Maestría en Finanzas

Bitcoin en tiempos de crisis e incertidumbre

Autoría: Bahl, Nahuel Ezequiel
Año académico: 2023

UNIVERSIDAD TORCUATO DI TELLA

Trabajo Final de Graduación

Maestría en Finanzas UTDT

Año Académico **2023**

Alumno: Nahuel Ezequiel Bahl

Tutor: Diego Iaccarino

Bitcoin en tiempos de crisis e incertidumbre

1. Abstract

Esta tesis explora el papel del BITCOIN en tiempos de incertidumbre y su potencial como depósito de valor y medio de intercambio. La primera parte de la tesis ofrece una visión general de las criptomonedas, sus definiciones, funciones y características únicas. La tesis también profundiza en el campo de la criptografía y su importancia para asegurar las transacciones de criptomonedas. La segunda parte de la tesis se centra en la tecnología que hay detrás de las criptomonedas, en concreto la cadena de bloques (*blockchain*), y su arquitectura, funciones y potencial para revolucionar nuestra forma de hacer negocios.

La tercera parte de la tesis ofrece un análisis detallado de BITCOIN, su oferta, demanda y características únicas. También exploramos su potencial como cobertura contra las recesiones económicas y cómo se compara con activos tradicionales de inversión como el oro, los bonos y las acciones. Por último, la tesis examina la reacción de BITCOIN ante acontecimientos macroeconómicos y monetarios

El propósito de este trabajo es analizar si BITCOIN, la moneda digital descentralizada más importante del mundo. Puede convertirse potencialmente en un activo de refugio y resguardo de valor frente crisis económicas y tiempos de incertidumbre financiera.

1. Introducción

La aparición de las criptomonedas, encabezadas por el BITCOIN, ha aportado una nueva dimensión al mundo financiero. El creciente interés por las monedas digitales ha puesto de manifiesto la necesidad de comprender en profundidad esta innovadora clase de activos. El objetivo de esta tesis es explorar las características y funciones de las criptomonedas, su tecnología subyacente y su papel en el sistema financiero mundial y principalmente analizar BITCOIN y su comportamiento en tiempos de incertidumbre con el objetivo de analizar si BITCOIN puede ser considera un activo de resguardo de valor como lo es el oro.

La primera parte de esta tesis ofrecerá una introducción detallada al concepto de criptodivisas, sus definiciones y sus funciones. También examinaremos los diferentes tipos de criptomonedas y sus características únicas. Además, profundizaremos en el campo de la criptografía, que es la base de la seguridad de las criptodivisas. Exploraremos las distintas clasificaciones de la criptografía, incluidas las firmas digitales, y cómo se utilizan para asegurar las transacciones.

Luego por otra parte la tesis se centrará en la tecnología que hay detrás de las criptomonedas, concretamente en la cadena de bloques. Analizaremos la arquitectura de la cadena de bloques, sus funciones y cómo garantiza la seguridad y la transparencia de las transacciones de criptomonedas. Además, discutiremos el concepto de contratos inteligentes y su potencial para revolucionar la forma en que hacemos negocios.

Después entenderemos el funcionamiento de BITCOIN, la criptodivisa más prominente del mercado. Exploraremos las características de BITCOIN, su oferta y demanda, y cómo se ha utilizado como depósito de valor y medio de intercambio. Además, discutiremos las características únicas de BITCOIN y cómo se diferencian de los activos tradicionales de inversión, como el oro, los bonos y las acciones.

Por otra parte, examinaremos cómo responde BITCOIN a los acontecimientos macroeconómicos. Analizaremos su reacción ante noticias significativas tanto macroeconómicas como monetarias. Esta investigación proporcionará información sobre el potencial de BITCOIN como cobertura contra las recesiones económicas y su impacto global en el sistema financiero mundial.

En conclusión, esta tesis pretende proporcionar una comprensión global de las criptomonedas, su tecnología subyacente y el papel de BITCOIN en el sistema financiero mundial y su uso como activo de resguardo de valor en tiempos de incertidumbre financiera.

2. Criptomonedas

2.1 Definición, funciones y valor

Las criptomonedas son activos digitales que utilizan un cifrado criptográfico con el cual garantizan su titularidad al poseedor de las mismas y aseguran la integridad de las transacciones.

Estas criptomonedas funcionan independientemente de un gobierno o banco central que las regule, como sucede con el dinero tradicional. Tienen la peculiaridad de que pueden ser transferidas entre usuarios sin la necesidad de un intermediario financiero, como bancos o entidades crediticias.

Al no estar reguladas por ningún ente gubernamental o financiero, las criptomonedas son consideradas descentralizadas, esto se debe a que estas están basadas en tecnología [1]*blockchain*, que se puede pensar como un libro contable descentralizado en el cual se registran las transacciones de manera segura y transparente. Cada transacción es verificada por un grupo de nodos computacionales de la red de dicha moneda, lo que garantiza su validez y dificulta que una entidad o grupo de personas manipule o controle la red. Algunas de las funciones básicas de las criptomonedas son (Andrew Loo, febrero 2023):

- Medio de intercambio: Las criptomonedas pueden intercambiarse por bienes y servicios como se hace con el dinero tradicional. A su vez una gran ventaja de las criptomonedas son las bajas comisiones por transferencias internacionales y también elimina el problema de conversión de divisas entre distintos países.
- Reserva de Valor: Las criptomonedas sirven como reserva de valor como lo hacen las monedas tradicionales fuertes como el euro y el dólar. Además, algunas personas las utilizan para proteger sus ahorros en momentos de alta inflación o inestabilidad económica. Así también frente a devaluaciones de moneda nacional como sucede en Argentina.
- Inversión y especulación: Se puede invertir y especular en criptomonedas de igual manera que se hace con bonos y acciones en el mercado bursátil tradicional. A su vez también se pueden hacer o pedir préstamos para conseguir rentas pasivas a través de lo que se conoce como "[2]*Defi"*.
- Privacidad: Las criptomonedas ofrecen funciones que permiten a los usuarios realizar transacciones de forma privada y anónima. Lo cual ayuda al usuario a mantener confidencialidad en sus transacciones.

El Valor de las criptomonedas está determinado casi en su totalidad por la oferta y demanda del mercado, excluyendo las monedas estables, las cuales mantienen su paridad con el valor que tienen preestablecido. En su mayoría monedas tradicionales como dólar/euro.

El ecosistema de las criptomonedas ha crecido de manera exponencial en los últimos años *Figura 1*, llegando a superar a la industria de las telecomunicaciones en 2021. (NGRAVE, 2021).
En 2021 solo BITCOIN llego a tomar el sexto lugar en la base monetaria del planeta, séptimo lugar cuando se consideran también el oro y la plata (Marty Bent, 2021).

[1] BLOCKCHAIN: Tecnología de registro digital de transacciones in necesidad de intermediarios centralizados
[2] DEFI: "Decentralized Finance" Nuevo sistema financiero construido sobre tecnología *blockchain*

Figura 1, *Capitalización total de mercado de criptomonedas*

Nota: Este grafico muestra la capitalización de mercado total de criptomonedas a nivel global, con un total de 12.298 de monedas rastreadas en 666 intercambios al 18 de febrero de 2023.
Fuente: CoinGecko, Gráficos globales. https://www.coingecko.com/es/global-charts

2.2 Tipos de criptomonedas

Dentro del ecosistema cripto existen diferentes tipos de criptomonedas, cada una con sus características y rasgos que las distinguen de las demás. Aunque la mayoría de las mismas comparten los mismos atributos generales, todas se basan en la tecnología *blockchain*. Podemos diferenciarlas en cuatro grupos (Andrew Loo, 2023): criptomonedas de pago, tokens de utilidad, monedas estables y monedas digitales de bancos centrales (CBDC por sus siglas en ingles).

- Criptomonedas de Pago: Las criptomonedas de pago tienen el propósito de ser un medio de intercambio, pero además buscan cumplir la función de convertirse en el nuevo efectivo electrónico y que éste sea puramente [3]*Peer to Peer* para así facilitar transacciones. Dado que este tipo de criptomonedas son pensadas para ser una moneda de uso general, tienen un *blockchain* especializado y dedicado solo a este propósito (el de ser un método de pago). Lo que significa que sobre el *blockchain* de estas monedas no se pueden ejecutar[4] *contratos inteligentes* tampoco aplicaciones descentralizadas (Andrew Loo, 2023). Además, estas criptomonedas tienden a tener

[3] Peer to Peer: Red descentralizada donde computadoras individuales pueden conectarse a la red y compartir recursos sin la necesidad de un servidor central
[4] Contratos inteligentes: Contratos digitales que se autoejecutan y aplican automáticamente los términos de un acuerdo entre partes

un número limitado de emisión, lo que las tiende a hacer deflacionarias y así al aumentar la demanda de las mismas con un numero finito de ellas en circulación, sus precios tienden a subir. Ejemplos de estas monedas son: BITCOIN y Dogecoin.

- Tokens de utilidad: Los tokens son activos criptográficos que están construidos sobre el *blockchain* de otra moneda (más adelante se explica esto en detalle). Los tokens de utilidad sirven a una o más funciones específicas pre establecidas en el *blockchain* sobre el que fue creado. Una particularidad de los mismos es que estos no tienen límite de creación, por lo tanto, son inflacionarios. Así que en general, es de esperar que el precio de muchos de estos, en donde no se tenga un buen cuidado de su emisión, la demanda de tokens tienda a caer con el tiempo. Como suele suceder con las monedas fiduciarias de los países que constantemente emiten efectivo. A su vez podemos subdividir estos tokens en subgrupos como:

    - Tokens de servicio: Ciertos proyectos criptográficos emiten este tipo de tokens que conceden al titular acceso o le permiten realizar o tomar algún tipo de acción en una red. Los usuarios pagan por este servicio con tokens de utilidad nativos del proyecto.

    - Tokens Financieros: El mejor ejemplo de este tipo de tokens es la moneda de [5]*Binance* (BNB, Binance coin). La cual fue creada para darle a sus tenedores descuentos en las comisiones de intercambio en su plataforma de compra/venta de criptomonedas. La mayoría de estos tokens se venden en un principio a través de un [6]ICO (*Initial coin offering*), que conecta en una fase inicial a los inversores con el proyecto.

    - Tokens de Gobernanza: Estos tokens dan a sus titulares la opción de votar sobre ciertas cosas dentro de una red de criptodivisas, estas cosas a decidir suelen ser significativas y permite a la comunidad decidir en forma descentralizada y así no dejar las decisiones a un grupo pequeño de control.

    - Tokens de Entretenimiento: Estos tokens suelen usarse para contenido de juegos y publicidad en línea. Los mismos otorgan a los usuarios que, tanto optan por ver ciertos anuncios o jugar ciertos juegos, la posibilidad de pagar a los creadores de contenido de los mismos.

- Criptomonedas estables: Estas criptomonedas están diseñadas para brindar un depósito de valor. Mantienen el mismo porque, aunque estén desarrolladas sobre *blockchain*, estas monedas pueden cambiarse por monedas fiduciarias, ósea que están vinculadas a una moneda física, la mayoría al dólar estadounidense. Que exista esto es super importante para el ecosistema cripto ya que las mismas brindan liquidez al mercado, siendo que la mayoría de las criptomonedas se intercambian por monedas estables. A su vez esto es una herramienta para manejar la volatilidad que tienen la mayoría de los cripto activos. Existen varios tipos de monedas estables, las más conocidas están gestionadas por organizaciones centralizadas, la más conocida es "Tether", estas monedas están respaldadas por activos financieros tradicionales de bajo riesgo como bonos soberanos de estados unidos y efectivo. Además, al estar controladas por estas organizaciones centralizadas permite que el control y respaldo de las monedas lo tenga en última instancia la organización y poder afrontar de manera activa cualquier inconveniente.
  Por otro lado, también existen monedas estables que pertenecen a organizaciones descentralizadas, la más conocida es "DAI", de "MakerDao". Estas monedas se rigen a través de un algoritmo por lo

[5] Binance: La Plataforma más grande del mundo, donde se compran y venden criptomonedas
[6] ICO: Oferta inicial de criptomonedas por el cual los inversores financian el Proyecto crypto en una primera etapa.

que no cuentan con intervenciones activas de un ente centralizado como en el caso anterior. Muchas de estas monedas han fracasado, un caso reciente es el de una moneda estable llamada "Terra". Esta moneda era descentralizada y se regia a través de un algoritmo, que frente a una fuerte caída de los activos que lo respaldaban perdió su paridad con el dólar hasta llegar a desaparecer. Estos son uno de los riesgos que conllevan ese tipo de monedas descentralizadas.

- Monedas digitales de bancos centrales: Estas monedas son cripto activos emitidos por bancos centrales de distintos países. Estos las emiten en forma de token o con un registro electrónico asociado a la moneda, vinculándola a la moneda nacional del país. La particularidad de estas monedas es que los bancos centrales tienen absoluto control sobre ellas, lo cual por un lado puede aumentar la eficiencia de pagos de una región y reducir sus costos transaccionales, pero por otro lado al estar totalmente controladas y supervisadas pierden el atractivo que comparten las criptomonedas y el efectivo, el anonimato y privacidad. Por el momento hay muchos países en la etapa de creación y búsqueda de la implementación de estas criptomonedas en sus bancos centrales. Aunque, cabe aclarar que, por ahora no hay ningún país que haya logrado su implementación por completo.

2.2.1 Diferencias entre criptomonedas y tokens

Dentro del ecosistema cripto se utiliza la palabra criptoactivos para todo. Pero hay que diferenciar entre dos grandes categorías. Criptomonedas y tokens (Kirsty Moreland, 2019).

- Criptomonedas: Estas monedas están desarrolladas sobre una red *blockchain* autónoma e independiente, el caso más conocido es BITCOIN. Estas monedas son creadas desde cero y su red está diseñada específicamente para lograr un objetivo determinado. Estos proyectos suelen inspirarse en tecnologías pasadas o en otras criptomonedas que se fusionan con una red o tecnología innovadora asignándole un propósito especifico a la misma. Por ejemplo, en el caso de BITCOIN su objetivo es ser un depósito de valor y método de intercambio resistente a cualquier efecto de censura, que a su vez tiene una política monetaria fija, segura e inmodificable. Otro caso muy conocido es Ethereum, esta criptomoneda es la moneda nativa de una plataforma de contratos inteligentes, con el propósito de crear programas computadorizados que se desarrollan en una red *blockchain* descentralizada. En ambos casos como se mencionó anteriormente, cada moneda esta desarrollada en su propia red *blockchain*, creada para un propósito y función específica.

- Tokens: Los tokens son criptoactivos que no tienen una red de *blockchain* propia, sino que estos viven dentro de otra red de *blockchain*. Pueden entenderse como un derivado de esa red. Son creados con propósitos distintos que la criptomoneda de su red nativa, pero se benefician de su tecnología. En otras palabras, los tokens pueden entenderse como contratos inteligentes derivados de una plataforma de contratos inteligentes. Siendo estos contratos inteligentes derivados de la red de *blockchain* primaria de la misma plataforma. Por ejemplo, Ethereum es una criptomoneda con su propia red de *blockchain* programable (podemos entender Ethereum como la plataforma de contratos inteligentes), a su vez a partir de Ethereum se derivan y crean, a través de un protocolo denominado [7]*ERC-20*, contratos inteligentes. Estos contratos podemos entenderlo como aplicaciones (un ejemplo de esto es [8]*MakerDao*) y sobre esta aplicación se crean tokens nativos con una función específica a esta aplicación (en el ejemplo de este caso

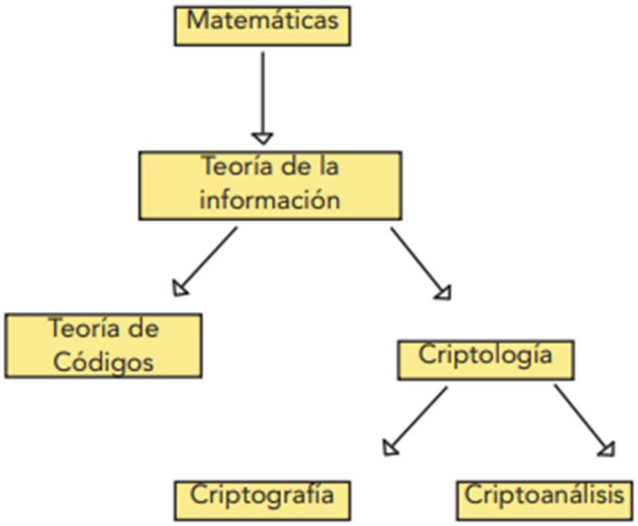
[7] ERC-20: Protocolo de estándar tecnico utilizado para crear tokens sobre la red de Ethereum
[8] MakerDao: Organización descentralizada que opera DAI sobre la red de Ethereum

[9]DAI). Con esta herramienta los usuarios pueden acceder a través de los contratos inteligentes de MakerDao a instrumentos de crédito y prestamos cripto utilizando los tokens de DAI. Todo esto ocurre sobre la red de *blockchain* programable de Ethereum. En simples palabras, sobre la red de *blockchain* de Ethereum, se programa una aplicación (MakerDao) que desde la cual se crean tokens nativos (DAI) que me permiten acceder a este mercado descentralizado de créditos cripto. Así como DAI es un token creado para una función específica sobre la red de *blockchain* de Ethereum, existen cientos de otros tokens con funcionalidades totalmente distintas dentro de la misma red *blockchain* de Ethereum.

2.3 Criptografía

La palabra criptografía proviene del griego Kriptos (sígnica ocultar) y Graphos (escritura), lo que significaba ocultar la escritura, más bien la aplicación de alguna técnica que haga ininteligible un mensaje. Dentro de la ciencia, la criptografía proviene de una rama de las matemáticas, iniciada por el matemático Claude Elwood Shannon en 1948, denominada "Teoría de la información". Esta rama a su vez se divide en Teoría de códigos y criptología. Donde a su vez la criptología se divide en criptoanálisis y criptografía (Gibrán Granados Paredes, julio 2006).

Figura 2: El origen de la criptografía



Fuente: https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

- Teoría de la información: está relacionada con las leyes matemáticas que rigen la transmisión y el procesamiento de la información. Se ocupa de la medición y representación de la información, así también de la capacidad de los sistemas de comunicación para transmitir y procesar la información.

[9] DAI: Moneda estable, que mantiene paridad con el dólar estadounidense, emitida por MakerDao

- Teoría de códigos: Es una especialidad matemática que estudia ciertos códigos detectores y correctores criptográficos utilizados en el proceso de enviar información. Trata ciertas leyes de codificación de la información para que la misma sea convertida en una señal que pueda usarse para su comunicación.

- Criptología: Es el estudio de la criptografía y criptoanálisis

- Criptoanálisis: es la ciencia que estudia los métodos que se utilizan para, a partir de mensajes cifrados, recuperar dichos mensajes en ausencia de las llaves o los elementos con los que los mismos fueron cifrados.

- Criptografía: es la ciencia que diseña funciones o dispositivos capaces de transformar mensajes legibles a mensajes cifrados de tal manera que esta transformación (cifrado) y su inversa (descifrado) solo pueden ser factibles con el conocimiento de una o más llaves (dispositivo o clave)

A los fines de este trabajo de investigación, se hará énfasis con un gran nivel de detalle a la criptografía, que es lo que nos permitirá entender el funcionamiento y diseño de las criptomonedas, particularmente BITCOIN.

2.3.1 Criptografía y seguridad

El uso de sistemas criptográficos emplea herramientas y recursos que nos permiten proteger la información en cuestión del peligro de ser interceptada o revelada a terceras partes que no están involucrada en la dinámica del evento emisor/receptor. Estas herramientas además protegen a los sistemas informáticos involucrados que están a cargo de administrar esta información. A razón de toda esta necesidad de proteger la información y los sistemas que lo administran surge el término de seguridad informática o seguridad de la información. Este término hace referencia a un conjunto de reglas, planes y acciones que permiten asegurar la información manteniendo ciertas propiedades y ofreciendo ciertas garantías. Estas propiedades son las siguientes, que a su vez son las primitivas criptográficas (Gibrán Granados Paredes, julio 2006):

- Confidencialidad: Convertir un mensaje desde su forma “legible” a una “cifrada” y viceversa. O sea que la información sea accesible solo para aquellos que están autorizados

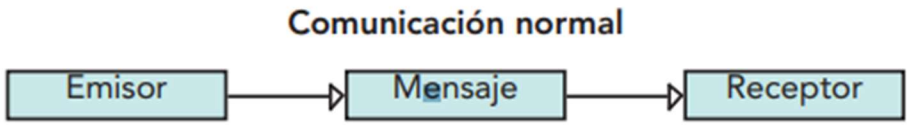
- Integridad: Garantizar que un mensaje llega a destino sin alteraciones por parte de un adversario. A su vez que la misma solo pueda ser creada y modificada por quien este autorizado a hacerlo.

- Disponibilidad: Que la información debe ser accesible para su consulta o modificación cuando se requiera y se pueda verificar la identidad de quien envía el mensaje.

Para garantizar la seguridad de la información tienen que cumplirse las propiedades mencionadas anteriormente, aquí es donde entra en acción la criptografía, ya que a través de métodos criptográficos se buscan garantizar estas propiedades. Veamos a continuación los siguientes casos de comunicación partiendo de una comunicación normal y atravesando etapas hasta llegar a la intercepción y corrupción del mismo.

En este primer caso se puede observar una comunicación normal, aquí no existe ningún problema de seguridad informática. El mensaje es recibido por el receptor sin ningún tipo de modificaciones.

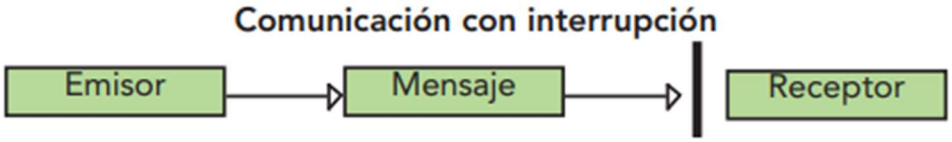
Figura 3. Comunicación normal



Fuente: https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

En un segundo caso, podemos observar uno de los problemas más importantes que existen, el de la interrupción de la transmisión del mensaje, la misma puede ser ocasionada por fallos dentro del sistema, siendo de forma intencional o natural. Aquí se puede observar un problema de disponibilidad ya que la información que estaba intencionada a ser recibida por el receptor, no está llegando a destino por algún motivo.

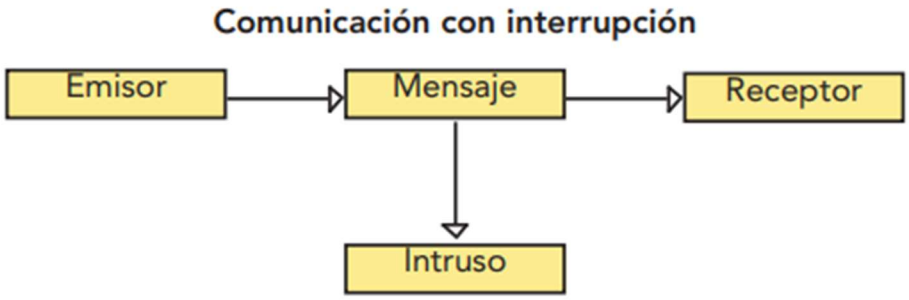
Figura 4. Comunicación con interrupción



Fuente: https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

La interceptación de información por parte de entidades externas (intrusos) al sistema es algo muy frecuente en comunicación, ya que muchas transmisiones se envían a través de protocolos de conocimiento público y los mensajes no reciben ningún tratamiento especial, es decir, se envían de la misma manera en la que fueron generados, lo único que se realiza es observar lo que pasa por el canal sin ningún tipo de alteración. A esto se lo puede entender como un problema de confidencialidad.

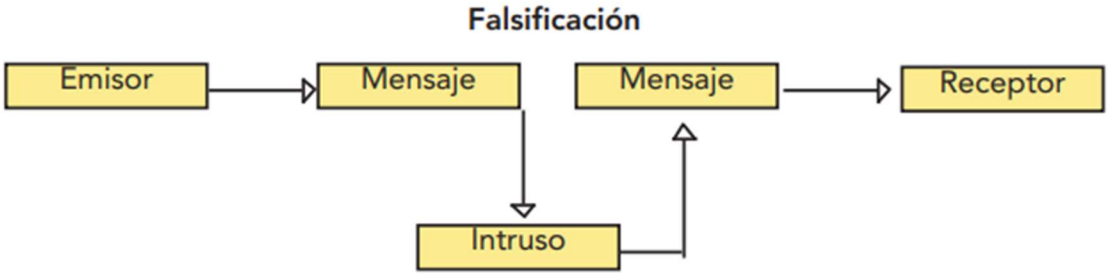
Figura 5 comunicación con interceptación



Fuente: https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

Otro problema muy grande en las comunicaciones es el de suplantación de identidad, en otras palabras, falsificación. Esto se da cuando el intruso intercepta y toma posesión del mensaje, se apropia del mismo y de la identidad del remitente. Produciendo así un nuevo mensaje con la identidad del que lo emitió. Aquí se pueden observar problemas de confidencialidad e integridad.

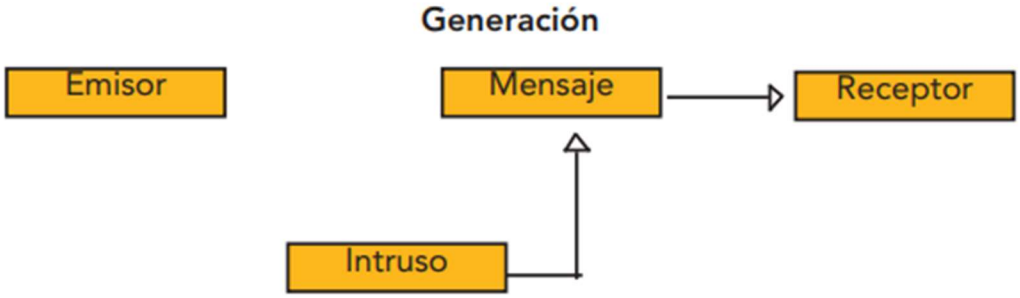
Figura 6. Comunicación con falsificación



Fuente: https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

Finalmente, el mensaje se genera a través de un intruso, siendo el fin del mismo engañar al receptor. Esto es un gran problema de integridad. El receptor del mensaje piensa que el mensaje proviene de un remitente confiable y valido. Mientras que, en realidad el mensaje ha sido intervenido y modificado.

Figura 7. Generación de una comunicación apócrifa



Fuente: https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

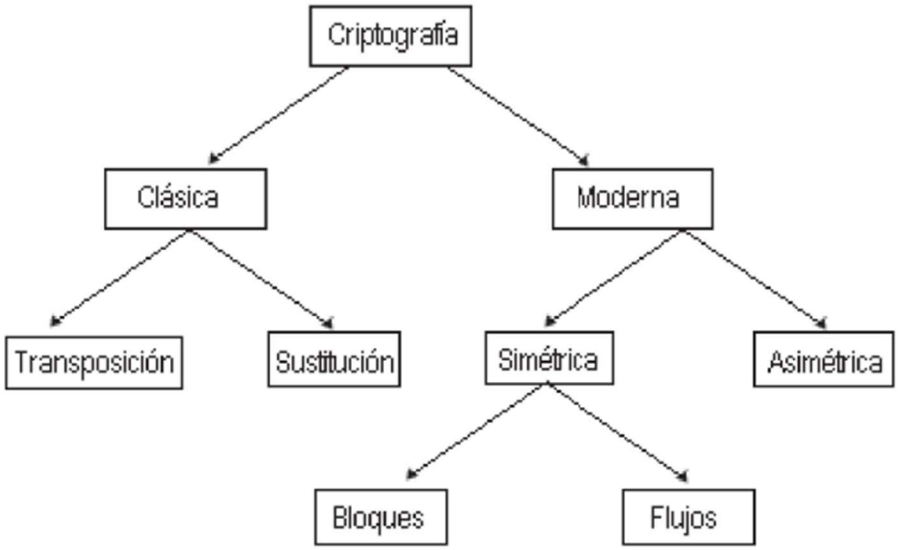
Se puede observar como una comunicación y un sistema informático se asemejan. Ya que en un sistema informático se guarda, procesa, envía y recibe información tal como en una comunicación. Entonces si existiera la manera de encontrar alguna forma de evitar los problemas mencionados anteriormente de integridad, disponibilidad y confidencialidad, podríamos decir que tendríamos un sistema seguro, pero para hacer eso tendría que aislarse el sistema de los posibles intrusos y lograr que el mismo sea anti fallos, lo cual es imposible. Lo que se puede hacer es crear herramientas y procesos que en cierta medida puedan garantizar que se cumplen estas tres propiedades. La disponibilidad se trata de resolver con [10]sistemas redundantes. La confidencialidad usando mecanismos que permitan que, aunque la información sea robada los ladrones no puedan acceder a ella o se garantice la imposibilidad de acceder a la misma hasta llegar al punto que se pierda la información. La integridad es la parte más difícil y se trata de obtener con el uso de mecanismos que permitan dar autorización de emitir o modificar partes del mensaje a ciertas entidades y posteriormente tener la posibilidad de verificar quienes y cuando fueron los que modificaron dicha información. Además de ver si en el viaje dicha información sufrió alguna modificación no autorizada. Esto se logra con la criptografía, de aquí nace la importancia y necesidad de la misma.

2.3.2 Clasificación de la Criptografía

La criptografía se clasifica históricamente en dos: Criptografía clásica y criptografía moderna.
La clásica se utilizó hasta aproximadamente la mitad del siglo XX. Es la criptografía "física" la no digitalizada. Los métodos que existían eran muy variados. Algunos simples y otros complicados de entender para la época, muchos de ellos nacieron a razón de las guerras, donde se necesitaban enviar mensajes de una manera encriptada por el caso en el que el enemigo tomara posesión del mismo, de manera que para éste sea ilegible. La moderna se inició después de tres hechos: el primero fue la publicación de la "Teoría de la Información" por Shannon; el segundo, la aparición del estándar del sistema de cifrado DES (*Data Encryption Standard*) en 1974 y finalmente con la aparición del estudio realizado por Whitfield Diffie y Martin Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifrado, denominado cifrado de llave pública en 1976. (Gibran granados paredes, julio 2006). Ambos tipos de criptografía se clasifican de acuerdo a los métodos que utilizan para cifrar los mensajes.

[10] Sistemas redundantes: Los sistemas redundantes se basan en duplicar elementos de un sistema de control de forma tal que el sistema pueda continuar su proceso, aunque componentes dentro del sistema fallen

Figura8, Clasificación de la criptografía



Fuente: https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=

2.3.3 Criptografía Clásica

Esta criptografía es muy antigua. Sus técnicas eran muy astutas. Este tipo de criptografía se usaba entre personas influyentes para compartir secretos entre sí. También información que no debía ser de público conocimiento. Pero especialmente se utilizaba para enviar coordenadas o instrucciones en momentos de conflicto y combate. Una particularidad y diferencia importante con la criptografía moderna es que, en la clásica, los algoritmos de estos sistemas se mantenían ocultos y nunca eran revelados.

La criptografía clásica, también se encargaba de construir maquinas (especialmente a base de engranajes). Transformaban un mensaje común en uno cifrado. El caso más conocido de estos es la maquina inventada por Arthur Scherbius (más conocida como enigma) utilizada por los alemanes durante los conflictos de la Segunda Guerra Mundial. Dentro de esta criptografía clásica los métodos utilizados en el proceso de cifrado era el de transposición y sustitución (Gibrán Granados Paredes, julio 2006).

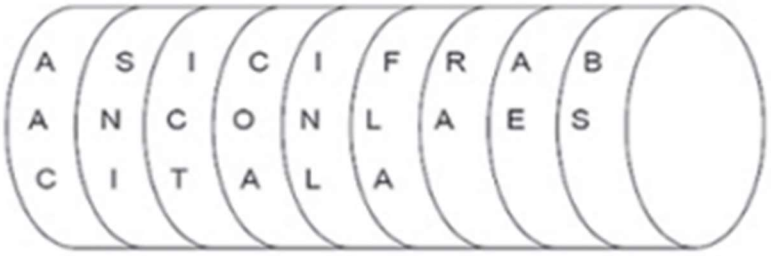
- Cifradores por transposición: Utilizaba una técnica que mediante un algoritmo especifico, reordenaba los caracteres del texto ya modificados.

- Cifradores por sustitución: Utilizaban la técnica de permutación en los caracteres del texto normal por otro carácter de un abecedario cifrado. A su vez, existían cifradores mono alfabético (solo había un único alfabeto en el proceso de transformación de texto a cifrar) o cifrador poli alfabético (en caso que en el proceso de cifrado se utilicen más de un alfabeto).

Para tener un mayor entendimiento de estos procesos, veremos los dos casos más conocidos uno de cifrado por transposición y otro por sustitución

- La Escitala: Este sistema utilizado por los griegos se basa en una cinta que se enrollaba alrededor de un palo en donde sobre dicho palo se escribía un mensaje en forma longitudinal. Luego de escribir el mensaje, se quitaba la cinta y era entregada a la persona. Esta cinta tenía caracteres en todo su contorno. La llave de este método se encontraba en el diámetro de este palo, de tal manera que la persona que estaba autorizada a recibir el mensaje, tenía en su posesión una copia exacta del mismo palo sobre el que se volvía a enrollar el mensaje recibido y solo así podía procesar y entender dicho mensaje de manera precisa.

Figura 9. La Escitala



Fuente: https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

- Cifrado Cesar: El cifrado César, también llamado desplazamiento de cifrado, es una de las técnicas más sencillas y populares de encriptación. Se basa en desplazar cada letra del abecedario un número fijo de posiciones hacia la derecha o hacia la izquierda. Por ejemplo, si desplazamos cada letra del alfabeto tres espacios a la derecha, la "A" se convierte en "D", la "B" en "E", y así sucesivamente, desde la "Z" hasta la "A". La cantidad de movimiento que se debe desplazar se denomina clave o valor de desplazamiento. Aquí se muestra un ejemplo del uso del cifrado César para encriptar el mensaje "HOLA" con una clave de 3 bits: En primer lugar, redactamos el mensaje sin formato de texto: "HOLA" Traspasamos cada palabra del texto a 3 espacios a la derecha. La H se convierte en K, la O en R, la L en O, y así sucesivamente. La clave para descifrar el mensaje es "KROD". Para descifrar el mensaje cifrado, solo debemos desplazar cada letra 3 posiciones a la izquierda, utilizando la misma clave que antes. Este procedimiento restaurará el mensaje original que fue alterado. Observado desde un punto de vista más matemático utilizado en criptografía. Podemos definir al módulo, siendo este una operación binaria que se realiza en los enteros positivos y se representa de la siguiente forma: *c = a mod b de tal forma que a, b y c son enteros positivos.*
  El valor de c al realizar la operación c = a modulo b es igual al residuo de dividir a entre b. Se puede observar claramente que 0<= c < b (Granados paredes, 2016). De este modo el cifrado cesar en forma matemática quedaría así:

Para Cifrar

$Ci = (3 + Mi) \bmod 27$
con i= 0,1,…,n ; n = número de letras del mensaje
donde *Ci* es la letra cifrada y *Mi* es la letra a cifrar
el alfabeto comienza con A = 0 , B=1, …, Z=26

Para descifrar:

$Mi = (Ci - 3) \bmod 27 = (Ci + 24) \bmod 27$
con i= 0,1,…,n ; n = número de letras del mensaje
donde *Ci* es la letra cifrada y *Mi* es la letra a cifrar
el alfabeto comienza con A = 0 , B=1, …, Z=26

Visto todo esto, cabe aclarar que, el cifrado César es sencillo de utilizar y aplicar. Es tan sencillo de descifrar que solo basta con realizar un análisis de tipo estadístico como un análisis de frecuencia. Dado esto, en la actualidad y básicamente desde el nacimiento de las computadoras, ya no se considera una técnica confiable de encriptación y se utiliza principalmente como parte de esquemas más complejos de encriptación o como parte de un enfoque educativo.

2.3.4 Criptografía Moderna

La criptografía actual se compone de dos tipos principales de técnicas criptográficas: la *criptografía de clave simétrica* y *la criptografía de clave pública*. El cifrado de clave simétrica se basa en la utilización de la misma clave secreta para cifrar y descifrar información. Este método es rápido y eficaz, pero requiere que la clave secreta sea compartida de forma segura entre el emisor y el receptor. La criptografía de clave pública, también conocida como criptografía asimétrica, utiliza un par de claves: una clave pública y una clave privada. La clave pública puede compartirse libremente y se utiliza para cifrar información, mientras que la clave privada se mantiene en secreto y se utiliza para descifrar la información. Este método tiene un mayor grado de seguridad porque nunca es necesario divulgar la clave privada. A continuación, para tener un mejor entendimiento, vamos a indagar sobre estos dos tipos de técnicas (Gibrán Granados Paredes, julio 2006)

Criptografía Simétrica

La criptografía simétrica o de llave secreta, es aquella que emplea un procedimiento matemático, un sistema de encriptación que, a través de una clave (llave) secreta, hace posible cifrar y descifrar un mensaje. Es posible observar en la siguiente figura que la línea punteada es el eje de simetría: lo mismo que existe en un lado es idéntico a lo que está en el otro lado, lo que evidencia el porqué, del uso de la palabra criptografía *simétrica.*

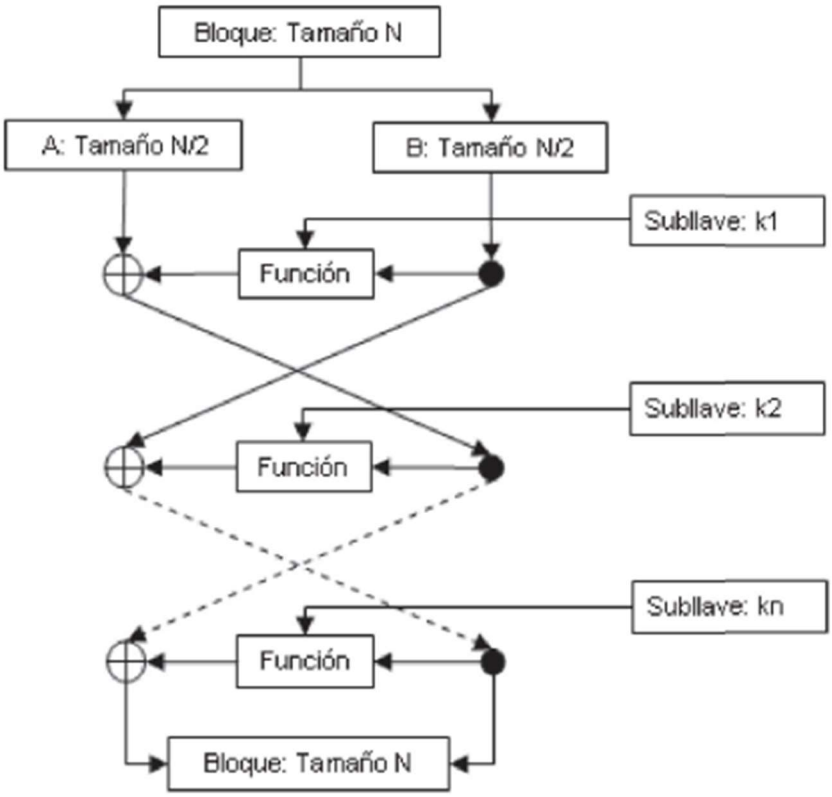
Figura 10. Criptografía Simétrica

Fuente: https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

Esta clase de criptografía tiene la particularidad de que utiliza únicamente una llave para encriptar y desencriptar. Por lo que si se encripta un mensaje "X" con una llave secreta "Y". Entonces el mensaje encriptado (llamémosle XY') solamente va a poder ser desencriptado con la llave "Y". Al mismo tiempo esta llave secreta debe ser compartida con todas las personas que se desea que reciban el mensaje y sean capaz de entenderlo. Este tipo de criptografía garantiza la propiedad de confidencialidad porque únicamente el tenedor de esta llave secreta, tendrá acceso a este mensaje. Este proceso tiene un problema. Si se quiere enviar el mensaje a muchas personas. El emisor deberá crear, para cada receptor, una llave secreta nueva. Esto implica la creación de muchas llaves secretas, lo que hace que la administración de todas estas sea muy difícil de llevar a cabo. A su vez la criptografía simétrica, se puede dividir en criptografía simétrica por bloques y criptografía simétrica de flujo.

- Criptografía simétrica por bloques: Este tipo de criptografía se basa en propuestas hechas por Horst Feistel, denominada "diseño de Feistel". La idea básica del diseño Feistel es dividir la información en dos mitades y aplicar una serie de rondas, cada una de las cuales manipula una de esas mitades basándose así en su otra mitad y en una clave secreta. El resultado de cada ronda se combina a su vez con la otra mitad y el proceso se repite durante varias rondas. Como se puede observar en la siguiente figura:

Figura 11. Cifrado por bloque de Feistel



Fuente:
https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

"Aquí podemos observar un bloque de tamaño N bits comúnmente N=64 o 128 bits se divide en dos bloques de tamaño N/2, A y B. A partir de aquí comienza el proceso de cifrado y consiste en aplicar una función unidireccional (muy difícil de invertir) a un bloque B y a una subllave k1 generada a partir de la llave secreta. Se mezclan el bloque A con el resultado de la función mediante un XOR. Se permutan los bloques y se repite el proceso n veces. Finalmente se unen los dos bloques en el bloque original" (Gibrán Granados Paredes, julio 2006)

- Criptografía simétrica de flujo: En este tipo de criptografía se realiza un cifrado "bit a bit". Esta es una técnica de cifrado, en donde los datos se codifican individualmente a través de un algoritmo de cifrado específico. Este algoritmo no tiene en consideración patrones o lógica. Este proceso se consigue llevar a cabo, a través de la aplicación de la operación "XOR". Aquí se usa un algoritmo determinístico que va generando bits que, junto a los bits del mensaje, se cifran mediante [11]XOR. Este tipo de criptografía es el que muchas veces se usa en los celulares.

[11] XOR: Es un operación criptográfica especifica que permite encriptar o desencriptar información a través de la combinación de la misma con una clave secreta. Es el bloque fundamental de muchos algoritmos criptográficos.

Figura 12. Criptografía simétrica de flujo

Fuente: https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

Criptografía Asimétrica

En la siguiente figura se puede observar el concepto de la llave publica criptográfica. Se puede apreciar que en la misma no hay simetría. Ya que de un lado de la figura estas se cifran o descifran con una llave pública mientras que del otro con una privada. De aquí es donde surge este concepto de criptografía asimétrica.

Figura 13. Criptografía Asimétrica

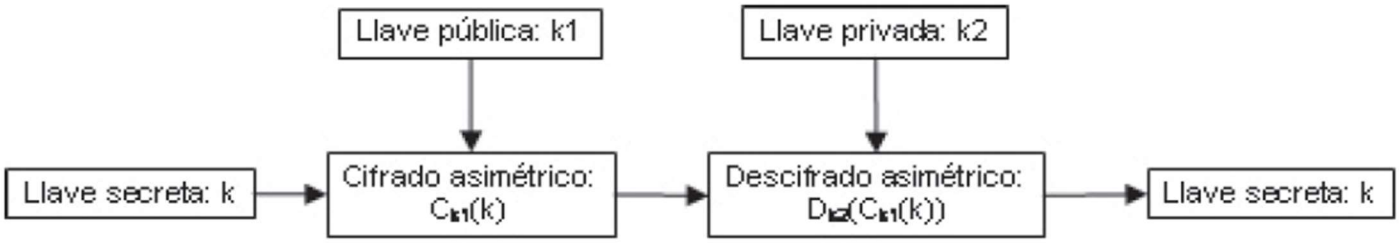
Fuente: https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

Hay que resaltar que en este tipo de criptografía, lo que se encripta con una llave puede desencriptarse con la otra. Es decir que podemos encriptar con la llave pública y desencriptar con la privada (y así en sentido

contrario). Este sistema tiene la ventaja de que el número de llaves que debo tener en mi posesión se reduce drásticamente. Si una persona quisiera enviar información encriptado a un número "x" de personas, necesitaría saber las "x" llaves públicas de cada una de estos individuos. Pero si "x" personas le quieren enviar un mensaje encriptado solo se requiere que las demás personas conozcan su llave pública. Así que mi único tema a verificar aquí es que esta llave pública realmente sea de la persona quien dice ser. Esta es la desventaja de la criptografía asimétrica: la autenticación de las llaves públicas.

Asumiendo el uso de criptografía asimétrica, el problema del intercambio de claves secretas puede resolverse. Esto consiste en enviar una clave confidencial a una persona para respaldar la comunicación cifrada entre ellos. El proceso implica cifrar la llave pública del destinatario previsto, De manera que el mensaje cifrado resultante se transmita de forma segura. La utilización de un sistema asimétrico con clave secreta hace imprescindible que se tenga una posesión exclusiva de la llave privada. Al descifrar el mensaje, se puede obtener la clave o llave secreta, como se ilustra en los pasos siguientes.

Figura 14. Intercambio de llaves secretas



Fuente: https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

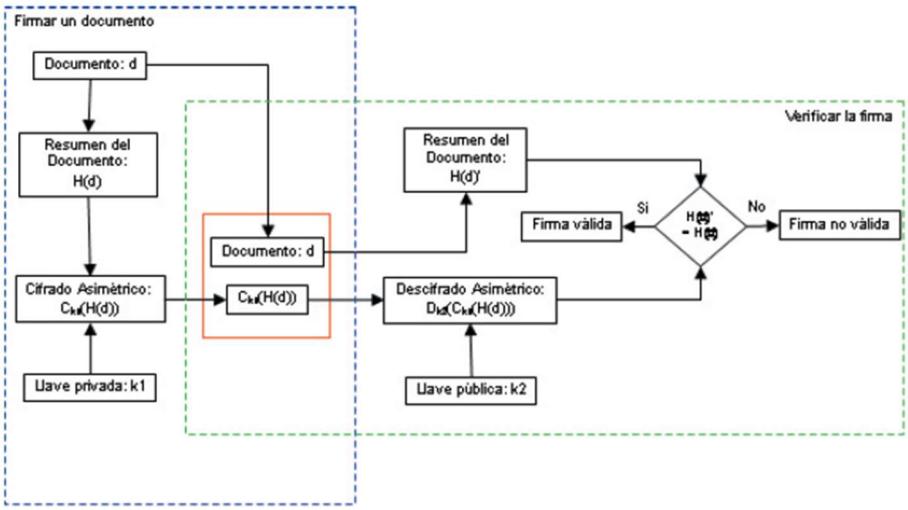
2.3.5 Firmas Digitales

La firma digital es una herramienta criptográfica que garantiza la autenticidad y la integridad de los documentos y mensajes digitales. Esencialmente, las firmas digitales, también conocidas como firmas electrónicas, se adhieren a los mensajes y documentos digitales, verificando su fuente y preservando su originalidad durante la transmisión. Para poder firmar electrónicamente un documento o mensaje, se utiliza la criptografía de clave pública.

Esta forma de cifrado asimétrico, *como fue explicada anteriormente,* depende de dos claves distintas: una clave privada y una clave pública. Mientras que el firmante mantiene en secreto la clave privada para firmar el documento, cualquiera que necesite autenticar la firma puede acceder a la clave pública. Para crear una firma digital, el usuario usa la llave privada para generar una firma digital única, que está relacionada con el documento o mensaje en cuestión. Esta firma es computada utilizando una función *Hash*, la cual produce una salida de tamaño fijo de información que es único a la información de entrada. Es decir que para cada entrada de información existe una sola función *hash. Esta función es* única a la salida de la misma información, la cual es inmutable. Esta función *hash* asegura que el más mínimo cambio que se le pudiese realizar al documento original o información en cuestión resultaría en un valor totalmente distinto de la función *hash*, dejando en evidencia que la información o mensaje fue alterado.

En otras palabras, para poder entender que hace la función *hash*, imaginemos que tenemos un baúl, en el cual se pueden guardar un número determinado de objetos y también imaginemos que este baúl tiene una cámara que toma una foto de los objetos que hay en él y además con esta foto genera un código que es único para esa foto por los objetos que hay en ella. Si un intruso cambiara algún objeto de este baúl, la foto seria distinta y de la misma manera el código sería distinto. Así el dueño del baúl sabría que el contenido del mismo ha sido alterado, ya que el código de su foto original es distinto a la actual. Algo así es lo que realiza la función *hash*, recopila información o mensajes que quieren ser enviados y genera un código para el mismo. Si alguno de los mensajes o la información es adulterados o reordenados de alguna manera, el código seria completamente distinto y nos daríamos cuenta que el mensaje o información no son los originales. La siguiente figura muestra el proceso de firmar y validar una firma digital

Figura 15. Firma Digital



Fuente: https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

2.4 Tecnología Blockchain

Blockchain significa una cadena de bloques, que es como un libro de contabilidad distribuido compuesto por bloques que contienen información sobre una única transacción y que se enlazan en orden cronológico para formar una cadena. En este libro de contabilidad distribuido los bloques son creados por usuarios de la red entre pares (P2P) en lugar de por un único administrador.

Blockchain es una tecnología que garantiza la integridad y fiabilidad de los registros de las transacciones sin necesidad de que exista una tercera parte que brinde confianza. Para ello, requiere que todos los participantes de la red creen, registren, almacenen y verifiquen conjuntamente la información de las transacciones. También tiene la estructura para realizar una variedad de servicios de aplicación basados en esa información de transacciones. Utiliza tecnología de *hash*, criptografía y firmas digitales. Un tipo de tecnología *blockchain*, la más conocida, es la que utiliza BITCOIN para su uso, funcionamiento y guardado. (Zhao, Fan, & Yan, 2016).

2.4.1Tipos de Blockchain

Podemos clasificar los mismos en función del acceso a los datos, del esquema de libro distribuido y quien tiene acceso a la participación en el sistema (Viriyasitavat & Hoonsopon, 2018).

Blockchain Publica: son de tipo abierto, en el que cualquiera puede participar. Todos los participantes pueden acceder libremente a datos y realizar transacciones, pero dado que numerosos usuarios no verificados están participando, se necesita cifrado y verificaciones avanzadas y, por lo tanto, la expansión de la red se torna lenta y difícil. Además, el *blockchain* público forma una perfecta estructura distribuida y los participantes de la red son pseudoanónimos. Por ende, no es apropiado para los servicios financieros que necesitan ser controlados por la información centralizada del sistema de gestión (Oh & Shong, 2017).

- Blockchain Privada: Son manejadas y administradas por un propietario. Los libros contables son validados por un grupo predefinido de nodos. Los nodos que serán parte deben ser previamente validados y serán los responsables de mantener el consenso. Los *blockchains* privados son buenos para sistemas cerrados en donde el propietario es la máxima autoridad para controlar el acceso de nuevos nodos. Los mismos serán totalmente confiables. (Viriyasitavat & Hoonsopon, 2018).

- Blockchain Hibridas: Es una combinación de las dos anteriores. Los participantes que ingresen pueden acceder a los datos y realizar transacciones libremente (como en la publica). Aunque para ingresar a la red y realizar ciertas operaciones se necesitan permiso (como en la privada). Los nodos preestablecidos son quienes tienen la autoridad. Este tipo de *blockchain* mantiene una estructura distribuida mientras que fortalece la seguridad limitando la participación de los mismos. Esto resuelve el problema de lentitud de la *blockchain* pública. Este tipo de *blockchain* es el adecuado para sistemas semicerrados.

En el siguiente cuadro se pueden observar las características según cada *blockchain*

Figura 16. Características según tipo de blockchain

Tipos de Blockchain	Blockchain Publica	Blockchain Híbrida	Blockchain Privada
Entidad gestora	Todos los participantes (descentralización)	Participantes que pertenezcan al consorcio.	Una institución central tiene toda la autoridad.
Gobernanza	Es muy difícil cambiar la regla que se ha hecho.	Las reglas podrían cambiarse con relativa facilidad de acuerdo con el acuerdo entre los participantes del consorcio.	Las reglas podrían cambiarse fácilmente de acuerdo con la decisión tomada por la institución central.
Velocidad de transacción	Es difícil expandir la red y la velocidad de transacción es lenta.	Es fácil expandir la red y la velocidad de transacción es rápida.	Es muy fácil ampliar la red y la velocidad de transacción es rápida.
Acceso a los datos	Cualquiera puede acceder	Solo usuarios autorizados pueden acceder	Solo usuarios autorizados pueden acceder
Identificabilidad	Seudo-anónimo	Identificable	Identificable
Prueba de transacción	La entidad para la prueba de la transacción se decide mediante algoritmos como PoW y PoS, y no se puede conocer de antemano.	La entidad para la prueba de la transacción se conoce a través de la autenticación, y la verificación de la transacción y generación de bloques se realizan de acuerdo con las reglas acordadas de antemano.	La prueba de transacción es realizada por la institución central.
Casos de utilización	Bitcoin	R3CEV	Linq, una plataforma de mercado bursátil para compañías sin cotización NASDAQ

Fuente: https://repositorio.usm.cl/bitstream/handle/11673/47346/3560900251199UTFSM.pdf?sequence=1&isAllowed=y

2.5 Contratos inteligentes

Podemos pensar los contratos inteligentes como acuerdos digitales que pueden ejecutarse automáticamente cuando se cumplen determinadas condiciones. Es como un tipo de programa informático que interactúa con la cadena de bloques (*blockchain*).

Podemos pensarlo con la siguiente analogía; pensemos que estamos viendo una carrera de fórmula 1 con un amigo y queremos apostar sobre quien va a ganar. Para hacer esto debemos asegurarnos que nuestro amigo es de confianza ya que necesitamos asegurarnos que nos pague en caso de que salga vencedor mi corredor favorito. Para evitar esta necesidad de confianza con mi amigo, o para poder apostarle a un amigo que no es de confiar, podríamos usar un contrato inteligente.

Este contrato tendría las condiciones y términos de nuestra apuesta, (como la cantidad de dinero a apostar y las condiciones para determinar el ganador). Esto se almacenaría en el *blockchain* y no podría ser modificado, la apuesta quedaría pactada. Al finalizar la carrera, el contrato determinaría automáticamente quien es el ganador, (en función a los parámetros previamente establecidos en el contrato). El pago se realizaría enviando los fondos estipulados a quien haya resultado ganador de la apuesta, todo esto se realizaría al instante, sin la necesidad de que exista una tercera parte que garantice que la apuesta se lleva a cabo en tiempo y forma. Ya que este contrato fue garantizado con el dinero que se ha pactado y registrado previamente en los parámetros del mismo.

2.5.1 Evolución de los contratos inteligentes

Primero, un ejemplo de la vida real que utiliza este concepto de contratos inteligentes que podríamos considerarlo un ancestro primitivo a los mismos, es la máquina expendedora. Esta máquina básicamente toma monedas del usuario que a través de un mecanismo, utilizando informática básica. Brinda al usuario el producto deseado con su respectivo cambio. El mismo está basado y calculado en el precio mostrado por la máquina previamente.

Podemos ver esta máquina como un contrato al portador. Cualquiera que tenga en su posesión monedas, puede participar en un intercambio con el vendedor (la máquina) en todo momento. La caja fuerte y otros mecanismos protegen las monedas y los productos de posibles atacantes. En este caso, generalmente la transacción se cumple y se concreta al instante. Los contratos inteligentes sugieren algo similar al proponer contratos de todo tipo de bienes controlados por medios digitales.

Segundo, sería bueno organizar cronológicamente la evolución de los contratos inteligentes de la siguiente manera:

1) "Formalizing and Securing Relationships on Public Networks" (Nick Szabo, 1997): En este paper se brinda una descripción de la idea de contratos inteligentes. Según Nick Szabo (1997). “Los contratos inteligentes combinan protocolos, interfaces de usuario y promesas expresadas a través de interfaces que formalizan las relaciones de una manera segura en redes públicas. Esto nos proporciona nuevas maneras de formalizar las relaciones digitales que son mucho más funcionales que sus ancestros inanimados basados en papel. Los contratos inteligentes reducen los costes de transacción mentales y computacionales, impuestos por los mandantes, los terceros o sus herramientas”.

2) BITCOIN (Satoshi Nakamoto, 2008): Es la primera implementación de un sistema de transacciones descentralizadas de una criptomoneda, pero no permite la programación de contratos. Este contrato es de un tipo muy específico que solo cumple una función.

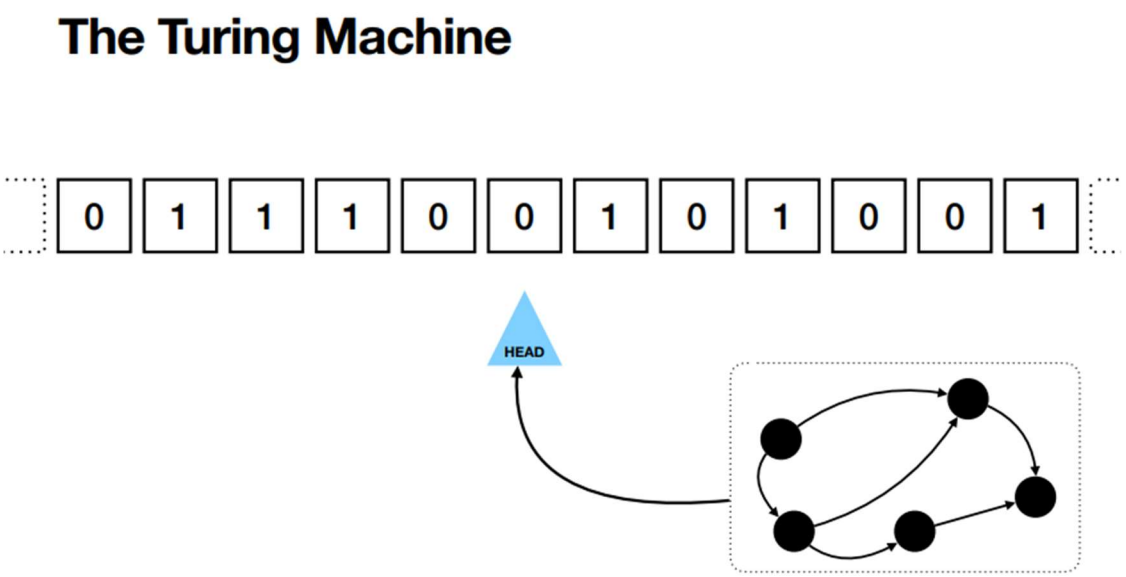
3) Ethereum (vitalik Buterin & Gavin Wood, 2015): Conocido como el primer sistema descentralizado que permite programar contratos, contratos inteligentes, aparte de transacciones de una criptomoneda. Ethereum es conocido como la “cadena de bloques programable mundial”.

2.5.2 Ethereum y La máquina de Turing

La máquina de Turing es un dispositivo informático teórico presentado en una primera instancia por el matemático Alan Turing en la década del ‘30. Se basa en una cinta en donde se puede escribir y leer, consiste en un cabezal de lectura-escritura que puede moverse hacia atrás y hacia delante a lo largo de la cinta, y está basado en un conjunto de reglas que determinan lo que la máquina debe realizar, basándose en el estado actual y la figura de la cinta bajo este cabezal.

La máquina de Turing se utiliza muchas veces como modelo de computación, ya que es una herramienta simple pero muy potente con la que se pueden realizar cualquier tipo de cálculo que pueda realizar un ordenador, siempre y cuando este disponga de memoria y tiempo suficiente. Se puede observar que cualquier problema algorítmico que pueda ser resuelto por una computadora, también puede ser resuelto por una máquina de Turing.

Figura 17. Proceso detrás de la máquina de Turing

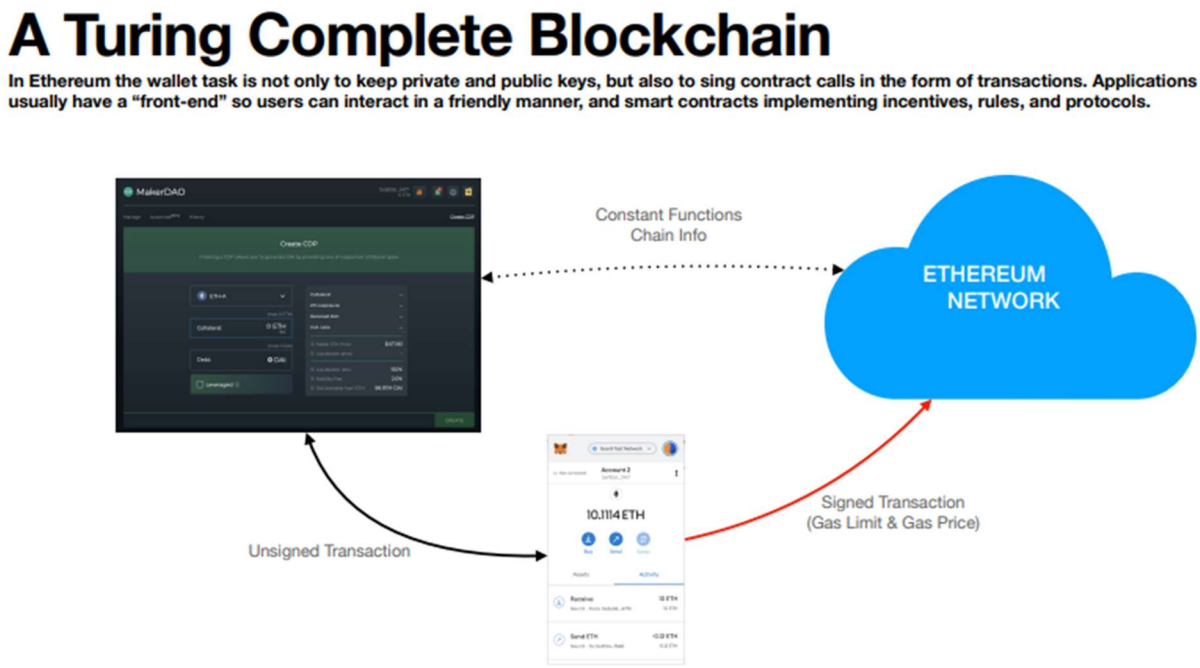


Fuente: (F. Kattan, comunicación personal, octubre 2020)

Lo relevante del modelo es que esta máquina es capaz, dado un algoritmo computacional, de simular la lógica de este modelo y replicarlo. A esto se lo denomina “Turing completo”, que quiere decir que, básicamente este sistema o algoritmo es capaz de simular y replicar cualquier otro sistema computacional.

Esto es importante ya que la *blockchain* de Ethereum, fue pensada desde el momento de su creación como “Turing completo”. Y es capaz de ejecutar código arbitrariamente. Esto marca una gran diferencia con las demás *blockchains*. A su vez, es lo que hace que Ethereum sea “programable”. Ya que a través de esta capacidad de ejecutar e interpretar códigos, crea un ambiente apto para programar los contratos inteligentes (F. Kattan, comunicación personal, octubre 2020).

Figura 18. Blockchain "Turing completo"



Fuente: (F. Kattan, comunicación personal, octubre 2020)

Sobre esta red de Ethereum se pueden programar una variedad de contratos inteligentes, que permiten desarrollar soluciones para un amplio rango de usos, desde contratos financieros, trazabilidad, comercio, entre otros. Todo esto estipulando de manera adecuada los incentivos, reglas y protocolos de estos contratos. Esto es muy diferente a por ejemplo BITCOIN, que la red solo permite el almacenamiento y transferencia de fondos en forma de BITCOINS.

3. BITCOIN

BITCOIN es la moneda digital o criptomoneda más conocida y con mayor capitalización en el mundo. Esta funciona a través de una red descentralizada. Las transacciones de BITCOIN se verifican y registran en la *blockchain*, que como se ha mencionado anteriormente, podemos pensarlo como un libro de contabilidad público, que permite realizar transacciones seguras y transparentes sin necesidad de una autoridad central o intermediario. El valor del BITCOIN viene determinado por la oferta y la demanda del mercado.

En palabras de su creador Satoshi Nakamoto, "Hemos propuesto un sistema para realizar transacciones electrónicas sin depender de la confianza. Empezamos con el marco habitual de monedas hechas a partir de firmas digitales, que proporciona un fuerte control de propiedad, pero es incompleto sin una forma de evitar

el problema de doble gasto. Para solucionarlo propusimos una red entre iguales que utiliza la prueba del trabajo para registrar un historial público de transacciones que rápidamente se convierte en computacionalmente poco práctico para un atacante cambiar si los nodos honestos controlan la mayoría de la CPU". (*Satoshi Nakamoto, (2008)).* En otras palabras, lo que esto significa es que, para que le sea "conveniente o practico" a un participante querer atacar la red de *blockchain*. Tendría que ser capaz de tomar el control de más del 50% del poder computacional de los hashes de la red. Esto es prácticamente imposible por el gran costo que esto conllevaría. Además de que no podría llevarse a cabo solo y a la mayoría de los participantes le conviene que la red siga funcionando normalmente debido las recompensas que reciben por s participación en la misma.

3.1 Características económicas y tecnológicas del dinero/moneda

3.1.1 Características Económicas

Podemos decir que las monedas son artículos que miden el valor de bienes y objetos. A su vez tienen tres funciones fundamentales:

1) Intermediarios en transacciones: Esto significa que puede intercambiarse fácilmente por bienes y servicios. En otras palabras, que reemplace al trueque. Es un consenso basado pura y exclusivamente en la confianza
2) Reserva de Valor: El dinero debe de servir como reserva de valor y riqueza durante el tiempo, manteniendo relativamente su poder de compra.
3) Unidad de cuenta: El dinero debe de servir como unidad de medida de estos bienes o servicios. Debe proveer un estándar de valor para así poder comparar el valor de estos bienes y servicios en el tiempo.

3.1.2 Características Tecnológicas

Las características tecnológicas del dinero se pueden resumir a los siguientes factores: Fuente: (Calderón, comunicación personal, octubre 2020):

En primer lugar, la pertenencia, el dinero debe poder pertenecer a una persona y esta persona debe ser capaz fácilmente de apropiarse o definir derechos de propiedad sobre el mismo. Además, este derecho de propiedad debe ser intercambiable entre personas. También por otro lado, cada moneda o dinero debe tener una identificación que la distingue y valida.

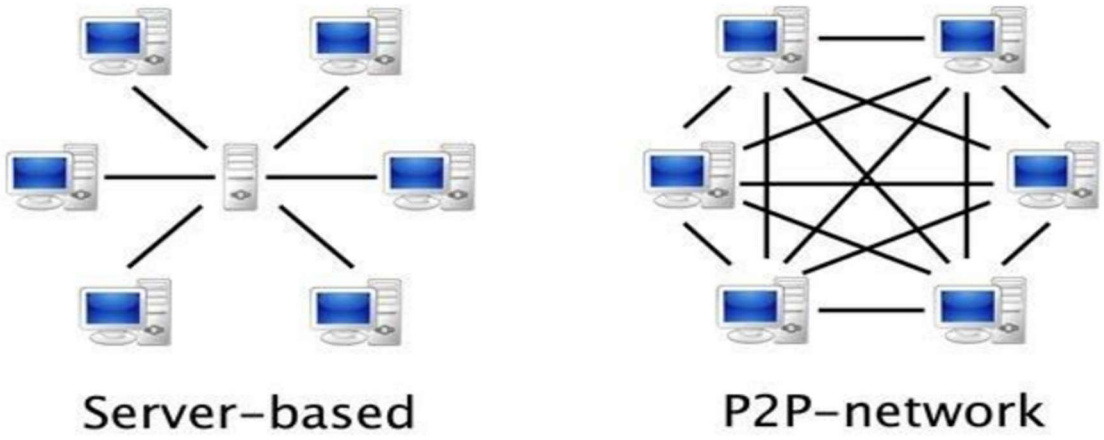
En segundo lugar, durante el intercambio de estas monedas o dinero, las mismas no deben ser capaz de gastarse dos veces. O sea, no debemos tener problema de "doble gasto". El mismo consiste en utilizar un medio de pago más de una vez para pagar varias cosas. Esto es un problema común a resolver con los medios de pagos digitales ya que los mismos podrían duplicarse y volver a usarse. Por ejemplo, que una persona envíe una moneda digital a dos receptores al mismo tiempo. Esto destruiría todo el sistema. Por eso, las monedas digitales utilizan ciertos algoritmos y mecanismos para evitar este problema de doble gasto.
Este problema no existe en el dinero físico. Ya que, al intercambiar una moneda física por un artículo, no hay manera de utilizar la misma moneda para adquirir dos artículos distintos en el mismo momento. La solución de este problema es clave para la robustez y legitimidad de un sistema de transacciones digitales.

Por último, el dinero debe tener la propiedad de la escasez. Debe tener algún tipo de limitación, debe existir un numero finito de unidades en circulación o posibles de emitir. Además la creación o emisión del mismo conlleve algún tipo de costo o esfuerzo.

3.2 ¿Qué es BITCOIN?

BITCOIN es un sistema de efectivo electrónico descentralizado que nos permite realizar pagos en línea y permite enviar dinero de una persona a otra sin la necesidad de tener un intermediario financiero. BITCOIN se basa en una cadena de firmas digitales, que a su vez también está basado en un sistema " Peer to Peer" que es el que soluciona el problema de doble gasto. Este sistema de "Peer to Peer" o red de pares, es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

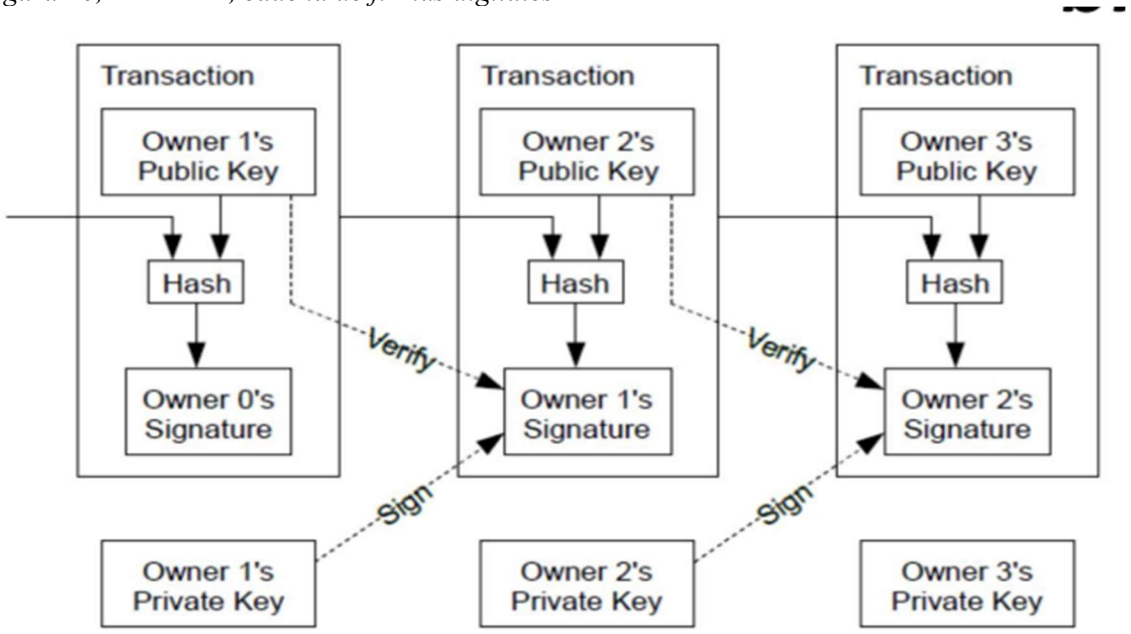
Figura 19. Red P2P



Fuente: (F. Kattan, comunicación personal, octubre 2020)

Usar este tipo de sistema soluciona el problema de doble gasto. Lo que se busca solucionar es cómo hacer para que, en este caso, un BITCOIN no sea usado dos veces. Al usar un sistema de pares, las transacciones son anunciadas públicamente en la red. Al mismo tiempo, todos los nodos están al tanto de que dicha transacción se está llevando a cabo. La misma es verificada con el uso de algoritmos y estos determinan si es válida.

Figura 20, BITCOIN*, cadena de firmas digitales*



Fuente: (F. Kattan, comunicación personal, octubre 2020)

Una vez verificada la transacción, se añade a un bloque dentro de la cadena de bloques, que a su vez se añade al final de esta cadena existente. Cada bloque de la cadena de bloques contiene un *hash* criptográfico de un bloque anterior, lo que crea un registro permanente e inalterable de cada transacción en la red. Este sistema garantiza que cada BITCOIN sólo pueda gastarse una vez, ya que cualquier intento de gastar el mismo BITCOIN dos veces será detectado por la red y rechazado.

3.3 El mecanismo de bitcoin

BITCOIN alcanza la descentralización a través de un mecanismo que es una combinación de aspectos técnicos y diseño de activos, los cuales los podemos organizar en tres partes (Calderon, comunicación personal, octubre 2020):

1) Minería
2) Protocolo de consenso distribuido
3) Prueba de trabajo

Minería

La minería es el mecanismo, a través del cual la seguridad de BITCOIN se vuelve descentralizada. Esta nos permite llegar a un consenso en toda la red sin la necesidad de tener una autoridad central. La actividad de minería tiene un premio o incentivo por llevare a cabo. Se basa en un esquema que alinea la acción de los mineros con la seguridad y confiabilidad de la red. A su vez produce la oferta monetaria.

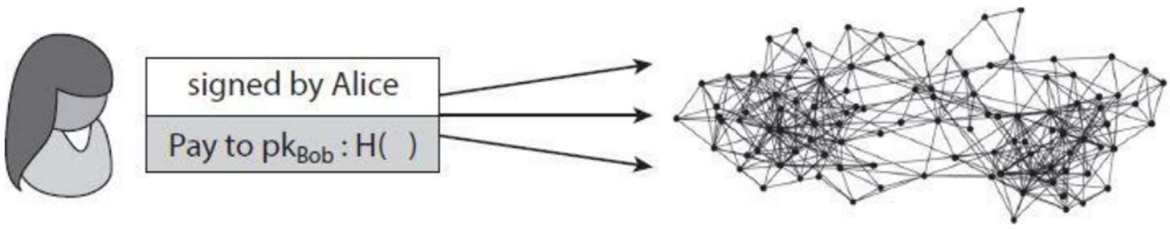
Solo se crean nuevos BITCOINS para recompensar a los mineros por su trabajo de validación de las nuevas transacciones que se agregan a la *blockchain*, también la cantidad máxima de BITCOIN a emitir nunca va

a superar los 21 millones. Esto fue estipulado intencionalmente por el creador de BITCOIN al momento de su creación. Esto se realizó para que solo exista una oferta limitada de BITCOIN. Este proceso de emisión está controlado por la misma *blockchain.* La misma dejara de emitir y dar recompensas a los mineros, una vez que se alcancen los 21 millones de BITCOINS emitidos.

Protocolo de consenso distribuido

Dentro de un protocolo de consenso distribuido existen "n" tipos de nodos, cada uno de estos con una propuesta de valor diferente. Alguno de estos nodos son maliciosos y otros honestos. Este tipo de protocolo tiene las siguientes dos propiedades: la primera es que debe terminar solo con nodos honestos y que estos estén de acuerdo con el valor; y la segunda es que este valor debe haber sido generado por un nodo honesto.

Figura 21. Consenso en BITCOIN



Fuente: (F. Kattan, comunicación personal, octubre 2020)

Nota: Cuando Alice quiere pagarle a Bob, emite una transacción a toda la red, es decir, a todos los nodos que conforman la red persona a persona

Dado que muchos usuarios emiten transacciones a la red, los nodos deben acordar exactamente que transacciones fueron emitidas y el orden en que ocurrieron. Esto resulta en que la red tenga un "Ledger o libro mayor para toda la red.

El protocolo tiene ciertos obstáculos que debe superar para alcanzar este consenso, esto son: imperfecciones en la red, de [12]latencia y caída de nodos. Y a su vez, intentos deliberados de atentar contra el buen funcionamiento del proceso. Los problemas de latencia generan que no haya una noción de tiempo global, es decir que no todos los nodos pueden estar de acuerdo sobre un ordenamiento común de los eventos. Para esto existe un algoritmo de consenso en BITCOIN, que se basa en los siguientes puntos:

1) Nuevas transacciones son emitidas a todos los nodos
2) Cada nodo agrega un conjunto de nuevas transacciones en un bloque
3) En cada ronda, supongamos que un nodo elegido al azar propone su bloque
4) Los otros nodos aceptan este bloque sólo si contiene transacciones válidas (BITCOINS no usados previamente y firmas válidas)
5) Los nodos expresan su aceptación del bloque propuesto al incluir su *hash* en el siguiente bloque que agreguen.

[12] Latencia: suma de retardos temporales dentro de una red

Prueba de Trabajo

Antes de hablar de prueba de trabajo, debemos preguntarnos si es posible dar a los nodos un incentivo para que estos se comporten honestamente. La respuesta es sí, el pago con BITCOINS y este incentivo se divide en dos partes:

1) "Block Reward": cada nodo recibe un pago en BITCOINS por añadir un nuevo bloque, pero este pago tiene valor para el nodo sólo si el nuevo bloque se agrega a la cadena de bloques que va a tener consenso en el largo plazo. Esto es un incentivo a que los nodos sigan una estrategia honesta
2) "Transaction Fee": pago al nodo por cada transacción validada.

Esto se lleva a cabo mediante la prueba de trabajo, que es una forma de implementar el mecanismo de selección aleatorio de un nodo, en función de su capacidad de resolver un problema de cálculo. La selección de nodos para cada ronda en función de su poder de cálculo es implementada usando "*Hash* Puzzles".

Para poder agregar su bloque propuesto, cada nodo tiene que encontrar un número, el [13]"nonce", tal que cuando se concatena el "nonce", el *hash* del bloque previo, y la lista de transacciones que configure el nuevo bloque, y luego se toma el *hash* de toda esta cadena de caracteres concatenados, el *hash* resultante tiene que ser un número que pertenezca a un conjunto determinado, cuyo tamaño es muy pequeño en relación al tamaño del conjunto de posibles valores de la función *Hash*.

Dado que es imposible predecir qué combinación de bits se traducirá en el *hash* correcto, se intentan muchos "nonce" diferentes y el *hash* se vuelve a calcular para cada valor hasta que se encuentre un *hash* que contenga el número necesario de bits a cero. Como este cálculo iterativo requiere tiempo y recursos, la presentación del bloque con el valor "nonce" correcta constituye una prueba de trabajo.

Si la función *Hash* satisface la propiedad de ser *puzzle-friendly*, *"una función hash es puzzle-friendly, si, Dado: H( ) (Función hash SHA-256), "k" (Un número aleatorio elegido entre una muestra de alta incertidumbre, llamado PUZZLE-ID) e "Y" (Y = Un rango de resultados/hash válidos). Para cualquier valor de salida "y" dentro del rango de valores de "Y", en este caso como es SHA-256 sería 2^256 valores posibles; con una "k" perteneciente a una muestra de alta incertidumbre, encontrar una "x" específica sería imposible en un tiempo significativamente menor a 2^256 computaciones, ya que no hay otra forma de encontrarla que recorrer el espacio de forma aleatoria (Ya que es inmenso). (*Munilla Garrido, noviembre 2017). Entonces la mejor estrategia para encontrar el "nonce" es probando números al azar. Si, por ejemplo, el tamaño del espacio *target* es un 1% del tamaño del espacio total de los valores posible de la función *Hash*, entonces en promedio habrá que probar cien números aleatorios (equiprobablemente distribuidos) antes de dar con uno que satisfaga el [14]*puzzle*.

La dificultad de la prueba de trabajo va aumentando a medida que crece el tamaño del *blockchain*. Los nodos de la red recalculan el tamaño del *target* automáticamente cada 2.016 bloques añadidos al *blockchain*. Este cálculo se hace de tal forma que el tiempo esperado que la red tarda en añadir un nuevo bloque sea de diez minutos. El recálculo del tamaño del *target* sucede aproximadamente cada dos semanas (F. Kattan, comunicación personal, octubre 2020).

[13]Nonce: Numero que debe encontrar el nodo para poder agregar el bloque propuesto a la cadena de bloques.
[14] Puzzle: Rompecabezas en ingles

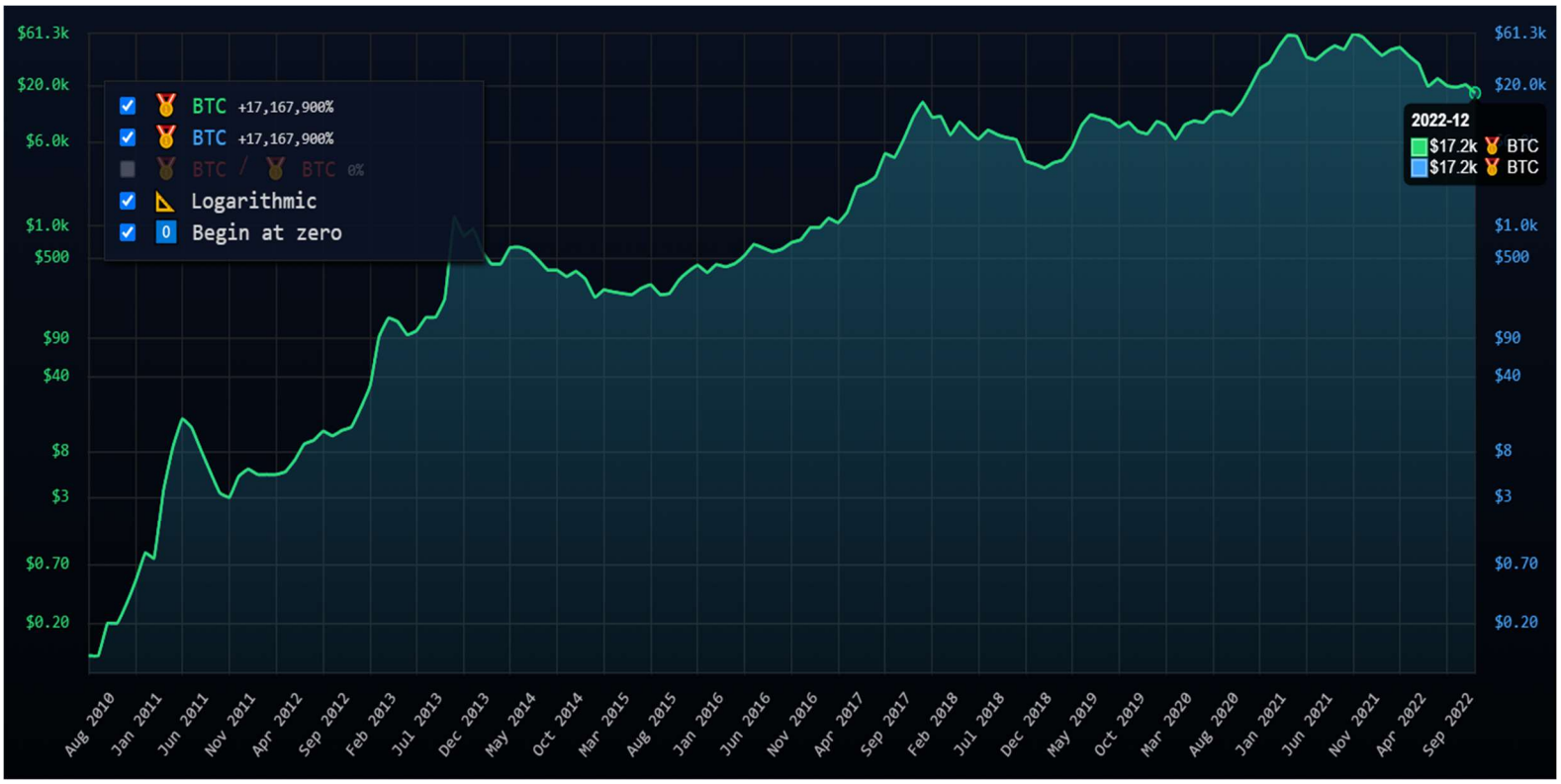
3.4 BITCOIN como reserva de valor

BITCOIN es visto como muchos inversores como un instrumento de reserva de valor y, personalmente, considero que es uno de los activos con mejor rendimiento en la historia de la humanidad. En el siguiente grafico podemos ver su desempeño, con una muestra que va desde el año 2010 hasta diciembre de 2022.

Aunque podríamos argumentar que en 2010 BITCOIN no era fácil de adquirir, siguen existiendo personas que ya desde ese entonces entendían la tecnología y vieron potencial en este activo y fueron capaces de comprar BITCOIN a 10 centavos de dólar por BITCOIN, con un BITCOIN en diciembre de 2022 a 17.2 mil dólares por BITCOIN, esto los deja con una apreciación del activo del 17.167.900%

Figura 22, Desempeño de bitcoin en el tiempo

Fuente: https://inflationchart.com/btc-in-btc/?show_divided_by=0&logarithmic=1&zero=1



4. Activos tradicionales de resguardo de valor

Los activos tradicionales de resguardo de valor que han utilizado los inversionistas a lo largo de los distintos ciclos económicos son los bonos soberanos, las acciones, el S&P 500 y los metales preciosos (Oro y Plata).

Sin embargo, antes de explicar el por qué se utilizan estos activos, debemos primero explicar que son y como interpretarlos.

4.1 Bonos como herramienta para resguardar valor.

Los bonos del tesoro americano son una herramienta muy utilizada en los mercados financieros a la hora de armar los portafolios. Estos se utilizan principalmente para disminuir el riesgo del mismo. También, en caso de tener cupones, para obtener unos ingresos periódicamente.

El precio de los bonos del tesoro americano lo denotamos con la fórmula de los bonos Bullet, los cuales están compuestos por cupones, su correspondiente *Yield-To-Maturity*, y sus periodos hasta su maduración. Analíticamente, los podemos expresar:

$$Precio\ de\ un\ Bono = \sum_{t=1}^{N} \left(\frac{Cupon}{(1 + Yield)^t} \right) + \frac{Nominal}{(1 + Yield)^N}$$

Como podemos observar, los precios de los bonos, dependen positivamente de los pagos de sus cupones, es decir, que mientras mayor sea el porcentaje del valor nominal que me abonen en cada periodo, mayor será su precio. Por otro lado, el precio del bono depende negativamente de su *Yield-To-Maturity*, es decir, a mayor YTM, menor será el precio del bono.

Dicho análisis nos puede beneficiar al momento de armar un portafolio para resguardar valor mirando todos los componentes del bono, ya que, ante periodos de inestabilidad económica, comprar bonos nos puede traer un poco más de estabilidad a nuestro portafolio y reducir los riesgos del mismo.

En el siguiente grafico podemos observar las distintas *Yields* que han tenido los distintos bonos americanos, donde los ciclos de color gris, son las recesiones que han tenido. Como se puede observar, desde la década de los ‘80s, las *Yields* tienen una tendencia decreciente analizada a largo plazo, lo que significa un aumento en los precios de los bonos americanos, cuya variación de precio la podríamos observar analizando la formula previamente detallada.

Figura 23. Yields bonos americanos

Fuente: https://www.macrotrends.net/2016/10-year-treasury-bond-rate-yield-chart

4.1.1 Duration: una medida del riesgo de los bonos

La "Duration" o "Duration Macaulay", es la vida promedio ponderada de los pagos futuros que hará el bono. La duration la podemos denotar de la siguiente manera:

$$Macaulay\ Duration = \frac{\sum_{t=1}^{n} t * \frac{1}{(1+Yield)^t} + n * \frac{M}{(1+Yield)^n}}{Precio\ del\ Bono}$$

Siendo *n* el número de cash flows, *t* el time of maturity, *C* el cash Flow, *Y* la required Yield, *M* la maturity (par) value.

"Cuanto mayor sea el periodo en que los inversores deban recibir cupones o, dicho de otra forma, cuanto más tiempo falte hasta que se les devuelva el capital, mayor será la duración del bono, y por tanto, más riesgoso será el bono" (omar venerio, septiembre 2020)

4.1.2 Modified Duration

La duration de un bono –en pocas palabras la vida promedio ponderada del bono– nos permite medir la volatilidad del precio del bono y a partir de ella se puede calcular la *duration* modificada.

La *Modified Duration* nos sirve para estimar cambios en los precios de los bonos cuando se modifica la tasa requerida por el mercado.

Si queremos obtener la *duration modificada*. Solo hay que ajustar la fórmula de la duration. La fórmula de la Modified Duration la podemos expresar:

$$Modified\ Duration = \frac{Duration}{(1 + Yield/n)}$$

Siendo *Yield* su YTM y *n* la frecuencia del pago del cupón.

Por tanto, la duration modificada nos sirve para calcular, de forma aproximada, cuánto cambia el precio del bono.

En adición, la *Modified Duration* nos sirve para poder estimar el cambio en el precio del Bono.

$$\Delta\ Precio\ \% = \ -Modified\ Duration * \Delta Yield\%$$

"La volatilidad del bono se expresa en términos del efecto que tendrá un shock en las tasas (tanto al alza como a la baja); es muy importante para que el inversor sepa cuánto ganará o perderá de un movimiento de la misma, es decir, cómo y cuánto se verá afectada su rentabilidad." (Omar Venerio, septiembre 2020)

4.1.3 Convexity

Cuando analizamos la *Duration* de un bono, estamos asumiendo que la relación precio-rentabilidad es constante. Sin embargo, en la actualidad no sucede así. Para variaciones pequeñas en la relación Precio-Rentabilidad, la *duration* es una medida aceptable. Pero cuando las variaciones son grandes, se vuelve imprescindible calcular la *convexity* del mismo.

"La convexity nos ofrece una medida mucho más exacta de los cambios precio-rentabilidad de un bono.". (José Francisco López, marzo 2020)

Matemáticamente se expresa como la segunda derivada de la curva precio-rentabilidad. La fórmula queda como sigue:

$$Convexity = \frac{1}{Precio * (1 + Yield)^2} * \sum_{1}^{t} [\frac{Cupon_t}{(1 + Yield)^t} * (t^2 + t)]$$

"Si la convexidad de un bono es igual a 100, el precio del bono variará un 1% extra cada 1% de variación de los tipos de interés, además de la calculada por la duración. Si la convexidad de un bono es igual a cero, el precio del bono variará ante cambios en los tipos de interés la cantidad motivada por la duración del bono." (José Francisco López, marzo 2020)

Teniendo la Convexity, podemos estimar la variación del precio de un bono. La fórmula es:

$$\frac{\Delta Precio}{Precio} = (-Modified\ Duration * \Delta Yield) + \left(\frac{1}{2} * Convexity * (\Delta Yield)^2\right)$$

Esta estimación nos servirá para analizar las variaciones del precio de los bonos teniendo en cuenta su convexity, los cual nos permitirá analizar dichas variaciones en los precios, aun con variaciones grandes en la relación Precio-Rentabilidad.

Dicho esto, podemos analizar las variaciones de los precios de los bonos, analizar sus *cash flows*, sus *Duration* y *Convexity*, y poder armar un portafolio diversificado con bonos del tesoro americano para poder disminuir el riesgo del mismo.

4.2 El índice S&P500

"El índice Standard & Poor´s 500, o más conocido como S&P 500, recoge 500 empresas estadounidenses seleccionadas por su tamaño, liquidez y representatividad por actividad económica, incluyendo 400 industriales, 20 del sector transporte, 40 de servicios y 40 financieras" (Carlos Olivieri, comunicación personal, septiembre 2021)

"El S&P 500 se calcula mediante una media aritmética ponderada por capitalización y representa la mayor parte de la capitalización bursátil de los Estados Unidos." (Carlos Olivieri, comunicación personal, septiembre 2021)

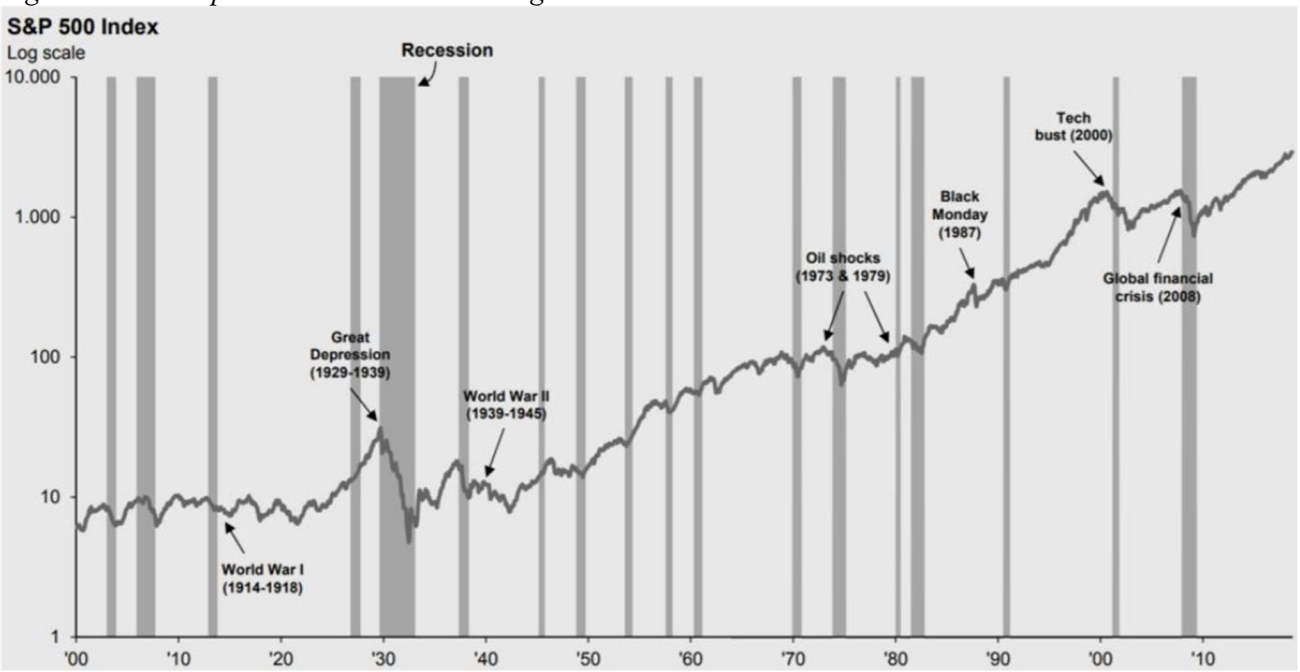
Dicho índice, es una de las principales herramientas para resguardo de valor que utilizan los inversionistas para tener un portafolio diversificado. Debido a que el mismo ha obtenido unos rendimientos anualizados del 8,26% desde el 1927 hasta el 2020.

A continuación, podemos observar en la siguiente imagen, una pirámide donde muestra los rendimientos que ha tenido el mercado de Estados Unidos desde el año 1825 hasta el año 2019. Cabe destacar que los rendimientos del mercado se distribuyen de forma normal.

Cabe destacar que el índice S&P500 nunca obtuvo un rendimiento mayor al 50% en un año natural. Sin embargo, acciones que componen el índice sí lo han hecho. Dicho esto, adquirir el índice es una forma de tener porcentaje de nuestro portafolio de manera muy diversificada pero no de la forma más óptima posible.

A continuación, en el siguiente gráfico, podemos ver la evolución del índice a lo largo del tiempo.

Figura 25. Desempeño S&P 500 en escala logarítmica



Fuente: https://www.bankinter.com/blog/mercados/mayores-caidas-subidas-wall-street-sp500

En dicho gráfico, podemos observar la misma idea explicada anteriormente, el S&P500 ha tenido rendimientos positivos y negativos a lo largo de los años, pero de forma anualizada, ha obtenido rendimientos del 8,26%.

Ahora bien, un inversionista racional siempre quiere obtener el mayor rendimiento posible al menor riesgo posible, por lo que, a la hora de armar su portafolio, deberá analizar cuál es el riesgo que está asumiendo a la hora de ponderar el peso de las acciones, fondos, bonos o lo que esté dispuesto a invertir para disminuir el riesgo. Por ende, analizar el riesgo del S&P500 es una buena forma de estimar los posibles rendimientos de nuestro portafolio.

Sin embargo, muchos inversionistas han optado en estos últimos años en un indicador para estimar la volatilidad del mercado (VIX), "*el cual es prospectivo, lo que significa que solo muestra la volatilidad implícita del S&P 500 (SPX) durante los siguientes 30 días. Además, el VIX se calcula utilizando los precios de las opciones del índice SPX y se expresa como un porcentaje. Si el valor del VIX aumenta, es probable que el S&P 500 caiga, mientras que, si el valor del VIX disminuye, es probable que el S&P 500 se mantenga estable."* (Carlos Olivieri, comunicación personal, septiembre 2021)

"Los instrumentos vinculados al VIX tienen una fuerte correlación negativa con el mercado de valores, por lo que se han convertido en una opción popular entre los inversores como herramientas de diversificación y cobertura" (Carlos Olivieri, comunicación personal, septiembre 2021)

La fórmula matemática del VIX, la podemos expresar como:

$$\sigma^2 = \frac{2}{T}\sum_i \frac{\Delta K_i}{{K_i}^2} e^{RT} Q(K_i) - \frac{1}{T}[\frac{F}{K_0} - 1]^2$$

Donde denotamos las siguientes variables:

$\sigma = \frac{\text{VIX}}{100}$ que es igual a $\text{VIX} = \sigma * 100$

T = Tiempo hasta el vencimiento

F = Nivel futuro del incide, derivado de los precios de la opción sobre el índice

$K_0 =$ Primer precio de ejercicio por debajo del nivel futuro del indice F

$K_i =$ Precio ejercicio de la i opcion out of the money

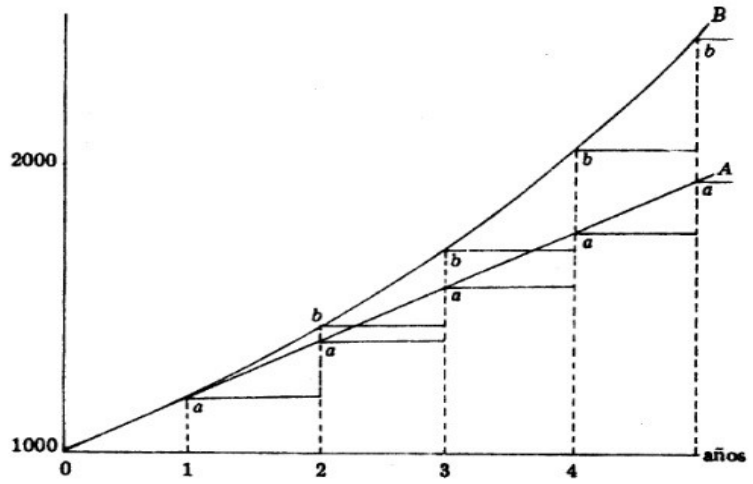
$\Delta K_i = \frac{K_{j+1} - K_{j-1}}{2}$

R = Tipo de interés sin riesgo hasta el vencimiento

$Q(K_i) =$ El punto medio del spread Bid $-$ ask de la opcion con el precio de K_i

Este indicador nos sirve para tomar decisiones a la hora de incorporar acciones del S&P500 dependiendo si optamos por disminuir el riesgo de nuestro portafolio, observando el VIX como medida para estimar la dirección del precio y tomando como datos que el S&P500 rinde de forma anualizada 8% aproximadamente. Esta herramienta es una de las más frecuentes para resguardo de valor a largo plazo, debido a que muchos inversionistas, adquieren capital y lo invierten con el fin de reinvertirlo al final de cada periodo, utilizando el interés compuesto para aumentar su capital. Además, de dicha inversión inicial, los individuos pueden invertir periódicamente un capital extra, generando un aumento aun mayor a final de cada año. Gráficamente, lo podemos observar de la siguiente manera

Figura 26. Inversión con interés simple vs compuesto.



Fuente: http://www.blog-top.com/diferencias-entre-el-interes-simple-y-compuesto/

Donde A representa una inversión con un interés simple, y B una inversión con interés compuesto. Esto quiere decir que mientras mayor tiempo mantengamos la inversión, reinvirtiéndola periodo tras periodo, mayor será nuestro capital.

Sin embargo, es una herramienta muy utilizada para resguardo de valor para largo plazo, por lo que ya dijimos, el S&P500 puede rendir negativamente, pero en el largo plazo, debemos tomar como dato que rinde aproximadamente 8% de forma anualizada como parámetro para calcular si nuestra inversión es rentable.

4.3 El Oro y Plata como resguardo de valor

El Oro y la Plata son activos que son utilizados para diversificar las carteras de inversión, ya que no tienen una estrecha relación con la renta variable tradicional, sino que tiene una directa relación con las tasas de interese reale. Además, el Oro se comporta relativamente mejor frente a otros activos cuando los tipos de interés son bajos y hay un crecimiento moderado en la economía.
En otras palabras *"El oro es un instrumento de inversión que presenta baja correlación y lo convierten en un instrumento atractivo en periodos de mala administración económica o crisis financieras, característica principal de los mercados emergentes".* (Carlos Laorga, marzo 2022)

En adición, los metales preciosos son utilizados muchas veces en periodos de crisis o recesiones como reserva de valor ante una devaluación de una moneda, por ejemplo, el dólar de Estados Unidos. No obstante, otra razón por la que se decide incorporar metales preciosos a un portafolio, es por posibles rendimientos negativos del S&P500. A continuación, en el grafico se puede observar las variaciones de los precios un metal precioso (Oro) con respecto al S&P500.

Figura 27. Precio oro vs S&P500

Fuente: https://www.libremercado.com/2016-06-19/por-que-el-oro-actua-como-valor-refugio-1276576393/

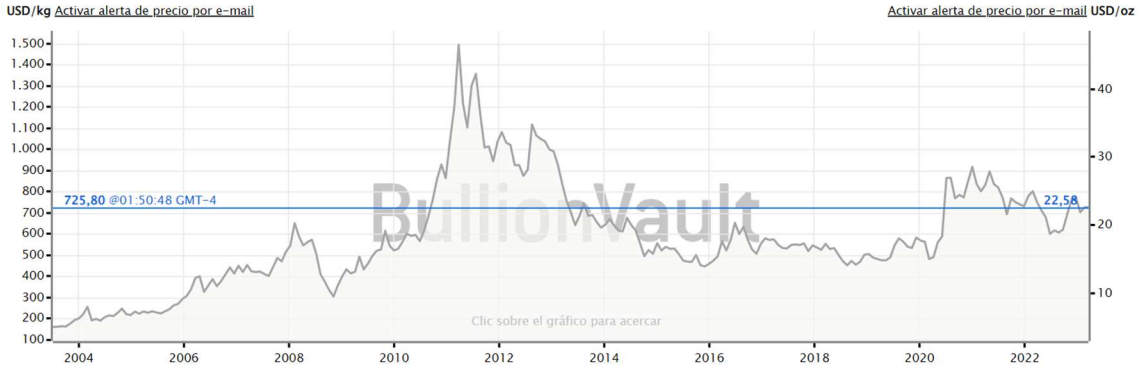
En este grafico podemos observar que cuando el S&P500 rinde negativamente, el oro ha rendido positivamente, siendo un resguardo de valor para reducir pérdidas de mi portafolio.
Por otro lado, podemos observar la evolución de los precios del Oro. Este ha tenido una tendencia alcista durante los últimos 20 años. A su vez, teniendo un periodo de rendimientos negativos entre los años 2012 a 2016. Por último, un fuerte crecimiento a partir del 2019 hasta 2021, momento en el cual se desarrollaba la pandemia por el Covid-19. Esto último, fue desacelerando la economía mundial, llevando a periodos de inflación en el mundo. El precio del oro subió por un aumento en la demanda del mismo, para resguardarse de la inflación.

Figura 28. Evolución de precios del oro

Fuente: https://oro.bullionvault.es/Precio-del-oro.do

En el siguiente gráfico, podemos ver la evolución del precio de la Plata durante los últimos 20 años, tendiendo variaciones similares al oro. Periodo 2009 al 2011 de crecimiento y periodo del 2012 al 2016 de rendimientos negativos

Figura 29. Evolución precio de la plata



Fuente: https://oro.bullionvault.es/Precio-del-oro.do

Por otro lado, invertir en metales preciosos, además de brindarte una diversificación a tu portafolio, también otorga cobertura frente al riesgo.

*"Una cobertura es una estrategia financiera que sirve para cubrir el riesgo de una inversión realizando la posición financiera opuesta mediante un activo financiero correlacionado con la inversión principal o mediante un Derivado financiero". (*Andrés Sevilla Arias, junio 2020)

La cobertura se realiza para evitar movimientos adversos en el precio del activo. Por lo que funciona como un seguro contra las pérdidas, ya que al haber tomado la posición contraria obtendremos ganancias del activo o pasivo utilizado como cobertura, compensando las pérdidas del elemento principal.

A continuación, en el siguiente gráfico, podemos observar un gráfico donde se realiza una comparación entre las evoluciones del Oro con respecto al S&P500.

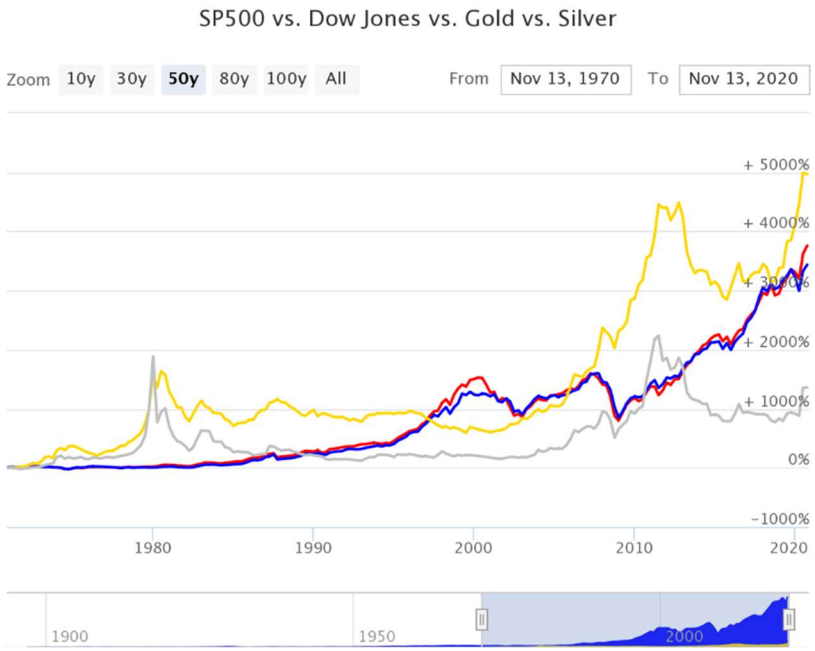
Figura 30. Oro vs S&P500

Fuente: https://topforeignstocks.com/2019/09/26/gold-vs-sp-500-long-term-returns-chart/

Como mencionamos anteriormente, en periodos de alto crecimiento económico en la economía, reflejadas por la suba de las acciones de las empresas que forman parte del S&P500, el oro pierde valor, ya que los individuos prefieren invertir en las acciones, asumiendo más riesgo, pero a su vez con mayores ganancias posibles. Sin embargo, el oro se aprecia cuando la economía se frena, reflejada en la baja del índice S&P500, momento en que los individuos de la economía optan por adquirir oro, para resguardo de valor. (David hunkar, septiembre 2019)

Ahora bien, si realizamos dicha comparación, pero incorporando otro índice (Dow Jones) y otro material precioso (Plata), podemos obtener una mirada más completa de lo anterior mencionado.

Figura 31. Oro vs S&P500 vs plata y Dow Jones



Nota: Las leyendas son las siguientes; S&P500, Dow Jones, oro y Plata
Fuente: https://topforeignstocks.com/2019/09/26/gold-vs-sp-500-long-term-returns-chart/

Podemos observar en el grafico que los comportamientos del oro y plata, como mencionamos anteriormente, son similares en términos de tendencias. A la vez, también podemos observar que los índices S&P500 y Dow Jones, tienen el mismo comportamiento, ya que están compuesta por acciones. Denotando nuevamente el pensamiento anterior, ante periodos de crecimiento en el mercado, los índices suben, mientras que en los metales preciosos no pasa eso. (David Hunkar, septiembre 2019)

Sin embargo, en los últimos años, con la aparición de las criptomonedas, las personas pueden optar como refugio de valor el BITCOIN. Nace de una idea similar al oro, un refugio de valor con cantidad limitada (recurso limitado como el oro), que, con el paso del tiempo, tiende a apreciarse, lo que conlleva a una suba en los precios, por ende, una capitalización mayor de nuestro portafolio.

A continuación, se muestra un gráfico que realiza una comparación entre el S&P500, el oro y el BITCOIN.

Figura 32. Oro, bitcoin y S&P500

Nota: El grafico comprende el periodo entre 2015 y 2021
Fuente: https://uncommonfinance.com/comparativa-de-largo-recorrido-entre-el-sp-500-el-bitcoin-y-el-oro/

En dicho gráfico podemos observar los rendimientos que han alcanzado cada uno, desde su mínimo hasta su máximo. A su vez, utilizamos datos desde 2015. Ya que se considera un momento donde bitcoin se volvió mas popular y accesible para todos. Partiendo del nacimiento de las plataformas de derivados de BITCOIN como BitMEX y BitVC en 2014. Sin embargo, la comparación se hace absurda en términos de rendimiento ya que deberíamos asumir que el individuo adquirió el activo en su mínimo, lo mantuvo un tiempo, y lo vendió en su máximo.

Por otro lado, esto nos sirve para comparar la evolución de los distintos activos durante los últimos años podemos ver que esta criptomoneda ya ha tenido un extenso periodo de crecimiento y en la actualidad es considerada como una opción valiosa al momento de invertir por muchas personas.

Para tener una visión más empírica, imaginemos que en enero de 2016 invertíamos 30 mil dólares, dividido en partes iguales entre BITCOIN, oro y el mercado accionario (S&P500) y manteníamos la posición hasta la fecha (siendo hoy marzo 2023). Veamos cual sería el rendimiento de cada posición en los distintos activos.

Para el mercado accionario, el retorno a lo largo de los siete años sería de 94.75%. lo que equivaldría en dinero a $19,475 dólares.

Figura 33. Desempeño S&P500

Nota: velas mensuales, el grafico es de los contratos E-mini del mercado de futuros que representan al índice del S&P500.
Fuente: Elaboración propia

Para el caso del oro, el rendimiento sería de 72.86%. En términos monetarios equivaldría a $17,286 dólares

Figura 34, Desempeño del oro

Notas: *velas mensuales, el grafico es de los contratos del mercado de futuros que representan al oro*
Fuente: Elaboración propia

Para el caso de BITCOIN, el rendimiento sería de 6493.08%, en términos monetarios seria $649,308 dólares. Esto conlleva una gran volatilidad y riesgo, no apta para la mayoría de los inversores tradicionales. Para este caso, se toma como punto de partida enero de 2016. Esta fecha fue seleccionada, ya que son unos meses posteriores al momento que comienza a cotizar el contrato de futuros más liquido del mercado (XBTUSD.P). Por lo tanto, se considera un momento en el que todas las personas tenían acceso a comprar bitcoins de manera sencilla.

Figura 35, Desempeño de bitcoin

Fuente: Elaboración propia
Nota: velas mensuales, el grafico es de los contratos del mercado de futuros de bitcoin.

5 BITCOIN frente los efectos macroeconómicos

Para analizar el impacto de los efectos macroeconómicos frente a BITCOIN, utilizaremos el paper de "The BITCOIN-Macro Disconnect" Gianluca Benigno y Carlo Rossa. Banco de la reserva federal de Nueva York.

El mismo investiga la conexión entre BITCOIN y las fundamentales macros. Partiendo de la estimación de los impactos que tienen las noticias macroeconómicas sobre BITCOIN. Para esto, se utilizan eventos con datos intradiarios. El resultado clave de esto determina que, al contrario de otras clases de activos norteamericanos. BITCOIN muestra ser ortogonal a las noticias macroeconómicas y monetarias. Esto significa que, no se ven afectados el uno al otro dado los resultados de los mismos. Además, hay que aclarar que se interpreta BITCOIN desde un punto de vista meramente especulativo.

5.1 introducción

Este trabajo, para su análisis empírico, interpreta las criptomonedas como activos cuyos precios actuales dependen del valor descontado de los precios futuros esperados. Esto implica que, desde un punto macroeconómico, los cambios en las tasas de interés actuales y futuras afectan el valor de las criptomonedas.

En este trabajo de estudio se analiza empíricamente como los factores macroeconómicos afectan las criptomonedas, partiendo de una perspectiva de alta frecuencia. Se elije a BITCOIN como el representante del mundo de las criptomonedas y se estudia su respuesta ante una variedad de noticias macroeconómicas.

El mayor beneficio de utilizar información de alta frecuencia es que en un periodo muy corto de tiempo, una ventana de treinta minutos con varios anuncios en simultaneo, se logra obtener la información más cercana posible en finanzas empíricas a un experimento de tipo natural.

El trabajo se presenta en la siguiente manera: primero se muestra un modelo estilizado para BITCOIN que sirve para el análisis empírico, luego se discuten los datos a utilizarse, luego se discuten los datos empíricos y lo que se encontró, siguiendo esto se examina la robustez de los resultados y por último se resumen los descubrimientos y se concluye.

Esta estrategia empírica consiste en varios elementos. Primero, se recolectan diferentes tipos de información de eventos macroeconómicos, como:

- Noticias de la economía real (Sueldos, solicitudes de subsidios por desempleo, producción industrial, Tasa de desempleo y balanza comercial
- Noticias de inflación (CPI "[15] Consumer Price index"),
- Noticias sobre los indicadores prospectivos (Índice de confianza y manufactura)

A su vez se utiliza la previsión y pronóstico de Bloomberg como proxy para expectativas de mercado.

[15] CPI: Consumer Price Index. "Índice de precios al consumidor"

Para noticias de política monetaria, se utiliza la distinción de (Swanson, 2021). Esta las separa en tres indicadores distintos:

- El primer factor es: "Target" (objetivo), el cual captura los cambios imprevistos en el objetivo actual de los fondos federales.
- El segundo es: "Path" (ruta o camino), captura los cambios imprevistos en el camino de la política.
- El tercero es: "LSAP", el cual captura los anuncios imprevistos de futuras compras de activos de gran escala (LSAP = Large scale asset purchases), por sus siglas en ingles.

Dado el reciente desarrollo de las bolsas de intercambio de criptomonedas, se restringe la muestra de información del periodo que va desde 2017 a 2022, partiendo del periodo en donde se considera que BITCOIN llega a una etapa más madura.
Luego, se estima la respuesta de los activos norteamericanos a estas noticias macroeconómicas mencionadas anteriormente. El mayor resultado que se encuentra es que BITCOIN es ortogonal a todas las noticias macroeconómicas, excepto al índice de precios al consumidor (CPI). Esto implica un contraste muy fuerte con los otros activos utilizados para la comparación como el oro, plata, S&P 500 y varias tasas de intercambios bilaterales. Todos los otros activos tradicionales responden a las noticias macroeconómicas con un coeficiente de significancia bastante alto.

Según Gianluca Benigno y Carlo Rosa (febrero, 2023) BITCOIN no resulta ser muy responsivo frente a noticias de objetivo y política monetaria:

> "Our analysis also points out a puzzle in terms of how BITCOIN responds to monetary news. Given our interpretation of BITCOIN as an asset with no intrinsic value whose current value depends on the discounted value of its future price, we should expect BITCOIN to respond to monetary policy news as it is reflected in changes in current and future real interest rates. Our analysis instead shows that, while other US asset prices respond to both the target and the path of monetary policy news, BITCOIN is unresponsive to unexpected changes in the short-term rate while its reaction to news about the future path of policy is not robust".
>
> [Nuestro análisis también señala un enigma en cuanto a la forma en que BITCOIN responde a las noticias monetarias. Dada nuestra interpretación de BITCOIN como un activo sin valor intrínseco cuyo valor actual depende del valor descontado de su precio futuro, deberíamos esperar que BITCOIN responda a las noticias de política monetaria en la medida en que se reflejen los cambios en los tipos de tasas de interés reales actuales y futuros. En cambio, nuestro análisis muestra que, mientras que los precios de otros activos estadounidenses responden a cambios de la política monetaria y objetivo, BITCOIN no responde a cambios inesperados en los tipos de interés reales actuales y futuros, a su vez BITCOIN no responde a los cambios inesperados en el tipo de interés a corto plazo, mientras que su reacción a las noticias sobre la senda futura de la política monetaria no es robusta.] (Gianluca Benigno y Carlo Rosa, febrero 2023, p. 3)

5.2. Modelo de activo especulativo simple

Aquí se interpreta BITCOIN como un activo especulativo sin valor intrínseco, en donde su valor depende de la apreciación del mismo activo. Se denota *bt* como el valor del activo en tiempo *t* y se considera la siguiente regla:

$$b_t = \frac{q_t b_{t+1}}{1+r_t} + \frac{(1-q_t)}{1+r_t}\varepsilon_{t+1} \qquad (1)$$

En donde *1 – qt* es la probabilidad de que el activo caiga en valor esperado a cero y *Rt* = 1 + *rt* es la tasa de interés real bruta. En terminología de Blanchard and Fischer (1989) *bt* es considerada una burbuja estocástica. Se asume lo siguiente:

Supuesto 1: La probabilidad qt es endógena y depende de las tasas de interés reales actuales y futuras

$$q_t = q_t\left(R_t, R_{t+1}, R_{t+2}, ...\right)$$

and

$$q_{t+1} = q_{t+1}\left(R_{t+1}, R_{t+2}, R_{t+3}, ...\right)$$

with $q_{t,R_t} = \frac{\partial q_t}{\partial R_t} < 0$, $q_{t,R_{t+1}} = \frac{\partial q_t}{\partial R_{t+1}} < 0$ and so on.

Supuesto 2: La sensibilidad de la probabilidad de una explosión de la burbuja i mas fuerte para tasas actuales que para tasas futuras.

$$q_{t,R_t} < q_{t,R_{t+1}} < 0$$

Ahora se resuelve (1) hacia delante desde el momento t=0. Iterando , obtenemos:

$$E_t b_{t+i} = b_t \left(\prod_{j=0}^{i-1} \frac{q_{t+j}}{R_{t+j}}\right)^{-1}$$

Si bt es positivo, entonces el valor esperado del activo especulativo es una función de las probabilidades actuales y futuras asociados con que el valor del activo será distinto de ε. Ya que no existe un valor intrínseco para este activo, los únicos determinantes macro para este activo especulativo son los movimientos en las tasas de interés. En la formulación propuesta en la cual la probabilidad es endógena y

depende de las tasas de interés reales presentes y futuras, tenemos la propiedad de que cambios en las tasas futuras tienen mayor efecto sobre el activo en cuestión que las tasas actuales.

Dado que se ha definido a BITCOIN como un activo sin un valor intrínseco, desde una perspectiva macroeconómica, los únicos determinantes directos de BITCOIN son las tasas de interés presentes y futuras. En el análisis empírico que se realiza, se examina la respuesta de BITCOIN frente a distintas noticias macroeconómicas.

Para remarcar la conexión entre estas noticias y el precio de BITCOIN, se modela la tasa de interés actual como si esta estuviera controlada por la autoridad de política monetaria para reaccionar a las desviaciones inflacionarias partiendo desde la tasa objetivo y los desarrollos macroeconómicos reales capturados por el diferencial de producción.

$$R_t = \Phi(\Pi_t, Y_t),$$

where $\Phi(.,.)$ is a generic reaction function with $\Phi_\Pi > 0$, and $\Phi_Y > 0$

Donde Φ es una función de reacción genérica como en la [16]regla de Taylor. En esta construcción las noticas inflacionarias y de actividad real influencian indirectamente el precio del activo especulativo a través de una función de reacción de la autoridad de política monetaria. Esto nos permite desarrollar las siguientes hipótesis empíricas acerca de la relación entre noticias monetarias y macroeconómicas y el precio del activo especulativo.

• **Hipótesis 1** : Las noticias monetarias afectan negativamente el valor del activo especulativo a través de un canal de tasa de interés

• **Hipótesis 2**: Las noticias monetarias acerca del camino futuro de la política tiene mayores efectos que aquellos incurridos con la tasa actual objetivo.

• **Hipótesis 3**: Las noticias macroeconómicas afectan el precio de activos especulativos a través del canal de la función de reacción de política monetaria. Además, el signo asociado con la inflación y las noticias macroeconómicas reales será negativo mientras se cumpla que ΦΠ > 0 y ΦY > 0 en la ecuación (2)

5.3 Datos

Aquí se describe brevemente los datos sobre precio de activos, sorpresas monetarias y macroeconómicas.

5.3.1 Datos de precios de activos

Este tipo de datos, incluye datos de alta frecuencia sobre BITCOIN, tipos de cambio de dólar contra monedas de países desarrollados como emergentes, metales preciosos y acciones norteamericanas.

[16] Regla de Taylor: Esta regla se basa en la tasa de interés nominal que debería adoptar un banco central, con la inflación y producto bruto interno. Relacionando estas variables

Se estudian las propiedades de BITCOIN y se las compara otra clase de activos tradicionales. La primera clase de estos activos está representada por varias tasas bilaterales de tipo de cambio del dólar norteamericano. La inclusión de estas tasas está motivada por el hecho de que BITCOIN es considerado como alternativa al dinero tradicional, según *(bank of international settlements, 2019*) los tipos de cambio de monedas seleccionas se encuentran entre las monedas más intercambiadas en el mercado.

Cuando se compara BITCOIN a los metales preciosos, este comparte muchas virtudes con el oro, como lo es la propiedad de resguardo de valor, el numero existente de unidades son finitas y también sirven para transferir valor. Aunque para saber si BITCOIN se comporta como un metal precioso, hay que ver los resultados empíricos. Para el estudio se usan los precios cada cinco minutos del oro y plata medidos en dólares norteamericanos por onza.

Por último se examinan las propiedades de las acciones. Existen diferencias clave entre BITCOIN y acciones, entre ellas: BITCOIN no es un producto regulado, por lo tanto, no opera en ningún mercado de intercambio tradicional, no paga dividendos, etc. Para analizar las acciones en general se utilizan los datos del "S&P E -Mini futures", esto sirve como el proxy más cercano a el precio de las acciones norteamericanas.

Las muestras se encuentran dentro del periodo de 2000 al 2022 para todos los activos, excepto BITCOIN. La selección del comienzo de la recolección de información está dada por la disponibilidad y alcance de la misma. Para BITCOIN es a partir del 2017, se elige esta fecha porque se considera que a partir de aquí BITCOIN comienza a estar accesible al público y también la volatilidad de sus retornos era más baja comparada a los comienzos de BITCOIN.

En un periodo de diez años, BITCOIN experimento un crecimiento muy rápido pasando de 5 dólares en 2012 a más de 60.000 dólares en marzo de 2021, esto nos deja en un crecimiento compuesto anual de aproximadamente 270% por año. Durante el mismo periodo el S&P500 creció alrededor de 11% por año entre 2012 y 2022. Mientras que el oro y la plata permanecieron prácticamente sin cambios.

5.3.2 Sorpresas monetarias

Aquí básicamente se utiliza un análisis de los componentes principales para extraer los dos factores más importantes en los cambios intradiarios en las tasas futuras de interés del mercado de dinero dentro de una ventana de treinta minutos para cada anuncio de [17]FOMC.

5.3.3 Sorpresas Macroeconómicas

La selección de anuncios macroeconómicos incluyen aquellos que han sido marcados como importantes según la literatura financiera internacional (Andersen et al. (2007), and Faust et al. (2007)). Es importante lograr aislar el componente inesperado de los anuncios macroeconómicos de la data macroeconómica cruda que sale en estos anuncios.

[17] FOMC = Federal open markets committe, es el comité de operaciones de mercado abierto de la reserva federal de EEUU, donde se toman las medidas de política monetaria.

Para construir el componente sorpresa de cada publicación de datos macroeconómicos. Se define como noticia macroeconómica, la diferencia entre el valor realizado de la publicación de estos datos macro en el día del anuncio y las expectativas de los mercados financieros para ese valor realizado.

Las noticias macroeconómicas norteamericanas pueden ser agrupadas en tres grandes categorías:

1) Noticas acerca del estado real actual de la economía: Indicadores acerca de la producción industrial, ventas minoristas, condiciones de mercado laboral, exportaciones netas.

2) Noticias acerca de indicadores futuros de la actividad real: Confianza consumidor, índice[18] ISM

3) Noticias acerca de indicadores futuros de la actividad real: Índice del precio al productor, índice de precios al consumidor. Ambos índices excluyen categorías volátiles como comida y energía.

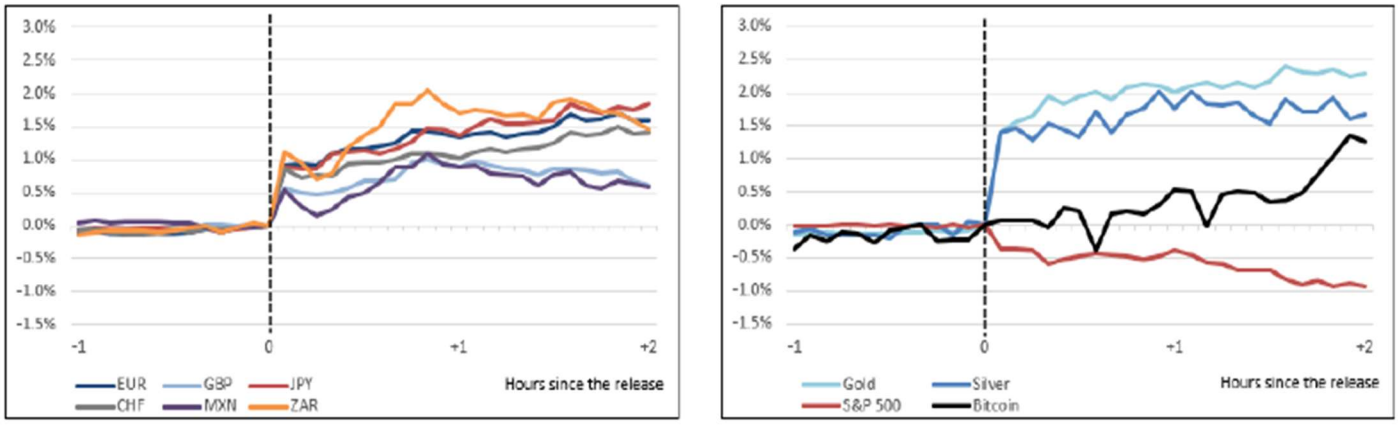
Dado que la muestra incluye el periodo de pandemia de COVID 19, se filtran y se dejan afuera, noticias macroeconómicas extremas.

5.4. Resultados Empíricos

5.4.1 Días de anuncios específicos

La próxima imagen, ilustra el impacto de las noticias en el mercado financiero. Nos muestra la respuesta de distintos precios de activos financieros norteamericanos al momento de la salida de dos tipos de noticias: noticias de la economía real, como reporte de mercado laboral (panel A) y noticias de política monetaria relacionado con los discursos del FOMC (panel B).

Figura 36, Respuesta frente a la publicación del reporte de desempleo del 3 de junio, 2016

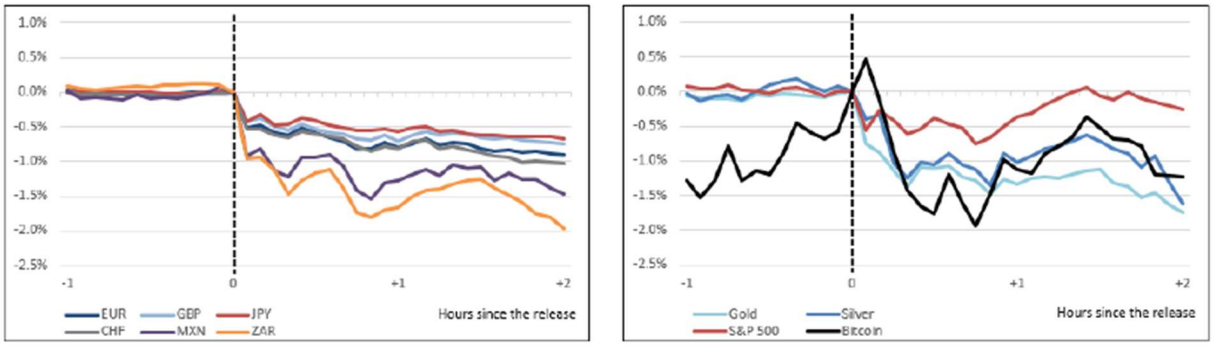


Fuente: (The Bitcoin–Macro Disconnect, Pagina 16)

[18] ISM index = Indicador mensual de la actividad económica en Estados Unidos

Los informes de nómina no agrícola salió con un valor más bajo de lo esperado (en este reporte de 2016). Lo que por consecuencia llevo a que el dólar se deprecie, el precio de las acciones cayó un 0.5% y el precio del oro se incrementó en un 2%. Contrario a esto BITCOIN se movió en un rango de lado a lado.

Figura 37, Respuesta frente la publicación del discurso del FOMC el 16 de junio, 2021



Fuente: (The Bitcoin–Macro Disconnect, Pagina 16)Al final de junio de 2021 en una reunión de la FED, la FOMC indica que las tasas deberían subirse antes de lo que anticipaba el mercado. De nuevo el dólar, el oro y las acciones reaccionan al instante mientras que BITCOIN no

4.2 Respuesta de precios de los activos ante sorpresas monetarias

Aquí se ponen a prueba las hipótesis 1 y 2. Poniendo a prueba la premisa de que las noticias monetarias afectan negativamente a BITCOIN a través del efecto de las tasas de interés. La hipótesis 1 remarca la dependencia de BITCOIN frente a cambios en las tasas de interés. Esta hipótesis sugiere que tendremos coeficientes negativos en todas las noticias monetarias que se han construido (Target, Path, LSAP a tal punto que este último afecte las tasas de interés). Por otro lado, la hipótesis 2 sugiere que el coeficiente en el coeficiente "Path" debe ser mayor comparado con el del "Target". Si todo esto se cumple, estas hipótesis indicarían que las sorpresas de política monetaria son un conductor de los precios de BITCOIN.

Para corroborar lo anterior se corre una regresión para los días en los que haya reuniones del FOMC. Siendo la regresión:

$$R_{[t-5min,t+25min]} = \alpha + \beta_T Target_t + \beta_P Path_t + \beta_L LSAP_t + \varepsilon_t$$

En donde $R_{[t-5min,t+25min]}$ es el porcentaje de cambio de las tasas de interés de 30 minutos. Los precios de metales preciosos, acciones y BITCOIN desde 5 minutos antes del evento hasta 25 minutos después del mismo.

La siguiente tabla muestra los resultados de la regresión para un periodo muestral desde enero de 2000 hasta diciembre de 2022 para todos los activos, excepto BITCOIN. Para el cual el periodo muestral es desde enero de 2017 hasta diciembre de 2022.

Figura 38. Respuesta del precio de los activos ante sorpresas monetarias

	EUR	GBP	JPY	CHF	MXN	ZAR	Gold	Silver	S&P 500	Bitcoin
Constant	0.02	0.02	0.01	0.03	0.05**	0.02	0.11***	0.18***	0.00	0.37*
Target	-1.88***	-1.64***	-0.7	-1.32*	-1.02*	-1.91***	-2.95**	-2.69**	-3.71**	-15.06
Path	-1.99***	-1.60***	-1.65***	-1.93***	-1.34***	-2.16***	-3.25***	-3.93***	-1.91***	-5.91**
LSAP	-3.26***	-2.91***	-3.60***	-2.98***	-1.94***	-2.08***	-5.74***	-5.61***	-2.36**	-0.29
R^2	0.461	0.47	0.535	0.427	0.223	0.269	0.463	0.294	0.256	0.239
Observations	183	183	183	183	183	176	154	153	182	47

Nota: La tabla muestra los resultados de la regresión de las variaciones porcentuales intradiaria de los tipos de cambio, los precios de los metales preciosos, las cotizaciones de acciones estadounidenses y el BITCOIN *(desde cinco minutos antes del acontecimiento hasta veinticinco minutos después). Los factores Target, Path y LSAP. Los tipos de cambio se definen como unidades de dólares estadounidenses necesarias para comprar una unidad de moneda extranjera, de modo que un cambio positivo implica una depreciación del dólar estadounidense. La variable Target mide los cambios no anticipados en la tasa objetivo actual de los fondos federales. La variable Path mide los cambios en las tasas futuras hasta un año, cuyas tasas son independientes a los cambios de la tasa objetivo actual. La variable LSAP mide el anuncio imprevisto de compras de activos. El método econométrico es el de mínimos cuadrados ordinarios con errores estándar coherentes con la heteroscedasticidad. Los superíndices ***, ** y * indican significación estadística en los niveles del 1%, 5% y 10%.*
Fuente: (The Bitcoin–Macro Disconnect, Pagina 18)

Aquí encontramos que las noticias acerca de la tasa objetivo, y el futuro de la política monetaria tienen grandes efectos estadísticamente significantes en todos los precios de los activos. En particular, podemos decir que una sorpresa de una baja de 1 punto porcentual en tasas de fondos federales incrementa el índice del S&P500 en un 3.7% en una ventana de treinta minutos desde que sale el anuncio, con una significancia del 5%. Esta magnitud es similar a la reportada por (Bernanke and kuttner, 2005) en donde se observa un efecto del 4.7% en el índice de acciones de valor ponderado por peso del [19]CRSP que va del periodo de junio de 1989 a diciembre de 2002.

Los efectos de las variables Path y Target también son negativas y significantemente distintas de cero. Hay que interpretar los efectos de LSAP como un límite inferior del efecto total de la compra de activos, ya que algunos anuncios de LSAP fueron realizados fuera de las reuniones del FOMC, y que además del efecto sobre las acciones también existen efectos de flujo como documentan (D'Amico and King, 2013).

Los efectos más interesantes de esto son las estimaciones de los efectos de estas sorpresas monetarias sobre BITCOIN en donde los coeficientes Target y LSAP son negativos, pero a su vez insignificantes, mientras que el coeficiente de la variable path es negativo y significante al 5%. A todo esto, el ajuste del modelo, medido por el R cuadrado ajustado es del 24%, y tiene una magnitud similar a la regresión del S&P500 y la tasa de cambio de mercados emergentes, pero a su vez es menor al de las tasas de cambio de economías desarrolladas.

Toda esta evidencia nos muestra un apoyo mixto a la hipótesis 1; las respuestas de BITCOIN ante cambios en la política monetaria son siempre negativos, mientras que los coeficientes nunca son significantes al 1% y solo en 1 de cada 3 casos el coeficiente es significantemente distinto de cero al nivel de 5%. La hipótesis 2 sugiere que los efectos de LSAP y path son mayores que los de target, ya que las unidades de medida de

[19] CRSP: "Center for research and securities Prices"

las noticias monetarias son diferentes, se normalizan los efectos al multiplicar el coeficiente de regresión por el desvió estándar de la sorpresa monetaria. Una sorpresa de un desvió estándar en target y path este asociado con cambio del 0.6% en BITCOIN, mientras que los efectos de LSAP son cercanos a cero. Por lo tanto, las noticias relacionadas al camino futuro de las políticas no tienen consistentemente efectos mayores que los de la tasa objetivo actual.

4.3 Respuesta de precios de activos ante noticias macroeconómicas

Desde un punto de vista teórico, los efectos de las noticias económicas sobre el precio de los activos son inciertos. La dirección en la cual las noticias mueven las tasas de tipo de cambio depende de la determinación del modelo de tasas de cambio y de la manera en la que las autoridades monetarias responden a esta nueva información (Almeida et Al, 1998).

Un aumento inesperado en inflación, puede llevar a que se incrementen los costos para las exportaciones. Esto puede provocar que una nación sea menos competitiva en los mercados globales. A su vez, este aumento inflacionario, podría generar un incremento en el déficit de balanza comercial. Provocando una depreciación de la moneda. En cambio, si la reserva federal emplea o sigue una función de reacción de tipo Taylor. Podría llevar a un incremento de las tasas de interés corto plazo. Las mismas intervendrían en la presión inflacionaria, lo que podría llevar a que la moneda se aprecie.

Con respecto a las acciones, de acuerdo al modelo de dividendos descontados en donde el precio de la acción de una compañía equivale a la suma de los pagos futuros por sus dividendos descontados al valor presente, como se debate en Pearce and Roley (1985), un incremento inesperado en la actividad económica real puede causar una revisión en los dividendos futuros descontados (efecto de flujo de fondos) y el exceso de retornos futuros (efecto de tasa de descuento). Todo esto debido a la respuesta del banco central frente a las noticias económicas donde el efecto que predomine al final es puramente empírico.

En el caso de BITCOIN, no existe ningún modelo desarrollado para valuar el activo pero dada nuestra base y estructura planteada anteriormente sugerimos que las noticias macroeconómicas tienen un efecto sobre los activos especulativos a través de funciones que reaccionan a las políticas monetarias. Por lo tanto, se conduce un caso de estudio, el cual examina el impacto de noticias importantes macroeconómicas sobre el mercado financiero, para el cual se estima el siguiente modelo de regresión lineal de manera separada para cada precio de activo y anuncios macroeconómicos, usando solo los días en los que hay anuncios macroeconómicos.

$$R_{[t-5min,t+25min]} = \alpha_i + \beta_i MacroNews_{i,t} + \varepsilon_{i,t}$$

La notación, es igual a la ecuación del caso anterior, con la diferencia que para una mejor y más fácil interpretación se dieron vuelta los signos de los anuncios de tasa de desempleo y peticiones por desempleo. αi y βi son coeficientes de regresión y el termino de error εi,t representan otros factores que afectan el precio de los activos al momento del anuncio.

El siguiente cuadro muestra los resultados de la estimación de la ecuación como respuesta del precio de activos frente a noticias macroeconómicas. En la cual se puede observar que la mayoría de las sorpresas macroeconómicas incluyendo: ventas minoristas, nóminas de pago (excluyendo agrícolas), balanza comercial, índice de precios al consumidor, tienen un efecto estadísticamente significativo en todos los

precios de los activos (tasas de cambio del dólar norteamericano, precios de metales preciosos, precio de acciones) excepto BITCOIN. Además, el signo del coeficiente estimado es negativo.

Figura 39: Respuesta del precio de activos frente a noticias Macroeconómicas.

	EUR	GBP	JPY	CHF	MXN	ZAR	Gold	Silver	S&P 500	Bitcoin
Industrial Production	-0.01	-0.01	-0.02***	-0.02**	0.01	0.04	0.01	0.01	0.05**	-0.02
R^2	0.3	0.2	3.4	2.3	0.9	2.4	0.1	0.1	4.2	0.1
Retail Sales	-0.04***	-0.03***	-0.08***	-0.06***	0.03**	-0.02	-0.07***	-0.07	0.10***	-0.01
R^2	4.0	3.3	14.6	8.1	1.4	0.3	4.0	1.2	10.7	0.0
Change in Nonfarm Payrolls	-0.11**	-0.08**	-0.13***	-0.13**	0.02	-0.06	-0.17***	-0.16***	0.10***	-0.06
R^2	7.6	7.1	9.4	8.3	0.3	1.4	6.7	3.3	3.9	0.3
Unemployment Rate†	-0.03*	-0.02*	-0.04**	-0.04**	0.03	0.02	-0.04	-0.06	0.04*	0.01
R^2	0.7	0.6	0.8	0.9	0.5	0.1	0.5	0.4	0.7	0.0
Initial Jobless Claims†	-0.01*	0.00	-0.02***	-0.02***	0.01***	0.01*	-0.04***	-0.04*	0.04***	-0.01
R^2	0.1	0.0	1.8	0.8	0.4	0.2	1.8	0.7	1.8	0.0
Trade Balance	-0.05***	-0.02**	-0.04***	-0.05***	0.00	-0.01	-0.02	-0.04	0.02*	-0.01
R^2	5.1	2.3	4.4	4.1	0.0	0.1	0.4	0.5	1.0	0.0
Consumer Confidence	-0.04***	-0.02*	-0.06***	-0.05***	0.03	0.01	-0.03	-0.02	0.16***	-0.01
R^2	4.5	1.7	13.0	7.2	1.8	0.1	0.9	0.2	16.4	0.0
ISM Manufacturing	-0.08***	-0.05***	-0.11***	-0.11***	0.02	-0.01	-0.11***	-0.10***	0.15***	-0.08
R^2	13.1	7.5	31.1	24.6	1.1	0.1	12.1	4.0	12.9	1.8
PPI Ex Food & Energy	-0.02*	-0.03***	-0.04***	-0.02**	-0.02*	-0.08***	-0.05**	-0.09***	-0.03**	0.07
R^2	1.3	3.7	4.7	1.8	1.1	9.1	3.4	2.9	1.7	1.0
CPI Ex Food & Energy	-0.09***	-0.09***	-0.10***	-0.07***	-0.13***	-0.17***	-0.10***	-0.16***	-0.24***	-0.66**
R^2	12.2	14.3	12.9	10.5	16	20.2	6.4	5.7	22.3	16.1

Nota: El cuadro reporta resultados de la regresión de cambios porcentuales intradiarios en las tasas de tipo de cambio. La muestra es de enero de 2017 a diciembre de 2022
Fuente: (The Bitcoin–Macro Disconnect, Pagina 21)

Un resultado mejor de lo esperado en términos de crecimiento en trabajo es asociado con una apreciación del dólar norteamericano, mientras que una expectativa menor a la esperada de la balanza comercial está asociada con una depreciación del dólar. La magnitud de estos efectos está alineada con los efectos estimados reportados en estudios anteriores como en Andersen et al. (2007) para los tipos de cambio de economías desarrolladas y Cai et al (2009) para divisas de mercados emergentes.

Podemos ver como una sorpresa de una desviación estándar en las nóminas de pago (excluyendo al sector agrícola) influye en el tipo de cambio del euro en 0.2%. Consistente con la literatura acerca de la respuesta de precios de activos norteamericanos frente a noticias macroeconómicas (faust et al, 2007), el R cuadrado estadístico es pequeño. Esto indica que el componente sorpresa de las noticias macroeconómicas solo explica una parte pequeña de los retornos de los precios de activos.

La hipótesis 3 sugiere que las noticias macroeconómicas afectan el precio de BITCOIN a través de las reacciones a la política monetaria. Para poner esto a prueba deberíamos esperar que los coeficientes estimados de inflación y noticias macroeconómicas reales son significativamente negativas.

La última columna del cuadro anterior reporta el efecto de las noticias macroeconómicas frente a BITCOIN, el R cuadrado estadístico suele ser más pequeño que comparado a otros activos, encontrándose en el rango de cero (para ventas minoristas, tasa de desempleo, balanza comercial y confianza del consumidor) y 16% (para el índice del precio al consumidor, excluyendo comida y energía). Además, el índice de precios al consumidor es el único coeficiente significativo, pero solo al 5%. En contraste a otros activos norteamericanos y a nuestra hipótesis 3, dicha información indica que BITCOIN no responde de manera sistemática a noticias macroeconómicas fundamentales.

Basado en la información y el análisis mencionado anteriormente y a su vez modelando BITCOIN como un activo que no posee un valor intrínseco, si no que su precio depende del valor descontado de su precio futuro, en el análisis empírico presentado se ve que BITCOIN no responde a noticias macroeconómicas ni tampoco a noticias monetarias.

6 Conclusión

A lo largo de esta tesis se ha explorado el papel de BITCOIN en tiempos de incertidumbre, centrándose en su potencial como reserva de valor y activo refugio. A través de un análisis de la tecnología subyacente, la criptografía, y el rendimiento histórico de BITCOIN en comparación con los activos de inversión tradicionales como el oro, los bonos y las acciones, es evidente que BITCOIN ha demostrado una respuesta única a los acontecimientos macroeconómicos, especialmente en tiempos de crisis.

Aunque todavía existen dudas sobre la volatilidad y la regulación de BITCOIN, su naturaleza descentralizada y su potencial de accesibilidad global lo convierten en una interesante opción de inversión para el futuro. En general, esta tesis subraya la necesidad de seguir investigando y analizando BITCOIN como posible cobertura frente a la incertidumbre económica, y su posible impacto en el futuro de las finanzas.

Basado en la literatura y los análisis vistos previamente en el transcurso de este escrito podemos ver que el índice de S&P500 (acciones) y el oro son los activos más utilizados tradicionalmente como inversión y resguardo de valor, los mismos son sensibles a las noticias y eventos tanto macroeconómicos como monetarios.

Podemos ver que BITCOIN viene a formar parte de este nuevo grupo de activos utilizados como inversión y resguardo de valor, teniendo como además un lado positivo que es que no es muy reactivo a las noticias macroeconómicas ni monetarias, lo que nos brinda una muy buena posibilidad de integrarlo a este grupo de activos, además de ser uno de los activos con mejor rendimiento en los últimos años.

Aunque BITCOIN y las criptomonedas son muy nuevos, BITCOIN ha demostrado la capacidad de ser un activo a considerar como refugio y resguardo de valor en tiempos de incertidumbre. Solo el tiempo y las futuras regulaciones dirán si en los próximos años, este activo se convertirá en una opción común de inversión para los inversores, como lo es hoy en día el oro y las acciones.

Bibliografía

Luis Rodrigo Álvarez Rojas (2018). Análisis de la tecnología *blockchain*, su entorno y su impacto en modelos de negocios. Recuperado de https://repositorio.usm.cl/bitstream/handle/11673/47346/3560900251199UTFSM.pdf?sequence=1&isAllowed=y

Nick Szabo, (1997). Formalizing and Securing Relationships on Public Networks, recuperado de http://myinstantid.com/szabo.pdf

Vitalik Buterin, (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Recuperado de https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf

Daniel Chichil, Y., (2000). Cómo reducir la incertidumbre en las finanzas. Política y Cultura, (13),81-95. ISSN: 0188-7742. Recuperado de: https://www.redalyc.org/pdf/267/26701305.pdf

Zurita González, J., Martínez Pérez, J. F., & Rodríguez Montoya, F. (2009). La crisis financiera y económica del 2008. Origen y consecuencias en los Estados Unidos y México. El Cotidiano, (157), 17-27. Recuperado de https://www.redalyc.org/pdf/325/32512739003.pdf

Shaun K. Roache and Marco Rossi (2009). The Effects of Economic News on Commodity Prices: Is Gold Just Another Commodity?. Recuperado de https://www.elibrary.imf.org/view/journals/001/2009/140/article-A001-en.xml

Gibrán Granados Paredes, (2006). Introducción a la criptografía. Recuperado de https://www.ru.tic.unam.mx/tic/bitstream/handle/123456789/1105/511.pdf?sequence=1

Andrew Loo, (2023). Types of cryptocurrency, CFI Team. Recuperado de https://corporatefinanceinstitute.com/resources/cryptocurrency/types-of-cryptocurrency/

Kirsty Moreland, (2019). The Difference Between Coins and Tokens. Recuperado de https://www.ledger.com/academy/crypto/what-is-the-difference-between-coins-and-tokens

Marty Bent, (2021). Bitcoin is holding steady at the #6 base money in the world. Recuperado de

https://tftc.io/martys-bent/issue-1066/

Ngrave, (2022). Too Big to Fail? Crypto Market Size vs Traditional Assets. Recuperado de

https://medium.com/ngrave/too-big-to-fail-crypto-market-size-vs-traditional-assets-eff4bb2ec529

M.A.García, L. Martínez, T.Ramírez. (2017). Introducción a la teoría de códigos. Recuperado de

https://ocw.ehu.eus/pluginfile.php/50556/mod_page/content/35/Resumen_total_con_portada.pdf

Luis Rodrigo Álvarez Rojas, (2018). Análisis de de la tecnología *blockchain*, su impacto y entorno en modelos de negocios. Recuperado de

https://repositorio.usm.cl/bitstream/handle/11673/47346/3560900251199UTFSM.pdf?sequence=1&isAllowed=y

Satoshi Nakamoto, (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Recuperado de

https://bitcoin.org/bitcoin.pdf

Gianluca Benigno and Carlo Rosa, *Federal Reserve Bank of New York Staff Reports*, no. 1052. (2023). The Bitcoin–Macro Disconnect. Recuperado de

https://www.newyorkfed.org/research/staff_reports/sr1052

Omar venerio, (2020). La Medida de Riesgo de los Bonos: la duration. Recuperado de

https://ucu.edu.uy/es/la-medida-de-riesgo-de-los-bonos-la-duration#:~:text=La%20duration%20tiene%20en%20cuenta,al%20inversor%20su%20inversi%C3%B3n%20inicial

José Francisco López, (2020). Convexidad de un bono. Recuperado de

https://economipedia.com/definiciones/convexidad-de-un-bono.html

Carlos arenas laorga, (2022). El oro como activo de refugio. Recuperado de

https://www.r4.com/analisis-actualidad/el-oro-como-activo-refugio

Andrés Sevilla Arias, (2020). Cobertura financiera. Recuperado de

https://economipedia.com/definiciones/cobertura-financiera.html

David Hunkar, (2019). Gold vs. S&P 500 Long-Term Returns. Recuperado de

https://topforeignstocks.com/2019/09/26/gold-vs-sp-500-long-term-returns-chart/

Daniel Tamayo, (2020). Comparativa de largo recorrido entre el SP 500, el bitcoin y el oro. Recuperado de

https://uncommonfinance.com/comparativa-de-largo-recorrido-entre-el-sp-500-el-bitcoin-y-el-oro/