



# LO QUE NECESITAS SABER SOBRE BITCOIN Y OTRAS CRIPTOMONEDAS



**Lesly Machorro**  
Consultora internacional  
Guatemala, julio 2021



*¿Estamos  
listos para las  
criptomonedas?*

FORO VIRTUAL

zoom  LIVE

Asociación de Investigación y Estudios Sociales © 2021  
10a. Calle 7-48, zona 9.  
PBX: 2201-6300  
www.asies.org.gt, asies@asies.org.gt  
Ciudad de Guatemala, Guatemala, C.A.

**Autora**  
Lesly Machorro

**Departamento de Investigación y Consultoría Económica**  
Fabián Juárez  
Pedro Prado  
Luis San José

**Grupo Editorial**  
Ana Lucía Blas  
Pablo Hurtado  
Lilliana López Pineda  
Guisela Mayén  
Ana María de Specher

**Diseño y diagramación**  
Cesia Calderón

**Imágenes e ilustraciones**  
freepik.com bajo licencia premium

La investigación y publicación se realizó con la colaboración de la Fundación Konrad Adenauer de la República Federal de Alemania (KAS). El contenido de esta publicación es responsabilidad exclusiva de ASIES. En ningún caso debe considerarse que refleja los puntos de vista de la Unión Europea. Se permite la reproducción total o parcial de este documento, siempre que se cite la fuente.



Este reporte está protegido por una licencia Creative Commons Reconocimiento - No Comercial - Sin Obra Derivada 3.0 Unported.

 /asiesgt  
 @ASIES\_GT  
 /ASIESGTNew



DESCARGUE ESTA PUBLICACIÓN EN  
[WWW.ASIES.ORG.GT](http://WWW.ASIES.ORG.GT)

**GRACIAS POR SU INTERÉS EN ESTA PUBLICACIÓN DE ASIES.**

SI DESEA RECIBIR INFORMACIÓN OPORTUNA SOBRE NUESTROS PRODUCTOS EDITORIALES Y ACTIVIDADES, LE INVITAMOS A REGISTRARSE CON NOSOTROS. PODRÁ ENCONTRAR MATERIAL DE SU INTERÉS Y ACCEDER A NUESTROS PRODUCTOS EN OTROS FORMATOS.



*Mira el foro virtual aquí*  
**¿Estamos listos para las criptomonedas?**

Mucho se escucha hablar de las criptomonedas en los últimos tiempos. Ahora es muy común que se haga referencia a ellas en los noticieros y en discusiones de negocios, principalmente cuando se habla de bitcoin. A simple vista parece ser un tema muy complejo y controversial, que sólo interesa a expertos.

Sin embargo, ya se comienza a escuchar de una adopción masiva y la actualidad exige tener al menos algún nivel de familiaridad con el tema.

Este documento busca informar al lector sobre los orígenes de las criptomonedas y los principios básicos de funcionamiento de bitcoin.



# I. ORIGEN Y CARACTERÍSTICAS DEL DINERO

Existen muchas definiciones de dinero, quizás la más común es la que se refiere al dinero como un medio de pago, comúnmente aceptado, que se entrega a cambio de bienes y servicios.

La primera forma de dinero que utilizó la humanidad fue el trueque; luego se requirieron medios de pago más fáciles de transportar y cuyo valor intrínseco fuera más estandarizado. Fue ahí cuando se comenzó a utilizar monedas de metales preciosos. Más adelante, apareció el papel moneda o “billetes” y su valor empezó a basarse en que el emisor pudiera respaldarlo con una contrapartida en un metal precioso.

Este sistema funcionó por muchos años, hasta que, en 1971, el entonces presidente de los Estados Unidos Richard Nixon anuló la convertibilidad directa del dólar respecto al oro durante los Acuerdos de Bretton Woods. Desde entonces, el dólar (y todas las demás monedas, que estaban relacionadas con él) se convirtió en **dinero fiduciario**, es decir, que se basa en la fe o confianza en su declaración como dinero por un Estado. Sin dicha declaración, el dinero no tiene ningún valor.

El dinero continuó evolucionando, y en paralelo con la digitalización de la sociedad, han irrumpido con fuerza diversos **medios de pago electrónicos**, que se basan en el uso del internet para pagar bienes y servicios. Hoy en día el uso de las tarjetas de crédito/débito y transferencias electrónicas forman parte normal de nuestro día a día.

El dinero actúa, principalmente, como:

- 1. Medio de pago o de cambio:** Esta es la función principal del dinero, facilitar un intercambio eficiente de bienes y servicios por tratarse de un bien convencional de aceptación general y garantizado por el estado. Las características de un buen medio de pago son: durabilidad (idealmente no debe dañarse o gastarse con su uso), transportabilidad (debe ser fácil de poner en una billetera o de transferir), divisibilidad (tener la posibilidad de intercambiar un billete de 100 por 10 de 10 o 20 de 5, etc.), fungibilidad (monedas idénticas e intercambiables), difícil falsificación (idealmente no debe ser fácil de imitar, debe tener características únicas que sólo su emisor oficial puede replicar. Esto es un problema irresuelto para algunas monedas del mundo actualmente).
- 2. Depósito de valor:** Es un mecanismo por el cual el dinero puede guardar su riqueza y permite rescatar su valor en el futuro con cierto nivel de predictibilidad. La cualidad de depósito de valor no es exclusiva del dinero, sino de los activos en general. Ejemplos clásicos de activos que funcionan como depósito de valor son el oro, diamantes, acciones, bonos y bienes raíces.
- 3. Unidad de cuenta o de cambio:** Los productos tienen un precio en función de su valor en dinero y no de otros productos, lo cual facilita hacer cálculos económicos.



## II. ESTADO ACTUAL DEL DINERO

---

La última evolución del dinero son las **criptomonedas**, que son medios digitales de intercambio. Se trata de una moneda electrónica que utiliza un cifrado digital en sus operaciones, como las transferencias de dinero o el pago de un determinado producto o servicio.

La primera criptomoneda, y la más popular hasta ahora, es bitcoin, que está en funcionamiento desde el año 2009. Después de ésta se han creado muchas criptomonedas más, con diferentes características y protocolos de funcionamiento como son ether, litecoin, stellar, entre muchas otras.

La plataforma de funcionamiento de las criptomonedas es la tecnología *blockchain* (o cadena de bloques). *Blockchain* es una base de datos, generalmente pública, compartida y descentralizada que funciona como un libro contable donde se registran operaciones de compraventa o cualquier otro tipo de transacción.

Las principales características de esta tecnología son: seguridad, confianza, trazabilidad, privacidad, y agilidad y transparencia.

El elemento principal que le otorga valor es su **seguridad**, siendo prácticamente imposible alterar los datos de alguna de esta cadena de bloques. Si un actor malicioso intenta realizar un ataque cibernético sobre la cadena, ve dificultada su operación porque un cambio en un apunte supone modificar todas las páginas siguientes en cascada. Adicionalmente, para que el cambio ocurriese de verdad habría que hacerlo en todas las copias existentes del libro, es decir, se tendrían que atacar los miles o millones de ordenadores que forman parte de la red descentralizada, volviéndose una misión de extrema dificultad y costo excesivo.

## III. ORIGEN DE LA CRIPTOMONEDA BITCOIN

---

El 1 de noviembre de 2008, una persona identificada con el seudónimo de Satoshi Nakamoto<sup>1</sup> envió un mensaje a una lista de correo sobre criptografía describiendo un proyecto para crear una moneda digital que sirviera para contabilizar y transferir valor, de persona a persona y sin la intervención de terceros.

Derivado de dicho sistema, nació la primera criptomoneda llamada Bitcoin, una moneda alternativa de control descentralizado, sin respaldo ni control de ningún Estado o banco central. El control de las transacciones realizadas con la moneda se realiza a través de la tecnología *blockchain* y sin intermediarios.

Bitcoin es una moneda intangible, pero puede ser utilizada como medio de pago, al igual que el dinero físico. La razón por la que esta moneda ha adquirido mayor valor y confianza de las personas, a pesar de las circunstancias poco comunes de su creación es su transparencia y su seguridad.

**SEGURIDAD:** El sistema está protegido por algoritmos criptográficos. Ninguna persona, país u organización puede controlar la red, permaneciendo segura aún sin la confianza entre los usuarios. Los pagos pueden hacerse sin depender de terceros. Utiliza el sistema de prueba de trabajo, el cual impide el doble gasto o la falsificación, basándose en el consenso entre los nodos (usuarios) que integran la red mediante el intercambio y comprobación de información.

**TRANSPARENCIA:** Bitcoin es de código abierto y descentralizado, lo que significa que cualquier persona tiene acceso al código y puede verificar cómo funciona. Todas las transacciones y bitcoins creados pueden ser consultados por cualquier persona. Si bien no es una moneda física ni respaldada por una autoridad, ésta obtiene su valor de la oferta y la demanda y de su adopción y aceptación como medio de intercambio de riqueza.

---

<sup>1</sup> Quien hasta el día de hoy es un personaje incógnito que bien podría ser una persona o grupo de personas.

## IV. ¿CÓMO FUNCIONA ESTE SISTEMA?

El sistema de Bitcoin está programado para generar un número fijo de bitcoins por unidad de tiempo a través de computadores a los que se les llama “mineros”. La forma en la que crea nuevas monedas es a través de procesos criptográficos.

Los mineros<sup>2</sup> compiten constantemente entre ellos para encontrar la solución a un problema criptográfico que solo se puede resolver por fuerza bruta de procesamiento. El primer minero en resolver dicho problema recibe un premio en bitcoins. En los primeros meses de funcionamiento de Bitcoin era posible minar bitcoins mediante un computador estándar, pero la aparición de software especializado en “minería” ha llevado a profesionalizar la minería de bitcoins y a llevarla a lugares de energía barata, ya que el costo energético de procesamiento es una variable muy importante para considerar.

El uso de bitcoin se hace a través de programas de software que funcionan como una especie de monedero virtual, que genera una dirección virtual única, pública pero anónima, la cual se puede usar para enviar y recibir transacciones, tal como lo es una dirección de correo electrónico.

Esto implica que los importes y fechas de las transacciones son de conocimiento público, no así el nombre del emisor ni del receptor, ni el saldo de sus cuentas. Las transacciones quedan a la vista del público de forma transparente sin posibilidad de borrarlas o modificarlas.

### 4.1 PERO ¿SE PUEDE DECIR QUE BITCOIN ES UNA MONEDA?

El protocolo de la red de Bitcoin ofrece algunas características interesantes desde la perspectiva monetaria, pero esto no necesariamente le convierte en moneda.

**Suministro fijo:** El abastecimiento de bitcoins está regulado desde el mismo protocolo del programa de tal forma que sólo se puedan producir 21,000,000 bitcoins (BTC), lo que se completará en el año 2140 aproximadamente. El abastecimiento de bitcoins se va reduciendo a la mitad aproximadamente cada 4 años. Hoy en día se producen 6.25 BTC cada 10 minutos, aproximadamente, y se estima que la próxima reducción será en marzo del 2024 y quedará en 3.125 bitcoins por cada 10 minutos.

**“Política monetaria” transparente:** Esta política está disponible para verificación de todos pues el protocolo está basado en código fuente abierto.

**Dirigido por consenso:** Cada usuario elige acordar las reglas propuestas, proponer las suyas propias o recrear la red de forma independiente a la original. Las características clave de la red no pueden ser cambiadas a menos que la mayoría de los participantes en secciones clave del sistema apruebe los cambios.

### 4.2 BITCOIN COMO MEDIO DE PAGO

Bitcoin muestra interesantes características que le potencian como un medio de pago digital: es altamente durable (por ser un código, no hay forma de que se degrade o se fracture con su uso); es altamente portable (no tiene intermediarios ni fronteras, se transfiere en aproximadamente 10 minutos); fungible (todos los bitcoin tienen el mismo valor sin perjuicio de quien los posea o su historia, se pueden intercambiar por bienes y servicios); divisible (cada bitcoin se divide en 100 millones de unidades), y es resistente a la falsificación (el valor del bitcoin se asigna a una dirección específica que no puede ser duplicada).

### 4.3 BITCOIN COMO DEPÓSITO DE VALOR

Bitcoin y las criptomonedas en general no son un medio de depósito de valor perfecto por las fluctuaciones significativas de su precio, que depende de la oferta

<sup>2</sup> Se les llama mineros por la analogía con la minería de oro.

y la demanda. Durante los últimos años el precio ha incrementado dramáticamente. En el año 2018 bitcoin vivió un invierno en que su precio descendió dramáticamente. Sin embargo, después de esa etapa su precio continuó incrementando de forma relevante, siendo objeto de atención y uso de inversionistas como un depósito de valor.

#### 4.4 BITCOIN COMO UNIDAD DE CUENTA

Bitcoin tampoco tiene un buen uso como unidad de cuenta dadas las altas fluctuaciones de su precio.

Sin embargo, no se descarta que el precio de bitcoin sea más estable en el tiempo conforme su contexto regulatorio sea más claro, el mercado entre bitcoin y las monedas de curso legal sea más líquido, exista un mayor desarrollo de mercado de futuros entre bitcoin y las monedas de curso legal, lo cual contribuiría a estabilizar los precios.

## REFERENCIAS BIBLIOGRÁFICAS

Britannica Encyclopedia. Historia del dinero, disponible en el siguiente link: <https://www.britannica.com/video/187664/history-money>

Historia de Bitcoin, disponible en el siguiente link: <https://www.britannica.com/topic/Bitcoin>

PLUS 500. World's Trading Machine. History of Bitcoin. <https://www.plus500.com/Instruments/BTCUSD/The-History-of-Bitcoin~3>

Nerdwallet. What is cryptocurrency? <https://www.nerdwallet.com/article/investing/cryptocurrency-7-things-to-know>

Kaspersky. What is cryptocurrency? <https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency>

Bitcoin. ¿Qué es Bitcoin? <https://bitcoin.org/es/>

IBM. What is blockchain technology? <https://www.ibm.com/topics/what-is-blockchain>

Aún no existe un consenso global sobre la naturaleza jurídica de bitcoin (y de otras criptomonedas), lo cual dificulta su regulación internacional. En distintas jurisdicciones del mundo, bitcoin ha sido abordado desde varias perspectivas: como una moneda electrónica, como una divisa extranjera, un bien intangible, un instrumento o activo financiero, una materia prima, un método de inversión, patrimonio digital de disposición, medio de cambio o de pago, unidad de cuenta, un sistema de liquidación, entre otros.

Hay una preocupación mundial compartida por su falta de regulación y supervisión dadas las implicaciones legales y riesgos que su uso acarrea. Diversos gobiernos del mundo hoy en día trabajan en desarrollar políticas públicas y marcos regulatorios adecuados que permitan proteger la integridad de los mercados financieros y los intereses económicos de los usuarios de criptomonedas.