immutable ledger that can be accessed only by permissioned network members. A blockchain network can track orders, payments, accounts, production and much more. And because members share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, as well as new efficiencies and opportunities.". [La *blockchain* es un libro mayor inmutable y compartido que facilita el proceso para grabar transacciones y rastrear activos en un entorno de negocio. Un activo puede ser tangible (una casa, coche, efectivo o terreno) o intangible (propiedad intelectual, patente, derechos de autor o marcas). Virtualmente, cualquier activo con valor puede ser seguido y comercializado en una red de *blockchain*, reduciendo riesgo y recortando costes para todos los afectados. Los negocios se basan en información. Cuanto más rápido se reciba y más precisa sea, mejor. *Blockchain* es el soporte ideal para obtener esa información porque la proporciona de manera inmediata, compartida y completamente transparente almacenada en un libro mayor inmutable que solo puede ser accedido por los miembros que la red permita. Una red basada en *blockchain* puede rastrear órdenes, pagos, cuentas, producción y mucho más. Debido a que los miembros de esta red comparten una misma visión sobre la verdad, se pueden observar todos los detalles de una transacción de principio a

fin, proporcionando mayor confianza al igual que nuevas eficacias y oportunidades].

En palabras de Ammous (2016), es el nombre que se le ha otorgado a la tecnología que soporta todo el sistema de Bitcoin, aunque el desarrollador de Bitcoin nunca usase el término *blockchain* en el documento en el que publicó Bitcoin. Lo esencial de la *blockchain* es que en el momento que se produce una transacción, los participantes de la misma anuncian al resto de miembros, denominados nodos (se profundizará más adelante en este término), de la red la operación que acaban de realizar. Este anuncio se materializa por medio de la adición de la operación a un bloque. De esta manera, los demás nodos tendrán la posibilidad de validarla cuando el bloque al que pertenece se complete.

Por su parte, Antonopoulos (2017) señalaba la dificultad de definir correctamente el término de *blockchain*. Considera que la red debe cumplir con una serie de características muy específicas que la hacen realmente una tecnología disruptiva y no una base de datos con un sistema de firmas electrónicas. La esencia principal de una *blockchain* sería la ausencia de confianza, o más bien la confianza en la red y en el sistema firmas y verificación de cada uno. Una *blockchain* deberá de ser un sistema en el que no sea necesario confiar en un tercero, en la contraparte de la operación, los otros nodos o los mineros para operar en ella. Este es el concepto innovador de la red, si se es capaz de utilizar el sistema sin la necesidad de confiar en un intermediario.

Aunque la tecnología *blockchain* existía desde mucho antes que se desarrollase la red de Bitcoin, es desde la aparición de esta última que la tecnología *blockchain* ha comenzado a despertar un gran interés y numerosos proyectos han adoptado esta tecnología para su desarrollo. Su aplicación principal ha sido en la industria financiera debido, especialmente, a la irrupción de Bitcoin y los problemas que sufre la industria en cuanto a la necesidad de la mediación de un tercero de confianza o agente externo que intervenga en la operación, como actualmente, costes, y determinación de la propiedad y eficiencia. Todos estos problemas que se acentuaron durante la crisis de 2008 (Nofer *et al*., 2017).

Estos problemas inherentes al funcionamiento del sistema financiero actual

podrían ser solucionados con la introducción de la tecnología blockchain. En primer lugar, el tiempo añadido que se consume, la operación realizada entre dos partes debe informarse a ese tercer organismo que deberá comprobarla. Con la entrada de la tecnología blockchain es la propia red de una manera más sencilla la que corrobora que se ha producido un traspaso de propiedad. Mientras mayor sea la red y más frecuente sea el intercambio de propiedad, más eficaz será la blockchain frente a un organismo externo, puesto que el tercero de confianza siempre tendrá que llevar a cabo un análisis exhaustivo para determinar la propiedad originaria del activo que se transfiere para confirmar que efectivamente es del transmisor, mientras que en la blockchain es la propia cadena de bloques la que señala que el que transfiere realmente es el dueño.

En segundo lugar, el coste que se deriva de este proceso externo a la operación, puesto que se necesita sufragar los gastos derivados del trabajo de este agente mientras que en la *blockchain* es el mismo trabajo computacional que determina

la realización de la transacción el que confirma que la transacción es válida.

Por último, existe un riesgo inherente al fallo de ese tercero al actuar como un sujeto más de la operación que carga con una posibilidad de falla humana, por su parte la *blockchain* no es más que un proceso computacional por lo que la opción de fallido es prácticamente inexistente, como se explicará a continuación. Además, no es necesario confiar en que no ha fallado, se puede comprobar cualquier aspecto de esta, si no hay confianza en la misma, gracias a su carácter abierto (Antonopoulos, 2017).

2.1.1 Funcionamiento y características.

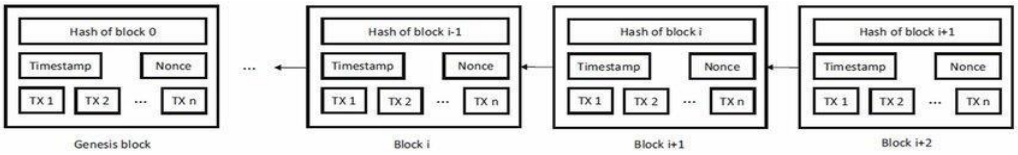
Blockchain está formada por una secuencia de bloques, su traducción al español es “cadena de bloques” lo cual ya nos da una descripción básica de su arquitectura, formando así una lista completa de transacciones que son recogidas como en una especie de libro público (Zheng *et al.,* 2016). Cada nuevo bloque que es validado por la red (en los próximos apartados se explicara como sucede este proceso de validación en la red de Bitcoin) se añade a la cadena. Por tanto, la figura de un bloque y la forma en que se encadenan entre ellos contiene las nociones

fundamentales para comprender el funcionamiento de la tecnología *blockchain*.

Internamente, cada bloque está compuesto por una serie de elementos fundamentales que son los que los permiten identificarlos, diferenciarlos a unos de otros y ubicar su posición dentro de la cadena .Los elementos que contiene cada bloque son: una marca temporal que identifica el momento en el que se originó el bloque (*timestamp*), el hash del bloque anterior que permite conocer cuál es el bloque que le precede y al que se debe encadenar, y el *nonce* (que proviene de su abreviación en inglés "*number only use once",* traducido al español "número que solo se usa una vez) que es un valor aleatorio que verifica el hash. Gracias a esta información, cualquiera puede comprobar la coherencia y veracidad de la cadena partiendo desde el último bloque hasta el primero de todos, que se denomina el bloque génesis (Nofer *et al*., 2017).

Toda esta información se incluiría dentro de lo que se denomina el cabecero del bloque, mientras que la información sobre el contenido de este se encuadra dentro de la parte denominada cuerpo del bloque. Esta sección incluye el número de las transacciones y las transacciones que en este se validan, cuya cantidad variara según la red. Toda la información incluida se validará por medio de la firma digital que se establece a través de procesos criptográficos que eliminan toda necesidad de la existencia de un tercero de confianza (Zheng *et al.*, 2016).

Imagen 3 Estructura de una *blockchain*



Fuente: Zheng *et al., 2016*

Los sujetos que participan dentro de la *blockchain* se denominan nodos, que pueden adoptar distintas funciones dentro de la red. La más conocida es aquella en la que actúan como mineros, es decir, son los que proponen y validan las transacciones por medio del mecanismo de consenso (este procedimiento se desarrollará en apartados posteriores). Sin embargo, según el tipo de *blockchain* y las funciones que esta encomienda al nodo podría desempeñar funciones más específicas como sería la verificación de pagos (Bashir, 2020).

Estos nodos son, además de validadores de las operaciones, participantes de la propia red, por lo que está en su interés que el registro de la cadena de bloques sea veraz. De esta manera, se incentiva a que estos actúen con responsabilidad y desarrollen una imagen fiable de la misma. Al mismo tiempo, la información que contienen los bloques de la cadena son los que permiten que los nodos puedan validar las distintas transacciones sin miedo a equivocarse, puesto que contiene la información mínima necesaria para verificar que esa operación se ha realizado correctamente. Como los valores de los hashes son únicos, la posibilidad de cometer el fraude se reduce a cuotas mínimas, puesto que, aunque un nodo de la red quisiera engañar al resto del sistema, los demás usuarios podrían rechazar la operación. Este proceso se explicará con más detalle en los próximos apartados (Nofer *et al*., 2017).

Nofer *et al*. (2017) señala la posibilidad de que el sistema siga funcionando a pesar de que algún nodo, por el motivo que sea, deje de hacerlo es un factor fundamental para incrementar la confianza de los usuarios en el sistema, puesto que elimina la necesidad de confiar en un tercero con unos intereses propios. Simplemente, con confiar en el correcto funcionamiento del sistema sería suficiente. Además, la ausencia de intermediarios también permite incrementar la seguridad del sistema y de los usuarios en sí, puesto que los terceros de confianza que suelen actuar requieren de una gran cantidad de información personal sobre los usuarios para poder confirmar la validez de las operaciones. Por el contrario, la *blockchain* no requiere de toda esta información personal, por lo que el riesgo de robo o filtración de información personal desaparece.

2.1.2 Características y tipos de *blockchain.*

2.1.2.1 Características de la Blockchain

Zheng *et al*. (2016) señalaban como principales características de la *blockchain* la descentralización, la persistencia, la inmutabilidad, el anonimato y la auditabilidad.

En cuanto a la descentralización, se observa el gran cambio con respecto del sector financiero como se conocía hasta ahora, puesto que se elimina el organismo central

que ha de validar todas las operaciones. Por ello, se suele hablar de *blockchain* como una red entre pares porque no se requiere de un tercero que garantice esas operaciones entre iguales, lo que también conlleva una reducción de costes considerable.

En segundo lugar, la persistencia de la red hace referencia al carácter permanente de todos los bloques que se registran en la red. Una vez es aprobado un bloque por el resto de los nodos y se añade a la cadena es prácticamente imposible que este sea alterado. De esta manera, cualquier intento de falsificación sería fácilmente detectable por los nodos, puesto que el hash cambiaría de uno a otro.

Esta característica se asocia al concepto de inmutabilidad. El hecho de que la información se aglutine en toda la red, es decir, que todos los nodos tengan acceso a ella elimina la opción de que el ataque a un nodo pueda provocar la alteración de alguna transacción. Se adentrará con mayor detalle sobre posibles ataques a la red de Bitcoin en el próximo capítulo.

Por otra parte, la anonimidad en la red nace gracias a la ausencia de ese tercero de confianza que necesita de información particular para corroborar la validez de las transacciones. Además, el sistema de claves de la red permite que no se exponga ningún tipo de dato personal si el usuario no lo desea, así como existe la posibilidad de generar tantas direcciones como considere conveniente.

Respecto de su auditabilidad, como ya hemos comentado la *blockchain* se puede entender como una especie de libro contable que almacena todas las operaciones que han sucedido bajo su red. Su carácter normalmente público (Bitcoin, al menos, lo es) permite que cualquiera que lo desee pueda comprobar los detalles de cualquier transacción desde el inicio de la red hasta la actualidad. Además, la marca temporal que se añade a cada bloque permite organizar y acceder a la información con una mayor facilidad.

A pesar de que en el siguiente apartado se verá que existen varios tipos de *blockchain*, Antonopoulos (2017) defiende que solamente la *blockchain* pública cumple los requisitos para ser considerado una *blockchain* propiamente dicha. Los otros tipos son realmente una especie de base de datos. Si la red no es pública se elimina la característica anterior, puesto que habrá alguien que decida en torno a

ella, por lo menos respecto a cuestiones como quien puede acceder y quien no. La única forma de poder confiar en el sistema y no tener que confiar en terceros depende de que esta sea abierta para todo el mundo, que el acceso al mecanismo de consenso no sea limitado para unos pocos.

Junto con este concepto de publicidad, vienen asociados una serie de elementos que se definen, por lo tanto, como característicos de una red *blockchain*. En primer lugar, que no tenga barreras, puesto que en el momento que se establezcan barreras para entrar dejará de ser pública. Esta idea incluye al hecho de que no debe limitarse a regiones concretas, ha de ser transnacional. También ha de ser neutral, puesto que, si busca los intereses de alguien o algo en particular, existiría la amenaza de que la red sea manipulada para servir a esos intereses. Por ello, las operaciones solo podrán ser clasificadas como válidas o inválidas de acuerdo con el mecanismo de consenso de la red. No existen operaciones buenas y malas, o legales e ilegales.

Todo esto deriva en otra característica en la que Antonopoulos (2017) hace hincapié: la ausencia o resistencia a la censura. Este es el elemento fundamental para que todas las demás características se materialicen. No podría darse una red pública y neutral si esta decide que tiene la capacidad de congelar, impedir o revisar ciertas transacciones. Para ello, resulta fundamental que la red sea efectivamente descentralizada, como Zheng *et al*. (2016) ya señalaba en el apartado anterior. La posibilidad de que la capacidad de decisión se reparte entre los distintos nodos de la red permite que todas estas características se materialicen en el sistema, de manera que la honestidad entre los nodos prevalezca.

2.1.2.2 Tipos de blockchain.

De acuerdo con Lin y Liao (2017), existen distintos tipos de *blockchain* que se pueden clasificar en cuatro grandes grupos:

1. *Blockchains* públicas. Como su propio nombre indica, cualquier interesado puede acceder a la red y participar en la misma, ya sea como minero, nodo o parte de una transacción. En gran medida, es la

definición de *blockchain* que se ha ido desarrollando en este capítulo, puesto que, como se verá ahora, los otros tipos eliminan alguna de sus características fundamentales. Algunas desventajas que podrían esgrimir sus detractores de esta red son la gran cantidad de energía que requiere o la falta de privacidad de las transacciones. Es el tipo de red que usa Bitcoin, de ahí que sea en la que se enfoque más este trabajo.

2. *Blockchains* privadas. La principal diferencia de este tipo de red es que el control de la misma recae en manos de un organismo. Aunque sus operaciones sigan realizándose entre pares, es el dueño de la red el que decide quien puede participar y el que toma las decisiones de consenso. Por ello, tampoco se puede referenciar a un consenso absoluto porque está limitado por el organismo central, lo que provoca a su vez la necesidad de confiar en este como un tercero o intermediario.
3. *Blockchains* autorizadas. Una subespecie de *blockchain* privada que está creada por una entidad, normalmente un negocio. Para acceder y participar de esta red se necesita de un permiso previo o recibir una invitación que es expedido por la organización que la controla.
4. *Blockchains* concertadas. Al igual que las anteriores, pero estas se caracterizan por estar controladas por un grupo, un consorcio entre diferentes instituciones o empresas. Nuevamente, se requiere del permiso o invitación para poder participar de la red. Aparece como una opción ideal para un conjunto de empresas que colaboren en algún proyecto, pudiendo así tener todos acceso a la misma plataforma.

2.2 BITCOIN

Si bien es cierto que el objetivo ulterior de este trabajo no se basa en un análisis de los fundamentales de Bitcoin, considero necesario establecer al menos las bases sobre las que se sustenta este sistema, cuáles son sus características principales y cómo funciona.

El 31 de octubre de 2008 una persona o conjunto de personas, bajo el pseudónimo, de Satoshi Nakamoto publicó el *whitepaper* de Bitcoin que lo definió como "un sistema de efectivo electrónico de usuario a usuario". De su propia definición ya surgen las primeras cuestiones sobre los conceptos de "efectivo electrónico" y "usuario a usuario". Para su desarrollo, basó el funcionamiento de la red en la tecnología *blockchain*. Como se indicaba en el bloque anterior, esta tecnología no era tan frecuente hasta este momento.

Antes de proseguir con el desarrollo teórico de este sistema, es de vital importancia remarcar la diferencia entre los términos "Bitcoin" y "bitcoin". El primero de los términos hace referencia a la red, es decir, al "sistema de efectivo electrónico de usuario a usuario". Por su parte, el segundo hace referencia a la moneda que se utiliza dentro de dicho sistema, el método de pago que se utiliza dentro de la red (Pérez, 2019).

2.2.1 Contexto histórico

En primer lugar, cabe ubicar el contexto en el que surge este sistema, que está claramente influenciado por dos factores. Por un lado, se encuentra el ascenso fulgurante de Internet desde el inicio del siglo XXI, pasando de 458 millones de usuarios en marzo de 2001 a 1.574 millones de usuarios en diciembre de 2008, lo que supone un incremento de casi el 250%. En términos porcentaje de usuarios respecto a la población mundial, creció desde un 7,6% a un 23,5%. Este aumento del protagonismo de Internet en nuestra población provoca que distintos aspectos de la vida cotidiana comiencen a tener su extensión en Internet. Entre ellos, los comercios se adaptan a esta nueva plataforma para aumentar sus canales de venta, lo que provoca que tengan que buscar una forma para que se puedan realizar estos pagos. En su gran mayoría, deciden apoyarse en instituciones financiares para que

intermedien en la realización de las transacciones (Nakamoto, 2008).

Por otro lado, dentro del plano económico internacional, después de la Segunda Guerra Mundial, el mercado internacional, con Estados Unidos a la cabeza, fue abandonando el patrón oro como sistema monetario para adoptar el dólar como la moneda de reserva internacional que derivó en un periodo caracterizado por la política monetaria expansiva. A partir de ese momento, cada burbuja o crisis que se iba formando era apaciguada por las instituciones financieras que, gracias a la inyección de liquidez, evitaban la caída del mercado. Esta forma de intervenir en el mercado por parte de las instituciones es totalmente opuesta al fundamentalismo que entiende que es el mercado tiende al equilibrio y es su curso natural el que permite llegar a ello. La globalización de los mercados provocó que el intervencionismo político se acentuara (Soros, 2008).

Este plan político estalló de la mano de la burbuja inmobiliaria que tuvo como principal protagonista al sistema bancario. La declaración de bancarrota por parte del banco Lehman Brothers en septiembre de 2008 mostró al mundo que las instituciones financieras podrían no ser capaces de rescatar a todos los bancos que entrasen en apuros, derivando en una gran desconfianza hacia el sistema bancario por parte de la población.

Esta crisis fue definida por George Soros, en enero de 2008, como la peor crisis financiera en 60 años. Sin embargo, la burbuja inmobiliaria era solo la punta del iceberg de la burbuja monetaria que entrañaba una mayor complejidad en su solución.

En este sentido, la mezcla de un contexto de crisis financiera con los bancos en el punto de mira y el auge de Internet crearon la situación idónea para el nacimiento de Bitcoin Por aquel entonces, el sistema de pagos en internet que ofrecían las instituciones financieras era muy primitivo. Además, se les había perdido la confianza, como intermediarios, debido a todos los problemas económicos que derivaron de la crisis bancaria en 2008.

Nakamoto, 2008, entendía que, aunque de una manera básica puede funcionar correctamente, el modelo de pagos basado en un tercero de confianza cuenta con ciertas carencias. Por un lado, el pago a ese tercero como remuneración por sus

servicios de intermediación supone un aumento del coste de las transacciones, reduciendo la posibilidad de realizar pequeñas operaciones. Además, su intervención permite la reversibilidad de estos pagos, por lo que la necesidad de confiar en la otra parte de la operación aumenta. Esto obliga a los comerciantes a exigir una cantidad superior de información a los clientes, que en persona no se verían en la necesidad de entregar.

Por este motivo, Nakamoto (2008) aboga por la introducción en el sistema de pagos de internet de un método basado en criptografía y la prueba de trabajo, que sustituyan a la confianza en un tercero como sustento de este. Defiende que ha logrado elaborar una solución que garantizaría la seguridad de los vendedores ante el fraude y que protege a los usuarios del problema del doble gasto que era una de las principales críticas a los medios de pago a través de un sistema de *blockchain.*

2.2.2 Transacciones y el problema del doble gasto.

Nakamoto (2008) en su documento original señala que:

"We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash off the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership". [Definimos una moneda electrónica como la cadena de firmas digitales. Cada propietario transfiere la moneda a través de la firma digital del hash de la transacción anterior y la llave pública del siguiente dueño y añadiendo estos al final de la moneda. Cualquier beneficiario puede verificar la firma para confirmar el traspaso de la propiedad].

Por tanto, para realizar una transacción el propietario deberá firmar en la moneda seguido a la última firma de la cadena (es importante tener presente que la moneda no es más que una cadena de firmas), que esto se realiza al aprobar la operación, de manera que su nueva firma pasa a formar parte de la cadena reconociendo el traspaso de la propiedad. Este proceso es público para el resto de los usuarios de la red que podrán comprobarlo si lo consideran necesario.

La problemática de este proceso deriva de la posibilidad de que el dueño glib esa misma moneda dos veces, es decir, que la utilice para realizar dos operaciones diferentes y como podría verificar un interesado que eso no sucede. La solución más común a este problema supone la introducción otra vez de un modelo de confianza, pues consistiría en la creación de un organismo que actúe a modo de Banco Central por el que pasen todas las operaciones y solo las monedas emitidas por este organismo tienen la confianza de no haber sido gastadas dos veces.

La solución que Satoshi Nakamoto encuentra parte de la premisa que la primera transacción que se realiza es la válida, la única forma de poder omitir la figura de un tercero que haga de árbitro es establecer una norma que no pueda derivar en formar posiciones opuestas entre las partes, por lo que establece el orden cronológico de entrada en la red. Una vez adoptada esta decisión, para omitir la confianza del tercero es necesario que todas las operaciones se registren públicamente y que los usuarios de la red participen activamente en el sistema aceptando las operaciones. De esta forma, si todos los usuarios aceptan y conocen que una operación se ha dado, no podrá gastarse esa moneda por segunda vez, pues estos usuarios podrían rechazarla.

Para que cualquier usuario pueda conocer si una transacción o un conjunto de estas existió y en qué momento, se añade un sistema de marca de tiempo. La forma de obtenerlo es por medio de la formación y publicación de un hash de un bloque de operaciones, añadiendo la marca de tiempo previa. De esta manera, se forma una cadena que reafirma las operaciones que se han realizado y en que orden.

2.2.3 Funcionamiento de la red y la prueba de trabajo.

Nakamoto (2008) describe el funcionamiento de su red de la siguiente manera: “

1 New transactions are broadcast to all nodes.

2 Each node collects new transactions into a block.

3 Each node works on finding a difficult proof-of-work for its block.

4 When a node finds a proof-of-work, it broadcasts the block to all nodes.

5 Nodes accept the block only if all transactions in it are valid and not already spent.

6 Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash

”.

[1) Nuevas transacciones son enviadas a todos los nodos.

2) Cada nodo recoge estas transacciones dentro de un bloque.

3) Cada nodo trabaja para encontrar una prueba-de-trabajo difícil para el bloque.

4) Cuando un nodo encuentra esa prueba de trabajo, envía el bloque al resto de nodos.

5) Los nodos aceptan el bloque solo si las transacciones que contiene son válidas y no han sido gastadas todavía.

6) Los nodos muestran la aceptación del bloque trabajando en la creación del próximo bloque en la cadena, usando el hash de este bloque aceptado como hash previo].

Respecto a la disyuntiva que surgiría si dos nodos encuentran la prueba de trabajo a la vez y lo envían al resto de bloques al mismo tiempo, se indica que cada nodo seguirá trabajando sobre el bloque que obtenga primero. Sin embargo, con la validación del siguiente bloque habrá una cadena que será más larga, esa será la cadena válida y a la que deberán cambiar los nodos que estuvieran trabajando en la otra.

2.2.3.1 Prueba de Trabajo

Un elemento fundamental dentro de la red es el sistema de Prueba de Trabajo que implementa Nakamoto. La prueba de trabajo es un mecanismo de consenso por el cual se valida un nuevo bloque. Es un proceso que requiere de un gran gasto de energía computacional por parte del usuario (minero) para resolver un complejo problema matemático que una vez resuelto se codifica en forma de hash como prueba ante el resto de los compañeros de que el trabajo se ha realizado. Una vez

validado el bloque, el usuario recibe una cierta cantidad de bitcoins como recompensa por su trabajo (Napoletano, 2023).

Esta recompensa que reciben los mineros es la manera de incentivar el trabajo honesto de los mismos, puesto que se requiere de la validación del resto de compañeros y solo encontrando la solución antes que el resto podrá realmente obtenerla.

Este es un elemento fundamental para solucionar el problema del doble gasto pues la gran cantidad de trabajo y el gasto que conlleva la validación de bloques incentiva a que se haga de forma correcta (Napoletano, 2023). De esta manera, se alinea la cooperación de los nodos honestos que estará representada por la cadena más larga que es la que cuenta con mayor prueba de trabajo gastado. Esto protege el sistema ante posibles ataques porque modificar la cadena requiere rehacer todas las pruebas de trabajo desde el bloque que se quiere modificar hasta el actual, lo cual cuenta con una posibilidad muy remota (Nakamoto, 2008).

Además, el propio sistema cuenta con ciertos incentivos económicos para los mineros que a cambio de su gasto computacional y eléctrico recibirán unas tasas por la labor realizado. Inicialmente, con la minería de monedas estas pasarán a su propiedad, mientras que respecto de la validación de las operaciones recibirán unas comisiones por ello.

Asimismo, Nakamoto (2008) considera que un atacante a la red si consiguiera la capacidad computacional suficiente como para superar a los nodos honestos, no obtendría mayor beneficio si intentara acabar con las reglas de Bitcoin (por ejemplo, logrando el doble gasto de un bitcoin), puesto que acabaría con la credibilidad y el valor del sistema. Por tanto, un ataque contra el mismo solo se daría en manos de alguien con un interés personal en acabar con Bitcoin (Nakamoto, 2008).

2.2.4 Otras cuestiones sobre Bitcoin

2.2.4.1 Oferta monetaria limitada.

En el código originario de Bitcoin, Satoshi Nakamoto decidió establecer 21

millones como número máximo de monedas que entrara en circulación si todos los bitcoins son minados. El motivo por el cual adoptó esta decisión se desconoce, puesto que en el *white paper* original no hizo referencia alguna a este hecho ni a su porqué.

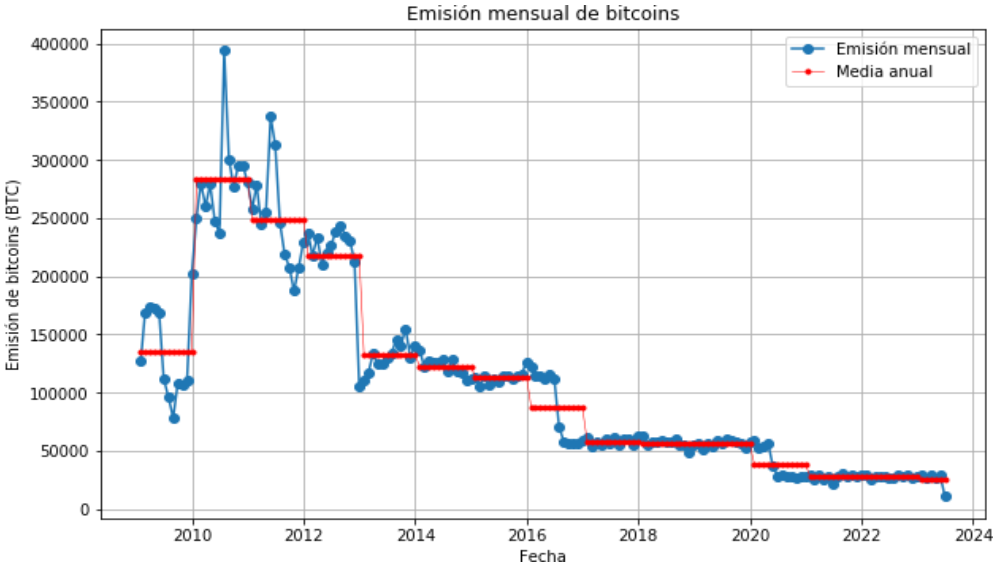
Según Ammous (2018), aunque es teóricamente posible, en la práctica los intereses políticos y personales han impedido que existe un bien con una tasa de crecimiento de la oferta baja. Sin embargo, la aparición de Bitcoin deja el crecimiento de la oferta monetaria en manos de un código informático ya programado que es prácticamente imposible modificar. Además, tras más de 10 años desde que se minó la primera moneda la credibilidad en el funcionamiento del sistema está fuera de toda duda.

Un nuevo bloque de Bitcoin es minado cada 10 minutos, aproximadamente, con una recompensa variable que se explicará en el apartado siguiente. Esta medida es aproximada debido a que Nakamoto estableció el denominado ajuste de dificultad que trata de lidiar con el incremento de velocidad de hardware y los posibles cambios de interés en resolver los problemas de la prueba de trabajo por parte de los mineros. De esta forma, a mayor capacidad de hardware o intereses en la minería más difícil será la prueba de trabajo a solventar, de manera que se mantengan un tiempo estable en torno a los 10 minutos. Lo mismo sucedería para el caso opuesto, menor capacidad de hardware o interés resultará en pruebas de trabajo más sencillas. Esto se logrará estableciendo una media móvil de bloques minados por hora, que ha resultado en este cálculo de unos 10 minutos (Nakamoto, 2008).

Así pues, el siguiente gráfico muestra la emisión mensual de Bitcoins desde que se minó el bloque génesis hasta datos de junio de 2023. Además, está dibujada la línea que representa la media de emisión anual. Se observa como durante el inicio de Bitcoin cuando su adopción era más limitada y los participantes de la red menores, el ritmo de minado era bastante más inestable. No obstante, desde que sucedió el primer halving en 2013 la emisión se ha estabilizado y a medida que han sucedido los demás halvings esta estabilidad se ha vuelto más latente. Sin embargo, como ya señalábamos anteriormente, el ajuste de dificultad provoca que

no sea exactamente igual la emisión de un mes a otro. Por ello, se ha querido mostrar en la gráfica la media anual de la emisión mensual de Bitcoin que permite confirmar el comportamiento estable de la emisión de bloques. Cabe resaltar como en 2016 y 2020, años de *halving*, la media de este tiempo se queda a medio camino entre las recompensas que se emitían de un *halving* a otro.

Imagen 4 Emisión mensual de Bitcoin



Fuente: Elaboración propia.

Como se puede observar, el ritmo de emisión es constante entre *halvings* (se explicará en el siguiente apartado), pero no es exacto. Es decir, si bien se mantiene dentro de un rango aproximado, el ajuste de la prueba de dificultad provoca que no sea el mismo número de bloques, por tanto, de bitcoins, los que se minan cada mes.

Esta nueva recompensa es la forma en la que se aumenta la oferta monetaria de Bitcoin. Como ya hemos explicado, para minar un nuevo bloque de Bitcoin se requiere el trabajo de los mineros, buscar la solución de la prueba de trabajo, pero solo uno de ellos obtiene la recompensa final. Por tanto, con el aumento del precio de bitcoin se prevé que el número de nodos que buscarán esa solución aumentará por lo que será más costoso obtener la recompensa. Por último, cabe añadir que Satoshi Nakamoto decidió dividir cada bitcoin en 100 millones de unidades, denominados satoshis como homenaje al pseudónimo (Ammous, 2018).

2.2.4.2 Bitcoin halving

La traducción literal al español del término *halving* es reducir a la mitad. El halving en Bitcoin es un el proceso por el cual se reduce a la mitad la recompensa que obtienen los mineros con la formación de un nuevo bloque, por lo que también supone una reducción a la mitad del ritmo de la tasa de creación de monedas en Bitcoin. Está establecido de forma automática que cada 210.000 bloques se produzca el halving, que tomando en consideración el ajuste de dificultad supone que aproximadamente cada cuatro años suceda este evento (Pastor, 2018).

Con esta medida, la tasa de emisión de bitcoin adopta una forma asintótica, con una emisión en sus primeros años muy acelerada, emitiendo la mayor parte de la oferta total. Posteriormente, la tasa de crecimiento se ralentizará hasta alcanzar los 21 millones establecidos como máximo. Inicialmente, el ritmo de expedición era de 50 bitcoins por bloque, en 2012 se redujo a 25, en 2016 a 12,5 y actualmente la recompensa se sitúa en 6,25 bitcoins por bloque hasta que, previsiblemente, en 2024 descienda a 3,125 (Ammous, 2018).

El comportamiento asintótico de la emisión de bitcoins supone que para en torno al año 2025 ya se habrán minado 20 millones de monedas, pero la oferta de moneda no se completará hasta el año 2021 aproximadamente (Ammous, 2018). No obstante, si no se hubiese programado la existencia del halving hace ya unos cuantos años, en 2016 para ser exactos, que toda la oferta de bitcoin ya estaría minada, puesto que en los primeros

210.000 bloques ya se emitió el 50% de la oferta. Por lo tanto, si la tasa de emisión se hubiese mantenido constante, en el segundo conjunto de 210.000 bloques se habría emitido la segunda mitad de la oferta (Pastor, 2018).

Esto hubiese implicado que los mineros solo obtendrían de su trabajo las comisiones recibidas por validar las transacciones, lo cual son cantidades muy inferiores a las del minado de bitcoins. Además, habría que añadir el hecho de que Bitcoin no habría tenido tiempo para asentarse y aumentar su valor, por lo que los incentivos para los mineros para seguir realizando su función serían aún menores (Pastor, 2018).

Existe un amplio consenso dentro de la doctrina acerca de que el *halving* que se produce cada cuatro años tiene un efecto altamente positivo sobre el precio de bitcoin. Desde la perspectiva de un minero, cada reducción de la recompensa que se produce supone que los beneficios que obtenían por su trabajo realizado se ven reducido a la mitad, si pensamos en los mineros como un colectivo (si pensásemos en un minero individual, esta reducción podría ser mayor o inferior, puesto que dependerá del número de pruebas de trabajo que consiga resolver lo cual no tiene porqué mantenerse constante). Por tanto, mientras que la oferta se ve reducida a la mitad, la recompensa no deja de ser lo que oferta Bitcoin a sus mineros a cambio de su trabajo, los gastos y la demanda se mantienen constantes. Incluso, algunos expertos defienden que se produce un aumento de la demanda, ya sea por un aumento del interés por parte de nuevos usuarios debido al aumento de cobertura mediática o por la realización por parte de los usuarios de que el *halving* ha sucedido sin mayores complicaciones y Bitcoin sigue funcionando tal cual se suponía (Schär, 2020). Por tanto, esta reducción de la oferta y aumento o, al menos, mantenimiento de la demanda conlleva a un aumento en el precio de Bitcoin que en los *halvings* sucedidos hasta el momento ha sido más que notable (Meynkhard, 2019).

Por tanto, el *halving* se configura como un proceso informático, un elemento técnico de Bitcoin, que tiene un efecto directo sobre el precio de bitcoin al reducir la oferta de la moneda, que según los estudios realizados por Meynkhard (2019) requiere de hasta 5 meses para que ese efecto se materialice. El coeficiente de correlación de rango de Kendall, estadística que se utiliza para medir la relación de dependencia entre dos variables, muestra unos valores de correlación altos entre el proceso del *halving* y el efecto en el precio de bitcoin (Meynkhard, 2019).

Sin embargo, Schär (2020) centraba su foco en que la llegada de este evento es previsible, que es otra característica del *halving* de Bitcoin que se suele omitir a la hora de hacer este análisis. De esta manera, cualquiera que con un conocimiento mínimo de Bitcoin puede saber que la reducción de la recompensa a la mitad se produce cada 210.000 bloques minados, lo cual sucede cada 4 años aproximadamente. Aunque no sea un cálculo exacto, se tiene conocimiento de cada bloque minado y a medida que este momento se acerca se puede ir

concretando aún más cuando sucederá. Por ello, según la teoría económica, un evento que es de dominio público debería ver afectado su precio antes de que este ocurra. Incluso, señala Schär que un inversor astuto que sabe que un suceso tendrá lugar en un momento concreto y que otros van a adquirir antes de que este suceda tratará no solo de anticiparse a ese momento si no a la comprar de sus competidores. Por tanto, el cambio en las recompensas recibidas por los mineros no debería tener un efecto en el precio de bitcoin, puesto que este cambio, al ser conocido, debería haberlo modificado previamente. De esta manera, en el momento que suceda el *halving* ese cambio en el precio debería de estar ya reflejado. Por tanto, considera que el repunte en el precio de bitcoin que ha acompañado a cada *halving* debería estar motivado por alguna cuestión más allá que la simple reducción de la oferta.

Además, Schär (2020) también destaca los riesgos que el *halving* de Bitcoin podría tener sobre la red, puesto que el mecanismo de seguridad de la cadena de bloques de Bitcoin se basa en el gasto de recursos computacionales, dificultando así lo intentos de doble gasto que se puedan producir. Como ya se ha explicado, cuantos más recursos computacionales se asignen al mecanismo de consenso de la cadena de bloques, más costoso y menos probable será un ataque de este tipo debido a que la mayor cantidad de nodos honestos trabajando en el mismo provocará que el atacante deba aumentar proporcionalmente su gasto computacional.

La relevancia de esta situación dentro del halving se debe a la relación de este con el beneficio obtenido por los mineros en su trabajo, puesto que se produce una reducción de la mitad de los mismos. Por tanto, podría darse la circunstancia de que para cierto minero no fuese rentable seguir dedicando ese gasto de energía y recurso computacional en comparación con la nueva recompensa que emite la propia red. Sin embargo, Schär considera que la cuestión es algo más compleja.

En primer lugar, se considera que el gasto en recursos computacional que ha ido experimentando la red ha derivado en que la seguridad de la red sea superior a la necesaria. Sin embargo, aunque esto no hay que entenderlo como algo negativo en cuanto a seguridad, implica que la lucha de los mineros por obtener la

recompensa por resolver la prueba de trabajo ha llevado a una sobreasignación de recursos sobre la red. Este exceso en el gasto computacional es una carga para el medio ambiente y representan un costo directo para los poseedores actuales de Bitcoin, quienes deben soportar la presión inflacionaria. Además, de ser un motivo de crítica directa al ecosistema de Bitcoin, aunque en este tema no se va a adentrar este trabajo. Por lo tanto, está lejos de ser claro si una disminución proporcional de la seguridad es un resultado negativo.

En segundo lugar, como la recompensa se recibe en bitcoins se encuentra en dependencia del valor de la moneda en ese momento. Por lo tanto, si el precio de bitcoin aumenta con el *halving*, como ha sucedido en los 3 que se han producido desde que se formó la moneda, esto podría compensar la disminución nominal de la recompensa, amortiguar los efectos o incluso resultar en un aumento de los beneficios obtenidos por los mineros, lo que podría derivar en un nuevo aumento del gasto en recursos computacionales. Después de todo, las personas que proporcionan los recursos computacionales se preocupan por el valor en dólares de su recompensa. Sin embargo, podría suceder en próximos *halvings* que el precio de Bitcoin disminuyese, por lo que la recompensa se vería afectada doblemente, es decir, a través de una disminución en la cantidad de unidades de bitcoin y por la supuesta disminución del valor en dólares por unidad del token. Esto inevitablemente obligaría a algunos mineros a cerrar sus operaciones, puesto que dejaría de ser positivo para estos el balance entre el gasto computacional y de energía con respecto a la recompensa recibida a cambio. Todo esto conllevaría a una mayor centralización en el negocio minero, pues posiblemente se mantendría aquellas grandes granjas de mineros que acumulan una mayor cantidad de potencia computacional. En consecuencia, esto podría socavar parcialmente la propuesta de valor de Bitcoin (Schär, 2020).

En definitiva, cada *halving* que Bitcoin ha ido superando con éxito supone sobrepasar una nueva prueba fundamental para la red, por lo que este evento se postula como uno de los más importantes para Bitcoin.

2.3 EL RATIO EXISTENCIAS/FLUJO Y EL MODELO STOCK-TO-FLOW

2.3.1 Ratio existencias/flujo

Ammous (2018) realiza una extensa reflexión sobre lo que es el dinero, cuáles son las características principales de este y qué hace que un dinero u otro se consolide como medio de intercambio en la sociedad. Si bien hablar sobre el dinero o si Bitcoin contiene los requisitos fundamentales para ser considerado dinero no se engloba dentro del ámbito de este trabajo, en su obra Ammous ofrece un análisis extenso y detallado sobre la importancia de que el dinero sea vendible en el tiempo. Sin embargo, esta explicación se podría trasladar por analogía a un activo que actúe como reserva de valor, para evitar entrar en la polémica sobre el carácter dinerario de bitcoin o no.

Que sea o no vendible en el tiempo está directamente relacionado con ser una reserva de valor, si el activo que estamos valorando es capaz de generar riqueza para su propietario mediante la conservación o aumento de su valor a lo largo del tiempo. Por ejemplo, algunos bienes como los alimentos perecederos no sería un ejemplo de reserva de valor, puesto que con el tiempo pierden las cualidades por las que se compró a ese precio. Por tanto, el bien debe ser inmune al paso del tiempo de una manera física, aunque esa no es su única condición necesaria.

La segunda cuestión fundamental se puede analizar a través de la ratio que interesa a este estudio, la ratio entre las existencias y el flujo. Para que un bien sea vendible en el tiempo es fundamental como su oferta se comporta, pues si se adquiere un bien y antes de que se venda su oferta crece de manera desproporcionada difícilmente podrá ser vendida al mismo valor que se adquirió. Por el contrario, si su oferta se comporta de una manera estable existe una mayor probabilidad de que este bien conserve su valor.

Por ello, la relación entre las existencias y el flujo es el indicador ideal para analizar esta cuestión. Ammous (2018) define el concepto de existencias como “la oferta existente integrada por todo lo que ha sido producido en el pasado, menos todo lo que ha sido consumido o destruido”. Por otro lado, define el término flujo como “la producción adicional que se llevará a cabo en el siguiente

periodo". Por tanto, las existencias en Bitcoin serían todas las monedas que ya han sido minadas hasta el momento actual, mientras que el flujo será el número de monedas que se obtengan como recompensa por bloque multiplicado por el número de bloques que se minen durante el periodo a analizar.

Básicamente, esta medida es una forma de analizar la oferta de un bien y el efecto que se deriva en el precio debido a la relación entre esta y la demanda. De esta manera, si la ratio es baja significa que la oferta de ese bien podrá aumentarse fácilmente, por lo que en caso de que aumente el interés en ese bien los productores trataran de aumentar su oferta al máximo posible. Presumiblemente, el precio de ese activo no solo no se incrementará si no que disminuirá y es por ese motivo por el que no se le consideraría apropiado como reserva de valor. Desde el otro prisma, una alta ratio de la relación entre existencias y flujo supondría que ante un aumento del interés (demanda) por parte de los posibles compradores, los productores no podrían aumentar a grandes niveles la oferta porque su flujo es bajo en comparación con el *stock* disponible. Por tanto, un aumento de la demanda sin su consecuente aumento de la oferta derivaría en un aumento de los precios del bien, por lo que se situaría como una buena reserva de valor.

Por eso, las propiedades de Bitcoin que establece un flujo monetario específico que se va reduciendo progresivamente en comparación con un aumento de las existencias, hacen que este tenga una alta ratio.

Sin embargo, Ammous (2018) en su análisis destaca que numerosos bienes se han utilizado como sistema de intercambio por su alta ratio existencias flujo a lo largo de la historia como pueden ser los cigarrillos en las cárceles o las conchas marinas antiguamente cuando no existía tanto avance tecnológico. Sin embargo, también señala que este tipo de bienes históricamente han visto como ante su aumento de valor se ha intentado obtener también un aumento de su oferta. Así sucedió con las conchas marinas cuando el desarrollo tecnológico facilitó su recogida e importación, lo que derivó en que dejara de ser una buena opción como reserva de valor. Esto realmente a quien perjudica es a quien había adquirido ese bien cuando su oferta no se había disparado y pensaba venderlo

cuando lo considerase necesario. En definitiva, perjudica al ahorrador a cambio del beneficio de aquellos que consiguen beneficiarse de ese aumento de la oferta, que no son otros que los productores.

Por ello, considera que para que exista un bien que se establezca como una verdadera reserva de valor (en realidad, Ammous trata de buscar lo que él denomina una moneda fuerte, para que esta exista considera que la característica fundamental es que sea una buena reserva de valor) necesitará contar con alguna limitación para que la oferta no pueda verse aumentada de manera radical en el momento en que ocupe mayor interés para la población como reserva de valor. En este sentido, Bitcoin cuenta en su propio código con una limitación clara en torno a la oferta total que existirá de bitcoins, un máximo de 21 millones, y también en cuanto a su ritmo de producción, que se irá reduciendo a la mitad cada 210.000 bloques minados (ver sección anterior BITCOIN para más información).

Por tanto, el problema de la oferta descontrolada se soluciona con Bitcoin porque la única manera de que esto se modifique sería que la mayoría de los nodos participantes se pusieran de acuerdo para aumentar la oferta. No obstante, una vez adoptaran esa decisión sería el principio del fin de Bitcoin, puesto que sería acabar con las características que la hicieron deseable inicialmente (Ammous, 2018).

2.3.2 Modelo Stock-to-Flow.

Desde el origen de Bitcoin, su precio ha mostrado una volatilidad muy elevada debido principalmente a todas las dudas e inseguridades que un mercado no regulado como este genera hacia los inversores. Además, el desconocimiento de gran parte de la población sobre cómo funciona correctamente este sistema informático ha dificultado aún más la transparencia de este mercado derivando también en escándalos como la estafa de Arbistar o situaciones como la caída de FTX o Terra Luna dentro del mercado de los criptoactivos. De la misma manera, cualquier noticia mínimamente positiva ha supuesto un despegue en el precio de bitcoin. Por todo ello, hasta ahora ha sido complicado realizar predicciones precisas sobre el precio de bitcoin (Ashmore, 2023).

No obstante, como se comentaba en el apartado anterior la oferta y el flujo de bitcoins están predeterminados, se pueden conocer con antelación. De acuerdo con la información de Coinmarketcap, al momento de redacción de este documento existen en torno a 19,4 millones de bitcoins en circulación sobre un total de 21 millones posibles. Además, se conoce que la recompensa actual de bitcoins para un minero por bloque minado es de 6,25 bitcoins y que un bloque nuevo es minado cada 10 minutos aproximadamente.

Siguiendo con esta relación, he calculado cual sería la relación entre flujo y existencias de Bitcoin. Para ello, se ha obtenido la aproximación de lo que sería la emisión de Bitcoin en un año según la recompensa actual. Cabe remarcar que es una aproximación porque los 10 minutos de minado entre bloque podría llegar a variar según las circunstancias del mercado, pero, en todo caso, el valor obtenido, 328.500 bitcoins minados en un año, es la mejor aproximación que podemos obtener sobre este dato con la información teórica que se cuenta de la moneda. Además, se ha calculado, a partir de la información histórica obtenida sobre la emisión de monedas diarias, el número de monedas que se emitieron durante 2021 y 2022 que son los dos años completos en los que se ha entregado esta recompensa de 6,25 bitcoins por bloque minado a los mineros. Por otro lado, se ha accedido a la información que ofrece Coingecko sobre la oferta en circulación de Bitcoin. Una vez obtenidos estos datos, resulta que la relación existencias-flujo de Bitcoin tiene un valor de 59,08 adoptando en el denominador (el flujo) el cálculo teórico de la emisión de bitcoins, 58,93 sería la ratio existencias-flujo si se adopta como flujo la emisión de 2021 y 58,38 con el flujo siendo la emisión de bitcoins en 2022. De acuerdo con los datos de Ashmore (2023), son todos valores muy cercanos al del oro, que cuenta con un valor de existencias-flujo de 62,3, que históricamente se ha alzado como un activo reserva de valor importante por la dificultad y lo costoso de aumentar de forma descontrolada su oferta.

El valor de esta ratio expresa cuántos años se necesitaría para obtener la misma cantidad de existencias que hay en circulación actualmente si se mantiene este ritmo de producción, es decir, si el flujo se mantiene constante. De esta manera, en caso de Bitcoin estaría en torno a 59 años y el oro en 62 años.

Sin embargo, según Ammous (2018), es más importante aún que con Bitcoin se logra que un producto cuente con una oferta que es estrictamente limitada. Gracias a esto, independientemente del crecimiento de Bitcoin, el interés que genere o cuanto se revalorice, no será posible aumentar la circulación por encima de los 21 millones de bitcoins que establece el código. Destaca que el bien material que más cerca ha estado de esta limitación es el oro gracias a su composición química que dificulta en gran medida el aumento del ritmo de extracción de este mineral.

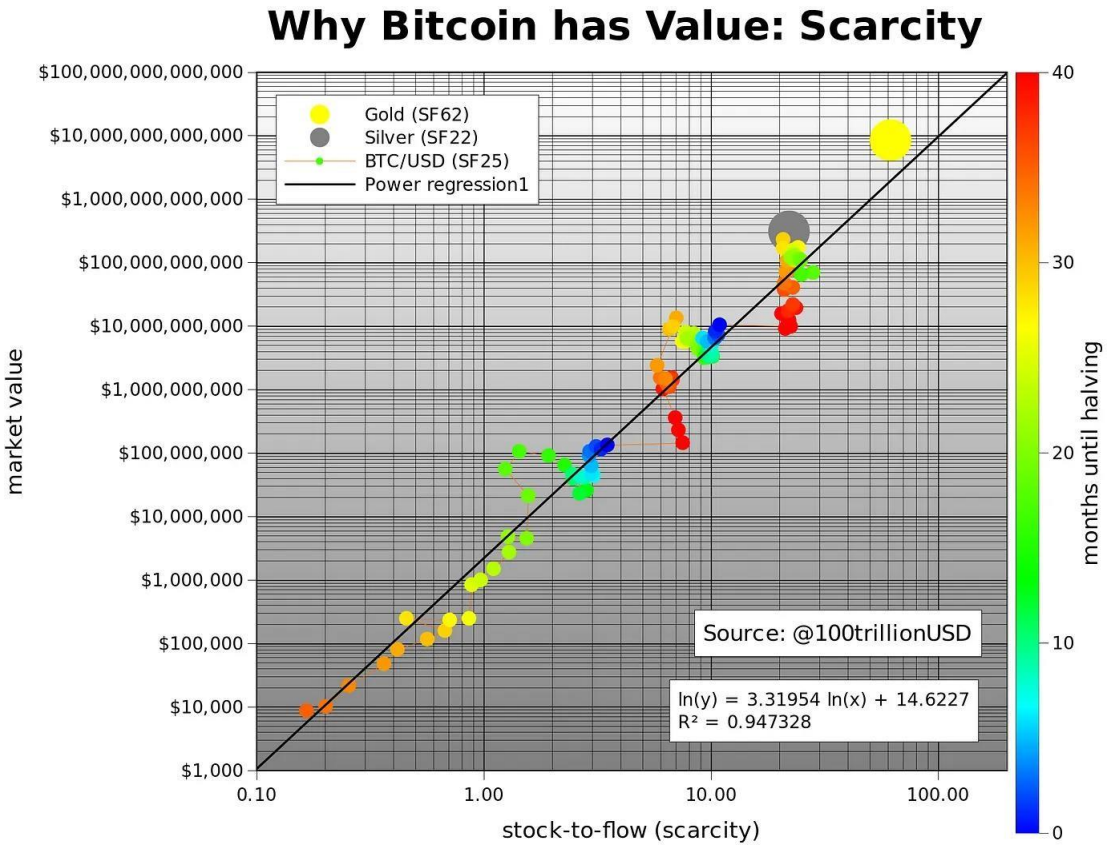
A 2017, año antes de que Ammous publicara su obra, el valor de la ratio existencias flujo de Bitcoin se establecía en torno a 25, cercano a los valores de la plata (Plan B, 2019). Al momento de redacción de este trabajo, ya ha alcanzado unos valores muy similares a los del oro, aunque no llega a superarlo aún como predijo Ammous, pero la ratio ha visto su valor más que duplicado. No obstante, lo más destacable de esta cuestión es que para el año 2140 aproximadamente cuando ya se hayan minado los 21 millones de bitcoins, la ratio de Bitcoin será infinita, convirtiéndose así en el primer bien que consiga este valor, lo convierte en un bien realmente escaso (Ammous, 2018). Esto confirma la importancia que esta ratio puede tener en el valor futuro de Bitcoin.

De esta manera, un usuario anónimo bajo el pseudónimo de Plan B publicó en 2019 un modelo para predecir el valor de Bitcoin a partir de su escasez, para ello se basa en la relación de su valor con la ratio existencias flujo. Es el denominado *Stock-to-Flow Model*. Plan B (2019) entiende que existe una relación directa entre la escasez de Bitcoin y su valor, mientras más escaso se vuelve (mayor ratio de existencias flujo) más valor tendrá la red.

Este modelo se realizó en 2019, por lo que se tomó inicialmente el valor mensual de la ratio flujo existencias desde que se minó el bloque génesis (2009) hasta esa fecha. Arbitrariamente decidió que no tomaría en consideración el primer millón de monedas minadas para así tener en cuenta el factor de que podrían existir monedas perdidas (se refiere a monedas asociadas a una cartera de las que se han perdido sus claves, por lo que nadie tiene acceso). Este número, supuestamente arbitrario, se cree que se puede deber a que se estima que durante

el primer año de vida de la red Satoshi Nakamoto minó en torno a un millón de monedas que desde entonces no se han movido (Bitbo, 2023).

Imagen 5: Relación entre el valor de Bitcoin y el ratio existencias-flujo



Fuente: Plan B (2019).

En cuanto al modelo, lo primero que se comprobó es que realmente existe una relación directa entre la ratio y el precio de Bitcoin. Para ello, se dibujó el gráfico de dispersión que se muestra a continuación, obteniéndose unos datos muy positivos. Un valor de R2 de casi el 95% con un p-valor inferior a 0,05 siendo, entonces, significativa la diferencia.

Además, Plan B (2019) decidió tomar como referencia los valores de el oro y la plata en cuanto a su ratio existencias flujo y a su valor de mercado. Por ello, que el valor de mercado de Bitcoin en 2017, cuando su ratio existencias-flujo valía 22 al igual que el de la plata, se acercara al valor de mercado de la plata se consideraba como un buen indicio del trabajo que se estaba realizando (valor de mercado de Bitcoin en ese momento era de $230 billones y el valor de la plata era

de $308 billones).

En base a esto, Plan B (2019) indicaba que existía una relación proporcional entre la escasez de Bitcoin y su valor. Con cada *halving* la oferta se reduce en la mitad, provocando que el valor de la ratio flujo existencias se duplique y hasta ese momento eso había supuesto un incremento de 10 veces el valor de mercado de Bitcoin.

Este nuevo modelo no era realmente preciso en los primeros años de vida de Bitcoin, hasta finales de 2013 aproximadamente, cuando todavía la inversión que existía dentro de la red era muy reducida. Posiblemente, estaría influenciado porque el precio adoptado en esos años no estaba establecido por un mercado consolidado sino por transacciones concretas entre particulares. A partir de 2015, una vez se introduce en grandes mercados, el modelo había mostrado una precisión asombrosa hasta noviembre de 2021 cuando bitcoin alcanzó su precio más alto en torno a los $ 69.000. La predicción del modelo señalaba que, a principios del año siguiente, se alcanzaría los $ 100.00, pero el valor de bitcoin empezó a descender desde ese momento. Mientras se escribe este trabajo, el valor de bitcoin se ha mantenido entre los encuentra entre los 30.000 $ y los 35.000 $ (Ashmore, 2023).

En el gráfico siguiente se muestra el modelo y el precio real de bitcoin. Plan B (2019) decidió que el modelo señalara a su vez la cercanía con el próximo *halving*, debido a que este hito marca la reducción de la oferta a la mitad y el consiguiente aumento de la ratio existencias flujo.

Imagen 6 Modelo Stock-to-flow comparado con el valor real de Bitcoin

Fuente: Glassnode

Se observa como desde noviembre de 2021, el modelo no ha reflejado el valor real de bitcoin, sobrevalorándolo unas 4 veces más que su precio. Por ello, se ha comenzado a dudar de la utilidad de este modelo.

En este trabajo vamos a tratar de analizar porqué el modelo ha dejado de ser capaz de predecir el valor de bitcoin.

2.4 OTROS MODELOS EXISTENTES PARA PREDECIR EL PRECIO DE BITCOIN

Sin embargo, antes de analizar los posibles motivos que llevaron al modelo *Stock-to-Flow* a dejar de ser preciso, parece conveniente observar otros modelos que se han podido generar durante este tiempo y que pueden aportar información significativa sobre qué causas provocan cambios en el precio de bitcoin.

2.4.1 Análisis técnicos (Elliot Wave Theory).

Este método se centra puramente en el análisis técnico de un activo, partiendo de la base de que el mercado está formado por corrientes que generan ciclos alcistas y bajistas, por lo que si el interesado es capaz de predecir estos ciclos podrá aprovecharse de las oportunidades del mercado para comprar y vender en los momentos adecuados. Estas corrientes se dividen entre impulsivas y correctivas. Las primeras provocan un aumento o descenso brusco del precio, motivado por la dirección a la que se dirige el mercado. Las segundas, por su parte, surgen como respuesta en sentido contrario a esa reacción brusca del mercado, como su propio nombre indica corrigen el descenso o aumento desmesurado del precio. El ciclo en su conjunto se entiende que consta de 5 ondas, de las cuales la primera, tercera y quinta corresponden al movimiento impulsivo; mientras que la segunda y la cuarta corresponden al movimiento correctivo (Tadvi, 2018).

En esta teoría el paso del tiempo es un elemento fundamental para poder determinar, con precisión, los precios y sus cambios de tendencia. Asimismo, la mezcla del tiempo con el entendimiento de las dos corrientes forma el engranaje básico de esta teoría. El tiempo en este caso es la única manera de confirmar que una corriente realmente se está formando o no. Esta cuestión deriva directamente del principio de alternancia de esta teoría, que es de la que se desprende que dos olas correctivas se forman dentro un patrón (Tadvi, 2018).

Junto con esta nace la teoría *neowave* como una evolución de la teoría anteriormente descrita para eliminar la subjetividad y las contradicciones de aquella. Esta teoría ha añadido nuevos patrones y normas con el objetivo de perfeccionar el modelo. Dentro de estos patrones destacan el *neutral triangle*,

diametric formation, *fifth failure terminal* y *third extension terminal*. Nuevamente, la lógica en estas cuestiones se centra en el análisis temporal de la información y en como este afecta al precio (Mtrading, s.f.).

2.4.2 Análisis fundamental: The Fulcrum Index.

Este índice fue desarrollado por Greg Foss tomando como premisa que Bitcoin podría ser usado como seguro ante la deuda pública de todos los países del mundo porque esta red se establece, según el propio Foss, como el anti-fiat (Foss, s.f.).

Esta medida se basa en establecer un precio razonable de bitcoin en el largo plazo, más centrado en sus cuestiones fundamentales que en un análisis técnico. De esta manera, considera que Bitcoin podría verse como un seguro ante el posible *default* de un conjunto de divisas de varios países. Este motivo estaría nuevamente basado en la oferta limitada de Bitcoin en 21 millones que supone una condición completamente antagónica a la del sistema Fiat actual que rige en los gobiernos. Por lo tanto, Bitcoin aparece como una posible cobertura ante el riesgo de default de las divisas y su precio, como todo seguro, iría determinado por el riesgo que ese contrato tenga que seguirá aumentando a medida que se siga aumentando la oferta monetaria de las divisas (Foss & Sansone, 2022).

Para ello, Foss decidió calcular el valor de los CDS (Credit Default Swaps) del conjunto de gobiernos pertenecientes al G20 tomando también en consideración cuales de sus obligaciones están financiadas o no. El valor de estos swaps alcanza una cifra aproximada de unos 4,5 trillones de dólares y, de ello, este modelo considera que un valor razonable de bitcoin estaría en torno a los $ 215.000, por lo que, en el momento que se produjeron sus cálculos, se encontraría infravalorada la red (Foss & Sansone, 2022). Entendiendo que el valor de los CDS se ha mantenido, por lo menos, constante, puesto que los gobiernos han seguido inyectando estímulos económicos durante este último año, y que el valor de bitcoin ha descendido a los $ 20.000 (en el momento en que Foss realizó sus cálculos estaba en torno a $ 40.000) debemos entender que ahora estaría aún más infravalorada la red.

3. CAPÍTULO III. ESTUDIO DE CAMPO

3.1 TRATAMIENTO DE DATOS

3.1.1 Datos utilizados.

Se ha obtenido información diaria relativa al precio de bitcoin desde su creación hasta el 17 de noviembre de 2023, la emisión de moneda, *hash rate* (carga computacional utilizada por los mineros) y el número de operaciones efectuadas, a partir de la web de Coinmetrics. La utilización de los dos primeros resulta obvia si estamos analizando el precio de Bitcoin y tomando como referencia el modelo *stock-to-flow* que basa todo su estudio en las monedas existentes y la emisión de nuevas monedas.

Respecto de las dos últimas variables, que la emisión de nuevas monedas está controlada por la energía computacional que se les exige a los mineros durante el proceso; es decir, el *hash-rate* (Kristoufek, 2015). Por tanto, su relación directa con el flujo podría aportar información extra para entender el precio de Bitcoin. El número de operaciones ha sido utilizado anteriormente en otros estudios como el realizado por Ciaian *et al.*, 2016, puesto que aporta información sobre el volumen y participantes de la red.

La información descargada en Excel ha sido tratada para poder utilizarla en el estudio. En primer lugar, se ha decidido calcular la información relativa a las existencias acumuladas y el flujo para el siguiente año en el mismo Excel. Para el cálculo de las existencias acumuladas en una nueva columna se añade la emisión diaria a la acumulada hasta esa fecha. Por ejemplo, para el 12 de enero de 2009 la emisión acumulada se calcularía sumando el valor de emisión acumulada de la fila anterior (que es la suma de los valores de la emisión diaria de los días anteriores) y la emisión diaria de esa fecha.

En segundo lugar, cabe destacar que el flujo se ha calculado de dos maneras distintas. Por un lado, se han tomado los valores de los próximos 365 días de emisión para cada día de la base de datos y se han sumado, obteniendo así el que fue el flujo real de los 365 días posteriores a cada fecha de observación. Por el otro lado, se adopta la estimación de 463 días (Bitbo, 2023) para estimar el flujo anual, de manera que se obtiene la información de la emisión de los 463 días posteriores a la fecha de observación se divide entre este mismo número(463) para obtener el valor medio diario

de esos 463 días y se multiplica por 365 para obtener la media anual. La razón de que sea 463 días nace de los cálculos de Preston Pysh que entendía que cada ciclo de Bitcoin abarca 200.000 bloques minado, contiene 3 fases (fase alcista, corrección y la reversión a la median) y se emiten 144 bloques por día. Por tanto, del resultado de dividir 200.000 entre 3 y el resultado entre 144 se obtiene el valor de 463 días.

Finalmente, una vez calculados los flujos y la emisión acumulada se han adaptado otras dos columnas para calcular directamente la relación entre existencias y flujo, que se realiza dividiendo a la emisión acumulada el flujo correspondiente a esa fecha. Son 2 columnas porque se debe calcular una relación para cada flujo calculado, por lo que habrá una columna con la relación existencias flujo de 365 días (S/F 365) y otra de 463 (S/F 463). Por lo tanto, esa base de datos quedaría de la siguiente manera:

Imagen 7: Primeras observaciones de la base de datos descargada de coinmetrics

	A	B	C	D	E	F	G	H	I	J
1	Time	BTC / Price	BTC / Issuance, continuous, native units	BTC / Hash rate, mean	BTC / Transactions, count	existencias	flujo_365	flujo_463	s2f_365	s2f_463
2	2009-01-03				0					
3	2009-01-04				0					
4	2009-01-05				0					
5	2009-01-06				0					
6	2009-01-07				0					
7	2009-01-08				0					
8	2009-01-09		950	9,44495E-07	0	950	1705450	2040018,9	0,000557	0,000466
9	2009-01-10		3050	3,03233E-06	0	4000	1710350	2046759,2	0,002339	0,001954
10	2009-01-11		4650	4,62306E-06	1	8650	1713650	2051173,9	0,005048	0,004217
11	2009-01-12		4700	4,67277E-06	6	13350	1717150	2056101	0,007775	0,006493
12	2009-01-13		6150	6,11436E-06	0	19500	1718150	2057520	0,011349	0,009477
13	2009-01-14		6450	6,41262E-06	1	25950	1718750	2058347,7	0,015098	0,012607
14	2009-01-15		6300	6,26349E-06	8	32250	1718700	2060003,2	0,018764	0,015655
15	2009-01-16		5400	5,36871E-06	2	37650	1719850	2061974,1	0,021891	0,018259
16	2009-01-17		5450	5,41842E-06	0	43100	1720650	2064142	0,025049	0,02088
17	2009-01-18		5350	5,319E-06	1	48450	1721500	2067019,4	0,028144	0,02344
18	2009-01-19		5750	5,71668E-06	2	54200	1723650	2069581,5	0,031445	0,026189
19	2009-01-20		5700	5,66697E-06	1	59900	1726700	2070882,3	0,03469	0,028925
20	2009-01-21		5100	5,07045E-06	2	65000	1728250	2072537,8	0,03761	0,031363

Fuente: Elaboración propia.

Además, quedaría señalar que para poder obtener información acerca del flujo de las últimas fechas se ha tenido que realizar una aproximación de la que sería la teórica oferta de bitcoins para valores futuros. Para ello, se ha decidido adoptar la media del último año como la emisión de los próximos 463 días. Aunque el ritmo de emisión en la práctica no es constante, es cierto que se mueve dentro de unos límites regulares, por lo que usar la media de un año para predecir el siguiente podría ser una buena aproximación para estimar la emisión diaria de las observaciones futuras.

Por otra parte, se podría hablar sobre las variables externas de Bitcoin que aportan información sobre la situación macroeconómica y de los mercados que podrían influir en el precio de Bitcoin.

En primer lugar, se incluye el par dólar/euro como indicador de la situación de la economía global. Al ser el dólar la moneda de referencia en la economía mundial,

previsiblemente una bajada del dólar respecto del euro supondría la misma situación frente a Bitcoin y viceversa (Ciaian *et al*., 2016).

En segundo lugar, como referencias macroeconómicas globales se ha adoptado el precio del petróleo y el índice de Dow Jones al ser dos valores que suelen reflejar con bastante precisión la situación macroeconómica y están aceptados en la comunidad como tal (Ciaian *et al*., 2016).

Por último, se ha escogido el precio del oro por ser el activo de referencia como protección ante la inflación y sus características similares a Bitcoin que han llevado a tantas comparaciones entre ambos activos. Además, ya ha sido incluido en varios estudios sobre este tema como en el Bouoiyour y Selmi, 2017, y el de Kristoufek, 2015.

Todas estas variables se han obtenido a través de Yahoo Finance directamente desde *python* usando la función "*yf.download*".

3.1.2 Tratamiento de datos

En primer lugar, se eliminó del dataset con las variables relativas a la red de Bitcoin todas aquellas variables que se utilizaron para obtener la ratio existencias-flujo. Estas fueron la emisión de bitcoins diaria, existencias, flujo_365 y flujo_463.

Imagen 8 Líneas del código sobre limpieza de datos (I)

```
# Como solo nos interesa las variables del ratio flujo existencias, antes de unir las tablas vamos a eliminar las variables que s
limpiar_datset = ['BTC / Issuance, continuous, native units', 'existencias', 'flujo_365','flujo_463']

# Elimina las columnas del DataFrame
btc_data_limpio = btc_data.drop(limpiar_datset, axis=1)
```

Fuente: Elaboración propia

Previo a la fusión de las variables en un único dataset, se requería cierto tratamiento de las variables. Respecto de las variables obtenidas de Yahoo, había que convertir "Date" en variable, puesto que al descargarse se incluía directamente como índice del dataset. Para ello, se utilizó la función "*reset_index*".

Imagen 9 Líneas del código sobre limpieza de datos (II)

```
# Antes de proceder a la fusión, reestablecemos Date como columna de los datasets
dataframes = [dow_jones_data, oro_data, petroleo_data, usd_eur_data]

for df in dataframes:
        df.reset_index(inplace=True)
        df['Date'] = pd.to_datetime(df['Date'])
```

Fuente: Elaboración propia

Los datasets descargados desde Yahoo contenían distintos precios o valores dentro de

un día para esa variable. Como solo nos interesaba uno de ellos y el mercado de Bitcoin no cierra nunca, era indiferente que valor adoptar. Por ello, se decidió quedarse con la variable "Open", valor a la apertura del mercado, como valor de cada variable y se eliminaron del dataset el resto de las observaciones.

Imagen 10 Líneas del código sobre limpieza de datos (III)

```
#Solo nos interesa uno de los precios de cada una. Por lo que nos quedaremos con el de Open.
#Además, le cambiaremos el nombre para distinguir cada variable.
dataframes = [dow_jones_data, oro_data, petroleo_data, usd_eur_data]
columnas_eliminar = ['High', 'Low', 'Close', 'Adj Close', 'Volume']

for df in dataframes:
        df.drop(columns=columnas_eliminar, inplace=True)



#Además, le cambiaremos el nombre para distinguir cada variable cuando se fusionen
oro_data=oro_data.rename(columns={'Open':"precio_oro"})
dow_jones_data=dow_jones_data.rename(columns={'Open':"valor_dowjones"})
petroleo_data=petroleo_data.rename(columns={'Open':"precio_petroleo"})
usd_eur_data=usd_eur_data.rename(columns={'Open':"precio_dolar"})
```

Fuente: Elaboración propia

Finalmente, usando la función "*merge*" de la librería pandas se fusionaron los datasets para crear el dataset que utilizaremos como *input* de los modelos.

Imagen 11 Líneas del código sobre limpieza de datos (IV)

```
# Unimos las tablas para formar un único dataset
datos_1 = pd.merge(btc_data_limpio, oro_data, on='Date', how='inner')
datos_1 = pd.merge(datos_1, petroleo_data, on='Date', how='inner')
datos_1 = pd.merge(datos_1, usd_eur_data, on='Date', how='inner')
mi_dataset = pd.merge(datos_1, dow_jones_data, on='Date', how='inner')
```

Fuente: Elaboración propia

Imagen 12 Base de datos unificada, con todas las variables

	Date	precio_BTC	hash_rate_diario	num_transacciones	s2f_365	\
0	2010-01-04	NaN	0.000011	2.0	0.486315	
1	2010-01-05	NaN	0.000012	0.0	0.489632	
2	2010-01-06	NaN	0.000010	0.0	0.492020	
3	2010-01-07	NaN	0.000009	0.0	0.494167	
4	2010-01-08	NaN	0.000009	0.0	0.496342	

	s2f_463	precio_oro	precio_petroleo	precio_dolar	valor_dowjones
0	0.493454	1117.699951	79.629997	0.69881	10430.690430
1	0.496626	1118.099976	81.629997	0.69314	10584.559570
2	0.499214	1135.900024	81.430000	0.69609	10564.719727
3	0.501398	1133.099976	83.199997	0.69430	10571.110352
4	0.503520	1138.199951	82.650002	0.69828	10606.400391

Fuente: Elaboración propia

Una vez obtenido nuestro dataset definitivo, con el objetivo de mantener la representatividad de todas las variables se decidió normalizar el valor de todas estas. En este proceso se excluyó tanto la variable dependiente del modelo, el precio de Bitcoin,

como la variable de fecha.

Imagen 13 Líneas del código sobre limpieza de datos (IV)

```
# Selecciono solo las columnas que quiero normalizar
normal_columnas = mi_dataset.columns.difference(['precio_BTC','Date'])

scaler = MinMaxScaler()

# Normaliza las columnas seleccionadas
mi_dataset[normal_columnas] = scaler.fit_transform(mi_dataset[normal_columnas])
```

Fuente: Elaboración propia

Por último, las primeras observaciones contaban con un valor *missing* para el precio de Bitcoin. Se podría haber adoptado que todos esos valores fuesen cambiados por un cero o eliminar estas observaciones sin valor. Es importante analizar porqué el valor del precio de Bitcoin era cero en ese momento. Tras su lanzamiento, la red de Bitcoin era utilizada mayoritariamente por curiosos de la informática que se centraban en comprender el funcionamiento de la red más que en sus fundamentos económicos o en su posible valor futuro. Las transacciones que se produjeron inicialmente no tenían valor en términos económicos, su precio era cero, porque el motivo por el que se realizaban carecía de un fundamento económico, es decir, no se utilizaba como un sistema de pago.

Por este motivo, se decidió que la opción más acertada era eliminar las primeras observaciones que contaban con valores *missing* para el precio de Bitcoin. El valor de Bitcoin durante ese tiempo se mantiene constante en cero dólares, pero la razón de este precio no estaba influenciada realmente por los valores que van adoptando las variables independientes, del mismo modo que los valores de estas variables anteriores a la creación de Bitcoin no afectaron a su precio. De esta manera, la base de datos que se utiliza comienza finalmente el 19 de julio de 2010 que cuenta con el primer valor registrado para Bitcoin.

Imagen 14 Base de datos normalizada

	Date	precio_BTC	hash_rate_diario	num_transacciones	s2f_365	s2f_463	precio_oro	precio_petroleo	precio_dolar	valor_dowjones
0	2010-07-19	0.080800	3.087034e-12	0.000471	0.009156	0.010062	0.129319	0.647050	0.275057	0.015226
1	2010-07-20	0.074736	3.211864e-12	0.000597	0.009210	0.010129	0.139105	0.651954	0.268623	0.017199
2	2010-07-21	0.079193	3.675521e-12	0.000349	0.009277	0.010208	0.139205	0.662412	0.276577	0.019956
3	2010-07-22	0.058470	3.122700e-12	0.000312	0.009330	0.010270	0.143100	0.652171	0.296911	0.016102
4	2010-07-23	0.060593	3.443692e-12	0.000310	0.009387	0.010342	0.135311	0.672652	0.275220	0.023475

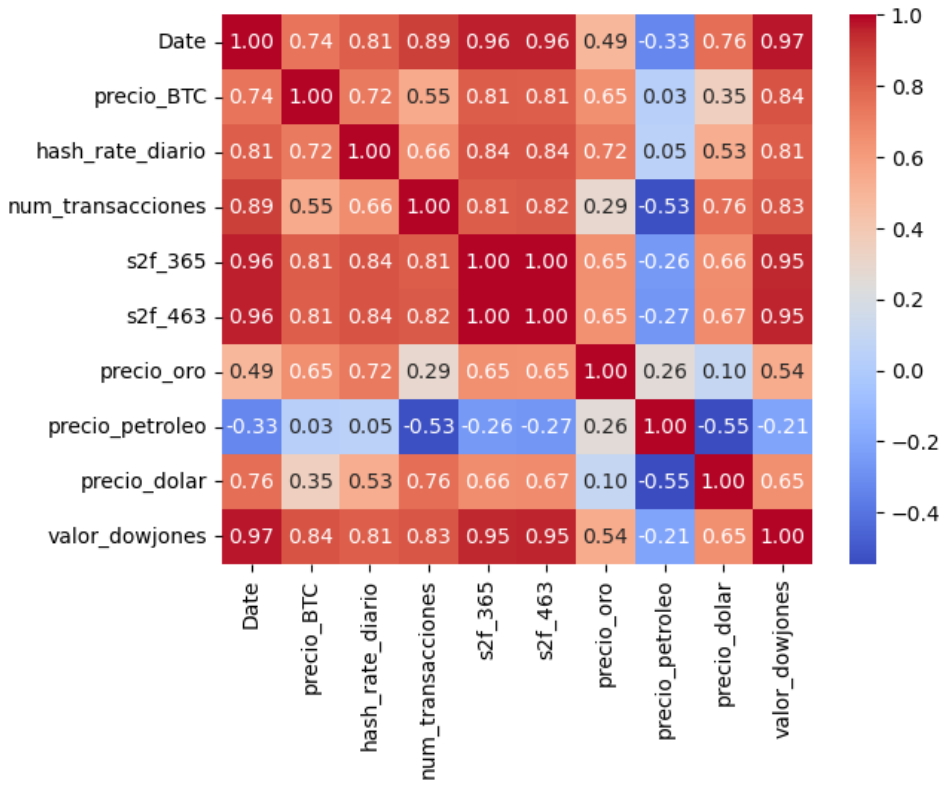
Fuente: Elaboración propia

3.1.3 Matrices de correlación

En primer lugar, se ha dibujado la matriz de correlación de las variables para valorar si existen variables con una correlación elevada que obligue a eliminar a alguna del modelo. En este caso, se puede observar que las variables “s2f_365” y “s2f_463” son prácticamente iguales, por lo que una de las dos debería de eliminarse del dataset para evitar que haya dos variables que expliquen lo mismo.

Finalmente, se decidió mantener la variable s2f_463 porque fue la que utilizó PlanB al desarrollar el modelo *stock-to-flow*. Se trata, así, de mantener la base teórica del modelo original que se intenta mejorar y que durante un tiempo fue la referencia del sector.

Imagen 15 Matriz de correlación de las variables.



Fuente: Elaboración propia

Por tanto, las variables que formarían el modelo son:

Imagen 16 Base de datos definitiva

	Date	precio_BTC	hash_rate_diario	num_transacciones	s2f_463	\
0	2010-07-19	0.080800	3.087034e-12	0.000471	0.010062	
1	2010-07-20	0.074736	3.211864e-12	0.000597	0.010129	
2	2010-07-21	0.079193	3.675521e-12	0.000349	0.010208	
3	2010-07-22	0.058470	3.122700e-12	0.000312	0.010270	
4	2010-07-23	0.060593	3.443692e-12	0.000310	0.010342	

	precio_oro	precio_petroleo	precio_dolar	valor_dowjones
0	0.129319	0.647050	0.275057	0.015226
1	0.139105	0.651954	0.268623	0.017199
2	0.139205	0.662412	0.276577	0.019956
3	0.143100	0.652171	0.296911	0.016102
4	0.135311	0.672652	0.275220	0.023475

Fuente: Elaboración propia

3.2 NUEVO MODELO

De cara a desarrollar un buen modelo que sea capaz de sustituir al modelo *stock-to-flow*, que lleva siendo referencia del sector durante un lustro, considero necesario tratar de valorar distintos modelos y compararlos para poder decidir cual se adapta mejor a las necesidades de la investigación. Se han desarrollado, modelos de regresión lineal, *random forest*, XGBoost y KNN. Para su desarrollo, en primer lugar, se han obtenido los modelos explicativos de cada uno y, posteriormente, se han desarrollado los modelos predictivos.

3.2.1 Modelos explicativos.

Todos los modelos han adoptado como variable dependiente el precio de Bitcoin y el resto de las variables han pasado a formar el conjunto de variables independientes. Estas variables son: valor de la relación existencias flujo a 463 días (*s2f_463*), número de transacciones diarias en la red de Bitcoin, capacidad de *hash rate* diario, precio del oro, el par dólar/euro (precio_dólar), precio del petróleo y el valor del índice *dow jones*.

3.2.1.1 Regresión Lineal

Para desarrollar este modelo se han utilizado la función *linearRegression* del paquete *sklearn.linear_model* y se han obtenido los siguientes resultados del modelo:

Imagen 17 Resumen estadístico del modelo de regresión lineal (I)

OLS Regression Results

Dep. Variable:	precio_BTC	R-squared:	0.811
Model:	OLS	Adj. R-squared:	0.810
Method:	Least Squares	F-statistic:	2045.
Date:	Thu, 30 Nov 2023	Prob (F-statistic):	0.00
Time:	00:34:44	Log-Likelihood:	-34138.
No. Observations:	3350	AIC:	6.829e+04
Df Residuals:	3342	BIC:	6.834e+04
Df Model:	7		
Covariance Type:	nonrobust		

Fuente: Elaboración propia

Imagen 18 Resumen estadístico del modelo de regresión lineal (II)

	coef	std err	t	P>|t|	[0.025	0.975]
const	-5491.0813	1084.552	-5.063	0.000	-7617.533	-3364.629
hash_rate_diario	-674.6999	1351.830	-0.499	0.618	-3325.198	1975.798
num_transacciones	-2.545e+04	1524.653	-16.695	0.000	-2.84e+04	-2.25e+04
s2f_463	2316.7679	1633.295	1.418	0.156	-885.592	5519.128
precio_oro	8927.7405	937.577	9.522	0.000	7089.458	1.08e+04
precio_petroleo	-3366.7661	1287.048	-2.616	0.009	-5890.247	-843.285
precio_dolar	-1.273e+04	992.416	-12.825	0.000	-1.47e+04	-1.08e+04
valor_dowjones	5.574e+04	1653.291	33.714	0.000	5.25e+04	5.9e+04

Omnibus:	855.867	Durbin-Watson:	0.042
Prob(Omnibus):	0.000	Jarque-Bera (JB):	2912.143
Skew:	1.260	Prob(JB):	0.00
Kurtosis:	6.810	Cond. No.	34.8

Fuente: Elaboración propia

Dados estos resultados, se observa que la capacidad predictiva del modelo alcanza niveles satisfactorios con un R cuadrado superior al 80%. Respecto de la importancia de las distintas variables, solo el p-valor de las variables *s2f_463* y *hash_rate_diario* no superan el umbral del 5% del p-valor por lo que no se puede afirmar que sean estadísticamente significativas. Todas las demás superan ese umbral, por lo que son estadísticamente significativas para el modelo.

3.2.1.2 Random Forest.

Para este modelo se ha utilizado del paquete *sklearn.enssemble* la función *RandomForestRegressor*. Además, para optimizar el valor de los hiperparámetros de este modelo se ha empleado validación cruzada. Para ello, se ha tratado de obtener el mejor valor para el número de estimadores del modelo, la profundidad de cada árbol, cómo se produce la división entre los distintos subconjuntos de la muestra y el mínimo de hojas a utilizar por muestra. Este proceso de optimización se ha realizado con la función de *cross_val_score*.

Imagen 19 Ajuste de los hiperparámetros por validación cruzada (I)

```
space_rf = {
    'n_estimators': hp.quniform('n_estimators', 50, 200, 1),
    'max_depth': hp.choice('max_depth', range(5, 21)),
    'min_samples_split': hp.uniform('min_samples_split', 0.1, 1),
    'min_samples_leaf': hp.uniform('min_samples_leaf', 0.1, 0.5)
}

def objective_rf(params):
    # Extraer los valores de los hiperparámetros del espacio de búsqueda
    n_estimators = int(params['n_estimators'])
    max_depth = int(params['max_depth']) if params['max_depth'] is not None else None
    min_samples_split = params['min_samples_split']
    min_samples_leaf = params['min_samples_leaf']

    # Crear un modelo de Random Forest con los hiperparámetros dados
    model_rf = RandomForestRegressor(
        n_estimators=n_estimators,
        max_depth=max_depth,
        min_samples_split=min_samples_split,
        min_samples_leaf=min_samples_leaf
    )
```

Fuente: Elaboración propia

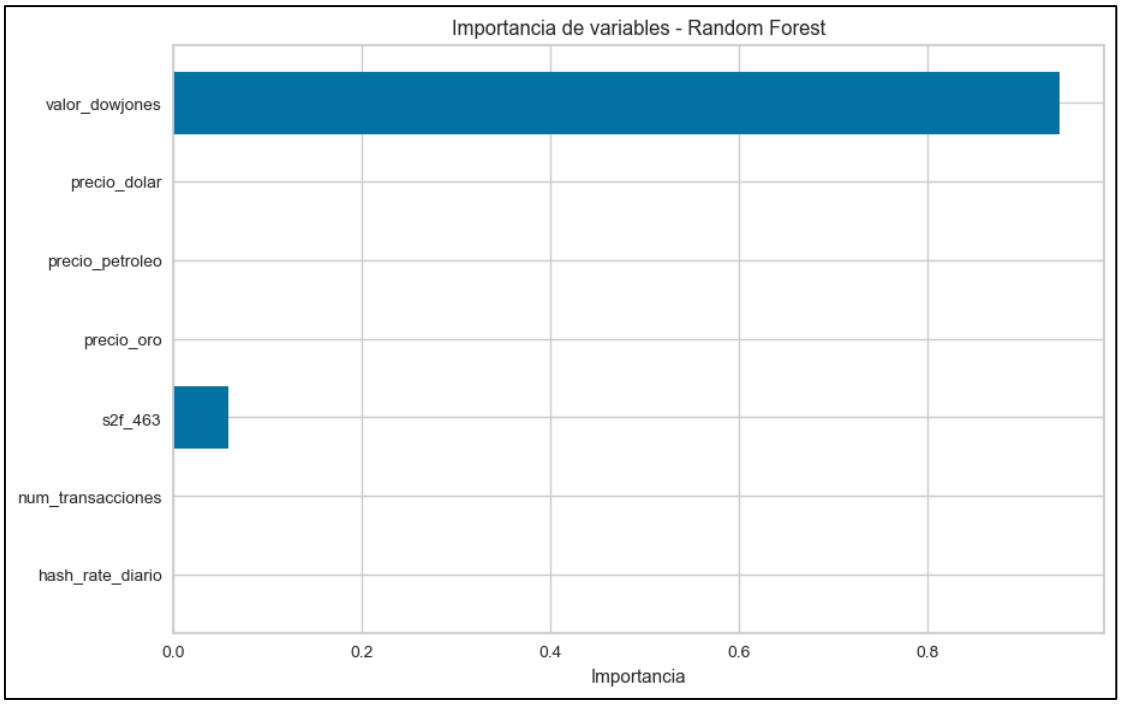
Imagen 20 Ajuste de los hiperparámetros por validación cruzada (II)

```
    scores = cross_val_score(model_rf, X_train, y_train, cv=5, scoring='r2')
    r2 = -scores.mean()

    return r2

best_rf_params = fmin(fn=objective_rf, space=space_rf, algo=tpe.suggest, max_evals=100)

best_max_depth = (
    int(best_rf_params['max_depth']) if best_rf_params['max_depth'] is not None else None
)

best_rf_model = RandomForestRegressor(
    n_estimators=int(best_rf_params['n_estimators']),
    max_depth=best_max_depth,
    min_samples_split=best_rf_params['min_samples_split'],
    min_samples_leaf=best_rf_params['min_samples_leaf']
)
```

Fuente: Elaboración propia

Con todo esto, la importancia de cada variable en el modelo se explica por medio de la siguiente gráfica:

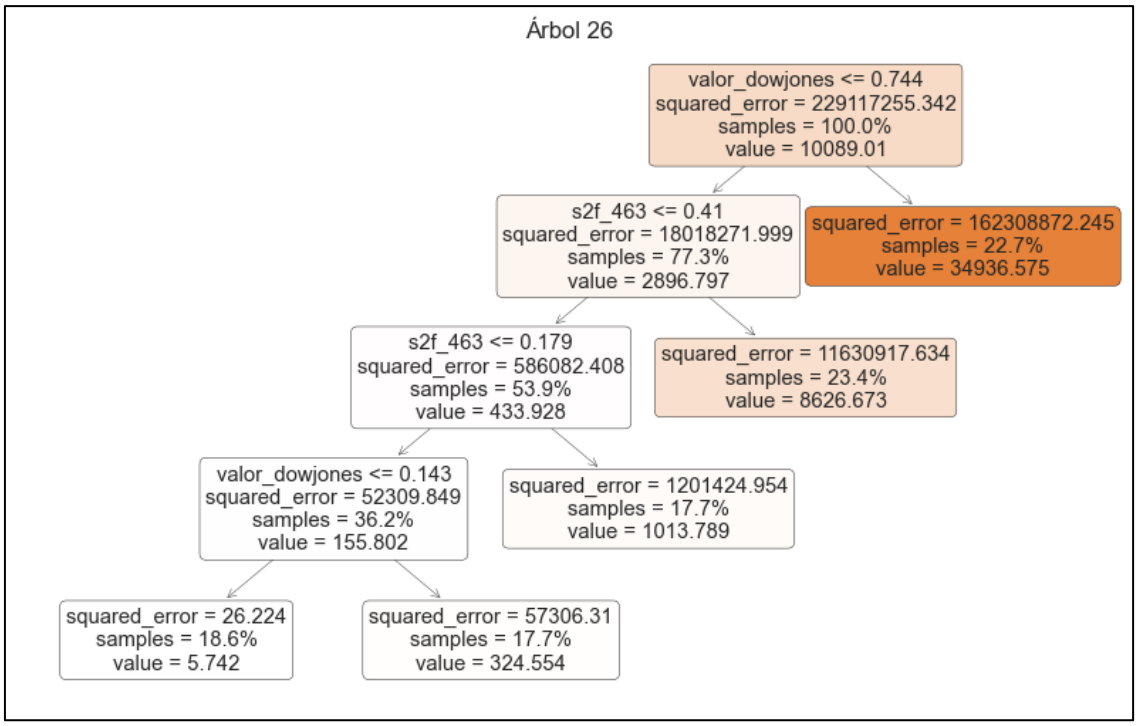
Imagen 21 Importancia de las variables del modelo *random forest*



Fuente: Elaboración propia

Se percibe que todo el modelo queda explicado principalmente por el valor del índice *dow jones* con una ligera ayuda de la variable que representa la ratio *stock-to-flow*. Esto significaría que la valoración del precio de Bitcoin estaría únicamente en función de los valores que fuese obteniendo este índice, sin tomar en consideración otras posibles cuestiones tanto de la propia red de Bitcoin como el número de transacción como de cuestiones externas a la red como el precio del dólar. A modo de ejemplo, uno de los árboles desarrollados por el modelo es:

Imagen 22 Árbol de decisión



Fuente: Elaboración propia

En este caso, el procedimiento de decisión del árbol seguiría la siguiente secuencia lógica. En primer lugar, observaría los valores de *dow jones* de cada observación y dividiría la muestra en función de los que tienen un valor superior a 0,744 y los que tienen uno inferior. Los primeros quedarían ya agrupados y representarían el 22,7% de la muestra con un precio de casi 35.000 dólares para Bitcoin. El segundo grupo se volvería a segmentar en función del *s2f_463*, proceso que se volvería a repetir en la siguiente hoja. En la última hoja se volvería a segmentar en función del valor del índice de *dow_jones.* Se comprueba en este caso como la variable de referencia para realizar el primer corte es *dow_jones* que durante el proceso es ayudada el valor de la ratio existencias-flujo.

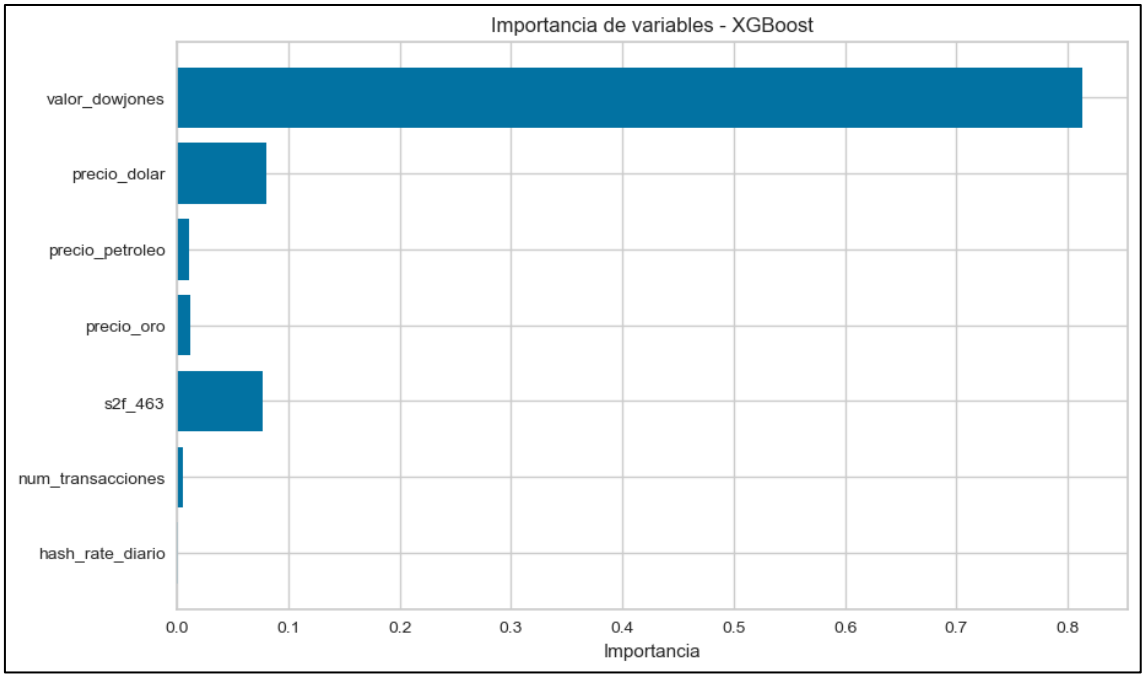
3.2.1.3 XGBoost

En este modelo, se utiliza del paquete *xgboost* de *pyhton* la función XGBRegressor para su desarrollo. Además, al igual que en modelo de *random forest*, se ha utilizado la validación cruzada, con la función *cross_val_score*, para ajustar los hiperparámetros del modelo. Este proceso sigue la misma casuística que el del *random forest*, con la diferencia de que los parámetros a optimizar aquí son el número de estimadores, la

profundidad máxima, la tasa de aprendizaje, la proporción de observaciones de entrenamiento y *gamma*.

Con la optimización de este modelo, se aprecia la siguiente importancia de cada variable:

Imagen 23 Importancia de las variables del modelo *XGBoost*



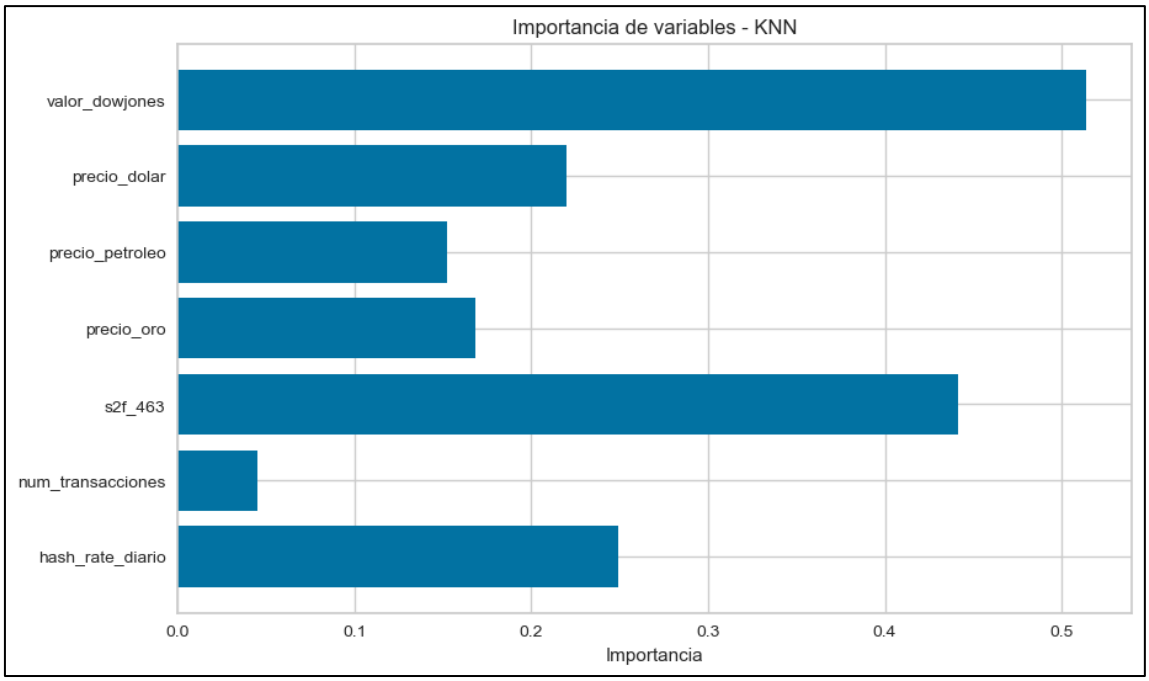
Fuente: Elaboración propia

Nuevamente, es el valor del índice de *dow jones* el que tiene una mayor importancia dentro del conjunto del modelo, superando el 80%. Sin embargo, en este modelo parece que un mayor número de variables tiene cierta importancia dentro del modelo, aunque ninguna alcanza una importancia superior al 10%.

3.2.1.4 K-Nearest Neighbor (KNN)

Este último modelo por su parte utiliza del paquete *skelarn.neighbors* la función *KNeighborsRegressor* para desarrollar el modelo de KNN. A su vez, la optimización de los hiperparámetros ha seguido el mismo proceso de ajuste que los dos modelos anteriores, por medio de la función *cross_val_score*. De esta forma, la importancia de sus variables queda desarrollada de la siguiente manera:

Imagen 24 Importancia de las variables del modelo de KNN



Fuente: Elaboración propia

Aunque la variable que representa el valor del índice *dow jones* vuelve a ser la más importante, su importancia relativa baja considerablemente hasta un 0,5 aproximadamente. Además, su importancia es muy similar a la de la variable *s2f_463*

3.2.2 Modelos predictivos.

Una vez desarrollados los modelos explicativos que han permitido comprender como se comportan los modelos, se preparan los modelos predictivos.

En primer lugar, como procedimiento común a los cuatros modelos se procedió a realizar la división entre el conjunto de entrenamiento y el de prueba. Al ser el modelo una serie temporal, se analiza el precio de Bitcoin por días, este procedimiento se realiza por medio de la función *TimeSeriesSplit* de *pyhton*. Por medio de este proceso, se garantiza el orden cronológico entre los dos conjuntos; es decir, que las observaciones que forman el conjunto de entrenamiento sean anteriores a las del conjunto de prueba. De esta manera, se evita que se tenga que predecir el precio de Bitcoin para una observación que se encuentra entre dos observaciones que han sido parte del conjunto de entrenamiento. Lo que se busca es que el conjunto de prueba esté formado por las primeras observaciones de la base de datos para que predigan el precio de Bitcoin de las

observaciones posteriores.

Este proceso se inicia con la función nombrada anteriormente que realiza tantas divisiones como se le indica en el código. Una vez hechas estas divisiones, se entrena los distintos modelos formados y se almacenan los resultados con el objetivo de quedarnos con aquel que ha tenido un menor MSE (error cuadradrático medio).

Imagen 25 División entre conjunto de entrenamiento y prueba

```
tscv = TimeSeriesSplit(n_splits=5)
models = []
metrics = []

for train_index, test_index in tscv.split(X):
    X_train, X_test = X.iloc[train_index], X.iloc[test_index]
    y_train, y_test = y.iloc[train_index], y.iloc[test_index]

    X_train = sm.add_constant(X_train)

    model_lr=LinearRegression()

    model_lr.fit(X_train, y_train)

    X_test = sm.add_constant(X_test)

    y_pred = model_lr.predict(X_test)

    # Almacena resultados
    mse = mean_squared_error(y_test, y_pred)
    models.append(model_lr)
    metrics.append(mse)

best_model_index = metrics.index(min(metrics))

# Obtén el mejor modelo y su correspondiente métrica
best_model = models[best_model_index]
best_metric = metrics[best_model_index]
```

Fuente: Elaboración propia

3.2.2.1 Modelo de Regresión Lineal

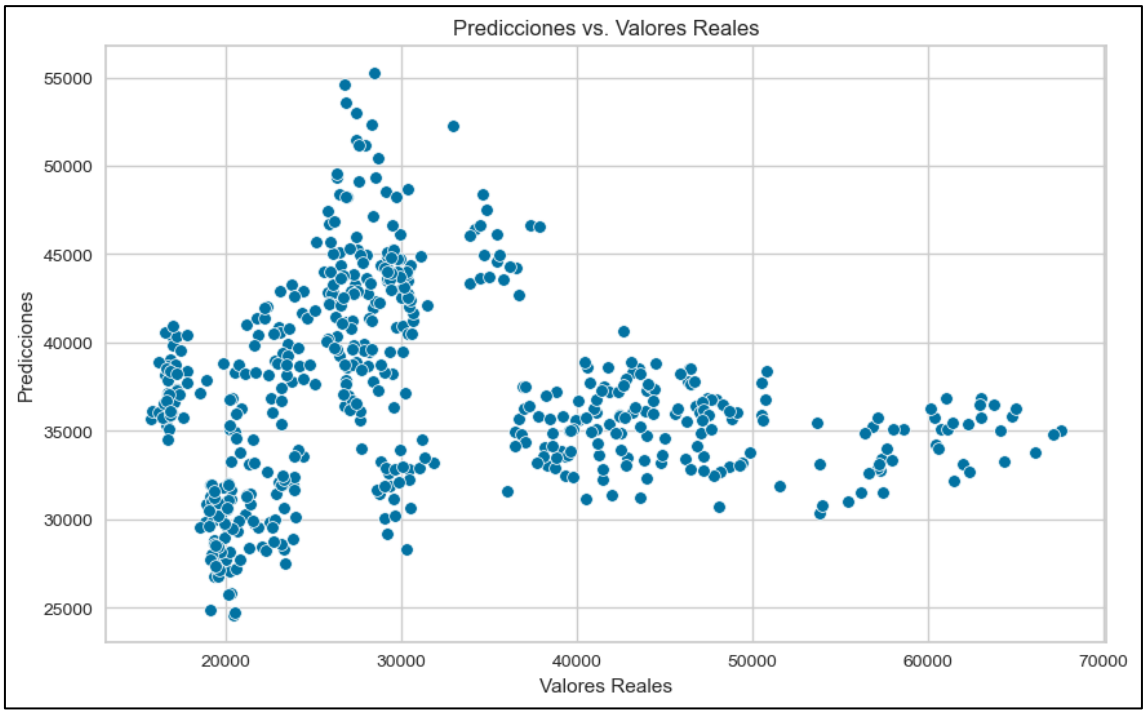
Una vez obtenido el mejor modelo de los 5 entrenados por el Split, se obtiene su valor de MSE y se grafican las diferencias entre los valores predichos y los valores.

Imagen 26 MSE del modelo de regresión lineal

```
Mejor modelo con MSE: 89756.57882624345
```

Fuente: Elaboración propia

Imagen 27 Diferencias entre las predicciones y los valores reales del modelo de regresión lineal



Fuente: Elaboración propia

Es innegable que tanto los valores obtenidos como el gráfico mostrado señalan que la capacidad predictiva del modelo es bastante limitada. La gráfica enseña que el reparto de los valores predichos por el modelo parece no seguir ningún patrón concreto. En todo caso parece que a medida que aumenta el valor real del precio de Bitcoin, el valor de la predicción disminuye en su conjunto.

3.2.2.2 Modelo de Random Forest

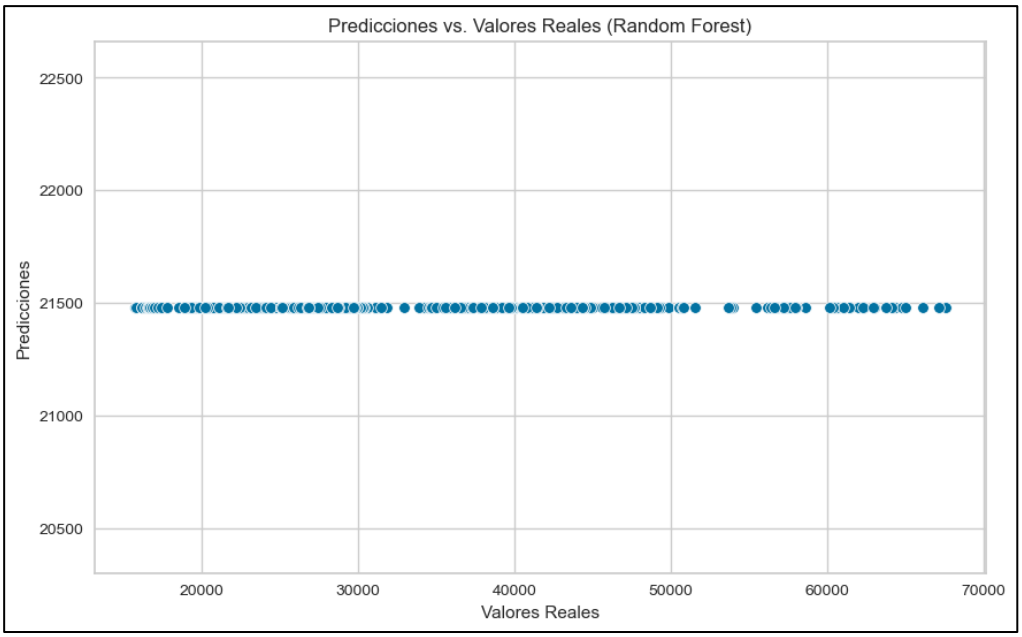
Al igual que en el modelo anterior, los resultados obtenidos son los siguientes:

Imagen 28 MSE del modelo de *random forest*

```
Mejor modelo con MSE: 70591.83683760812
```

Fuente: Elaboración propia

Imagen 29 Diferencias precio real y predicciones del modelo de *random forest*



Fuente: Elaboración propia

Se constata que el valor de MSE de este modelo mejora significativamente al modelo anterior. No obstante, en la gráfica se aprecia que el valor que predice el modelo para el precio de Bitcoin es un valor constante de 21.500 dólares, lo cual tampoco se podría entender como un resultado satisfactorio porque en la comparativa con el valor real de Bitcoin se observa una diferencia notable.

3.2.2.3 Modelo de XGBoost

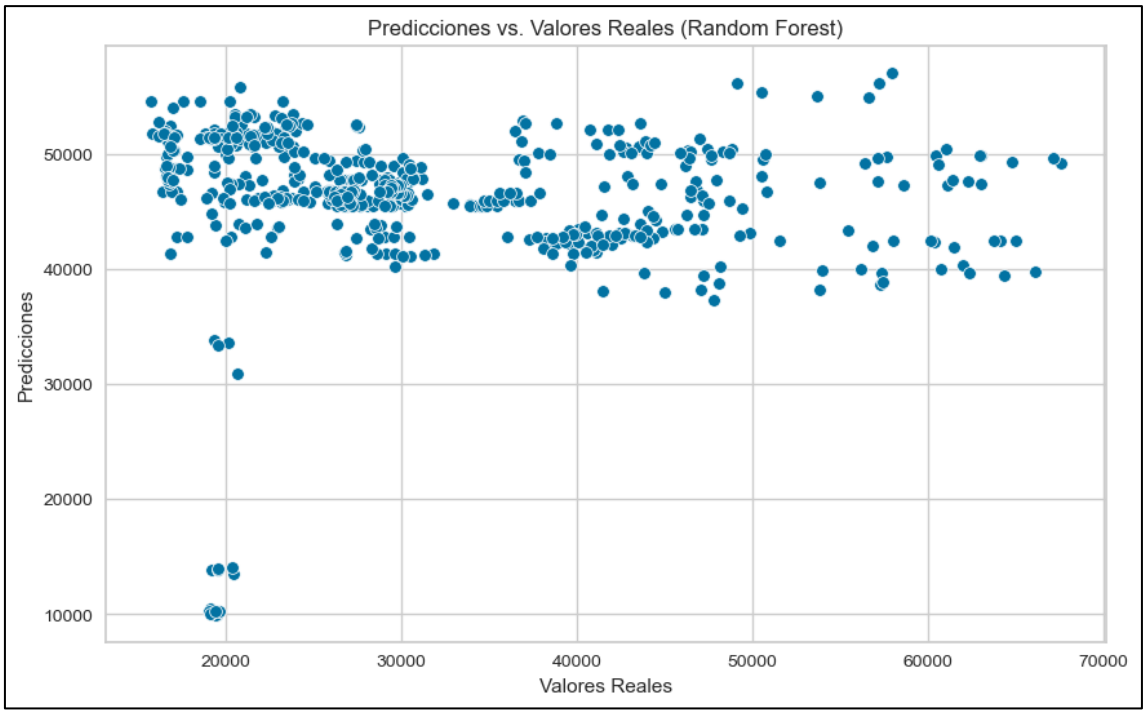
Los resultados para este modelo son los siguientes:

Imagen 30 MSE del modelo de XGBoost

```
Mejor modelo con MSE: 88403.75316353881
```

Fuente: Elaboración propia

Imagen 31 Diferencias precio real de Bitcoin y predicciones del modelo XGBoost



Fuente: Elaboración propia

Este nuevo modelo no mejora los resultados del modelo *random forest* en cuanto a MSE. Observando la diferencia entre los valores reales y predichos se denota que este modelo tiende a valorar el precio de Bitcoin entre los 40.000 y 50.000 dólares independientemente del valor real de Bitcoin. Ni siquiera, a medida que aumenta el valor real de la moneda es capaz de aumentar el valor predicho, aunque sea dentro de ese intervalo en el que predice la mayoría de los precios.

3.2.2.4 Modelo de KNN

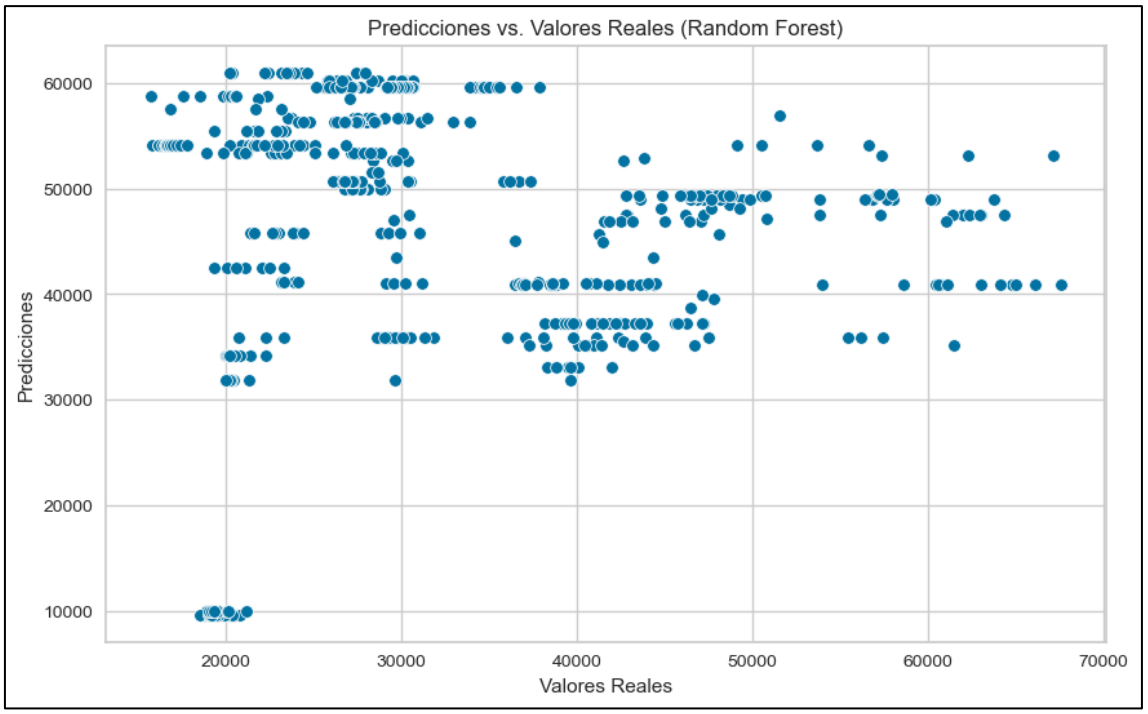
Los resultados obtenidos para este modelo son los siguientes:

Imagen 32 MSE del modelo de KNN

```
Mejor modelo con MSE: 85465.34604659305
```

Fuente: Elaboración propia

Imagen 33 Diferencias entre el precio real de Bitcoin y las predicciones del modelo KNN



Fuente: Elaboración propia

Este modelo tampoco mejora al modelo de *random forest*, que se establece como el mejor modelo de los 4. Omitiendo unas observaciones que agrupan en torno a los 10.000 dólares, el resto de las observaciones se reparten por encima de los 30.000 dólares, pero sin seguir ningún criterio concreto.

4. CAPÍTULO IV. CONCLUSIONES

- El modelo con mejor capacidad predictiva desarrollado es el modelo de *random forest* que obtiene el error cuadrático medio más bajo y parece ser el único que sigue un criterio estable dentro de sus predicciones.
- No obstante, ninguno de los 4 modelos parece demostrar una capacidad predictiva alta a la vista de sus valores de error cuadrático medio y la gráfica comparativa entre las predicciones y el valor real del precio de Bitcoin.
- Por ello, cabría considerar que estos modelos no mejorarían lo realizado hasta el momento por el modelo *stock-to-flow* al que se trataba de perfeccionar. De esta manera, no habría un nuevo modelo que pudiese sustituirlo como nuevo modelo de referencia dentro del mercado.

5. CAPÍTULO V. BIBLIOGRAFÍA

Ammous, S. (2016, September 1). *Blockchain technology: What is it good for?*. SSRN. Disponible en https://deliverypdf.ssrn.com/delivery.php?ID=194116069100029016014093018004101122123035068045044085007112018075102009006126072066019021099031023051029090104073087064065024054018089018064000086127096025020080072002007039028083078001104067122102088069001109004094094007080019026003031096112029085111&EXT=pdf&INDEX=TRUE

Ammous, S. (2022). *El Patrón Bitcoin: La Alternativa Descentralizada a Los Bancos Centrales*. Deusto.

Antonopoulos, A. [aantonop] (22 de abril de 2017). *Blockchain vs. Bullshit: Thoughts on the Future of Money [Classic Bitcoin & Open Blockchain Talk]*. Disponible en https://www.youtube.com/watch?v=SMEOKDVXlUo

Ashmore, D. (2023, March 1). *Understanding the bitcoin stock-to-flow model*. Forbes. Disponible en: https://www.forbes.com/advisor/investing/cryptocurrency/bitcoin- stock-to-flow-model/#:~:text=The%20stock%2Dto%2Dflow%20model%20is%20commonly%2 0used%20to%20price,that%20is%20created%20each%20year

Bashir, I. (2020). *Mastering blockchain: A deep dive into distributed ledgers, consensus protocols, Smart Contracts, Dapps, cryptocurrencies, Ethereum, and more*. Packt Publishing.

Bitbo. (n.d.). *Bitcoin stock to flow model live chart*. Charts Bitbo. Disponible en: https://charts.bitbo.io/stock-to-flow/

Bouoiyour, J., & Selmi, R. (n.d.). The Bitcoin price formation: Beyond the fundamental sources. Disponible en: https://arxiv.org/ftp/arxiv/papers/1707/1707.01284.pdf

Ciaiana, P., Rajcaniovab, M., & Kancs, d'Artis. (n.d.). The Economics of Bitcoin Price Formation. Disponible en: https://www.tandfonline.com/doi/full/10.1080/00036846.2015.1109038

Foss, G., & Sansone, J. (2022, March 30). *BITCOIN PORTFOLIO INSURANCE: BTC VALUATION MODELS*. Bitcoin Magazine. Disponible en: https://bitcoinmagazine.com/markets/exploring-bitcoin-valuation-models

Internet growth statistics 1995 to 2023 - the global village online. Internet World Stats. (n.d.). Disponible en: https://www.internetworldstats.com/emarketing.htm

Kristoufek, L. (2015). What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis. Disponible en: https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0123923&type=printable

Lin, I.-C., & Liao, T.-C. (n.d.). Survey of blockchain security issues and challenges. Disponible en: https://iefpedia.com/english/wp-content/uploads/2017/12/A-Survey-of-Blockchain-Security-Issues-and-Challenges.pdf

Meynkhard, A. (2019, November 28). *Fair market value of bitcoin: Halving effect*. Researchgate. Disponible en: https://www.researchgate.net/publication/337606604_Fair_market_value_of_bitc oin_halving_effect

Nakamoto, S. (2008, October 31). *A peer-to-peer electronic cash system*. Bitcoin. Disponible en: https://bitcoin.org/en/bitcoin-paper

Napoletano, E. (2023, February 16). *Proof of work explained*. Forbes. Disponible en: https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-work/#:~:text=Proof%20of%20work%20is%20a%20consensus%20mechanism% 20to%20choose%20which,don't%20cheat%20the%20system

Neo Wave Pattern and theory explained. MTrading. (2023, February 15). Disponible en: https://mtrading.com/education/articles/forex-strategy/neo-wave-theory-and- pattern-explained

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017, March 20). Blockchain. Disponible en: http://www.cs.unibo.it/~danilo.montesi/CBD/Articoli/2017Blockchain.pdf

Notariya, H. (2023, September 15). *Bitcoin: Michael Saylor's amazing prediction will soon come true*. BeInCrypto. Disponible en: https://beincrypto.com/michael-saylor-bitcoin-prediction/

Pastor , J. (2023, March 10). *¿Qué es el halving bitcoin y qué función tiene?*. Bit2Me Academy. Disponible en: https://academy.bit2me.com/que-es-

halving-bitcoin/

Perez, R. (2022, May 16). *What is the difference between Bitcoin and Bitcoin?*. Bitnovo Blog. Disponible en: https://blog.bitnovo.com/en/difference-bitcoin-and-bitcoin- uppercase-lowercase/

PlanB. (2019, March 22). *Modeling bitcoin value with scarcity*. Medium. Disponible en: https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity- 91fa0fc03e25

Saylor, M. (2023, October 22). *Microstrategy bolsters bitcoin holdings amid rising performance by Investing.com*. Investing.com. Disponible en: https://www.investing.com/news/cryptocurrency-news/microstrategy-bolsters-bitcoin-holdings-amid-rising-performance-93CH-3204958

Schär, F. (2020, April 21). *Understanding the bitcoin halving*. CfC St. Moritz. Disponible en: https://cfc-stmoritz.com/blog/understanding-the-bitcoin-halving

Schiff, P. (2023, October 24). *Bitcoin at $35,000: Peter Schiff predicts crash ahead of ETF verdict*. U.Today. Disponible en: https://u.today/bitcoin-at-35000-peter-schiff-predicts-crash-ahead-of-etf-verdict

Soros, G. (2008, January 22). The Worst Market Crisis in 60 years. Disponible en: https://www.ft.com/content/24f73610-c91e-11dc-9807-000077b07658

Tadvi, A. A. (2018, March). Bitcoin Price Prediction. Disponible en: https://www.multidisciplinaryjournal.in/assets/archives/2018/vol3issue2/3-2-286- 297.pdf

What is blockchain technology - IBM Blockchain. IBM. (n.d.). Disponible en: https://www.ibm.com/topics/blockchain

Zheng, Z., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. Disponible en: https://www.henrylab.net/wp-content/uploads/2017/10/blockchain.pdf